
Dokumentation 0945-1889/2

TinkerTool System 8

Referenzhandbuch

Marcel Bresink
Software-Systeme



Version 8.98, 22. Januar 2025. Deutsche Ausgabe.
MBS-Dokumentation 0945-1889/2

© Copyright 2003 – 2025 by Marcel Bresink Software-Systeme
Marcel Bresink Software-Systeme
Ringstr. 21
56630 Kretz
Deutschland

Alle Rechte, insbesondere die der Vervielfältigung, Übersetzung oder Übertragung von Programmen und Handbüchern oder Teilen daraus in irgendeine andere Form vorbehalten. Vertrieb nur mit schriftlicher Genehmigung des Herstellers gestattet.

Etwaige in diesem Handbuch enthaltene Beispiele wurden möglichst praxisnah ausgewählt. Die verwendeten Namen von Personen, Firmen, Produkten, etc. sind frei erfunden; irgendwelche Ähnlichkeiten mit tatsächlichen Namen oder Vorfällen sind nicht beabsichtigt und rein zufällig.

Die Informationen in diesem Handbuch können ohne vorherige Ankündigung geändert werden. Die Dokumentation kann technische Ungenauigkeiten oder satztechnische Fehler enthalten. Der Inhalt wird in regelmäßigen Abständen überarbeitet und an technische Neuerungen angepasst. Diese Änderungen werden in neueren Auflagen berücksichtigt. Stellen Sie sicher, dass die Versionsnummern von Software und Handbuch exakt übereinstimmen. Die entsprechenden Angaben sind oben auf dieser Seite zu finden.

Apple, macOS iCloud und FireWire sind eingetragene Warenzeichen der Apple Inc. Intel ist ein eingetragenes Warenzeichen der Intel Corporation. UNIX ist ein eingetragenes Warenzeichen der Open Group. Broadcom ist ein eingetragenes Warenzeichen der Broadcom, Inc. Amazon Web Services ist ein eingetragenes Warenzeichen der Amazon.com, Inc. Google Cloud Storage ist ein eingetragenes Warenzeichen der Google LLC. Microsoft Azure ist ein eingetragenes Warenzeichen der Microsoft-Firmengruppe. Warenzeichen oder Dienstleistungsmarken werden lediglich zu Identifikationszwecken verwendet.

Dieses Produkt enthält grafische Arbeiten der Corel Corporation, die durch Urheberrechtsgesetze der USA, Kanada und anderen Ländern geschützt sind. Benutzung erfolgt mit Genehmigung.

Haupttext gesetzt mit der Fontin Sans, einer Schrifttype von Jos Buivenga (exljbris Font Foundry).

Inhaltsverzeichnis

1	Einführung	1
1.1	Was ist TinkerTool System 8?	1
1.1.1	Die verschiedenen Funktionsbereiche von TinkerTool System 8	2
1.1.2	Systemanforderungen	3
1.2	Die Sicherheitsrichtlinien von TinkerTool System	3
1.2.1	Sicherheitsarchitektur	3
1.2.2	Genehmigung der Sicherheitskomponente	4
1.2.3	Bestätigen eines privilegierten Vorgangs	5
1.2.4	Momentane Einschränkungen in macOS	6
1.2.5	Entfernen alter Generationen der Sicherheitskomponente	6
1.2.6	Aktivieren von strengeren Richtlinien für Verwalterautorisierung	7
1.3	Grundlegende Bedienungshinweise	8
1.3.1	Das Steuerungsfenster von TinkerTool System	8
1.3.2	Bedienelemente in der Symbolleiste	10
1.3.3	Suche nach Funktionen per Stichwort	11
1.3.4	Fenstergröße minimieren	11
1.3.5	Kontexthilfe	11
1.3.6	Das Dockmenü	12
1.3.7	Felder für Dateisystemobjekte	12
1.3.8	Verstehen, wann Änderungen aktiv werden	13
1.3.9	Allgemeine Einstellungen	13
1.3.10	Kartensteuerung	13
1.3.11	Sicherheit	15
1.3.12	Anzeigen von Speichergrößen	16
1.3.13	Andere Einstellungen	16
1.3.14	Alle dauerhaften Änderungen an Systemeinstellungen rückgängig machen	17
1.3.15	Suche nach Softwareaktualisierungen	18
1.4	Systemintegritätsschutz	18
1.4.1	Technischer Hintergrund	18
1.4.2	Abschalten des Schutzes	19
1.5	Datenschutzeinstellungen Ihres Mac	20
1.5.1	Hintergrundinformationen	20
1.5.2	Datenschutzeinstellungen, die TinkerTool System betreffen	21
1.5.3	Ändern der Datenschutzeinstellungen	21
1.6	TinkerTool in TinkerTool System 8 einbinden	22
1.6.1	Einbindung einschalten	22
1.6.2	Einbindung abschalten	23

2	Systemwartung	25
2.1	Die Einstellungskarte Wartung	25
2.1.1	Verzeichnis-Cache	25
2.1.2	Verzeichnisdaten exportieren	26
2.1.3	Locate-Datenbank	28
2.1.4	Gemeinsamer Benutzerordner	29
2.2	Die Einstellungskarte Caches	29
2.2.1	Ungeschützte und geschützte Caches	31
2.2.2	Verwenden der Cache-Wartungsfunktionen	33
2.2.3	Schrift-Caches	34
2.2.4	Symbol-Caches	36
2.2.5	Die Staging-Ablage von Treibern	37
2.3	Die Einstellungskarten für Time Machine	39
2.3.1	Time Machine-Grundlagen	39
2.3.2	Allgemeine Hinweise zum Arbeiten mit der Time Machine-Karte	39
2.3.3	Die unterschiedlichen Versionen von Time Machine für macOS 10 und spätere Versionen von macOS	39
2.4	Die Einstellungskarte Time Machine X	40
2.4.1	Wartung nach dem Austausch einer Datenquelle von Time Machine (macOS 10-Betrieb)	40
2.4.2	Überprüfung und Statistik der Datensicherung (macOS 10-Betrieb)	43
2.4.3	Vergleich von Time Machine Sicherungsschnappschüssen (macOS 10-Betrieb)	46
2.4.4	Arbeiten mit lokalen APFS-Schnappschüssen (macOS 10-Betrieb)	49
2.4.5	Löschen von Time Machine-Sicherungsdaten (macOS 10-Betrieb)	52
2.4.6	Auslesen von Time Machine-Protokollen (macOS 10-Betrieb)	53
2.5	Die Einstellungskarte Time Machine	55
2.5.1	Wartung nach dem Austausch einer Datenquelle von Time Machine	55
2.5.2	Überprüfung der Datensicherung	60
2.5.3	Vergleich von Time Machine Sicherungsschnappschüssen	61
2.5.4	Arbeiten mit lokalen APFS-Schnappschüssen	64
2.5.5	Löschen von Time Machine-Schnappschüssen	66
2.6	Die Einstellungskarte Fehler	67
2.6.1	Beheben von Problemen mit der Softwareaktualisierung von macOS	67
2.6.2	App Store-Aktualisierungen	73
2.6.3	Xcode-Schlüsselbunde	73
2.6.4	Hintergrundobjekte	75
2.6.5	Probleme mit automatischer Zeitsynchronisation beheben	81
2.6.6	Hinzufügen von Farb-Tags auf Servern im Netzwerk	81
2.6.7	Löschen von Partitionierungsdaten auf Platten zur Lösung von Problemen mit dem Festplattendienstprogramm	84
2.7	Die Einstellungskarte Diagnose	86
2.7.1	RAM-Größe auswerten	86
2.7.2	Finder Kopieren testen	90
2.7.3	Optische Disks inspizieren	93
2.7.4	SSDs	95
2.7.5	Flash-Zustand	96
2.7.6	Schnelltest mit Kühlungslüftern durchführen	101
2.7.7	Anmeldezeitabrechnung	103
2.7.8	Monitore testen	105
2.8	Die Einstellungskarte Notfallwerkzeug	108
2.8.1	Einführung in das Notfallwerkzeug	108

2.8.2	Ausdrucken der Anleitung	109
2.8.3	Struktur des Startbefehls	109
2.8.4	Verwenden des Notfallwerkzeugs	111
2.8.5	Alte Versionen des Notfallwerkzeugs	111
2.9	Die Einstellungskarte Netzwerk	112
2.9.1	Informationen über Netzwerkschnittstellen	112
2.9.2	Routing-Tabellen und Netzwerkstatistiken	113
2.9.3	Netzwerkverbindung per Echosignal prüfen	114
2.9.4	Zuordnung zwischen Host-Namen und Adressen ermitteln	116
2.9.5	Weg von Datenpaketen nachverfolgen	116
2.9.6	Datenbanken des Whois-Dienstes abfragen	117
2.9.7	Nutzerinformationen per Finger-Dienst ermitteln	118
2.9.8	Antwortverhalten	120
2.10	Die Einstellungskarte Info	122
2.10.1	Mac-Systemdaten	122
2.10.2	Betriebsumgebung	126
2.10.3	Malware-Schutz	129
2.10.4	Sperrliste Programme	130
2.10.5	Klassische Protokolle und Berichte	132
2.10.6	Moderne Protokollierung und Ablaufverfolgung	137
3	Dateioperationen	145
3.1	Die Einstellungskarte Ablage	145
3.1.1	Link	145
3.1.2	Schutz	147
3.1.3	Attribute	148
3.1.4	Zeitattribute ändern	150
3.1.5	Quarantäne	151
3.1.6	Inhalt	153
3.1.7	Aliasobjekte analysieren	153
3.1.8	Zwangslöschung	156
3.1.9	Verschachtelung	157
3.1.10	Erweiterte Attribute	162
3.2	Die Einstellungskarte Bereinigen	164
3.2.1	Allgemeine Hinweise zum Löschen von Dateien	164
3.2.2	Versteckte Hilfsdateien	164
3.2.3	Protokollarchive	167
3.2.4	Absturzberichte	167
3.2.5	Verwaiste Dateien	170
3.2.6	Aliase	173
3.2.7	Entfern timer Platten	175
3.2.8	Zeitlupen-Bildschirmschoner (nur macOS 14 Sonoma oder höher)	176
3.2.9	Speicherabzüge	178
3.3	Die Einstellungskarte Programme	178
3.3.1	Deinstallationsassistent	178
3.3.2	Entfernen von Software-Komponenten und zugehöriger Dateien	180
3.3.3	Besonderer Start von Programmen	183
3.3.4	Datenschutz	185
3.3.5	Sicherheitsprüfung	186
3.4	Die Einstellungskarte ACL-Rechte	192
3.4.1	Einführung in Berechtigungen	192
3.4.2	POSIX-Berechtigungen	192

3.4.3	Zusätzliche Berechtigungsmarkierungen	194
3.4.4	Zugriffssteuerungslisten	195
3.4.5	Zugriffsrechte zeigen oder einstellen	199
3.4.6	Wirksame Zugriffsrechte	206
3.4.7	Spezielle Rechte	206
3.4.8	Verwaiste Zugriffssteuerungslisten entfernen	209
3.4.9	Berechtigungen in einem Benutzerordner auf Standardwerte stellen	211
3.4.10	Interne Identifikationen von Benutzer- und Gruppen-Accounts finden	214
3.5	Die Einstellungskarte Installationsmedien	216
3.5.1	Betriebssysteminstallation	216
3.5.2	Notwendige Voraussetzungen	216
3.5.3	Herunterladen von Installationsprogrammen ohne den App Store	218
3.5.4	Herunterladen von IPSW-Dateien	218
3.5.5	Anlegen des Installationsmediums	219
3.5.6	Ein Installationsmedium als ISO-Datei anlegen	221
3.5.7	Reparieren der Oktober-2019-Ausgabe des Sierra-Installers	221
3.5.8	Mängel und Einschränkungen im laufenden Betriebssystem	221
3.6	Die Einstellungskarte Systemsicherheit	222
3.6.1	Speicherplatz	222
3.6.2	Programmintegrität	225
3.6.3	Systemprotokoll auf verdächtige Benutzeraktivität prüfen	227
3.7	Die Einstellungskarte APFS	228
3.7.1	Überblick über APFS-Volumes	228
3.7.2	APFS-Schlüssel und Volume-Eigentum	230
3.7.3	Automatische Defragmentierung	232
3.7.4	Arbeiten mit APFS-Schnappschüssen	234
3.7.5	Kopieren von APFS-Daten	235
4	Systemeinstellungen	239
4.1	Die Einstellungskarte System	239
4.1.1	Laufwerk	239
4.1.2	Volumes	241
4.1.3	Spotlight	243
4.1.4	Spotlight-Indexdatenbanken	244
4.1.5	Netz	247
4.1.6	Zugriffsrechtsfilter für neue Dateisystemobjekte	250
4.1.7	Verschiedenes	252
4.2	Die Einstellungskarte „Immer an“-Mobilcomputer	256
4.2.1	Automatisches Einschalten	256
4.3	Die Einstellungskarte Systemstart	256
4.3.1	Hinweise zu Macs mit Apple-Prozessoren	257
4.3.2	Optionen	257
4.3.3	Job-Übersicht	260
4.3.4	NVRAM	263
4.3.5	FileVault	265
4.3.6	Sprache (nur macOS Ventura)	268
4.4	Die Einstellungskarte Anmeldung	269
4.4.1	Einstellungen	269
4.4.2	Benutzer ausblenden	272
4.5	Die Einstellungskarte Programmsprache	273
4.5.1	Startsprache für ein Programm dauerhaft überschreiben	275
4.6	Die Einstellungskarte Cloud-Schutz	276

4.7	Die Einstellungskarte Energiezeitplan	279
4.7.1	Termine für wiederkehrende Ereignisse	279
4.7.2	Termine für einmalige Ereignisse	280
4.7.3	Allgemeine Hinweise zum Energiezeitplan	281
5	Benutzereinstellungen	283
5.1	Die Einstellungskarte Benutzer	283
5.1.1	Einstellungen („Präferenzen“)	283
5.1.2	Benutzte Objekte	287
5.1.3	Startdienste	288
5.1.4	Wörterbücher	290
5.1.5	Reparatur	291
5.1.6	Indexdatenbank von Apple Mail löschen	293
5.1.7	Info	294
5.2	Arbeiten mit Einstellungskarten aus TinkerTool	294
6	Arbeiten in der macOS-Wiederherstellung	297
6.1	Allgemeine Informationen	297
6.1.1	Das Hauptmenü des Programms	297
6.1.2	Beenden des Programms	299
6.2	macOS-Wiederherstellung: Grundfunktionen	299
6.2.1	Reparieren des Temporärordners des Systems	299
6.3	macOS-Wiederherstellung: Arbeiten mit Benutzer-Accounts	300
6.3.1	Auswahl des zu bearbeitenden Benutzer-Accounts	300
6.3.2	Deaktivieren von beschädigten Einstellungsdateien	300
6.3.3	Deaktivieren aller Caches eines Benutzers	300
6.3.4	Reaktivieren aller Caches eines Benutzers	302
6.3.5	Deaktivieren aller Einstellungen eines Benutzers	302
6.3.6	Reaktivieren aller Einstellungen eines Benutzers	303
6.4	macOS-Wiederherstellung: Verwaltung und Reparatur	303
6.4.1	Deaktivieren von beschädigten Systemeinstellungsdateien	303
6.4.2	Deaktivieren systembezogener Caches	303
6.4.3	Reaktivieren systembezogener Caches	305
6.4.4	Zurücksetzen von gemanagten Einstellungen	305
6.4.5	Anmeldebildschirm zurücksetzen	305
6.4.6	Entfernen von angepassten Startobjekten	306
6.5	macOS-Wiederherstellung: Fortgeschrittene Funktionen	308
6.5.1	Abschalten der automatischen Anmeldung	308
6.5.2	Erneuten Lauf des Einrichtungsassistenten erzwingen	308
6.6	macOS-Wiederherstellung: Abrufen von Informationen	309
6.6.1	Hardware- und Systemdaten	309
6.6.2	S.M.A.R.T.-Status von Festplatten	310
6.6.3	Versionsdaten von TinkerTool System für macOS-Wiederherstellung	311
7	Allgemeine Hinweise	313
7.1	Registrierung und Freischalten des Programms	313
7.1.1	Testmodus	313
7.1.2	Demomodus	314
7.1.3	Uneingeschränkte Nutzung	315
7.1.4	Bestellung von Registrierungen	315
7.1.5	Verschiedene Arten von Registrierungen	315

7.1.6	Freischalten der Software mit einem einfachen Registrierungsschlüssel	316
7.1.7	Freischalten der Software mit einer Registrierungsdatei	316
7.1.8	Freischalten der Software mit einem Paar aus Name und Schlüssel	318
7.1.9	Aktivieren einer Crossgrade- oder Upgrade-Registrierung	319
7.1.10	Freischaltung zurücknehmen	319
7.1.11	Vorgehen bei Aktualisierungen und Migrationen	319
7.1.12	Ein Kombi-Ticket für Upgrade-Lizenzen anlegen	319
7.1.13	Arbeiten mit Volumenlizenzen	320
7.2	Wichtige technische Hinweise	321
7.2.1	Abhilfen bei bestimmten Problemen	321
7.3	Versionshistorie	323
7.3.1	Release 8.98 (Build 250122)	323
7.3.2	Release 8.97 (Build 241121)	323
7.3.3	Release 8.96 (Build 240910)	324
7.3.4	Release 8.95 (Build 240731)	324
7.3.5	Release 8.94 (Build 240712)	324
7.3.6	Release 8.93 (Build 240612)	325
7.3.7	Release 8.92 (Build 240515)	325
7.3.8	Release 8.91 (Build 240417)	325
7.3.9	Release 8.9 (Build 240214)	326
7.3.10	Release 8.89 (Build 240111)	326
7.3.11	Release 8.88 (Build 231116)	327
7.3.12	Release 8.87 (Build 231024)	327
7.3.13	Release 8.86 (Build 230925)	328
7.3.14	Release 8.85 (Build 230816)	328
7.3.15	Release 8.8 (Build 230712)	328
7.3.16	Release 8.7 (Build 230614)	329
7.3.17	Release 8.6 (Build 230515)	329
7.3.18	Release 8.5 (Build 230418)	330
7.3.19	Release 8.4 (Build 230315)	330
7.3.20	Release 8.3 (Build 230215)	331
7.3.21	Release 8.2 (Build 230123)	331
7.3.22	Release 8.14 (Build 221220)	332
7.3.23	Release 8.12 (Build 221214)	332
7.3.24	Release 8.11 (Build 221212)	332
7.3.25	Release 8.1 (Build 221205)	332
7.3.26	Release 8.0 (Build 221019)	333
A	Aufgaben und Lösungen	335
A.1	Wo ist diese Funktion jetzt?	335
A.2	Sollte ich regelmäßige Wartungsarbeiten durchführen?	336
A.3	Wie kann ich das System reparieren, wenn macOS durcheinandergewürfelten Text bei der Verwendung bestimmter Schriftarten zeigt?	337
A.4	Wie kann ich die tatsächlichen Zugriffsrechte auf eine Datei oder einen Ordner anzeigen lassen?	337
A.5	Was sollte ich tun, wenn macOS die Online-Hilfe nicht mehr öffnen kann?	337
A.6	Freischalten des Programms	338

Kapitel 1

Einführung

1.1 Was ist TinkerTool System 8?

TinkerTool System 8 ist eine Sammlung von Systemwerkzeugen, die Ihnen dabei hilft, fortgeschrittene Verwaltungsaufgaben auf Macintosh-Computern zu erledigen. Alle Funktionen werden von einem einzelnen Programm aus gesteuert, das als allgemeiner Werkzeugkasten und Erste-Hilfe-Assistent dient. Dies schließt unter anderem ein:

- eingebaute Wartungsfunktionen von macOS, die normalerweise nicht auf der grafischen Benutzeroberfläche sichtbar sind,
- erweiterte Dateioperationen, die im macOS-Finder nicht zur Verfügung stehen,
- die Möglichkeit, auf fortgeschrittene Systemeinstellungen zuzugreifen, die im Programm Systemeinstellungen nicht sichtbar sind,
- grafische Oberfläche für „Pro“-Funktionen, für die Apple in modernen Versionen von macOS keine grafische Oberfläche mehr zur Verfügung stellt,
- originäre und einzigartige Funktionen von TinkerTool System, die dazu gedacht sind, typische Probleme bei der realen Arbeit von Systemverwaltern zu lösen und die Effekte von gewissen Defekten („Bugs“) im Betriebssystem zu reparieren,
- Features, um Ihre Privatsphäre zu schützen,
- ein Notfallwerkzeug, das bei der Fehlersuche und Reparatur von macOS hilft, in Fällen, in denen die normale Benutzeroberfläche nicht mehr startet oder der Account des Systemverwalters beschädigt ist,
- Funktionen, um fortgeschrittene Daten über Hardware, Betriebssystem und Programme abzurufen.

TinkerTool System kennt macOS sehr gut. Es macht von einer selbstanpassenden Benutzeroberfläche Gebrauch, die sich automatisch auf das Computermodell und die Version von macOS, die Sie verwenden, einstellt. Alle verfügbaren Auswahlmöglichkeiten sind über „Einstellungskarten“ verfügbar, ganz ähnlich der Technik, die Sie bereits aus dem Programm Systemeinstellungen kennen.

Im Rest dieses Handbuchs werden wir der Einfachheit halber die Bezeichnung „TinkerTool System“ verwenden, also die „8“ weglassen. Beachten Sie allerdings, dass es in Wirklichkeit sieben Produktgenerationen mit leicht unterschiedlichen Bezeichnungen gibt.

- **TinkerTool System (Version 1):** für Mac OS X 10.2 Jaguar, Mac OS X 10.3 Panther und Mac OS X 10.4 Tiger
- **TinkerTool System Release 2:** für Mac OS X 10.5 Leopard, Mac OS X 10.6 Snow Leopard, Mac OS X 10.7 Lion, OS X 10.8 Mountain Lion und OS X 10.9 Mavericks
- **TinkerTool System 4:** für OS X 10.10 Yosemite und OS X 10.11 El Capitan
- **TinkerTool System 5:** für macOS 10.12 Sierra und macOS 10.13 High Sierra
- **TinkerTool System 6:** für macOS 10.14 Mojave und macOS 10.15 Catalina
- **TinkerTool System 7:** für macOS 11 Big Sur und macOS 12 Monterey
- **TinkerTool System 8:** für macOS 13 Ventura und macOS 14 Sonoma
- **TinkerTool System 9:** für macOS 15 Sequoia

Diese Varianten stellen komplett voneinander getrennte Produktlinien mit unterschiedlichen Lizenzen, Registrierungen und Symbolen dar.

Das Programm ist eine „echte“ macOS-Anwendung und macht von unsicheren Skriptmechanismen keinen Gebrauch. TinkerTool System folgt Apples neuesten Sicherheitsrichtlinien für macOS. Die grafische Oberfläche ist streng vom ausführenden Kern des Programms getrennt, der dazu in der Lage ist, bevorrechtigte Systemvorgänge auszuführen. Dieser Kern wird vom Sicherheitssystem von macOS überwacht, das verantwortlich dafür ist, jede einzelne Operation zu erlauben oder zu verweigern und den Benutzer falls nötig, um Identifikation zu bitten. TinkerTool System fragt den Benutzer nicht selbst nach Kennworten, so dass sichergestellt wird, dass Ihre Anmeldedaten nicht von böartigen Benutzerprogrammen abgefangen werden können.

Beim Beheben typischer Systemprobleme versucht TinkerTool System jeweils, Apples offiziellen Support-Richtlinien zu folgen. Dies bedeutet nicht unbedingt, dass TinkerTool System eine bestimmte Prozedur, die Apple in Schritt-für-Schritt-Anleitungen zur Problembehebung aufführt, Wort für Wort ausführt, sondern dass es direkt interne Befehle verarbeitet, die genau die gleiche Wirkung erzielen. Benutzer können einen speziellen Hilfefknopf betätigen, um zu prüfen, ob Apple offizielle Dokumente über Systemprobleme in deren Datenbank anbietet. Falls solche Dokumentation bereitsteht, kann der Benutzer einen oder mehrere Internet-Links anklicken, um hochaktuelle Informationen über das in Frage kommende Problem zu erhalten.

1.1.1 Die verschiedenen Funktionsbereiche von TinkerTool System 8

Die Funktionen von TinkerTool System gliedern sich in vier unterschiedliche Bereiche:

- **Systemwartung:** Funktionen, die Verwaltern bei verschiedenen Problembehebungen helfen
- **Dateioperationen:** Funktionen, um mit fortgeschrittenen Operationen auf Dateien, Berechtigungen und Programmen zu arbeiten
- **Systemeinstellungen:** Steuermöglichkeiten zum Zugriff auf systemweite Einstellungen, die in macOS vorhanden sind
- **Benutzereinstellungen:** Funktionen zur Fehlersuche und Wartung, die sich nur auf den aktuellen Benutzer beziehen.

Falls Sie das Schwesterprogramm TinkerTool als Ergänzung zu TinkerTool System einsetzen, haben Sie die Möglichkeit, die Einstellungskarten von TinkerTool direkt in das Steuerungsfenster von TinkerTool System zu integrieren. Auf diese Weise können Sie die Funktionen beider Programme unter einem Dach vereinigen und brauchen diese nicht mehr getrennt voneinander zu starten. (Beide Programme müssen jedoch weiterhin vorhanden sein.) Die Einstellungskarten von TinkerTool erscheinen ebenso unter der Rubrik **Benutzereinstellungen**.

1.1.2 Systemanforderungen

Um TinkerTool System 8 zu nutzen, brauchen Sie einen *Apple-Computer*, auf dem eines der folgenden Betriebssysteme installiert ist:

- macOS 13 Ventura
- macOS 14 Sonoma

Es wird empfohlen, auf die neueste Version von macOS zu aktualisieren, die von Apple verfügbar ist. Dies kann über die Funktion **Softwareupdate** > **Automatische Updates** geschehen.

TinkerTool System kann nicht von Benutzer-Accounts aus benutzt werden, die ein leeres Kennwort verwenden. Moderne Versionen von macOS sehen dies als Konfigurationsfehler an und erlauben nicht, dass solche Benutzer Zugang zu privilegierten Teilen des Betriebssystems erhalten.

1.2 Die Sicherheitsrichtlinien von TinkerTool System

1.2.1 Sicherheitsarchitektur

Wenn Sie TinkerTool System zum ersten Mal starten, integriert sich das Programm automatisch in das Sicherheitsmodell von macOS. Dies ist notwendig, da das Programm benutzt werden kann, um kritische Vorgänge in macOS durchzuführen, zum Beispiel um Betriebssystemdateien zu ändern oder sogar zu löschen. Nur verantwortliche Systemverwalter, die den jeweiligen Computer warten, sollten das Recht für solche Aktionen haben. Um einen hohen Sicherheitsstandard zu garantieren, arbeitet TinkerTool System zweigeteilt: Das normale Hauptprogramm mit der grafischen Oberfläche koordiniert alle Vorgänge. Es führt außerdem alle Arbeiten durch, für die keinen besonderen Berechtigungen erforderlich sind. Sobald jedoch ein sogenannter *privilegierter Vorgang* ausgeführt werden muss, also eine besondere, mit Berechtigungen geschützte Operation, wie zum Beispiel das Ändern einer Einstellung, die sich auf *alle* Benutzer des Computers, nicht nur den aktuellen, auswirkt, hält das Programm an, macht auf den bevorstehenden Vorgang aufmerksam, und prüft, ob der aktuelle Benutzer sich als Systemverwalter ausweisen kann. Wenn dies der Fall ist, wird die Arbeit fortgesetzt und die entsprechende privilegierte Operation kann starten.

Der privilegierte Vorgang wird jedoch nicht vom Hauptprogramm selbst abgearbeitet. Eine zweite Komponente, das *privilegierte Hilfsprogramm*, übernimmt diese Arbeit, indem es über einen geschützten, abhörsicheren Kanal den Auftrag des Hauptprogramms entgegennimmt. Selbst wenn es einem unbefugten Angreifer gelingen würde, das Hauptprogramm zu manipulieren, kann es keine kritischen Schadfunktionen im Computer auslösen, weil es dazu nicht berechtigt ist. Nur die privilegierte Komponente, die von macOS überwacht

wird und besonders geschützt ist, hat diese technische Möglichkeit. Es findet also eine *Trennung der Benutzerrechte* statt. Das Hilfsprogramm wird in diesem Zusammenhang auch als *Sicherheitskomponente* bezeichnet.

Kann sich der aktuelle Benutzer nicht als Systemverwalter ausweisen, wird der privilegierte Vorgang abgewiesen und die Ausführung verweigert. Sie erhalten in der grafischen Oberfläche den Hinweis, dass die anstehende Aktion aus Berechtigungsgründen nicht fortgeführt werden konnte.

1.2.2 Genehmigung der Sicherheitskomponente

Apples Richtlinien erfordern es, dass ein Administrator den automatischen Start der Sicherheitskomponente genehmigt, bevor TinkerTool System genutzt werden kann, da die Sicherheitskomponente Dienste *für alle Benutzer gleichzeitig* erbringt. Solche Programme werden von Apple als *Hintergrundobjekt* bezeichnet.

Die Sicherheitskomponente wird von macOS automatisch gestartet, wenn Sie TinkerTool System starten. Sie läuft nicht im Hintergrund, wenn TinkerTool System nicht läuft.

Die Genehmigung kann auf zwei Arten erteilt werden, entweder beim ersten Start des Programms oder jederzeit über das Programm **Systemeinstellungen**. Beim ersten Start ist der normale Ablauf wie folgt:

1. Starten Sie TinkerTool System zum ersten Mal. Das Programm öffnet sein Bedienungsfenster *nicht*, sondern zeigt stattdessen einen Assistenten an, der Sie durch alle erforderlichen Schritte leitet, die Sicherheitskomponente zu genehmigen.
2. macOS blendet über die Mitteilungszentrale rechts oben eine Anfrage ein, ob Sie ein neues Hintergrundobjekt zulassen möchten. Wählen Sie in diesem Dialog **Optionen > Erlauben**.
3. Bestätigen Sie über das Kennwort eines Administrators, dass Sie dies für alle Benutzer erlauben.
4. TinkerTool System entfernt sein Hinweisfenster und startet die volle Bedieneroberfläche.

In älteren Versionen von macOS kann während des allerersten Starts des Programms ein Neustart des Computers erforderlich sein. Leider wird dieser Schritt von Apple erzwungen.

Sie können die Genehmigung auch jederzeit über das Programm Systemeinstellungen erteilen:

1. Beenden Sie TinkerTool System, falls es läuft.
2. Starten Sie **Systemeinstellungen**.
3. Öffnen Sie **Allgemein > Anmeldeobjekte**.
4. Suchen Sie TinkerTool System in der Liste **Im Hintergrund erlauben**.
5. Stellen Sie sicher, dass der Schalter bei diesem Eintrag eingeschaltet ist.

1.2.3 Bestätigen eines privilegierten Vorgangs

Um die erwähnte, von macOS überwachte Bindung zwischen Hauptprogramm und privilegierter Komponente aufzubauen, fragt macOS beim ersten Start von TinkerTool System nach der Berechtigung, ein Hilfsprogramm einrichten zu dürfen. Wurde das spezielle Vertrauensverhältnis zwischen Hauptprogramm und Hilfsprogramm aufgebaut, übernimmt ab da an TinkerTool System die Steuerung der Sonderrechte. Für das Überprüfen der Berechtigung, einen geschützten Vorgang ausführen zu dürfen, gelten folgende Regeln:

Aus Sicherheitsgründen können nur diejenigen Benutzer einen privilegierten Vorgang in TinkerTool System aufrufen, für die der Punkt **Der Benutzer darf diesen Computer verwalten** in der Benutzerverwaltung von macOS eingeschaltet ist. Solche Benutzer werden auch als Administratoren bezeichnet. Dieses Sonderrecht ist die Standardeinstellung für denjenigen Benutzer, dem der Computer gehört und der ihn eingerichtet hat.

Das Programm liest Ihr Kennwort nicht mit: Weder das Hauptprogramm noch die privilegierte Komponente sind direkt an der Kennworteingabe und an der Überprüfung dieses Kennworts beteiligt. Beide Vorgänge werden ausschließlich durch macOS vorgenommen, so dass Ihr Kennwort nicht mitgelesen werden kann. Erst nachdem macOS Ihre Identität überprüft hat, wird das Ergebnis dem Programm mitgeteilt.

Die vorgenannte Regel gilt für die Freigabe privilegierter Vorgänge, jedoch nicht für andere Anmeldevorgänge, die ebenso mit Kennworten geschützt sein können. Wenn das Programm sich bei Server-Diensten oder anderen Computern im Netzwerk anmelden muss, kann es aus technischen Gründen erforderlich sein, dass das Programm das Kennwort in diesem Fall vorübergehend selbst entgegennehmen muss. In solch einem Fall werden Sie vorher ausdrücklich auf diesen Umstand hingewiesen.

Auf Computern mit Touch ID kann die Überprüfung auch per Fingerabdruck erfolgen: Ist Ihr Computer mit Apples Fingerabdrucklesegerät *Touch ID* ausgestattet, kann die Überprüfung Ihrer Identität wahlweise auch per Fingerabdruck erfolgen. Wie in macOS üblich, können Sie jederzeit wählen, ob Sie sich per Kennwort oder per Fingerabdruck identifizieren möchten.

Eine Bestätigung gilt jeweils für den laufenden Vorgang und auf Wunsch fünf (5) Minuten für weitere Vorgänge: In einigen Fällen muss TinkerTool System mehrere privilegierte Einzeloperationen schnell hintereinander ausführen, um einen bestimmten Ablauf zu erreichen, z.B. muss oft eine geschützte Datei gelöscht und dann eine neue Datei in einem geschützten Ordner angelegt werden. Das Programm ist darauf ausgelegt, solche zusammengesetzten Vorgänge als Einheit zu behandeln, auch wenn diese intern als zwei einzelne Operationen verarbeitet werden, die unterschiedliche Rechte erfordern. Sie müssen sich nur einmal und nicht zweimal identifizieren. Aber auch mehrere nicht zusammengehörende Vorgänge führen nicht immer zu einer erneuten Kennworteingabe: Falls zwischen einem privilegierten Vorgang und Ihrer letzten Bestätigung im Programm weniger als fünf Minuten liegen, wird auf eine erneute Überprüfung Ihrer Identität verzichtet.

Falls Sie diese 5-Minuten-Regel aufheben möchten, um jeden zusammenhängenden Vorgang einzeln zu schützen, ist dies möglich. Sie können über die Einstellungen des Programms eine noch strengere Prüfung erzwingen:

1. Wählen Sie den Menüpunkt **TinkerTool System > Einstellungen ...** oder drücken Sie die Tastenkombination  + .
2. Kreuzen Sie die Auswahl **Nach jedem abgeschlossenen Vorgang Verwalterautorisierung aufheben** an.

Eine Bestätigung wird nicht mit anderen Programmen geteilt: Wenn Sie TinkerTool System Ihre Identität bestätigt haben, um einen privilegierten Vorgang auszuführen zu können, gilt diese Bestätigung nur für das Programm selbst, jedoch nicht für andere Programme. Auch dies ist strenger als die üblichen Sicherheitsregeln in macOS, die es zulassen würden, innerhalb von fünf Minuten nach der Kennworteingabe auf weitere Bestätigungen in allen Programmen der gleichen Anmeldesitzung zu verzichten.

1.2.4 Momentane Einschränkungen in macOS

TinkerTool System hält sich streng an die aktuellen Vorgaben von Apple für das Bereitstellen von privilegierten Sicherheitskomponenten. Leider sind die neuesten Techniken, die Apple zur Realisation vorschreibt, nicht immer ausgereift. Das kann im Detail von der macOS-Version abhängen, die Sie einsetzen. Im Moment gelten insbesondere folgende Einschränkungen:

- Es darf sich nur ein einziges Exemplar des Programms auf Ihrem Computer befinden. Sie sollten es vermeiden, beim Start des Programms mehrere Versionen oder mehrere Kopien auf Ihrem Mac zu haben. Nur Sicherheitskopien auf Time Machine-Volumes sind zulässig.
- Nachdem Sie die Genehmigung **Im Hintergrund erlauben** wie oben beschrieben erteilt haben, sollten Sie das Programm nicht umbenennen oder in einen anderen Ordner verschieben. Sie müssen sonst den gesamten Genehmigungsvorgang wiederholen.
- Während Sie den Mac starten, muss macOS das Programm auf dem Start-Volume „sehen“ können. Es sollte sich also im Ordner **Programme** des Start-Volumes oder einen Unterordner davon befinden.

In manchen Versionen von macOS können weitere Einschränkungen bestehen. Ausführliche Informationen finden Sie möglicherweise auch im Kapitel Wichtige technische Hinweise (Abschnitt 7.2 auf Seite 321).

1.2.5 Entfernen alter Generationen der Sicherheitskomponente

TinkerTool System weist eine lange Geschichte auf und hat mit seiner Sicherheitsarchitektur bereits viele Generationen des Betriebssystems geschützt. Da Apple die Vorgaben und Techniken für diesen Aspekt des Systems häufig geändert hat, kann es in der Vergangenheit erforderlich gewesen sein, die Sicherheitskomponente auf eine komplett neue Technik umzustellen. Sie müssen sich in der Regel nicht darum kümmern.

In älteren Versionen von macOS konnte es jedoch Fälle geben, in denen sich eine aktualisierte Sicherheitskomponente so stark von den Vorgängerversionen unterscheidet, dass die alte aus technischen Gründen nicht vollautomatisch entfernt werden konnte. Es bleibt also eine veraltete Version des privilegierten Hilfsprogramms im System zurück, auch wenn das Hauptprogramm gelöscht oder aktualisiert wurde. Dies stört normalerweise nicht, da macOS diese Programme nur bei Bedarf startet. Sie können sich jedoch dazu entscheiden, diese alten Komponenten zu löschen, um einen möglichen Missbrauch zu verhindern und Ihren Computer aufzuräumen.

TinkerTool System unterstützt dies mit einer speziellen Wartungsfunktion, die nach alten Hilfsprogrammen sucht und diese auf Wunsch entfernen kann. Führen Sie hierzu folgende Schritte durch:

1. Starten Sie TinkerTool System falls es noch nicht läuft.

2. Wählen Sie den Menüpunkt **Zurücksetzen > Alte Sicherheitskomponenten bereinigen**

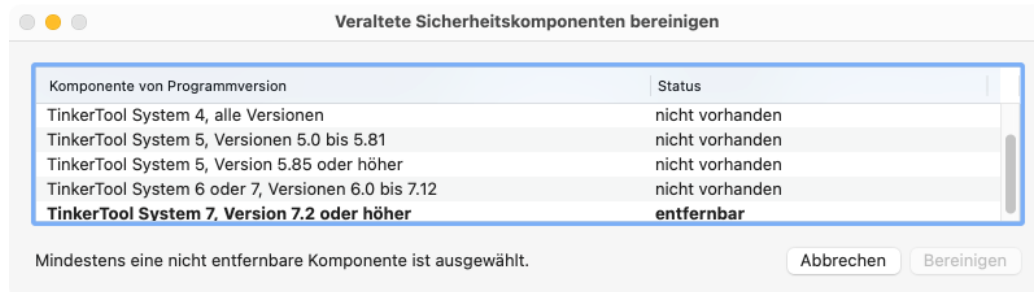


Abbildung 1.1: Veraltete Fassungen des privilegierten Hilfsprogramms können auf Wunsch bereinigt werden.

Es erscheint ein Fenster wie im abgebildeten Beispiel. Die Tabelle listet alle Komponenten auf, die theoretisch aus alten Versionen des Programms vorhanden sein könnten. Fett markierte Komponenten sind tatsächlich vorhanden und werden als **entfernbar** ausgewiesen. Sie können eine oder mehrere dieser Komponenten auswählen und den Knopf **Bereinigen** drücken, um diese zu löschen. Sollten Komponenten unerwartet noch in Benutzung sein, wird dies automatisch erkannt. Solche Hilfsprogramme können erst dann gelöscht werden, wenn Sie das zugehörige Programm beenden.

1.2.6 Aktivieren von strengeren Richtlinien für Verwalterautorisierung

In älteren Versionen des Programms gab es Sonderfälle bei der Genehmigung privilegierter Vorgänge, bei denen eine Anmeldung eines Benutzers mit Verwaltungsrechten aus Sicherheitsgründen *nicht* erlaubt war. Auf Wunsch können Administratoren dieses frühere, stärker eingeschränkte Verhalten wieder wirksam werden lassen.

Autorisierung in der laufenden Anmeldesitzung eines Benutzers, der keine Verwaltungsrechte hat

Ein Benutzer, der gerade nicht als Administrator bei macOS angemeldet ist, kann trotzdem privilegierte Vorgänge ausführen, falls er die Anmeldedaten eines Administrators kennt. Er braucht dazu die laufende Anmeldesitzung nicht zu unterbrechen. Falls diese Möglichkeit aus Sicherheitsgründen nicht gewünscht ist, kann ein Administrator dies sperren, indem er folgenden Befehl in die Kommandozeile des betroffenen Computers eingibt:

```
sudo defaults write /Library/Preferences/com.bresink.system.tinkertoolsystem8.plist
MBSBlockAuthForNonAdminLogin -bool true
```

Rückfall von lokaler Benutzeridentifikation auf Administratoranmeldung mit Name und Kennwort

Um Benutzer als berechtigt für einen privilegierten Vorgang zu erkennen, verwendet das Programm eine Funktion von macOS, die als *lokale Benutzeridentifikation* bekannt ist. macOS überprüft hierbei die Identität des Benutzers durch ein Dialogfenster, das zur Eingabe von Name und Kennwort auffordert. Alternativ ist aber auch die Verwendung von Sicherheits-Hardware möglich, z.B. das Einlesen eines Fingerabdrucks per *Touch ID* oder die Verwendung einer Smartcard.

Es gibt Sonderfälle, bei denen macOS die lokale Benutzeridentifikation ablehnt und den Benutzer als unberechtigt zurückweist:

- Der Administrator hat ein leeres Kennwort und dies ist im laufenden Betriebssystem nicht generell verboten.
- Es sind gerade mehrere Benutzer bei macOS in einer Bildschirmsitzung angemeldet und der Administrator greift über die Funktion *Schneller Benutzerwechsel* oder über eine Netzwerkverbindung per Bildschirmfreigabe zu, aber er besitzt gerade nicht die „vorderste“ Bildschirmsitzung (am physischen Bildschirm), so dass nicht geklärt ist, wer gerade Zugriff auf Touch ID oder andere Sicherheits-Hardware hat. Dies wird in macOS als *nicht-interaktive Situation* bezeichnet.
- Es steht spezielle Hardware zur Benutzeridentifikation zur Verfügung, aber hierbei ist ein technisches Problem aufgetreten.

In solchen Fällen schaltet das Programm automatisch auf die herkömmliche Anmeldung eines Administrators über Name und Kennwort um. Falls diese Möglichkeit aus Sicherheitsgründen nicht gewünscht ist, kann ein Administrator dies sperren, indem er folgenden Befehl in die Kommandozeile des betroffenen Computers eingibt:

```
sudo defaults write /Library/Preferences/com.bresink.system.tinkertoolsystem8.plist
MBSBlockLocalAuthFallback -bool true
```

Zusätzliche Hinweise zur Änderung der Sicherheitsrichtlinien

Beide oben genannten Richtlinien können unabhängig voneinander ein- oder ausgeschaltet werden. In der Regel tritt die Änderung beim nächsten Start des Programms in Kraft. Es kann allerdings besondere Betriebssituationen geben, in denen macOS die Aktivierung verzögert. Soll sichergestellt sein, dass die Änderung auf jeden Fall wirksam wird, ist zu empfehlen, den Computer neu zu starten.

Erst am Ende des Befehls darf die Eingabetaste gedrückt werden, auch wenn ein Befehl aus Platzgründen eventuell mehrzeilig angegeben ist. macOS fragt nach der Eingabe nach dem Kennwort des gerade angemeldeten Administrators. Dieses wird verdeckt eingegeben, erscheint also nicht auf dem Bildschirm.

Um das Verhalten wieder auf den Standard zurückzuschalten, können die folgenden Befehle verwendet werden:

```
sudo defaults delete /Library/Preferences/com.bresink.system.tinkertoolsystem8.plist
MBSBlockAuthForNonAdminLogin
beziehungsweise
sudo defaults delete /Library/Preferences/com.bresink.system.tinkertoolsystem8.plist
MBSBlockLocalAuthFallback
```

1.3 Grundlegende Bedienungshinweise

1.3.1 Das Steuerungsfenster von TinkerTool System

Nach dem Start von TinkerTool System erscheint das Hauptsteuerungsfenster. Je nach Computermodell und Systemkonfiguration kann es ein paar Sekunden dauern, bis das Fenster sichtbar wird. TinkerTool System führt eine große Anzahl von Gültigkeits- und Sicherheitsprüfungen beim Start durch, die etwas Zeit zur Ausführung benötigen. Diese Prüfungen sind notwendig, um sicherzustellen, dass TinkerTool System tatsächlich erfolgreich arbeiten kann, auch wenn Sie es als Erste-Hilfe-Maßnahme auf einem Computer mit teilweise beschädigtem Betriebssystem verwenden.

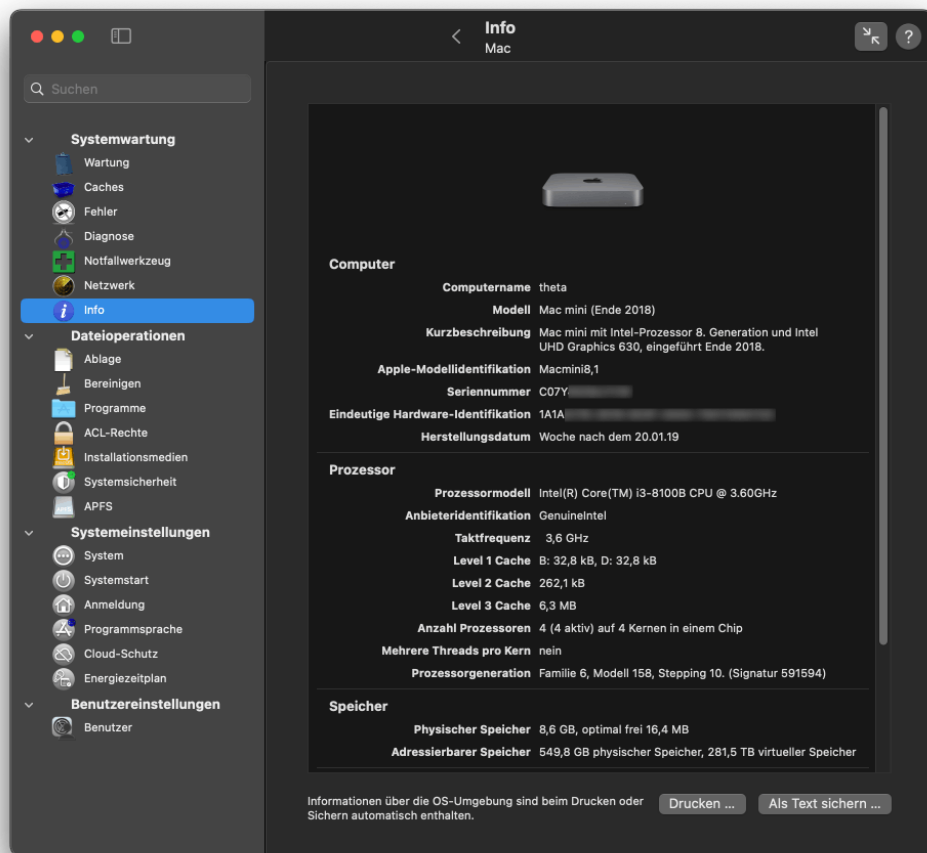


Abbildung 1.2: Das Steuerungsfenster von TinkerTool System

TinkerTool System hat eine lange Tradition, seine Bedieneroberfläche ähnlich zur jeweils passenden Version des Programms Systemeinstellungen zu gestalten. Auf der linken Seite befindet sich die Seitenleiste, in der alle Funktionsbereiche des Programms zu finden sind. Sie sind gegliedert, wie in der Einführung (Abschnitt 1.1 auf Seite 1) beschrieben. Nach Anklicken eines Punktes erscheint die zugehörige Einstellungskarte im rechten Bereich des Fensters. Einstellungskarten können weiter unterteilt sein. Dies kann je nach Funktion entweder durch Tabs (Karteireiter) oder durch wechselnde Unterpunkte geschehen, die sich über eine Übersichtsliste öffnen lassen.

Am oberen Rand der Seitenleiste befindet sich ein Suchfenster, mit dem Sie ein bestimmtes Feature auch per Stichwort suchen können. Der rechte Teil des Fensters enthält oben den Fenstertitel, über den sich die gewählte Einstellungskarte und ein eventuell gewählter Unterpunkt ablesen lassen. Außerdem ist ein Knopf zur Verkleinerung des Fensters und ein Knopf zum Aufrufen der Kontexthilfe zu finden. Diese Punkte werden in den nächsten Abschnitten beschrieben.

Sie können eine Einstellungskarte von TinkerTool System durch Anklicken in der Seitenleiste auswählen. Alternativ können Sie auch die Tasten  oder  verwenden, um zwischen den einzelnen Funktionsbereichen zu wechseln. Ebenso ist es möglich, eine Einstellungskarte über das Menü **Darstellung** auszuwählen. Dort sind alle Karten mit zugehörigem Symbol auch noch einmal aufgelistet. Über die Tastenkombinationen  +  oder  +  können Sie zusätzlich zwischen den einzelnen Karten nach den Begriffen **rückwärts**, bzw. **vorwärts** wechseln. Hierbei haben Sie über eine Einstellung (siehe unten) die Wahl, ob dies räumlich oder zeitlich verstanden werden soll. TinkerTool System merkt sich, mit welcher Karte Sie das letzte Mal gearbeitet haben. Beim nächsten Start des Programms werden Sie automatisch wieder an diese Stelle geführt.

1.3.2 Bedienelemente in der Symbolleiste

Neben der Seitenleiste ist die Symbolleiste am oberen Fensterrand ein wichtiges Hilfsmittel bei der Bedienung des Programms. Ganz links befinden sich die üblichen drei Knöpfe zum Schließen, Zoomen oder zur Dockablage des Fensters. Mit dem Symbol daneben können Sie die Seitenleiste auf Wunsch ausblenden und später wieder einblenden. Dies ist nützlich, wenn Sie sich vorübergehend auf eine bestimmte Funktion des Programms konzentrieren und die größtmögliche Arbeitsfläche hierfür verwenden möchten.

Der freie Platz neben dem Seitenleistensymbol ist für wichtige Hinweise oder Warnungen reserviert, die das gesamte Programm betreffen. Sollten dort Symbole erscheinen, können Sie diese anklicken, um ausführliche Informationen über ein eventuell vorliegendes Problem zu erhalten.

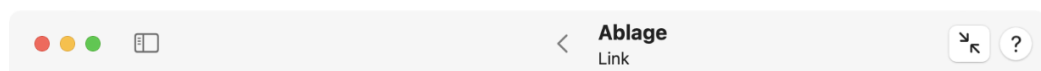


Abbildung 1.3: Neben der Seitenleiste ist die Symbolleiste ein wichtiges Bedienungselement

Ungefähr in der Mitte des Fensters finden Sie den Titel der gerade ausgewählten Einstellungskarte. Handelt es sich um eine Karte, die Unterfunktionen anbietet, die über eine Liste (also nicht über einen Karteireiter) abgerufen werden, finden Sie dort in der zweiten Zeile auch den Namen der entsprechenden Unterfunktion. Das nebenstehende Symbol  dient als Knopf, um wieder zur Übersicht zurückzukehren. Stattdessen können Sie auch den Menüpunkt **Darstellung** > **Aufwärts zur Übersicht** aufrufen oder die Tastenkombination  +  betätigen. Ebenso ist dies möglich, indem Sie die Karte in der Seitenleiste anklicken.

Am rechten Rand der Symbolleiste finden Sie einen Knopf zur Optimierung der Fenstergröße und einen Knopf zur Einblendung der schnellen Kontexthilfe. Beide Punkte werden in den folgenden Abschnitten näher erläutert.

Die Symbolleiste kann nicht ausgeblendet werden, da sie für die Bedienung des Programms zu wichtig ist.

1.3.3 Suche nach Funktionen per Stichwort

TinkerTool System bietet eine hohe Zahl unterschiedlicher Funktionen. Für Einsteiger kann es schwierig sein, sofort zu wissen, auf welcher Karte und in welchem Unterpunkt sich eine gesuchte Funktion befindet. Um Ihnen in diesem Fall zu helfen, können Sie nach Features und Einstellmöglichkeiten per Stichwort suchen. Tippen Sie den Suchbegriff in das Feld **Suchen** links oben im Fenster ein. Bereits nach jedem eingetippten Buchstaben macht TinkerTool System Vorschläge, um welche Funktion es sich handeln könnte. Die Treffer werden in der Seitenleiste mit den zugehörigen Karten aufgelistet. Je nach Situation werden auch die Namen der jeweiligen Unterpunkte in Klammern angegeben. Ist die Seitenleiste zu schmal, um den Begriff vollständig zu zeigen, können Sie den Mauszeiger über diesen Punkt bewegen und der gesamte Text wird eingeblendet. Durch Anklicken kann die Karte und der jeweilige Unterpunkt sofort geöffnet werden.

Das eingegebene Suchwort kann über die Schaltfläche mit dem Kreuz im Suchfeld gelöscht werden. Die Seitenleiste kehrt dann zum Normalbetrieb zurück.

1.3.4 Fenstergröße minimieren

Durch die Vielfalt unterschiedlicher Funktionen in TinkerTool System bestehen oft große Unterschiede im Platzbedarf, den eine bestimmte Karte im Fenster hat. Das Steuerungsfenster vergrößert sich automatisch, falls erforderlich, Sie können aber auch jederzeit selbst das Fenster durch Ziehen des Randes vergrößern oder durch Betätigen des grünen Knopfes auf Vollbildmodus schalten.

Möchten Sie das Fenster wieder auf optimale Größe bringen, d.h. die kleinstmögliche Größe einstellen, die TinkerTool System zur Darstellung eines bestimmten Punktes benötigt, können Sie auf den Knopf mit den zwei Pfeilen in der Titelleiste des Fensters klicken. Je nach gerade ausgewähltem Feature ist das Ergebnis unterschiedlich.

1.3.5 Kontexthilfe

Jede Einstellungskarte von TinkerTool System bietet ein Anzeigefenster mit Kontexthilfe an, das über den runden Knopf mit dem Fragezeichen in der oberen rechten Ecke geöffnet werden kann. Ein zweites Fenster wird an eine der Seiten des Hauptfensters andocken und eine kurze Hilfeinformation über die Einstellungskarte und den gerade geöffneten Funktionsbereich zeigen. Der Hilfetext ist in die folgenden Abschnitte unterteilt:

- **Was passiert:** eine kurze Beschreibung, welche Funktion im gerade geöffneten Unterpunkt angeboten wird und was passieren wird, wenn Sie diese Funktion aufrufen.
- **Zu verwenden wenn:** eine oder mehrere Beschreibungen typischer Situationen, in denen diese Funktion nützlich sein kann.
- **Nicht zu verwenden wenn:** eine Liste von Gegenanzeigen, bei denen es nicht empfehlenswert ist, diese Funktion zu nutzen, oder wo sie sogar schädlich sein kann.

- **Hinweise:** eine optionale Liste zusätzlicher Hinweise.
- **Internet-Informationen von Apple:** Falls verfügbar, ein oder mehrere Links zu Webseiten von Apple, die aktuelle Informationen aus erster Hand über das zur Diskussion stehende Thema geben.

1.3.6 Das Dockmenü

Einige oft genutzte Funktionen von TinkerTool System können auch über das Dockmenü aktiviert werden: Suchen Sie nach dem Symbol des Programms im Dock und führen Sie dann einen Rechtsklick auf das Symbol aus, um das Kontextmenü zu öffnen. Die Menüpunkte folgen den üblichen Macintosh-Regeln. Falls der Text eines Punktes *nicht* mit einem Ellipsenzeichen (...) endet, wird die Funktion sofort ausgeführt, nachdem Sie sie im Menü ausgewählt haben. Im anderen Fall wird TinkerTool System nur die entsprechende Einstellungskarte und den zugehörigen Unterpunkt öffnen, so dass Sie die Gelegenheit haben, Einstellungen zu prüfen und anzupassen, bevor irgendetwas geschieht.

1.3.7 Felder für Dateisystemobjekte

Viele Funktionen von TinkerTool System arbeiten mit Dateien und Ordnern. Im Unterschied zu anderen Programmen ist es oftmals wichtig zu wissen, an welchem genauen Ort diese Objekte gespeichert sind. macOS verwendet UNIX-Pfade, um solche Ortsangaben zu beschreiben. Aus diesem Grund verwendet TinkerTool System besondere Felder, um Dateisystemobjekte zusammen mit ihren Pfaden innerhalb des Programms anzuzeigen. Diese Felder sind eine besondere Eigenschaft von TinkerTool System und sehen wie folgt aus:

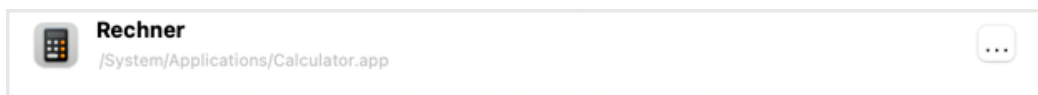


Abbildung 1.4: Pfadeingabefeld

- Auf der linken Seite des Feldes können Sie das Symbol für das ausgewählte Dateisystemobjekt sehen. Dies ist das gleiche Symbol, das auch der Finder und andere Programme verwenden, um dieses Objekt darzustellen.
- Oben im Feld wird der Name des Objekts angezeigt. Er ist möglicherweise in Ihrer bevorzugte Sprache übersetzt und Dateinamenserweiterungen könnten versteckt sein.
- Der tatsächliche UNIX-Pfad dieses Objekts wird in kleinerer Schrift unten im Feld angezeigt. Da Pfade sehr lang werden können, werden möglicherweise mehrere Zeilen benötigt, um den Pfad darzustellen.
- Auf der rechten Seite ist ein Auswahlknopf zu erkennen. Dieser Knopf ist nur dann vorhanden, falls es Ihnen erlaubt ist, den Inhalt des Feldes zu ändern. Nach Betätigen des Knopfes wird ein normaler Öffnen-Dialog von macOS angezeigt, der es Ihnen erlaubt, in einen anderen Ordner zu navigieren und ein anderes Objekt auszuwählen.

In allen Fällen, in denen TinkerTool System möchte, dass Sie ein Dateisystemobjekt angeben, können Sie irgendeine der folgenden Methoden anwenden, um die angefragten Daten einzugeben:

- Sie können, falls vorhanden, auf den Auswahlknopf drücken, wie es oben bereits erwähnt wurde. Ein Navigationsdialog wird erscheinen. Alternativ können Sie auch einen Doppelklick oder einen alt-Klick in das Feld ausführen. Letzteres ist insbesondere dann hilfreich, wenn Ihre Sehkraft beeinträchtigt ist.
- Sie können in das Feld klicken und einen UNIX-Pfad von Hand eingeben. Beachten Sie, dass Pfade immer mit einem führenden Schrägstrich (/) beginnen. Beenden Sie die Dateneingabe durch Betätigen der Taste .
- Sie können ein einzelnes Objekt aus dem Finder in das Feld hineinziehen.

1.3.8 Verstehen, wann Änderungen aktiv werden

Wenn Sie TinkerTool System verwenden, eine Systemeinstellung von macOS zu ändern, versucht es grundsätzlich, diese sofort wirksam werden zu lassen. Beachten Sie, dass macOS möglicherweise nach Name und Kennwort eines Benutzers mit Verwaltungsberechtigung fragt, bevor die eigentliche Änderung stattfindet. Sie können erkennen, dass eine Änderung erfolgreich durchgeführt worden ist, wenn die Bedienerschnittstelle im neuen Zustand verbleibt, also z.B. wenn ein gesetztes Häkchen angekreuzt bleibt, oder ein Umschaltknopf, den Sie betätigt haben, mit seiner Markierung in der neuen Position verharret. Bei Funktionen, die nicht nur eine einfache Einstellung ändern, sondern einen gewissen Vorgang auslösen, zum Beispiel die Löschung einer ausgewählten Datei, wird TinkerTool System ein herausgleitendes Dialogfenster anzeigen, nachdem der Vorgang abgeschlossen wurde. Das Fenster bestätigt entweder, dass der Vorgang erfolgreich war oder dass er aus irgendeinem Grund fehlgeschlagen ist. Komplexere Vorgänge, die eventuell mehrere Minuten laufen, werden von einem Textbericht begleitet, der entweder bereits während des Vorgangs oder nach dessen Beendigung angezeigt wird, je nach technischer Situation. Solche Berichte können in Textdateien gespeichert oder zum späteren Nachschlagen auch ausgedruckt werden.

1.3.9 Allgemeine Einstellungen

TinkerTool System unterstützt ein paar Einstellungen, die grundlegende Richtlinien steuern. Sie können diese über die Auswahl des Menüpunktes **TinkerTool System > Einstellungen ...** öffnen oder durch Druck auf  + .

1.3.10 Kartensteuerung

Das Setzen eines Häkchens bei der Auswahl **Beim Start automatisch letzte benutzte Karte öffnen** hat zur Folge, dass sich das Programm an diejenige Karte erinnert, die Sie zum letzten Mal verwendet haben, als Sie das Programm beendeten. TinkerTool System schaltet automatisch beim nächsten Start wieder zu dieser Karte und dem richtigen Karteireiter, bzw. der richtigen Unterfunktion.

Die Pfeilknöpfe, -tasten oder -menüpunkte erlauben Ihnen, zwischen den verschiedenen Karten in der Reihenfolge hin- und her zu schalten, in der sie im Fenster dargestellt sind. Das heißt, Sie navigieren *nach Position*. In vielen anderen Programmen, z.B. Web-Browsern, erlauben es Ihnen die Pfeile stattdessen, vorwärts oder rückwärts *in der Zeit* zu gehen. Falls Sie lieber diesen Ansatz verwenden möchten, wählen Sie die Option **Pfeile navigieren durch Verlauf**.

Wie erwähnt sind die meisten Karten so gestaltet, dass es ähnlich wie in den Systemeinstellungen eine Art Hauptmenü mit einer Liste der Unterfunktionen gibt, die Sie abrufen können. Wenn Sie sich beim Start des Programms oder beim Durchblättern zwischen den

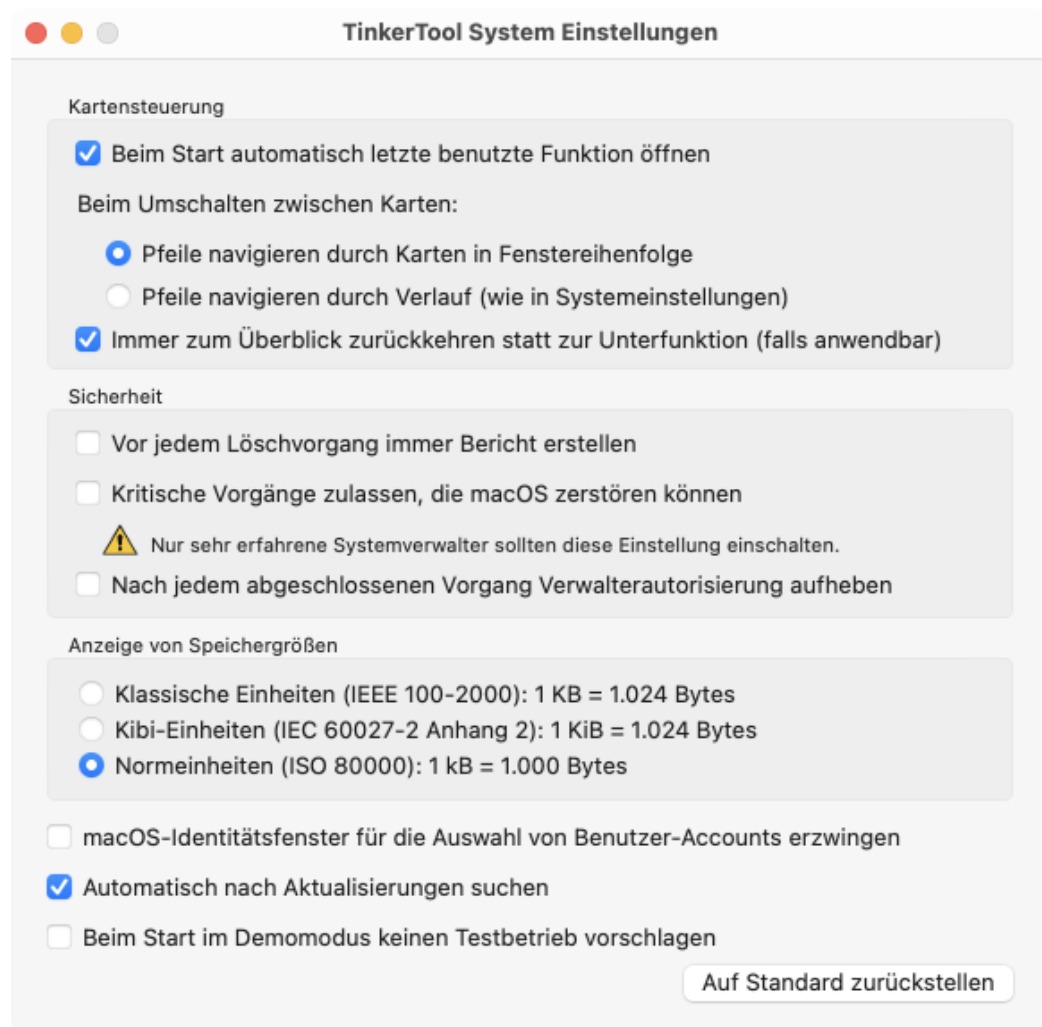


Abbildung 1.5: Das Einstellungsfenster

verschiedenen Karten auf die zuletzt benutzte Unterfunktion leiten lassen, kann es für Ungeübte verwirrend sein, dass Sie immer nur die zuletzt verwendete Unterfunktion und nicht alle Funktionen der Karte sehen. Über die Einstellmöglichkeit **Immer zum Überblick zurückkehren statt zur Unterfunktion (falls anwendbar)** können Sie dies ändern. Beim Wechsel auf eine Karte sehen Sie dann immer den Überblick mit der Liste der abrufbaren Funktionen. Diese Option wird ab Version 8.4 des Programms standardmäßig eingeschaltet, kann aber von jedem Benutzer wieder abgeschaltet werden, falls gewünscht.

1.3.11 Sicherheit

Die Auswahl **Vor jedem Löschvorgang immer Bericht erstellen** steuert, ob TinkerTool System einen Bestätigungsdialog anzeigen soll, bevor Objekte aus dem Dateisystem entfernt werden. Dies bezieht sich hauptsächlich auf die Einstellungskarte **Bereinigen** und ein paar andere Features von TinkerTool System, die möglicherweise Dateien oder Ordner löschen, die im Vorhinein unbekannt sind. Im Bestätigungsdialog können Sie voraussehen, was TinkerTool System tun wird, wenn die Löschoperation zur Ausführung kommt. Sie können entweder den ganzen Vorgang abbrechen, oder bestimmte Dateien und Ordner aus der Löschmenge ausschließen. Es wird empfohlen, diese Einstellung angeschaltet zu lassen. Das Ausschalten führt dazu, dass TinkerTool System nicht auf eine Bestätigung wartet, sondern Dateien sofort löscht. Die Einstellungskarte **Bereinigen** besitzt jedoch noch weitere Schalter, mit denen diese Vorgehensweise für eine einzelne Operation wieder überschrieben werden kann.

Die Auswahl bezieht sich nicht auf alle Löschvorgänge. Beim Entfernen von Cache-Dateien können Zehntausende von Dateien betroffen sein, so dass eine Bestätigung jeder einzelnen Datei nicht sinnvoll sein würde.

TinkerTool System enthält einen Sicherheitsmechanismus, der versucht, zu erkennen, ob Sie dabei sind, Änderungen vorzunehmen, die das gesamte Betriebssystem unbrauchbar machen könnten. Beispiele hierfür sind das Ändern von Berechtigungseinstellungen für Dateien, die Teil des Betriebssystems sind oder das Entfernen von Dateien, die zu macOS gehören. In diesen Fällen könnten die Änderungen dazu führen, dass TinkerTool System oder der ganze Computer nicht mehr richtig arbeiten, so dass es auch nicht mehr möglich ist, eine solche Veränderung rückgängig zu machen, ohne das ganze System neu zu installieren.

Sehr erfahrene Systemverwalter können diesen Schutzmechanismus abschalten, indem sie ein Häkchen bei **Kritische Vorgänge zulassen, die macOS zerstören könnten** setzen. Danach wird TinkerTool System gefährliche Dateioperationen nicht mehr blockieren. Der Systemverwalter ist allein für die durchgeführten Aktionen verantwortlich.



Es wird nicht empfohlen, diese Auswahlmöglichkeit einzuschalten. Vollständiger Datenverlust kann auftreten. Sie sollten genau wissen, was Sie tun, wenn die Sicherheitsvorkehrung inaktiv ist.



Sie dürfen diese Sicherheitsfunktion nicht als Garantie missverstehen.

hen, dass TinkerTool System nicht doch dazu missbraucht werden kann, wichtige Benutzer- oder Systemdateien zu beschädigen, selbst wenn die Funktion aktiv ist.

Die Wahlmöglichkeit **Nach jedem abgeschlossenen Vorgang Verwalterautorisierung aufheben** steuert, ob TinkerTool System macOS erlauben soll, die erfolgreiche Autorisierung eines Systemverwalters zwischenspeichern und wiederzuverwenden, wenn Name und Kennwort korrekt eingegeben wurden, und noch nicht mehr als 5 Minuten seit der letzten Sicherheitsfreigabe vergangen sind. Für weitere Informationen verwenden Sie bitte das Kapitel Die Sicherheitsrichtlinien von TinkerTool System (Abschnitt 1.2 auf Seite 3).

1.3.12 Anzeigen von Speichergrößen

Die Knöpfe im Kasten **Anzeige von Speichergrößen** erlauben es, auszuwählen, wie das Programm Byteangaben runden soll, wenn die Größen von Plattenspeicher oder Hauptspeicher angegeben werden:

- **Klassische Einheiten** verwenden die alte, übliche Praxis in der Informationstechnik, Speichergrößen als Vielfache von Zweierpotenzen anzugeben. 1 Kilobyte entspricht 1.024 Bytes. Kilo wird in diesem Fall mit einem großen K abgekürzt, was andeuten soll, dass eine binäre Interpretation gemeint ist und nicht das übliche dezimale Präfix mit der Bedeutung 1.000. Bei größeren Vielfachen (1 MB = 1.048.576 Bytes, nicht 1.000.000 Bytes) wird diese Unterscheidung jedoch nicht gemacht.
- **Kibi-Einheiten** lösen diese Mehrdeutigkeit auf, indem zusätzlich die Markierung „bi“ eingefügt wird, was einen binären Präfix anzeigt. 1 Kibibyte (1 kiB) sind 1.024 Bytes. 1 Mebibyte („Megabinär“, 1 MiB) sind 1.048.576 Bytes.
- **Normeinheiten** erzwingen die Einhaltung von „korrekten“ internationalen Konventionen für Messgrößen und Einheiten. 1 Kilobyte sind 1.000 Bytes, nun abgekürzt als 1 kB. 1 Megabyte (1 MB) entspricht 1 Million Bytes.

Die Auswahlmöglichkeit **Normeinheiten** ist der empfohlene Standard für macOS, da viele von Apples Programmen (leider nicht alle) die gleiche Vorgehensweise bei der Anzeige von Speichergrößen verwenden.

1.3.13 Andere Einstellungen

TinkerTool System enthält mehrere Funktionen, bei denen Sie einen Benutzer oder eine Gruppe aus einer Liste von Accounts wählen müssen, die auf Ihrem Mac vorhanden sind, beispielsweise um den Eigentümer einer Datei zu ändern. In professionellen Netzwerkumgebungen wird die Liste der Benutzer- und Gruppen möglicherweise nicht von Ihrem Mac alleine verwaltet, sondern auch von einem oder mehreren *Verzeichnisdienstservern* im Netz. Auf diese Weise kann Ihr Mac mit einigen tausend Benutzer-Accounts arbeiten, die in Ihrem Netz bekannt sind. Einige Versionen von macOS sind allerdings von Leistungsproblemen betroffen, wenn sie mit solchen externen Account-Listen arbeiten müssen. Da TinkerTool System Ihnen die vollständige Liste von Benutzern oder Gruppen in Situationen präsentieren möchte, in denen Sie einen Account wählen müssen, kann das Abrufen dieser Listen wesentliche Zeit beanspruchen. Einige Versionen von macOS können sogar die Bedienerschnittstelle für mehrere Minuten blockieren, aufgrund von internen Konstruktionsfehlern in der Art und Weise wie das Betriebssystem die notwendigen Daten sammelt. Um solche Probleme zu vermeiden, können Sie TinkerTool System zwingen, eine sehr einfache Bedienerschnittstelle zu verwenden, wenn es notwendig ist, aus einer Liste von

vorhandenen Benutzern und Gruppen auszuwählen. Setzen Sie ein Häkchen bei **macOS-Identitätsfenster für die Auswahl von Benutzer-Accounts erzwingen**, um nur die eingebauten Funktionen von macOS zu verwenden.

Falls das simple Account-Fenster ebenso Geschwindigkeitsprobleme zeigt, weist dies darauf hin, dass diese macOS-Version dies im Moment nicht effizienter handhaben kann.

Apples Account-Fenster hat allerdings die folgenden Nachteile:

- Es ist nicht möglich, einen Eintrag vorauszuwählen, um Sie in einer bestimmten Situation besser zu führen.
- Sie müssen je nach Kontext entscheiden, ob ein Benutzer- oder ein Gruppen-Account ausgewählt werden muss.
- Sie können die internen Bezeichnungen der Accounts nicht sehen, nur deren Präsentationsnamen.
- Sie können nicht auf systeminterne Accounts zugreifen.

Mit der Option **Automatisch nach Aktualisierungen suchen** lässt sich steuern, ob das Programm Sie automatisch darüber informieren soll, wenn neue, kostenlose Updates der Software verfügbar werden. Die automatische Prüfung findet in regelmäßigen Abständen statt während Sie das Programm starten.

Die Einstellung **Beim Start im Demomodus keinen Testmodus vorschlagen** ist nur dann anwendbar, wenn Sie keine gültige Registrierung für TinkerTool System besitzen. Unter normalen Umständen bietet es Ihnen TinkerTool System an, das Programm während eines begrenzten Zeitraums kostenlos zu testen, was Testmodus genannt wird. Wird diese Einstellung angekreuzt, wird TinkerTool System beim Start auf dieses Angebot verzichten (falls es noch verfügbar ist), und stattdessen sofort in den gesperrten Demomodus wechseln. Um mehr über den Demomodus, das Freischalten von TinkerTool System und den Testmodus zu erfahren, verwenden Sie bitte das entsprechende Kapitel (Abschnitt 7 auf Seite 313).

Der Knopf **Auf Standard zurückstellen** stellt alle Wahlmöglichkeiten, die in diesem Abschnitt erläutert wurden, wieder auf die empfohlene Einstellung ab Werk zurück. Nur die Einstellung zur Update-Benachrichtigung behält ihren Wert.

1.3.14 Alle dauerhaften Änderungen an Systemeinstellungen rückgängig machen

Zu den vielen Features von TinkerTool System zählt die Möglichkeit, Systemeinstellungen, die in macOS eingebaut sind, zu ändern. Falls Systemprobleme auftreten, möchten Sie eventuell alle Einstellungen wieder auf Apples Werkseinstellungen zurücksetzen. Dies ist möglich, indem Sie den Menüpunkt **Zurücksetzen > Alle permanenten Änderungen zurücksetzen ...** wählen oder die Tastenkombination  +  +  betätigen und den Anweisungen folgen.

Dieser Schritt ist auch hilfreich, wenn Sie TinkerTool System ohne Lizenz im Testmodus ausprobiert haben, aber die Testzeit abgelaufen ist. In diesem Fall fällt TinkerTool System in den Demomodus zurück und Sie können es nicht mehr länger verwenden, um Systemeinstellungen zurückzustellen, die Sie möglicherweise geändert hatten. Die Rücksetzfunktion bleibt jedoch immer verfügbar, egal ob Sie eine Nutzungslizenz erwerben oder nicht. Dies stellt sicher, dass Sie nicht aus bestimmten Einstellungen ausgeschlossen werden, auch wenn der Testmodus abgelaufen ist.

Beachten Sie, dass es nicht möglich ist, zu unterscheiden, ob Systemeinstellungen von TinkerTool System, von einem anderen Programm eines Drittanbieters oder über die Befehlszeile von macOS geändert wurden. Aus diesem Grund muss TinkerTool System *alle* Systemeinstellungen auf Werkseinstellung zurückstellen, *die es theoretisch geändert haben könnte*, auch wenn Sie das Programm gar nicht dazu genutzt haben, sondern etwas Anderes die ursprüngliche Änderung ausgelöst hat. Hiervon ausgenommen ist das Abschalten von IPv6, da volle Kontrolle hierüber jederzeit im Programm **Systemeinstellungen** möglich ist, falls Sie vorher eine diesbezügliche Abschaltung vorgenommen haben.

1.3.15 Suche nach Softwareaktualisierungen

TinkerTool System befindet sich unter ständiger Weiterentwicklung und neue Versionen werden in unregelmäßigen Zeitabständen veröffentlicht. Diese Aktualisierungen sind üblicherweise kostenlos, falls nicht ein vollständig neu überarbeitetes Produkt angeboten wird. Die neueste Version steht jeweils zum Herunterladen auf der offiziellen Web-Seite zur Verfügung. TinkerTool System kann überprüfen, ob ein neues kostenloses Update für die Version bereitsteht, die Sie aktuell verwenden. Um dies zu tun, wählen Sie den Menüpunkt **TinkerTool System > Nach Aktualisierungen suchen**. Das Programm verbindet sich mit dem Internet und informiert Sie über das Ergebnis. Falls tatsächlich eine neuere Version verfügbar ist, können Sie auswählen, ob Sie Ihren Web-Browser öffnen möchten, um automatisch zur Seite zum Herunterladen geführt zu werden. Statt eine manuelle Prüfung über das Anklicken eines Menüpunkts durchzuführen, können Sie alternativ auch eine Einstellung aktivieren (siehe oben), um das Programm automatische Prüfungen in regelmäßigen Zeitabständen ausführen zu lassen.

Das Programm unterstützt keine automatischen Funktionen zum Herunterladen, denn solche Features können und dürfen in professionellen Umgebungen nicht verwendet werden, bei denen die Software auf geschützten Datei-Servern gespeichert ist. Die automatische Ersetzung von Software-Produkten entspricht möglicherweise weder den Sicherheitsstandards von großen Organisationen, noch den gesetzlichen Bestimmungen in bestimmten Ländern.

1.4 Systemintegritätsschutz

1.4.1 Technischer Hintergrund

Das Betriebssystem wird durch eine Sicherheitsfunktion namens *Systemintegritätsschutz* (*System Integrity Protection*) geschützt. Auf der technischen Ebene wird auch der englische Begriff *Customer System Restriction (CSR)* verwendet. Zu Marketingzwecken verwendet Apple außerdem den Begriff *rootless*.

Systemintegritätsschutz bedeutet, dass nur bestimmte Programme des Betriebssystems selbst, z.B. das **Apple-Installationsprogramm**, die Erlaubnis haben, gewisse Dateien des Betriebssystems zu ändern oder gewisse Funktionen zu nutzen. Nicht einmal die höchste Systemautorität, der Benutzer-Account *root*, kann diese Einschränkung umgehen. Diese Vorgehensweise stellt sicher, dass das System nicht beschädigt oder absichtlich durch einen Angreifer manipuliert werden kann. Zugriff auf die folgenden Betriebsmittel wird durch den Systemintegritätsschutz eingeschränkt:

- Das Ändern oder Löschen von Betriebssystemdateien, die mit dem speziellen Attribut *eingeschränkt (restricted)* versehen sind.
- Das Ändern oder Löschen bestimmter NVRAM-Einträge.
- Die Nutzung von Kernel-Erweiterungen, denen nicht vertraut wird.
- Die Verwendung des Kernel-Debuggers.
- Die Nachverfolgung bestimmter Systemprozesse über das Dienstprogramm *dtrace*.

Einige Funktionen von TinkerTool System können vom Systemintegritätsschutz betroffen sein. Wenn Sie beispielsweise die Wahlmöglichkeit **Kritische Vorgänge zulassen, die macOS zerstören könnten** einschalten und Sie versuchen, die Funktion **Ablage > Zwangslöschung** bei einer Datei zu verwenden, die mit dem Attribut **eingeschränkt** markiert ist, wird der Löschvorgang von macOS verhindert. In solchen Fällen zeigt TinkerTool System eine Fehlermeldung folgender Art an:

„Dein Computer ist dazu eingerichtet, diesen Vorgang nicht zu gestatten. Die laufende Aufgabe kann nicht abgeschlossen werden, da der Systemintegritätsschutz auf diesem Computer aktiv ist. Es könnte möglich sein, diese Funktion abzuschalten, indem eine Hardware-Einstellung über das Wiederherstellungsbetriebssystem geändert wird. Weitere Informationen findest du im Referenzhandbuch.“

Der Systemintegritätsschutz kann ausgeschaltet werden, falls der Besitzer des Computers das bevorzugt. Um wirksam zu sein, schützt sich der Systemintegritätsschutz allerdings selbst. Das heißt, dass die Abschaltung dieser Funktion innerhalb des laufenden Betriebssystems nicht möglich ist. Darüberhinaus wird diese Einstellung nicht in einer Datei, sondern in der System-Hardware gespeichert. Falls Sie mehrere Exemplare von macOS auf Ihrem Computer installiert haben, wird die Einstellung für alle wirksam.

1.4.2 Abschalten des Schutzes

Falls Sie den Systemintegritätsschutz aus irgendeinem Grund abschalten möchten, können Sie dies wie im vorigen Abschnitt erwähnt tun. Führen Sie dazu die folgenden Schritte durch:

Die Schritte sind je nach Prozessortyp Ihres Macs leicht unterschiedlich. Wenn Sie nicht sicher sind, ob Sie einen Intel-Prozessor oder einen Apple-Chip verwenden, finden Sie diese Daten in dem Unterpunkt Mac auf der Karte Info (Abschnitt 2.10 auf Seite 122) von TinkerTool System.

1. *Falls Sie einen Mac mit Intel-Prozessor verwenden:* Starten Sie den Computer neu (bzw. schalten Sie ihn ein) und halten Sie  +  gedrückt, um das Wiederherstellungssystem auszuwählen. Sie können die Tasten loslassen, sobald das Apple-Logo erscheint. *Falls Sie einen Mac mit Apple-Chip verwenden:* Stellen Sie sicher, dass Ihr Mac eine Verbindung zum Internet hat. Schalten Sie den Computer mithilfe der Einschalttaste ein und halten Sie diese Taste gedrückt, bis Startoptionen auf dem Bildschirm zu sehen sind. Wählen Sie den Punkt **Optionen**, der mit einem Zahnradsymbol markiert ist, und klicken Sie dann auf **Weiter**.
2. Abhängig von den Sicherheitsfunktionen, die auf Ihrem Mac aktiv sind, erscheint möglicherweise das Fenster **Wiederherstellungsassistent**. Falls dies der Fall ist, folgen Sie dessen Anweisungen, um sich als Administrator anzumelden.

3. Warten Sie, bis der Bildschirm **macOS Dienstprogramme** erscheint, und wählen Sie dann den Menüpunkt **Dienstprogramme > Terminal**, um das Terminal-Programm zu starten.
4. Geben Sie den folgenden Befehl in das Terminal ein, um den Systemintegritätsschutz für den gesamten Computer auszuschalten. Betätigen Sie danach die Eingabetaste:

```
csrutil disable
```

Wir empfehlen nicht, diese Funktion abzuschalten.

Die Änderung wird wirksam, wenn Sie das nächste Mal den Computer neu starten. Der Neustart kann mit dem diesbezüglichen Menüpunkt im Apfel-Menü eingeleitet werden. Um den Systemintegritätsschutz später wieder einzuschalten, können Sie die gleichen Schritte mit dem Befehl

```
csrutil clear
```

ausführen.

1.5 Datenschutz Einstellungen Ihres Mac

1.5.1 Hintergrundinformationen

Ab Version 10.14 des Betriebssystems hat Apple eine weitere Ebene des Systemschutzes hinzugefügt: Fast alle Programme laufen nun in einer *sandbox-geschützten* Umgebung, was bedeutet, dass jede Anfrage, die ein Programm an das Betriebssystem stellt, überwacht und geprüft wird, bevor diese zur Ausführung kommt. Nicht nur Apps aus dem Mac App Store, sondern auch alle anderen Programme, darunter auch einige von Apple selbst, sind nicht mehr frei darin, jeden beliebigen Befehl auszuführen, auch wenn er sonst gemäß Nutzerberechtigungen zulässig wäre. Der Zugriff auf Daten, die die Sicherheit des Systems oder den Datenschutz beeinflussen könnten, benötigt vorher eine ausdrückliche Genehmigung eines Systemverwalters des Macs. Diese Genehmigung wird pro Programm erteilt. Zum Beispiel kann ein Administrator sagen, „Programm A hat Zugriff auf die Fotos-Datenbanken der jeweiligen Benutzer“. Solch eine Datenschutzrichtlinie wird danach für den gesamten Computer und alle Benutzer wirksam, sowie für alle Exemplare des Programms A. Falls Programm A gerade läuft, während seine Datenschutzeinstellungen geändert werden, muss das Programm neu gestartet werden bevor die Änderung wirksam wird.

Die Einstellungen für Datenschutzrichtlinien sind ein leistungsfähiges Werkzeug, um zu verhindern, dass Programme hinter dem Rücken der Benutzer auf kritische Daten zugreifen, egal ob absichtlich oder unabsichtlich. Dies gilt besonders für ungewollte Programme wie Adware, Computerviren, Trojanische Pferde oder andere Typen von Malware. Dieser zusätzliche Schutz bedeutet gleichzeitig jedoch zusätzliche Arbeit für Systemverwalter. Nachdem neue Software installiert wurde, sollte überprüft werden, ob das jeweilige Programm Zugriff auf geschützte Teile des Macs benötigt, um seine Aufgaben erfüllen zu können. Falls eine notwendige Genehmigung nicht erteilt wurde, kann das Programm bestimmte Vorgänge nicht ausführen. Solche Vorgänge schlagen dann entweder stillschweigend fehl, oder sie werden mit einer Fehlermeldung angehalten. Die nötige Genehmigung muss dann von einem Administrator erteilt und das Programm neu gestartet werden.

1.5.2 Datenschutzeinstellungen, die TinkerTool System betreffen

Wie der Name schon andeutet, ist TinkerTool System ein Programm, das dazu ausgelegt ist, systembezogene Aufgaben durchzuführen. Einige Bereiche, auf die TinkerTool System zugreifen kann, sind für den Datenschutz der Benutzer kritisch, z.B. ist das Programm in der Lage, die Größe der Spotlight-Indexdatenbank zu bestimmen. Der Spotlight-Index enthält Informationen über alle Dateien aller Benutzer, und Teile dieser Daten können sich auf Personen beziehen oder vertraulich sein, so dass sie von macOS geschützt werden. Ohne vorherige Genehmigung kann TinkerTool System den Spotlight-Index oder seine Größe überhaupt nicht „sehen“.

TinkerTool System verwendet spezielle Vorsichtsmaßnahmen, um zu prüfen, ob ein bestimmter Vorgang von macOS aufgrund von Datenschutzeinstellungen blockiert werden *könnte*, bevor dieser Vorgang ausgeführt wird. Durch diese Vorgehensweise sollte ein „stillschweigendes Versagen“ vermieden werden. TinkerTool System wird also nicht fälschlicherweise so tun, als ob ein Vorgang scheinbar erfolgreich war, obwohl der Vorgang möglicherweise von macOS blockiert wurde und in Wirklichkeit überhaupt nicht stattgefunden hat. In solchen Fällen zeigt TinkerTool System spezifische Fehlermeldungen an, die Detailinformationen darüber enthalten, welche Genehmigung erteilt werden muss, bevor die betroffene Funktion genutzt werden kann.

Eine besondere Warnmarkierung mit einem roten Schild erscheint in der Titelleiste des Steuerungsfensters wenn TinkerTool System erkennt, dass grundlegende Funktionen des Programms aufgrund der aktuellen Datenschutzeinstellungen nicht wie erwartet arbeiten werden. Wenn Sie auf diese Markierung klicken, zeigt TinkerTool System im Detail, welche Bereiche betroffen sind:

- **Festplattenvollzugriff für deinen Benutzer-Account:** Das Programm kann während normaler Vorgänge, die keine besonderen Privilegien erfordern, nicht auf kritische Dateien zugreifen.
- **Festplattenvollzugriff während privilegierter Vorgänge:** Das Programm kann beim Ausführen privilegierter Vorgänge, die erfordern, dass Sie sich als Systemadministrator ausweisen, nicht auf kritische Dateien zugreifen.
- **Zugriff auf andere Volumes:** Das Programm kann auf Daten nicht zugreifen, die sich auf sekundären Volumes befinden, z.B. externe Festplatten oder Dateiserver im Netzwerk. Alle Volumes, die nicht das System-Volume sind (auf dem das Betriebssystem und Ihr lokaler Privatordner beherbergt sind), können betroffen sein.

Falls Sie die Knopf mit dem roten Schild in der Titelleiste sehen oder einige der Detailpunkte immer noch mit einer roten Warnmarkierung versehen sind, sollten Sie die Datenschutzeinstellungen von macOS so ändern, wie in der Anleitung im nächsten Abschnitt beschrieben. Sie können TinkerTool System zwar auch ohne diese Maßnahme betreiben, aber dann könnten einige Funktionen mit einer Fehlermeldung fehlschlagen.

1.5.3 Ändern der Datenschutzeinstellungen

Um alle Features von TinkerTool System nutzen zu können, müssen die folgenden Datenschutzeinstellungen erteilt werden:

- **Festplattenvollzugriff**
- **Automation** zwischen TinkerTool System und dem Finder, falls Sie die Funktion **Finder Kopieren testen** auf der Einstellungskarte Diagnose (Abschnitt 2.7 auf Seite 86) nutzen möchten.

macOS fragt automatisch nach Ihrer Genehmigung zur Automation sobald Sie die Funktion **Finder Kopieren testen** zum ersten Mal nutzen. Wenn Sie den Vollzugriff auf die Festplatte für TinkerTool System genehmigen möchten, führen Sie die folgenden Schritte durch:

1. Starten Sie **Systemeinstellungen**.
2. Öffnen Sie die Einstellungskarte **Datenschutz & Sicherheit**.
3. Wählen Sie den Punkt **Festplattenvollzugriff** aus.
4. Prüfen Sie, ob ein Eintrag für **TinkerTool System** in der Tabelle vorhanden ist. Falls ja, stellen Sie sicher, dass der Schalter bei diesem Eintrag eingeschaltet ist. Falls nein, drücken Sie den Knopf **+** unterhalb der Liste der Apps und fügen Sie TinkerTool System zur Tabelle hinzu.
5. Starten Sie TinkerTool System erneut.

1.6 TinkerTool in TinkerTool System 8 einbinden

1.6.1 Einbindung einschalten

TinkerTool System verwendet einige der Techniken, die auch im kostenlosen Schwesterprodukt TinkerTool zum Einsatz kommen. TinkerTool ist ein Programm, um ausgewählte persönliche Einstellungen abzurufen und zu ändern, und zwar solche, die Apple für fortgeschrittene „Profi“-Benutzer als Teil von macOS zur Verfügung stellt. TinkerTool und TinkerTool System überschneiden sich in keinem Punkt, so dass Verwalter, die Zugriff auf das komplette Funktionsangebot der beiden Programme haben möchten, auch beide Programme auf ihre Computer kopieren müssen.

Alle Funktionen von TinkerTool können auch von TinkerTool System aus aufgerufen werden, wenn Benutzer dies wünschen. In diesem Fall werden die Einstellungskarten von TinkerTool zu Plugins von TinkerTool System. Es ist hierbei immer noch notwendig, dass beide Programme auf dem Computer vorhanden sind. „Vorhanden“ heißt hierbei, dass TinkerTool System auf die Dateien von TinkerTool über einen bekannten Ordner zugreifen kann. Es ist nicht notwendig, beide Programme im gleichen Ordner zu halten. Sie können verschiedene Ordner, verschiedene Plattenlaufwerke oder sogar verschiedene Computer (bei gemeinsam verwendeten Netzwerkordnern) einsetzen.

Um die Einstellungskarten von TinkerTool in TinkerTool System einzubinden, führen Sie die folgenden Schritte durch:

1. Starten Sie TinkerTool System.
2. Wählen Sie den Menüpunkt **Darstellung > Karten von TinkerTool hinzufügen**
3. Navigieren Sie zum Exemplar von TinkerTool, das eingebunden werden soll. TinkerTool System sucht automatisch nach der neuesten Version, die auf Ihrem Computer vorhanden ist und bietet diese als Vorschlag an. Da es möglich ist, mehrere Exemplare gleichzeitig auf dem System zu haben, ist dies aber vielleicht nicht in allen Fällen die gewünschte Wahl. Drücken Sie den Knopf **Öffnen ...**, um die richtige Auswahl zu bestätigen.

Nach ein paar Sekunden werden alle Einstellungskarten von TinkerTool, die für Ihren Computer und Ihr Betriebssystem verwendbar sind, zusätzlich in der Rubrik **Benutzereinstellungen** erscheinen. Diese Einbindung verhält sich wie eine Benutzereinstellung und bleibt

bei jedem Start erhalten. Das heißt auch, dass jeder Benutzer für sich selbst entscheiden kann, ob die Verbindung zwischen den beiden Programmen genutzt werden soll oder nicht. Jedem Benutzer steht auch frei, verschiedene Versionen von TinkerTool einzubinden, falls nötig.

Aufgrund der Vielzahl unterschiedlicher Varianten von TinkerTool und TinkerTool System gibt es ein paar Einschränkungen bezüglich der Frage, welche Varianten miteinander kombiniert werden können. *TinkerTool System 8 Version 8.87* und höher kann Exemplare von *TinkerTool 9.6* oder höhere Versionen von TinkerTool 9 einbinden.

TinkerTool System unterstützt keinen Betrieb in gemischten Sprachen, aufgrund von internen Einschränkungen von macOS und um Verwirrung zu vermeiden. Falls Ihre primäre Sprache beispielsweise Französisch ist, läuft TinkerTool als selbständiges Programm mit einer französischen Bedieneroberfläche, aber nur auf deutsch oder englisch, wenn es in TinkerTool System integriert ist, da TinkerTool System nur diese beiden Sprachen unterstützt. Um Ihre persönliche Priorität von Sprachen einzustellen, öffnen Sie **Systemeinstellungen** und gehen Sie zu **Allgemein > Sprache & Region**. Sie können Sprachen zur Tabelle **Bevorzugte Sprachen** hinzufügen und diese je nach Wunsch in eine andere Reihenfolge bringen.

1.6.2 Einbindung abschalten

Die Verbindung beider Programme wird automatisch gelöst, wenn das angebundene Exemplar von TinkerTool nicht mehr länger in dem vom Benutzer ausgewählten Ordner vorzufinden werden kann. Aus Sicherheitsgründen verfolgt TinkerTool System nicht nach, ob das Programm vielleicht in einen anderen Ordner bewegt wurde. Um TinkerTool manuell aus der Bindung zu lösen, wählen Sie den Menüpunkt **Darstellung > TinkerTool-Karten entfernen**. Die Änderung wird sofort wirksam. Ein Neustart des Programms ist nicht erforderlich.

Kapitel 2

Systemwartung

2.1 Die Einstellungskarte Wartung

2.1.1 Verzeichnis-Cache

macOS enthält einen Hintergrunddienst, der mit den Verzeichnisdiensten kommuniziert, die für Ihr System eingerichtet sind. Dieser Dienst ist der zentrale Informationsbeschaffer, um Daten über Benutzer, Computer, IP-Adressen, Benutzergruppen und viele andere Dinge zu sammeln, die für das Betriebssystem relevant sind. Unter besonderen Umständen kann der interne Speicherinhalt dieses Dienstes unrichtige oder veraltete Daten enthalten, insbesondere falls Ihr System auf einen DNS-Server oder Verzeichnis-Server zugreift, der nicht zuverlässig arbeitet, oder falls sich die Netzkonfiguration abrupt geändert hat. Dies kann sich in unerwarteten Verzögerungen äußern (drehender Regenbogenmauszeiger), besonders wenn Netzfunktionen genutzt werden.

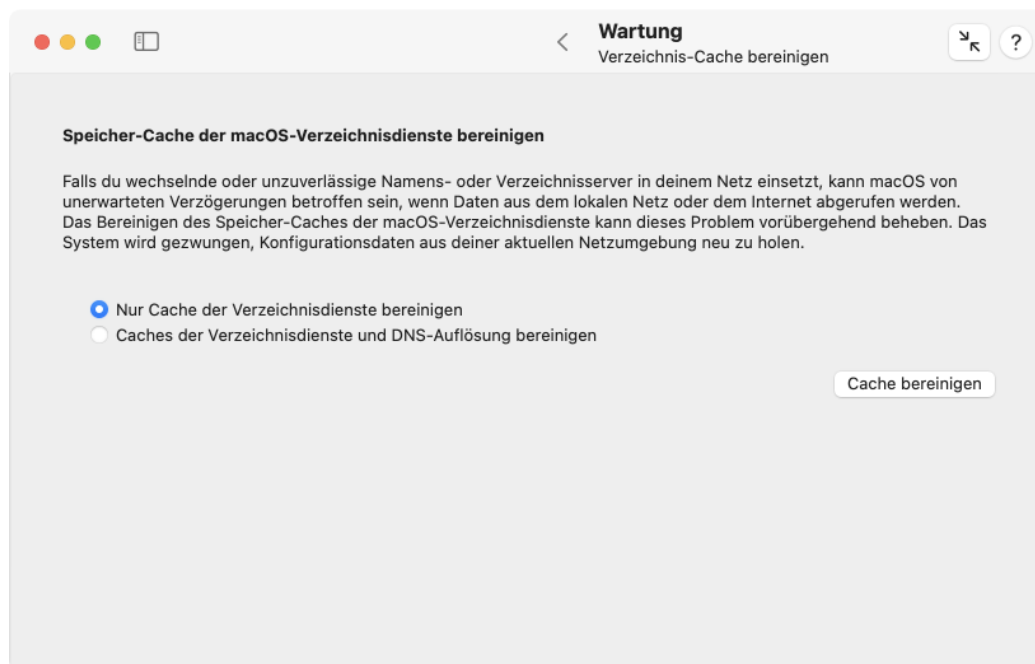


Abbildung 2.1: Verzeichnis-Cache bereinigen

In dieser Situation kann das Bereinigen des Online-Caches der Verzeichnisdienste das Problem möglicherweise beheben: Der Informationsbeschaffer wird wieder mit frischen Daten beginnen, die er aus Ihrem Netzwerk oder dem lokalen Computer ermittelt. Beachten Sie, dass dieser Cache nicht in irgendeiner Datei gespeichert ist. Er wird live im Hauptspeicher des Verzeichnisdienstesubsystems von macOS gehalten.

Das Wort „Verzeichnis“ wird manchmal als technischer Fachbegriff für einen Ordner verwandt, der Dateien enthält. Dies ist hier allerdings nicht gemeint. In diesem Kontext bezieht sich das Wort Verzeichnis auf eine Inventarliste von Namen, Objekten und Netzadressen, die für Ihren Computer relevant sind. macOS verwendet und betreibt immer einen Verzeichnisdienst, auch wenn der Computer nicht an ein Netzwerk angeschlossen ist.

Beim Ermitteln von Daten über Namen und Netzadressen anderer Computer stellen die Verzeichnisdienste nicht die einzige Quelle von Informationen dar, die für einige Zeit Einträge in einem internen Speicher-Cache vorhält. Der Systemdienst, der als „DNS-Auflöser“ arbeitet, also dafür zuständig ist, die Adressen zu Computernamen und umgekehrt zu bestimmen, unterstützt die Verzeichnisdienste bei ihrer Arbeit. Wenn Sie den Speicher-Cache bereinigen, können Sie entscheiden, ob nur die Einträge der Verzeichnisdienste als solche bereinigt werden sollen, oder ob ebenso zwischengespeicherte DNS-Daten entfernt werden sollen.

Um den Verzeichnis-Cache von macOS zu bereinigen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Verzeichnis-Cache bereinigen** auf der Einstellungskarte **Wartung**.
2. Betätigen Sie einen der Auswahlknöpfe, um anzugeben, ob der Cache der DNS-Auflösung in den Bereinigungsverfahren mit einbezogen werden soll.
3. Drücken Sie den Knopf **Cache bereinigen**.

2.1.2 Verzeichnisdaten exportieren

Wie bereits im letzten Abschnitt beschrieben, speichern die Verzeichnisdienste wichtige Daten über den lokalen Computer. Eine solche Datenbank wird *Verzeichnisknoten* genannt. In professionellen Netzwerken ist es üblich, dass nicht nur jeder Computer einen Verzeichnisknoten beherbergt, oft werden auch ein oder mehrere zentrale Datenbanken von speziellen Verzeichnisdienst-Servern gespeichert. Damit lassen sich beispielsweise netzwerkweite Benutzer-Accounts realisieren, so dass sich ein Benutzer an jedem beliebigen Computer des Netzwerks anmelden kann und einheitliche Berechtigungsdaten für alle Datenträger und File Server verwendet werden.

Muss an der Organisation der Verzeichnisdaten etwas verändert werden, z.B. weil ein neuer Computer oder ein anderes Betriebssystem zum Einsatz kommt, ist es hilfreich, bestimmte oder alle Verzeichnisdaten aus einem Verzeichnisknoten zu exportieren, um diese auf dem anderen System weiterzuverwenden. TinkerTool System unterstützt den Export, indem alle von Open Directory unterstützten Datentypen aller an einen Mac gebundenen Verzeichnisknoten ausgelesen und in eine Textdatei gespeichert werden können.

Apple hat im April 2022 bekanntgegeben, die Software *macOS Server* nicht mehr zu unterstützen. In dieser App war ein Dienst enthalten, netzwerkweite Verzeichnisdaten über einen *Apple Open Directory Server* bereitzustellen. Muss ein solcher Server

in Zukunft auf ein anderes Betriebssystem umziehen, kann TinkerTool System dabei helfen, dessen bisherige Daten zu retten, um diese ohne Änderung auch weiterhin nutzen zu können.

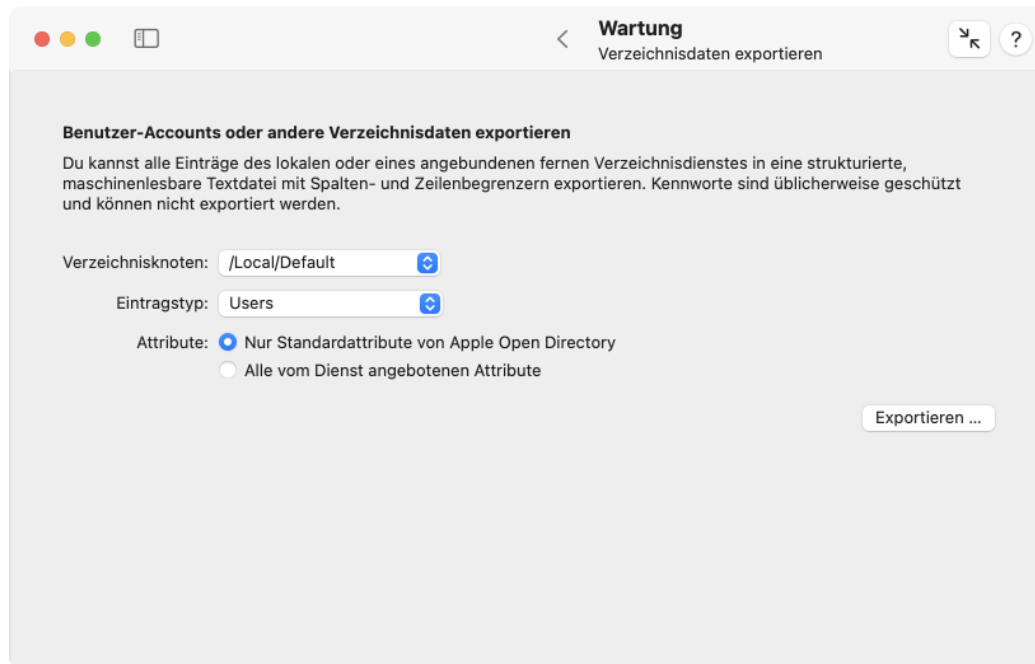


Abbildung 2.2: Exportieren von Verzeichnisknoten

Gehen Sie wie folgt vor, um Verzeichnisknoten in eine Textdatei zu exportieren:

1. Wählen Sie mit dem Menü **Verzeichnisknoten** den Dienst aus, von dem die Daten gelesen werden sollen. Die lokale Datenbank von macOS hat immer den Namen **/Local/Default**. Alle anderen mit macOS kompatiblen Verzeichnis-Datenquellen, mit denen dieser Mac im Moment verbunden ist, werden automatisch aufgelistet und lassen sich ebenso über ihren offiziellen Open Directory-Knotensuchpfad auswählen.
2. TinkerTool System ermittelt automatisch, welche Datentypen der Verzeichnisknoten bereitstellt. Wählen Sie die zu exportierende Datenart unter **Eintragstyp** aus.
3. Bestimmen Sie, ob nur die üblichen Attribute des gewählten Datentyps exportiert werden sollen, die durch den Open Directory-Standard vorgegeben sind, oder ob alle Attribute, die von Open Directory „verstanden“ werden, mit eingeschlossen werden sollen.
4. Drücken Sie auf **Exportieren ...** und wählen Sie Ort und Name für die Zielfeld aus.

Ist der Export erfolgreich, öffnet TinkerTool System nach dem Speichervorgang automatisch ein Kontrollfenster, in dem in einer Tabelle dargestellt wird, welche Daten abgespeichert wurden. Dieses Fenster dient nur der Endkontrolle. Die Überschriftenfelder jeder Spalte enthalten die offiziellen englischen Attributnamen gemäß Verzeichnisdienst. Sind Attribute exportiert worden, die keinen Text enthalten, werden diese mit der Markierung **Binäre Daten** angegeben und in diesem Fenster nicht weiter ausgewertet.

Der zweite Schritt, also der Import in ein anderes Betriebssystem muss in der Regel maßgeschneidert werden, so dass eine Software wie TinkerTool System hier nicht weiterhelfen kann. Die erzeugte Textdatei hat jedoch eine maschinenlesbare Tabellenstruktur, die sich mit üblichen Standardwerkzeugen zur Tabellen- oder Textverarbeitung weiterverarbeiten lässt. Erfahrene Systemadministratoren können die Daten in der Regel mit wenigen Schritten so anpassen, dass sie von einem fremden Betriebssystem gelesen werden können. Auf diese Weise lassen sich Open Directory-Daten zum Beispiel in einer Datenbank auf Basis von Microsoft Active Directory, Azure Active Directory oder einem Unix-Server mit LDAPv3-Datenbank nach RFC 2307 importieren. Zielsysteme mit macOS bieten je nach Version möglicherweise den Befehl `dsimport` an, um die Textdatei sofort weiterzuverarbeiten.

2.1.3 Locate-Datenbank

Da macOS ein UNIX-System ist, wird es mit dem Programm „locate“ geliefert, einem Kommandozeilenbefehl, der sehr schnell in der Lage ist, Dateien über deren Namen oder Namensteile zu finden. Locate ist bei der Suche nach Namen üblicherweise schneller als Spotlight und unterscheidet nicht zwischen sichtbaren und unsichtbaren Dateien. Ähnlich wie Spotlight benötigt locate eine interne Datenbank, um seine Aufgabe durchzuführen. Diese Datenbank wird in regelmäßigen Zeitabständen aktualisiert, um sicherzustellen, dass das Programm aktuelle Daten über neue und gelöschte Dateien zur Verfügung hat.

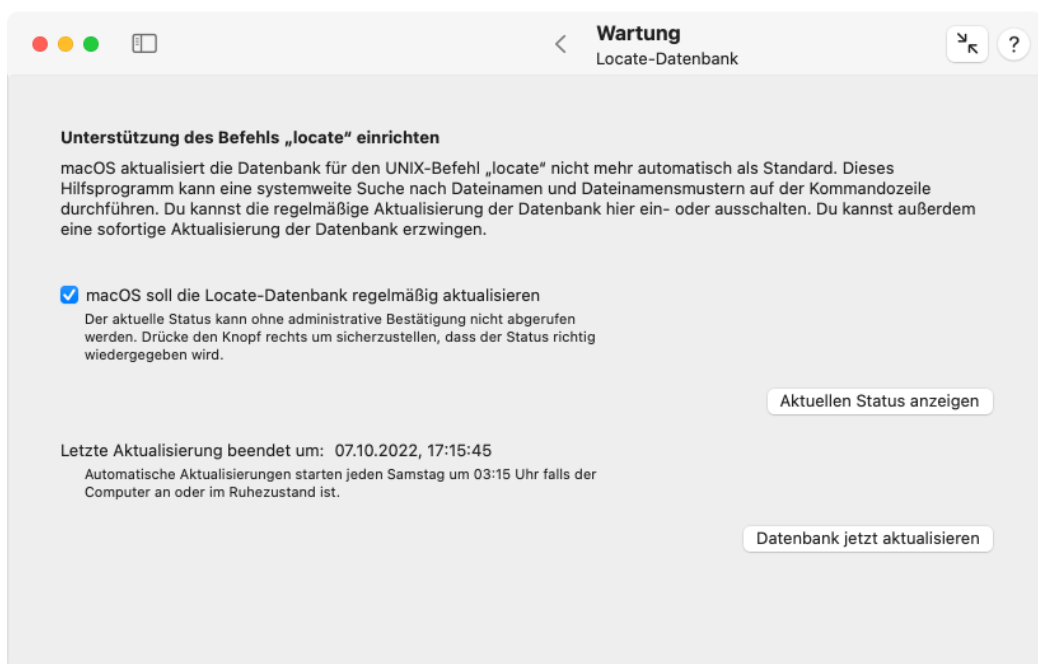


Abbildung 2.3: Locate-Datenbank

Da die meisten Anwender nicht mit der macOS-Befehlszeile arbeiten, ist der automatische Dienst, der die Locate-Datenbank aktualisiert, standardmäßig abgeschaltet. Die Information darüber, ob der Dienst zurzeit ein- oder ausgeschaltet ist, steht nur Benutzern mit Verwaltungsberechtigung zur Verfügung. Führen Sie die folgenden Schritte durch, um zu sehen, ob der Dienst aktiv ist oder nicht:

1. Öffnen Sie den Unterpunkt **Locate-Datenbank** auf der Einstellungskarte **Wartung**.
2. Drücken Sie den Knopf **Aktuellen Status anzeigen**.

Der aktuelle Zustand wird nun über das Häkchen **macOS soll die Locate-Datenbank regelmäßig aktualisieren** angezeigt. Sie können das Feld entweder ankreuzen, um die automatische Wartung der Datenbank einzuschalten, oder das Häkchen entfernen, um diesen Dienst abzuschalten.

In einer Standardinstallation von macOS aktualisiert das System die Locate-Datenbank automatisch jeden Samstag um 3:15 Uhr nachts. Falls Ihr Computer zu dieser Zeit ausgeschaltet oder im Ruhezustand ist, wird die Aktualisierung automatisch auf einen späteren Termin verschoben, an dem das System aktiv ist. Um eine sofortige Aktualisierung der Locate-Datenbank „jetzt“ zu erzwingen, drücken Sie den Knopf **Datenbank jetzt aktualisieren**.

2.1.4 Gemeinsamer Benutzerordner

macOS stellt auf dem System-Volume unter **Benutzer:innen > Geteilt (/Users/Shared)** einen besonderen Ordner dazu bereit, der dazu gedacht ist, dass mehrere Nutzer eines Mac lokale Dateien gemeinsam verwenden können. Alle Benutzer können Daten auf diese Weise miteinander teilen, indem der Ordner über spezielle Einstellungen so hergerichtet ist, dass Jeder Lese- und Schreibrecht hat. Gleichzeitig ist sichergestellt, dass nur der Ersteller und damit Eigentümer einer Datei diese auch wieder löschen kann, ohne dass das Risiko besteht, versehentlich die Daten anderer Benutzer zu entfernen.

Auch viele Programme von Apple und anderen Herstellern nutzen diesen Ordner automatisch, um Daten zu speichern, die für alle Benutzer interessant sein können. Dazu gehören auch Lizenz- oder Registrierungsdaten. Zum Beispiel nutzt Apples Programm Musik versteckte Inhalte in diesem Ordner, um die Nutzungsrechte für urheberrechtlich geschützte Medien zu verwalten.

Manche Benutzer löschen diesen wichtigen Systemordner, weil er anfänglich leer ist und auf den ersten Blick keinen Zweck zu erfüllen scheint. Dies kann jedoch zu Ausfällen und Fehlern in zahlreichen Programmen führen. Aufgrund der besonderen Einstellungen dieses Ordners ist es nicht einfach, ihn wieder korrekt neu anzulegen.

TinkerTool System prüft, ob dieser Ordner auf Ihrem Mac vorhanden ist. Falls nein, kann er auf Wunsch wieder in korrekter Form angelegt werden, um das Betriebssystem zu reparieren.

1. Öffnen Sie den Unterpunkt **Gemeinsamer Benutzerordner** auf der Einstellungskarte **Wartung**.
2. Drücken Sie den Knopf **Ordner wieder anlegen**.

2.2 Die Einstellungskarte Caches

Einführung in Cache-Techniken

Fast alle Programme, die mit macOS laufen, machen von Cache-Dateien Gebrauch. Diese Caches sind kleine Dateien, die vorausberechnete oder im Voraus geholte Daten speichern, die sehr oft benötigt werden. Durch „Erinnern“ und Wiederverwenden dieser bereits früher angefragten Ergebnisse können Programme spürbar beschleunigt werden. Sie greifen einfach auf die bereits bekannten Daten in ihren Cache-Dateien zurück und müssen so diese Daten nicht erneut berechnen oder erneut wiederbeschaffen. Beispiele für die Daten, die in solchen Cache-Dateien gespeichert sind, sind einige der letzten Internet-Seiten,

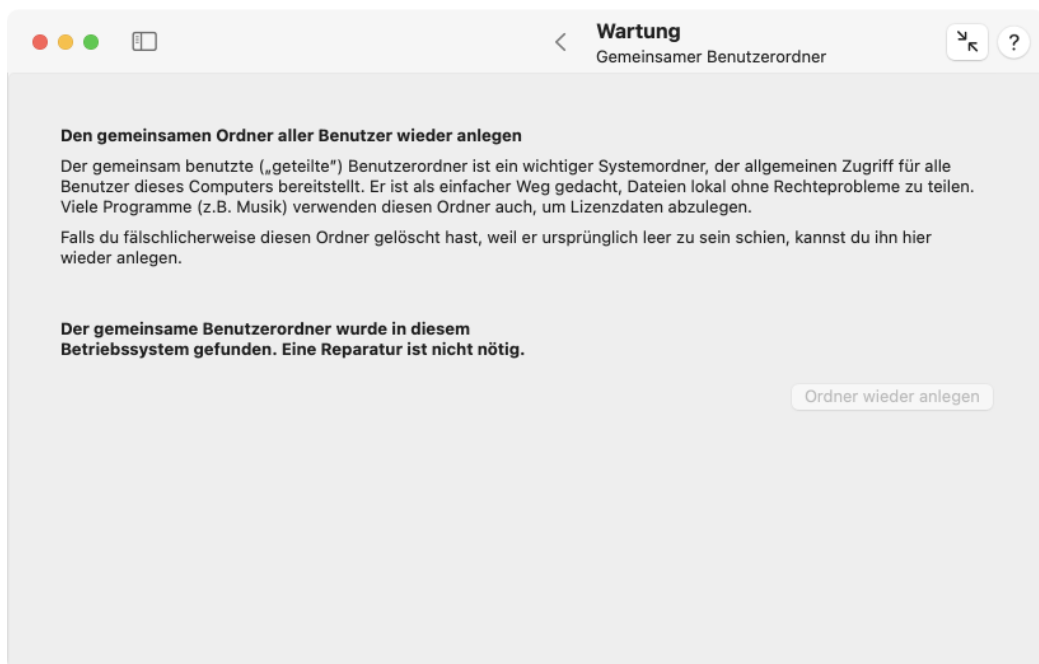


Abbildung 2.4: Gemeinsamer Benutzerordner

auf die ein Programm zugegriffen hat, die Fotos Ihrer Chat-Gesprächspartner, mit denen Sie sich üblicherweise unterhalten, oder die Daten, um schnell das Bild für den Hintergrund des Schreibtischs anzuzeigen, bereits dekomprimiert, vergrößert/verkleinert und optimiert auf den Bildschirm, den Sie einsetzen.

Vielen Programmen ist in Wirklichkeit nicht „bewusst“, dass sie Cache-Dateien verwenden, denn macOS erstellt die Caches in vielen Fällen automatisch, sobald die Programme Daten über das Betriebssystem abrufen, und zwar in den Fällen, in denen bereits im Voraus klar ist, dass die Cache-Technik ähnliche Anfragen in Zukunft beschleunigen wird. Beispielsweise kontaktiert jedes Programm, das eine „Suche-nach-Updates“-Funktion anbietet, einen bestimmten Web-Server, um Statusinformationen über das Internet abzurufen. Falls dies über die Standardsystemfunktionen geschieht, legt macOS automatisch einen persönlichen Web-Cache für dieses Programm an, so dass der Zugriff auf den Update-Server beschleunigt wird. Das Programm „weiß“ davon nichts, erhält aber von macOS die abgefragten Daten dank des Cache schneller als gewöhnlich geliefert.

Caches sind für sehr entscheidende Geschwindigkeitsgewinne verantwortlich, es können jedoch Probleme auftreten, wenn ein Cache aus irgendeinem Grund beschädigt wird. In dieser Situation enthält der Cache falsche, veraltete oder anderweitig unbenutzbare Daten, die sehr merkwürdige Effekte in allen Programmen auslösen können, die diesen Cache verwenden. Unter normalen Umständen sollten macOS oder die betroffenen Programme erkennen, dass etwas mit dem Cache nicht stimmt, so dass die zwischengespeicherte Information verworfen und der Cache neu wiederaufgebaut wird, sobald neue Daten angefordert werden. In der Praxis klappt diese Erkennung jedoch nicht immer, besonders wenn eine Netzverbindung unterbrochen wurde, wenn ein Programm unerwartet abgestürzt ist oder wenn Ihr Computer Probleme mit seiner Uhr hatte, so dass er nicht mehr nachverfolgen konnte, welche Daten aktuell und welche Daten veraltet sind.

Aufgrund der besonderen Natur von Caches im Verborgenen zu arbeiten, sind Probleme, die wegen beschädigter Cache-Inhalte auftreten, schwierig zu finden. Der Benutzer stellt

lediglich fest, dass „manchmal irgendetwas sehr falsch in manchen Programmen“ abläuft. Wenn Sie seltsame Probleme mit einem Programm feststellen, könnten diese das Ergebnis eines beschädigten Caches sein, aber sicher ist das nicht. Eine einfache, aber radikale Methode, dies genauer herauszufinden, besteht darin, alle Caches zu löschen, dann das betroffene Programm neu zu starten und zu prüfen, ob das Problem nun behoben ist. Falls ja, ist das in Ordnung, aber falls nein, haben Sie nun alle wertvollen Daten verloren, die in den Caches gespeichert waren. Es kann Stunden, Tage oder Wochen dauern, bis sich das System von dieser Situation erholt hat und die Caches mit neu berechneten, bzw. neu geholten Daten wieder aufgebaut sind. Während dieser Wiederaufbauphase wird der Computer spürbar langsamer arbeiten als normal.

Obwohl das Bereinigen von Caches ein wirkungsvoller Schritt bei der Fehlersuche sein kann, um bestimmte Probleme zu beheben, hat es, wie wir gesehen haben, schädliche Nebenwirkungen. Aus diesem Grund führt TinkerTool System einen viel intelligenteren Ansatz ein: Sie können Caches vorübergehend deaktivieren und diesen Schritt wieder zurücknehmen, falls Sie bemerken, dass die Entfernung der Caches keine positive Wirkung hatte. Diese neue Vorgehensweise vermeidet das Problem, dass das Bereinigen von Caches das ursprüngliche Problem noch viel schlimmer machen kann.

Einige Internet-Sites empfehlen, Cache-Bereinigung als regelmäßigen oder sogar mit festem Terminplan versehenen Wartungsschritt einzusetzen. Wie wir in diesem Abschnitt skizziert haben, ist dies einer der schlechtesten Ratschläge, die man geben kann. Cache-Bereinigung hat immer die negative Nebenwirkung, Ihren Computer danach langsamer als normal arbeiten zu lassen. Diese Maßnahme sollte nur als letzter Ausweg während der Fehlersuche bei einem wohldefinierten Problem verwendet werden, wenn man genau weiß, dass die positiven Effekte tatsächlich die negativen Wirkungen des Verlustes der Cache-Daten aufwiegen.

2.2.1 Ungeschützte und geschützte Caches

TinkerTool System bietet intelligente Deaktivierung für die folgende Cache-Kategorie an:

- Persönliche Standard-Caches des aktuellen Benutzers,

Drei andere Kategorien können nur bereinigt, statt deaktiviert werden, da die intelligente Deaktivierung durch die Funktion *Systemintegritätsschutz* (Abschnitt 1.3 auf Seite 8) von macOS verhindert wird:

- Persönliche Hochgeschwindigkeits-Caches,
- systemweite Caches, die benutzt werden, um computerbezogene Daten zu speichern, die für alle Benutzer relevant sind,
- interne Caches des Betriebssystems, die unabhängig von Benutzer und Computer sind.

In professionellen Umgebungen werden die privaten Ordner von Benutzern üblicherweise auf einem zentralen Dateiserver gespeichert, nicht auf den jeweiligen Festplatten der Computer vor Ort. Da Netzwerkzugriffe etwas oder sogar spürbar langsamer als Zugriffe auf eine lokale Platte sind, hält macOS alle Caches, bei denen schneller Zugriff wichtig ist, in einem getrennten Bereich auf der Systemplatte. TinkerTool System bezeichnet diese als *Hochgeschwindigkeits-Caches*. Sie werden zum Beispiel beim Browsen im Internet oder zum vorübergehenden Speichern von Vorschaubildern verwendet.

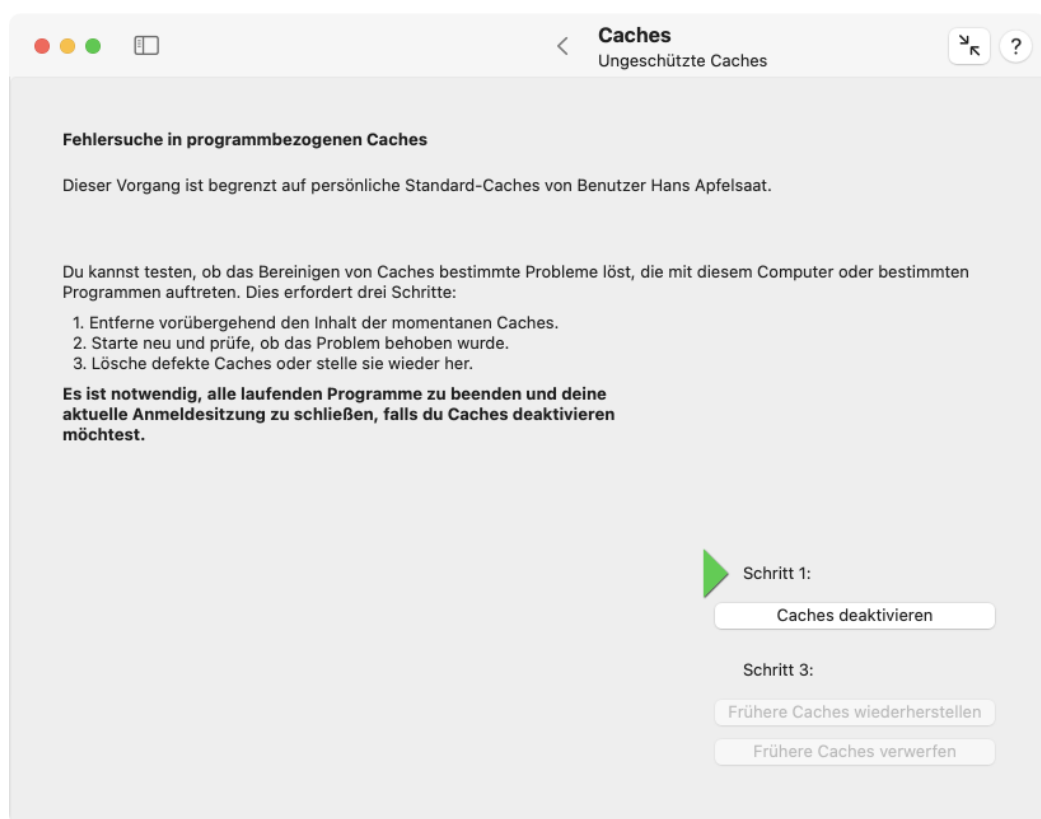


Abbildung 2.5: Ungeschützte Caches

2.2.2 Verwenden der Cache-Wartungsfunktionen

Intelligente Cache-Deaktivierung

Das intelligente Deaktivieren von Caches bei der Fehlersuche läuft anhand der folgenden Schritte ab:

1. Definieren Sie für sich selbst, welches genaue Problem – möglicherweise verursacht durch einen beschädigten Cache – Sie beheben möchten. Finden Sie ein Programm, mit dem Sie genau dieses Problem reproduzieren können und testen Sie, ob nur ein einziger Benutzer-Account oder alle Accounts dieses Computers von diesem Problem betroffen sind.
2. Starten Sie TinkerTool System und öffnen Sie den Punkt **Caches > Ungeschützte Caches**. Drücken Sie den Knopf **Caches deaktivieren**.
3. TinkerTool System wird Sie darum bitten, alle betroffenen Programme zu beenden. TinkerTool System kann dies auch automatisch für Sie erledigen. Danach wird eine Abmeldung durchgeführt.
4. Melden Sie sich wieder beim System an (mit dem gleichen Benutzer-Account, der in den vorherigen Schritten verwendet wurde). TinkerTool System startet automatisch und gibt Ihnen die Auswahl, entweder die Caches wiederherzustellen oder zu verwerfen. Lassen Sie das Programm weiter laufen.
5. Testen Sie, ob das Problem, das Sie im ersten Schritt definiert haben, wirklich durch das Abschalten der Caches behoben wurde. Falls ja, können Sie die schädlichen Auswirkungen des Verlustes von Cache-Daten akzeptieren. Drücken Sie in diesem Fall den Knopf **Frühere Caches verwerfen**. Falls nein (das Problem wurde nicht behoben und kann immer noch wie vorher reproduziert werden), drücken Sie den Knopf **Frühere Caches wiederherstellen**. Im letzteren Fall führt TinkerTool System nochmals eine Abmeldung durch und alle ausgewählten Caches werden auf ihren früheren Stand zurückgebracht. Es werden sich keine negativen Nebenwirkungen ergeben.

Zusätzliche Hinweise

TinkerTool System versucht, Sie automatisch durch den intelligenten Deaktivierungsprozess zu leiten. Eine kurze Zusammenfassung der Anweisungen und eine große grüne Pfeilmarkierung werden verwendet, um optisch darzustellen, in welchem Zustand sich der Computer gerade befindet. Zusätzliche Statusnachrichten und Hinweise werden Ihnen in Fettschrift in der unteren linken Ecke der Einstellungskarte gegeben.

Sie sollten es vermeiden, die Entscheidung, ob Sie die Caches entweder wiederherstellen oder verwerfen, für zu lange Zeit aufzuschieben. Bitte treffen Sie die Entscheidung so schnell wie möglich.

Caches bereinigen (Geschützte Caches)

Um eine Kategorie von Caches vollständig zu bereinigen, wobei alle deren Inhalte gelöscht werden, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Punkt **Geschützte Caches** auf der Karte **Caches**.
2. Wählen Sie die Cache-Sätze aus, die das Problem verursachen.

3. Drücken Sie den Knopf **Caches bereinigen**.

Es sei nochmals darauf hingewiesen, dass das Bereinigen von Caches grundsätzlich vermieden werden sollte. Es bewirkt, dass Ihr System für einige Zeit spürbar langsamer läuft. Verwenden Sie das Löschen von Caches nur als letzten Ausweg, wenn Sie mit Sicherheit wissen, dass der Inhalt einer bestimmten Cache-Kategorie ein technisches Problem verursacht.

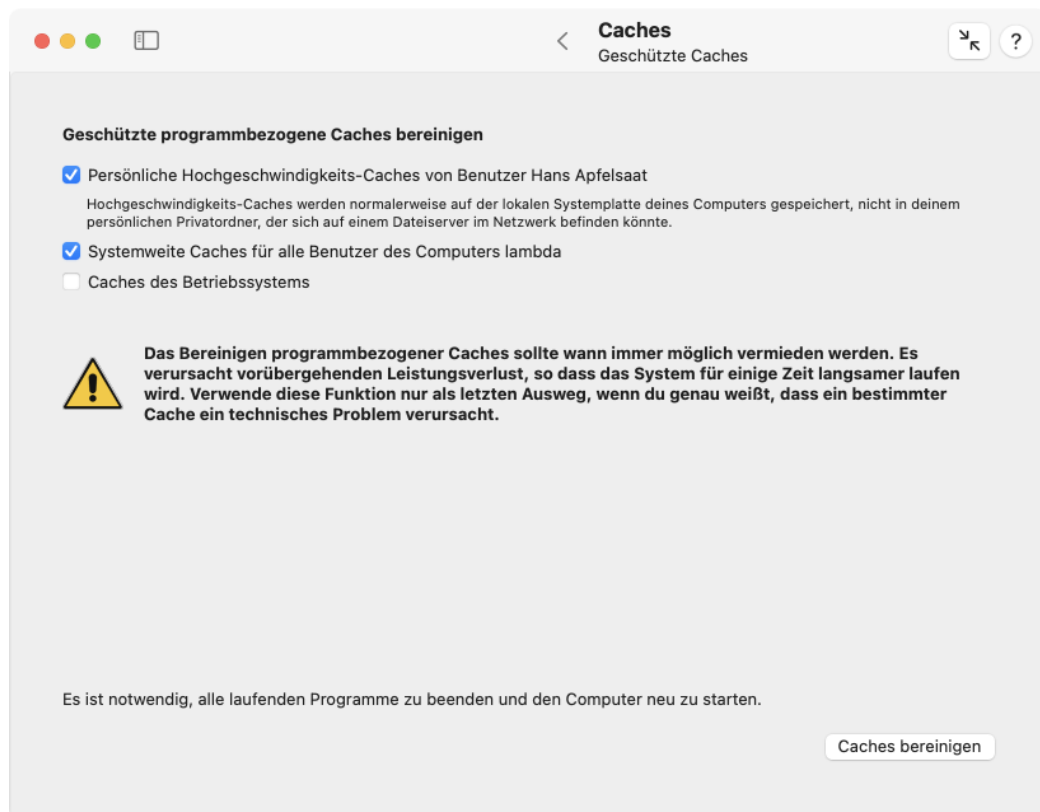


Abbildung 2.6: Bereinigen geschützter Caches

2.2.3 Schrift-Caches

macOS verwendet einen spezialisierten Hintergrunddienst für das Schriftenmanagement, den *Schriftregistrierungsserver*. Dieses Hintergrundprogramm ist dafür verantwortlich, herauszufinden, welche Schriften auf Ihrem System verfügbar sind, es verfolgt nach, welcher Benutzer welche Schriften aktiviert hat, welche der mehr als 200.000 Schriftzeichen, die von macOS unterstützt werden, in welchen Schriften verfügbar sind, es verwaltet die automatische Aktivierung von Schriften und führt viele weitere schriftbezogene Aufgaben durch.

Ihr Computer enthält möglicherweise Dutzende von Benutzer-Accounts, mehrere hundert Schriften und Millionen von unterschiedlichen Zeichen. Um dies alles zusammenzubringen, müssen raffinierte Datenbanken von Glyphen, Zeichen, Schriften und individuellen

Benutzereinstellungen geführt werden. Diese Hintergrunddatenbank wird aus den sogenannten *Schrift-Caches* gebildet. Das Betriebssystem als Ganzes und jeder Benutzer hat jeweils eigene Schrift-Caches.

Falls im Schriftregistrierungsserver ein technisches Problem auftritt, können die Schrift-Caches beschädigt werden. Dies kann bei der Arbeit mit Schriften seltsame Probleme auslösen, z.B. Verzögerungen bei der Anmeldung, unerwartete Fehler im Programm Schriftsammlung, die spontane Aktivierung von Schriften, die eigentlich inaktiv geschaltet waren, oder – im schlimmsten Fall – ein komplettes Versagen, die richtigen Zeichen für gewisse Schriften anzuzeigen, was sich, einfach ausgedrückt, als „durcheinandergewürfelter Text“ äußert.

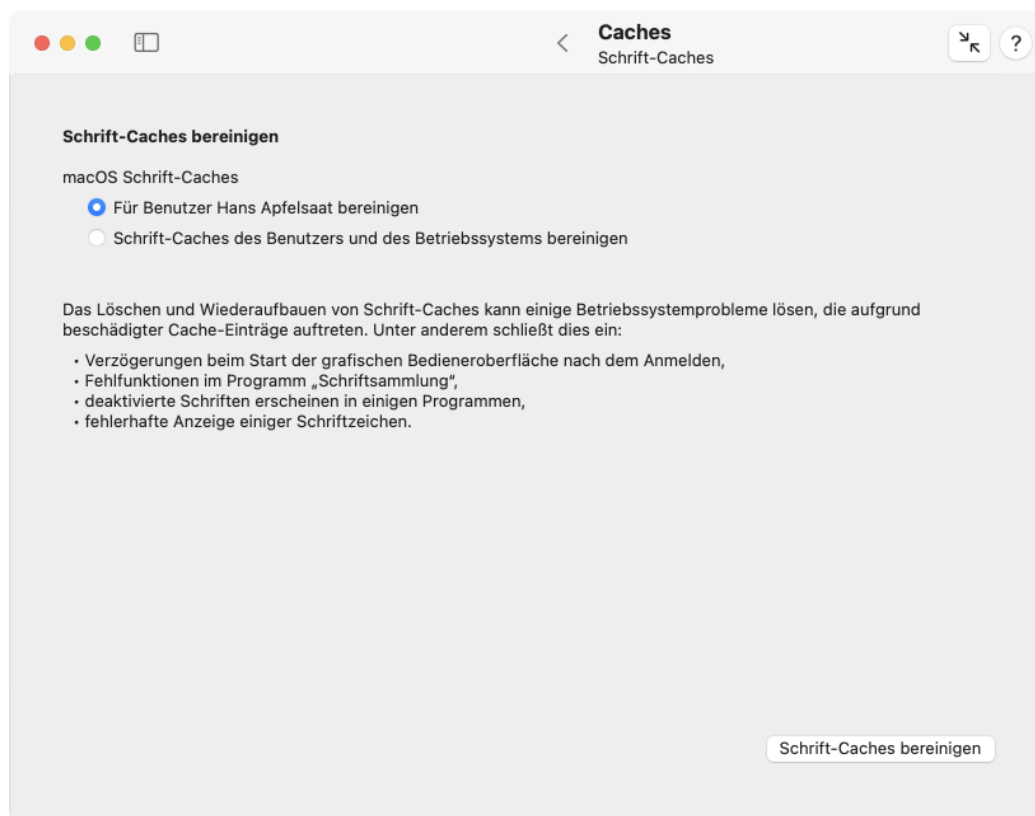


Abbildung 2.7: Schrift-Caches

Falls Sie von einem solchen Problem betroffen sind, kann TinkerTool System Sie beim Bereinigen von Schrift-Caches unterstützen. Der Bereinigungsverfahren kann entweder für den aktuellen Benutzer-Account oder für diesen Account und das ganze restliche System erfolgen.

Beim Bereinigen der Caches des Schriftregistrierungsservers ist ein Abmelden notwendig. macOS baut die Schrift-Caches bei der nächsten Anmeldung automatisch wieder neu auf. Dieser Vorgang sollte innerhalb weniger Sekunden oder Minuten abgeschlossen sein. TinkerTool System führt Sie durch alle notwendigen Schritte.

Führen Sie die folgenden Schritte durch, um Schrift-Caches zu bereinigen:

1. Öffnen Sie den Unterpunkt **Caches** > **Schrift-Caches**.
2. Wählen Sie die macOS-Schrift-Caches aus, die bereinigt werden sollen.

3. Drücken Sie den Knopf **Schrift-Caches bereinigen**.
4. Folgen Sie den Anweisungen des Programms.

2.2.4 Symbol-Caches

Das Dock, der Finder und andere Bestandteile des Betriebssystems verwenden Symbole (*Icons*), um sich auf die Programme zu beziehen, die auf Ihrem Mac gespeichert sind. Um schnell das richtige Bild für jedes Programm finden zu können, sammelt das Betriebssystem Informationen über die Symbole in zentralen Datenbanken, den *Symbol-Caches*. Unter bestimmten Umständen können diese Datenbanken allerdings beschädigt werden. In solch einem Fall werden die Programmsymbole nicht mehr länger korrekt angezeigt, oder einige von ihnen werden durch das allgemeine Programmsymbol ersetzt, ein graues, abgerundetes Quadrat mit Konstruktionslinien.

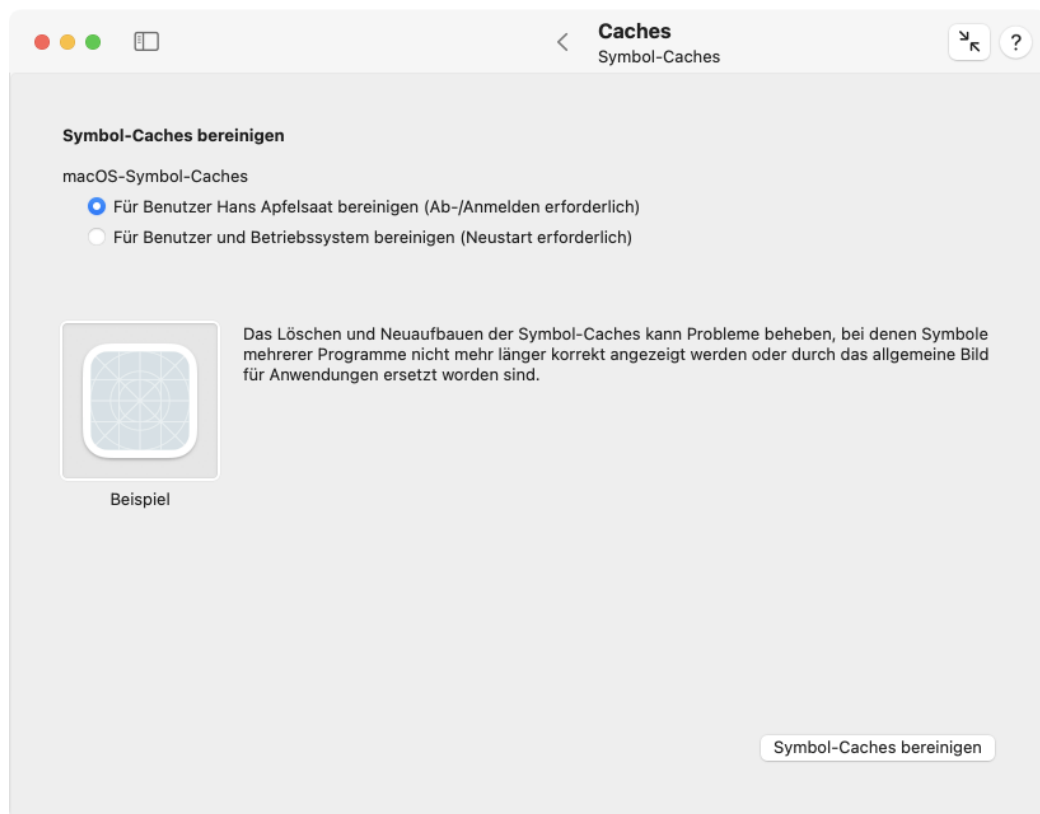


Abbildung 2.8: Symbol-Caches

Falls Sie von solch einem Problem betroffen sind, können Sie TinkerTool System die verschiedenen Symbol-Caches Ihres Benutzer-Accounts löschen lassen, was das Betriebssystem veranlasst, die notwendigen Informationen neu zu sammeln und die Datenbanken neu aufzubauen. Falls alle Benutzer-Accounts Ihres Computers von einem Ausfall der Programmsymbole betroffen sind, können Sie zusätzlich den Symbol-Cache des Betriebssystems löschen. Sie müssen sich abmelden, um diesen Vorgang abzuschließen. Falls die Symbol-Caches des Betriebssystems bereinigt wurden, muss stattdessen der Computer neu gestartet werden.

Führen Sie die folgenden Schritte durch, um Symbol-Caches zu bereinigen:

1. Öffnen Sie den Unterpunkt **Caches > Symbol-Caches**.
2. Wählen Sie die Caches aus, die bereinigt werden sollen.
3. Drücken Sie den Knopf **Symbol-Caches bereinigen**.
4. Folgen Sie den Anweisungen des Programms.

2.2.5 Die Staging-Ablage von Treibern

Moderne Versionen von macOS erlauben es nicht mehr, dass jeder Anbieter Kernel-Erweiterungen als Teil seiner Programme installieren darf, auch wenn diese Programme Installationspakete verwenden, die ein Administrator aufgerufen hat. Die Software-Entwickler benötigen eine ausdrückliche Erlaubnis von Apple, solche Erweiterungen herstellen zu dürfen, was von macOS über digitale Unterschriften überprüft wird. Zusätzlich muss die Installation dieser Treiber ausdrücklich in einem getrennten Schritt genehmigt werden, wofür normalerweise unsichtbare Bedienelemente unter **Systemeinstellungen > Datenschutz & Sicherheit > Andere** zum Einsatz kommen.

Um alle Kernel-Erweiterungen, die von Drittanbieterprogrammen bereitgestellt werden, unter Quarantäne zu stellen, bevor der Benutzer deren Nutzung entweder genehmigt oder verweigert, werden die diesbezüglichen Dateien in der sogenannten *Staging-Ablage* gesammelt, wozu ein oder mehrere besondere Systemordner verwendet werden. Diese Ordner stehen unter dem *Systemintegritätsschutz* und können von niemandem verändert werden, egal welche Rechte benutzt werden. Das heißt, falls ein Benutzer die Aktivierung eines bestimmten Drittanbietertreibers abgelehnt hat, werden die Dateien dieses Treibers in der Staging-Ablage quasi für immer liegen bleiben, da sie nicht gelöscht werden können. Die Ordner, die für das Staging zum Einsatz kommen, sind üblicherweise

- /Library/StagedDriverExtensions und
- /Library/StagedExtensions,

aber Apple kann dies jederzeit ohne Ankündigung ändern.

TinkerTool System kann in diesem Fall helfen, indem es dem Betriebssystem meldet, es soll seine Staging-Ablage für Kernel-Erweiterungen bereinigen. Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Caches > Treiber-Staging**.
2. Verwenden Sie die Umschaltknöpfe, um entweder *alle* im Staging befindlichen Objekte zu löschen (**Alle Objekte bereinigen**), oder das Löschen auf diejenigen Fälle zu beschränken, wo die zugehörigen Programme nicht mehr länger an ihren ursprünglichen Installationsorten vorgefunden werden können. (Dies stellt sicher, dass Treiber, die gerade auf Genehmigung oder Ablehnung während eines laufenden Installationsvorgangs warten, nicht versehentlich gelöscht werden können.)
3. Betätigen Sie den Knopf **Staging-Bereich bereinigen**.

Es gibt spezielle Treiber, die von Drittanbietern entwickelt wurden, aber von Apple offiziell als Teil von macOS mitgeliefert werden. Auch diese Kernel-Erweiterungen werden ge-staged und entfernt, wenn Sie mit der Option **Alle Objekte bereinigen** arbeiten. macOS stellt jedoch die betroffenen Dateien eventuell später automatisch wieder her.

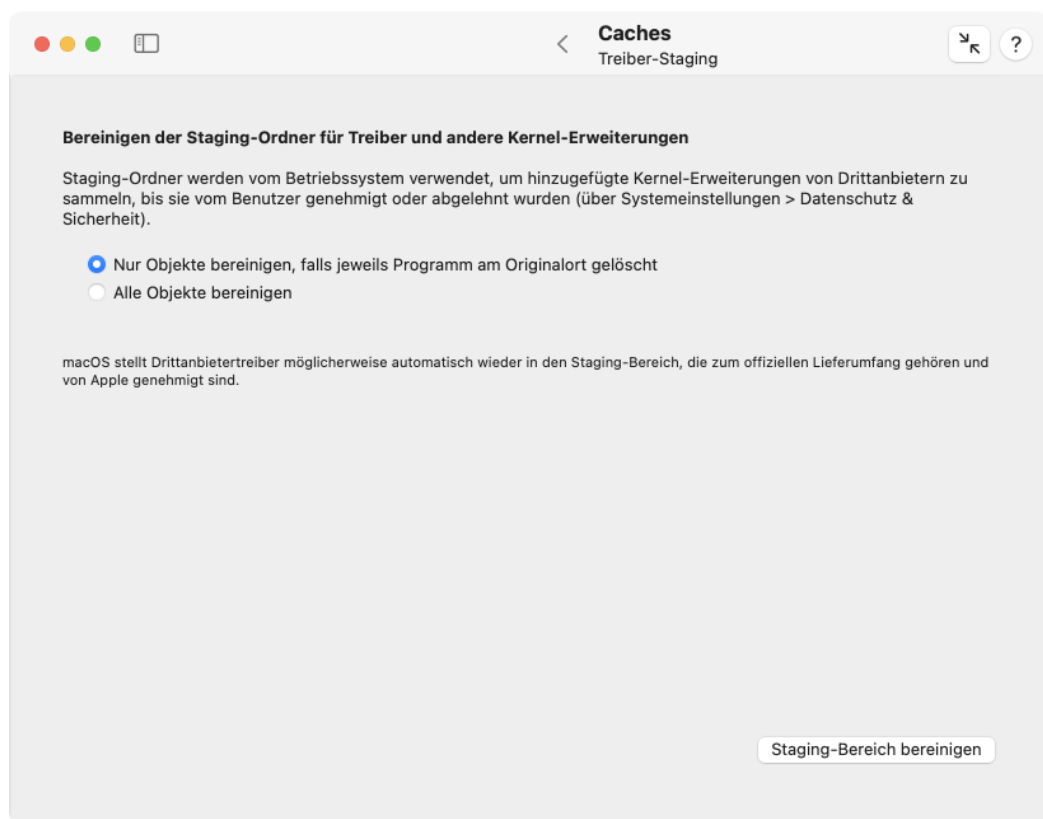


Abbildung 2.9: Treiber-Staging

2.3 Die Einstellungskarten für Time Machine

2.3.1 Time Machine-Grundlagen

Time Machine ist der Name von Apples Technologie zur automatischen Erstellung von Datensicherungen der Festplatten Ihres Computers. Die Sicherungen werden üblicherweise stündlich im Hintergrund angelegt und veraltete Dateisätze werden automatisch entfernt, wobei stündliche Sicherungen für den letzten Tag, tägliche Sicherungen für den letzten Monat und monatliche Sicherungen solange beibehalten werden, bis das Zielgerät voll ist. Jeder Sicherungssatz enthält eine fast vollständige Momentaufnahme des Inhalts aller Platten, für die Time Machine aktiviert ist. „Fast“ heißt dabei, dass Time Machine automatisch Dateien weglässt, die als unwichtig gelten oder die wiederhergestellt werden können, wie Protokolldateien, der Papierkorb, Caches, der Spotlight-Suchindex, etc. Dies schließt auch das Betriebssystem selbst mit ein, das sich auf einem nicht beschreibbaren Volume befindet. Obwohl Ihre Dateien für jeden Zeitpunkt vollständig wiederhergestellt werden können, für den eine Datensicherung verfügbar ist, speichert Time Machine rein technisch nur die Unterschiede zwischen zwei aufeinanderfolgenden Sicherungsvorgängen ab (*inkrementelle Sicherung*). Unterschiede werden auf Datei-Ebene ermittelt, d.h. wenn sich ein einziges Byte in einer Datei X geändert hat, wird die gesamte Datei X im nächsten Lauf der Time Machine-Sicherung kopiert.

2.3.2 Allgemeine Hinweise zum Arbeiten mit der Time Machine-Karte

Time Machine kann dazu eingerichtet werden, mit mehreren Zielmedien gleichzeitig zu arbeiten. Das Ziel kann außerdem so definiert werden, dass nicht auf ein Plattenlaufwerk, sondern auf einen Server im Netz gesichert wird, z.B. eine Time Capsule, einen Mac, auf dem Time Machine-Dateifreigabe läuft (verfügbar in alten Versionen von macOS Server oder in Standardversionen von macOS ab 10.13) oder ein NAS mit Time Machine-Unterstützung. TinkerTool System erkennt Ihre derzeitige Konfiguration automatisch und arbeitet immer mit demjenigen Time Machine-Ziel, das von macOS als „aktiv“ angesehen wird.

Name und Typ des Ziels werden in der oberen Box der Time Machine-Karte angezeigt. Bei plattenbasierten Sicherungen wird der Name des Volumes bei **Ziel** angegeben. Netzwerkbasierende Backups werden über eine Überschrift mit dem Hinweis **Netzwerkbetrieb** gekennzeichnet. Der obere Kasten zeigt außerdem, ob automatische Sicherungen gerade eingeschaltet sind, und ob eine erfolgreiche Wartungsverbindung zwischen TinkerTool System und Time Machine aufgebaut werden konnte. Wenn dabei ein Fehler aufgetreten ist, z.B. falls die aktuellen Datenschutzeinstellungen des Computers nicht erlauben, dass Sie auf Time Machine-Platten zugreifen, wird dies in der oberen Box vermerkt.

Falls Sie die moderne APFS-Version von Time Machine verwenden (siehe nächster Abschnitt), wird in der Zeile **Ziel** zusätzlich angegeben, ob die Sicherung verschlüsselt ist. Außerdem erhalten Sie in der Zeile **Automatische Sicherung** einen Hinweis, auf welchen Zeitabstand die Sicherung im Moment eingestellt ist.

2.3.3 Die unterschiedlichen Versionen von Time Machine für macOS 10 und spätere Versionen von macOS

Ab macOS 11 wurde die Technik von Time Machine stark erweitert und verändert: Während in früheren Versionen des Betriebssystems Datensicherungen nur auf Zielmedien erlaubt waren, die mit dem Dateisystem *Mac OS Extended (HFS+)* formatiert waren, sind hier Sicherungen auf das *Apple File System (APFS)* der Standard. Wird Time Machine frisch auf einer Sicherungsplatte eingerichtet, wird standardmäßig APFS verwendet und es läuft im

„modernen“ Betrieb. Bei Übernahme alter Datensicherungen, die ursprünglich mit macOS 10, OS X oder Mac OS X angelegt wurden, kommt weiterhin HFS+ zum Einsatz. Der Funktionsumfang der beiden Varianten von Time Machine im macOS 10- und modernen Betrieb ist sehr unterschiedlich. Aus diesem Grund verwendet TinkerTool System verschiedene Einstellungskarten um Time Machine zu steuern, je nach dem, welche Variante vorgefunden wurde. Im Modus macOS 10 wird die jeweilige Einstellungskarte als **Time Machine X** gekennzeichnet.

Dieses Handbuch enthält zwei unterschiedliche Kapitel für die Verwendung der beiden Karten Time Machine X (Abschnitt 2.4 auf Seite 40) und Time Machine (Abschnitt 2.5 auf Seite 55).

TinkerTool System schaltet die Time Machine-Betriebsart nicht hin und her, während es läuft. Wenn Sie die Zielplatte von HFS+ zu APFS austauschen, während TinkerTool System gerade geöffnet ist, wird das Programm dies bemerken, wenn Sie einen Wartungsvorgang vorbereiten und eine entsprechende Fehlermeldung in diesem Fall anzeigen. Um diese Situation aufzulösen, reicht es einfach, das Programm zu beenden und wieder neu zu starten.

2.4 Die Einstellungskarte Time Machine X

Dieses Kapitel bezieht sich auf die Karte **Time Machine X** und beschreibt den Betrieb im Kompatibilitätsmodus für macOS 10, d.h. wenn Sie auf ein Medium sichern, das im Format HFS+ unter macOS 10 erstellt wurde. Wenn Sie die aktuelle Variante von Time Machine (Sicherung auf APFS) verwenden, lesen Sie bitte im nächsten Kapitel (Abschnitt 2.5 auf Seite 55) weiter.

2.4.1 Wartung nach dem Austausch einer Datenquelle von Time Machine (macOS 10-Betrieb)

Das inkrementelle Vorgehen bei der Datensicherung, das in der Einleitung erwähnt wurde, funktioniert nur dann, wenn Time Machine absolut sicher sein kann, welche Dateien sich zwischen zwei aufeinanderfolgenden Läufen geändert haben und welche nicht. Wenn es den kleinsten Zweifel daran gibt, dass eine Datei nicht mehr länger identisch mit dem Exemplar ist, das Time Machine beim vorhergehenden Lauf gesehen hat, muss die Datei im nächsten Lauf vollständig neu gesichert werden.

Wenn sich die Identität des Computers ändert, z.B. weil Sie einen neuen gekauft haben oder er bei einer Reparatur ausgetauscht werden musste, muss Time Machine annehmen, dass sich *alle* Dateien des Computers verändert haben, auch dann, wenn Sie ein fremdes Kopier- oder „Klon“-Programm eingesetzt haben, um alle Dateien des alten auf den neuen Computer zu kopieren. Dies hat zur Folge, dass beim nächsten Time Machine-Lauf alle Dateien noch einmal kopiert werden müssen, obwohl Sie selbst dafür gesorgt hatten, dass die Dateien die gleichen sind wie vorher. Nur wenn *Time Machine selbst* zum Einsatz gekommen ist, um eine vollständige Wiederherstellung des Computers aus der Datensicherung durchzuführen, „weiß“ Time Machine, dass es die vorige inkrementelle Sicherung problemlos verwenden kann.

Genau das gleiche Problem tritt auf, wenn Sie ein Volume Ihres Mac ersetzen, aber nicht Time Machine, sondern ein fremdes Programm dazu genutzt haben, die Daten zurückzuspielen. Ersetzen eines Volumes kann bedeuten

- Sie haben ein Plattenlaufwerk physisch ausgetauscht,

- Sie haben eine Partition gelöscht oder neu formatiert,
- Sie haben ein Volume über ein Programm eines Drittanbieters geklont, aber das originale und das kopierte Volume waren vorübergehend gleichzeitig an den Computer angeschlossen, so dass das System gezwungen war, die Identität eines Volumes zu ändern, um nachverfolgen zu können, welches welches ist.

Nur dann, falls Sie ein Plattenlaufwerk oder eine Partition physisch kopiert haben (durch das Kopieren der rohen Datenblöcke, nicht Datei für Datei) und falls Sie sichergestellt haben, dass das Betriebssystem, auf dem Time Machine aktiv ist, nicht beide Volumes zur gleichen Zeit aktiviert hatte, kann Time Machine sein inkrementelles Vorgehen nahtlos fortsetzen. In allen anderen Fällen muss es annehmen, dass sich alle Dateien auf dem ganzen betroffenen Volume geändert haben, so dass diese noch einmal komplett kopiert werden müssen.

TinkerTool System kann in diesem Fall helfen, indem es Sie von Hand bestätigen lässt, dass ein Computer oder ein Volume immer noch als gleich anzusehen sind, obwohl sich deren Identität geändert hat. Auf diese Weise kann das neue Objekt die Rolle des ersetzten Objekts übernehmen, und dessen Historie in Time Machine kann fortgeführt werden, ohne dass eine komplett neue Datensicherung nötig ist.

Beachten Sie, dass in Fällen Voraussetzung ist, dass das Betriebssystem mit allen seinen Benutzer-Accounts identisch geblieben ist. Sie können diese Wartungsfunktionen zum Beispiel nicht nutzen, wenn Sie einen neuen Mac (mit einer anderen Installation von macOS) haben und Daten aus der Time Machine-Sicherung eines alten Mac übernehmen möchten. Auch wenn Systemversionen und Namen der Benutzer gleich sind, ist eine Übernahme einer Time Machine-Sicherung in diesem Fall nicht möglich, da in der Sicherung Zugriffsrechte für Benutzer-Accounts einer anderen Systeminstallation gespeichert sind. Sie können das Problem lösen, indem Sie die Accounts und Time Machine-Daten gleichzeitig über Apples Migrationsassistent kopieren.

Erben einer Time Machine-Datensicherung eines ersetzten Computers (macOS 10-Betrieb)

Wenn Sie bestätigen müssen, dass Time Machine einen Sicherungssatz, der von einem anderen physischen Computer oder einer anderen Betriebssysteminstallation auf dem gleichen Computer erstellt worden ist, sicher übernehmen darf, können Sie den Sicherungssatz Ihrem aktuellen System neu zuweisen. Sie sollten dies nur dann tun, wenn die skizzierte Situation genau zutrifft und Sie die Dateien tatsächlich auf eine andere Weise (also nicht unter Kontrolle von Time Machine) auf die neue Systeminstallation kopiert haben. Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Wartung** auf der Karte **Time Machine X**.
2. Betätigen Sie den Knopf **Fremde Sicherung diesem Mac zuweisen**

TinkerTool System führt Sie dabei durch allen notwendigen Schritte. Sie müssen den Ort des fremden Datensicherungssatzes angeben, um den Vorgang abschließen zu können. Im Falle einer lokalen Time Machine-Platte handelt es sich dabei um den obersten Ordner dieser Datensicherung. Bei Verwendung von HFS+ trägt er den Namen des vorigen Computers und befindet sich im Ordner *Backups.backupdb* auf der Zielplatte. Bei Verwendung von APFS ist als Ordner das Sicherungs-Volume selbst anzugeben.

Abhängig davon wie Time Machine konfiguriert war, bevor die fremde Datensicherung zugewiesen wurde, müssen Sie möglicherweise Time Machine im Abschnitt **Allgemein** >

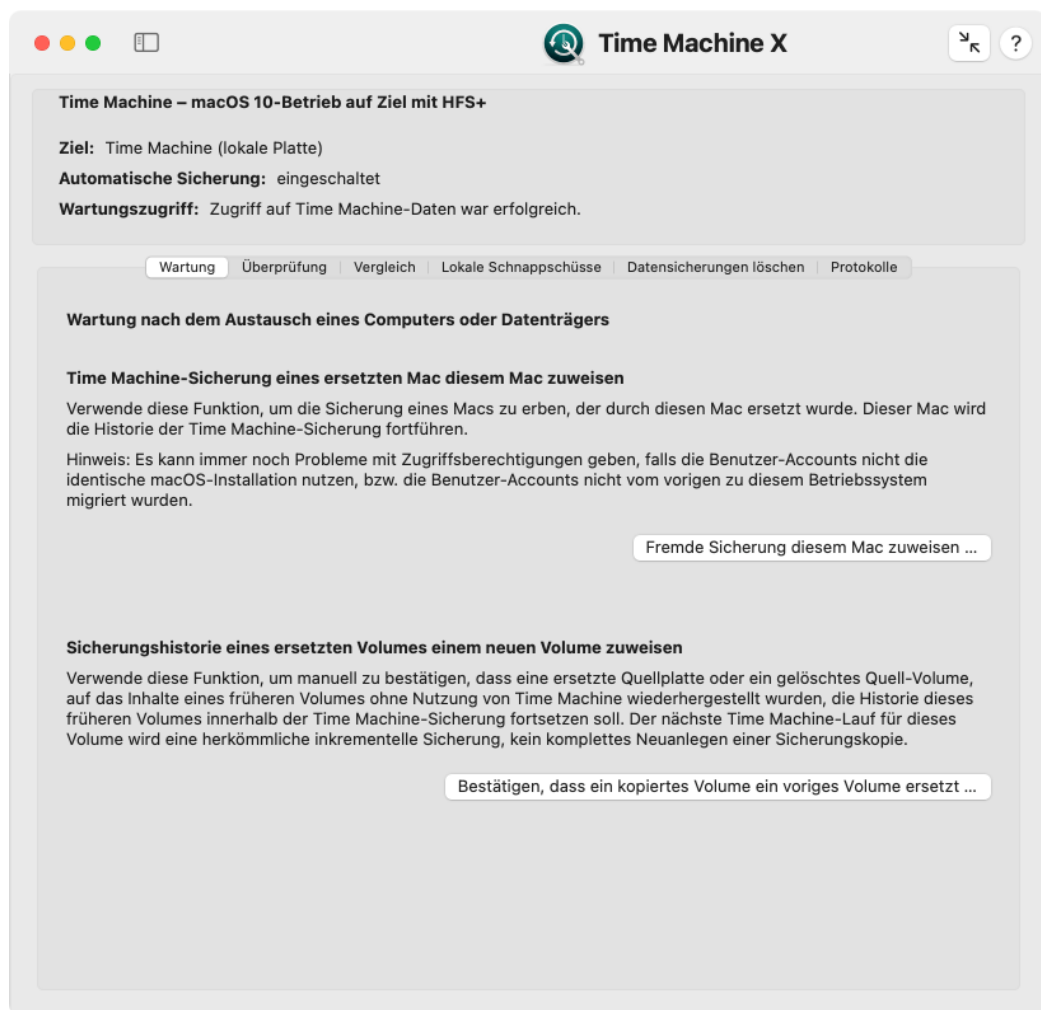


Abbildung 2.10: Wartung nach Austausch einer Time Machine-Datenquelle

Time Machine der **Systemeinstellungen** wieder einschalten und das Ziel für die Datensicherung neu einstellen.

Falls die lokalen Volumes des aktuellen Computers sich von denen des früheren Computers unterscheiden, *reicht die Neuuzuweisung der Datensicherung alleine nicht aus*. Sie müssen auch jedes Volume neu zuordnen, was im nächsten Abschnitt behandelt wird.

Neuzuweisung eines ersetzten Volumes mit einem Volume aus der Datensicherung (macOS 10-Betrieb)

Wie in der Einleitung beschrieben, kann es ebenso Fälle geben, in denen Sie Time Machine bestätigen müssen, dass es die Historie eines Volumes in der Datensicherung ohne Risiko übernehmen kann, obwohl sich die Identität des originalen Quell-Volumes geändert hat. Sie können ein Volume in der Datensicherung (in allen Schnappschüssen, die von Time Machine aufgezeichnet wurden) einem Volume Ihrer jetzigen Konfiguration neu zuweisen, so dass diese übereinstimmen. Sie sollten dies nur in dem skizzierten Fall tun, wenn alle Dateien tatsächlich vom vorigen auf das neue Volume kopiert wurden (wobei nicht Time Machine zum Einsatz gekommen ist, so dass es hiervon nichts „weiß“). Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Wartung** auf der Karte **Time Machine X**.
2. Drücken Sie den Knopf **Bestätigen, dass ein kopiertes Volume ein voriges Volume ersetzt**

Drei Dinge müssen angegeben werden:

- ein Schnappschuss im aktuellen Datensicherungssatz, der eine Sicherung dieses Volumes enthält,
- der Name dieses Volumes, wie er zum Zeitpunkt des ausgewählten Schnappschusses gelautet hat,
- der Name des neuen Volumes in Ihrer aktuellen Installation, das mit dem Volume in der Sicherung übereinstimmen soll.

TinkerTool System weist dieses Volume für die gesamte Zeitlinie, die im Datensicherungssatz aufgezeichnet wurde, neu zu, d.h. *für alle Schnappschüsse*. Es spielt keine Rolle wenn das frühere Volume während des aufgezeichneten Zeitabschnittes seinen Namen geändert hat. Time Machine identifiziert das Volume korrekt, indem die interne Historie nachverfolgt wird.



Missbrauchen Sie die beiden Wartungsfunktionen nicht, um die Datensicherung in anderen Fällen zu manipulieren, die hier nicht genannt wurden. Die Datensicherung könnte unbrauchbar werden.

2.4.2 Überprüfung und Statistik der Datensicherung (macOS 10-Betrieb)

TinkerTool System gibt Ihnen den Zugriff auf interne Prüffunktionen von Time Machine. Sie können mehr über den tatsächlichen Speicherbedarf einzelner Schnappschüsse erfahren, und Sie können einen Prüflauf auf ausgewählten Schnappschüssen laufen lassen, um zu gewährleisten, dass der Inhalt einer Datensicherung immer noch intakt ist.

Berechnen der Statistik der Änderungsraten zwischen allen Schnappschüssen (macOS 10-Betrieb)

Wie in der Einführung erwähnt, simuliert Time Machine, dass jeder Schnappschuss eine vollständige Kopie aller Daten enthält, die zum jeweiligen Zeitpunkt Teil der Datensicherung waren. Wenn also Ihr Computer immer eine Menge von etwa 500 GB Daten auf seinen Platten gespeichert hatte und 50 Schnappschüsse von Time Machine aufgezeichnet wurden, enthält das Ziel-Volume virtuell die scheinbare Menge von $500 \text{ GB} \times 50 = 25.000 \text{ GB}$ Daten. Diese große Datenmenge ist allerdings nicht wirklich auf der Platte gespeichert. In Wirklichkeit optimiert Time Machine den Speicherplatzbedarf seiner Zielplatten, indem nur die Änderungen zwischen aufeinanderfolgenden Datensicherungen abgespeichert werden. Um die Speichermenge abzuschätzen, die üblicherweise von jedem Schnappschuss verbraucht wird, kann es hilfreich sein, die Änderungen zwischen den Sicherungsläufen auszuwerten und die durchschnittliche Änderungsrate berechnen zu lassen. Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Überprüfung** auf der Karte **Time Machine X**.
2. Drücken Sie den Knopf **Statistik berechnen**.

Beachten Sie, dass alle Dateien der gesamten Time Machine-Platte für diese Berechnung analysiert werden müssen. Dies kann längere Zeit in Anspruch nehmen.

TinkerTool System erstellt einen Textbericht nachdem Time Machine die Berechnung abgeschlossen hat. Der Bericht kann in eine Datei abgespeichert werden, falls notwendig.

Den Inhalt eines Volume-Schnappschusses überprüfen (macOS 10-Betrieb)

Um absolut sicher zu sein, dass die Sicherungskopie eines Volumes für einen bestimmten Zeitpunkt ohne Probleme gelesen werden kann und vollständig intakt ist, können Sie Time Machine zwingen, seine internen Prüfsummen auszuwerten. Seit Version 10.11 des Betriebssystems schützt Time Machine jede Datei in der Datensicherung dadurch, dass eine Prüfsumme für den Inhalt jeder Datei berechnet und abgespeichert wird. Um einen Datensicherungslauf für ein Volume überprüfen zu lassen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Überprüfung** auf der Karte **Time Machine**.
2. Verwenden Sie das Klappmenü **Schnappschuss**, um den Zeitpunkt der Sicherung auszuwählen, der überprüft werden soll.
3. Verwenden Sie das Klappmenü **Volume**, um das Volume in diesem Schnappschuss auszuwählen, das überprüft werden soll.
4. Drücken Sie den Knopf **Ausgewählte Sicherung prüfen**.

Die Prüfung wird einige Zeit in Anspruch nehmen. Wenn Probleme festgestellt werden, zeigt TinkerTool System eine Tabelle mit allen Auffälligkeiten an, nachdem der Prüflauf abgeschlossen ist. Die Tabelle listet die vollen Pfade der Dateien in der Datensicherung auf, bei denen ein Problem erkannt wurde. Es kann zwei Arten von Problemen geben, die wie folgt gekennzeichnet sind:

- **Datei verändert:** die Datei in der Datensicherung stimmt nicht mit ihrer Prüfsumme überein. Entweder konnte die Datei nicht korrekt gelesen werden oder der Inhalt hat sich unerwartet geändert.

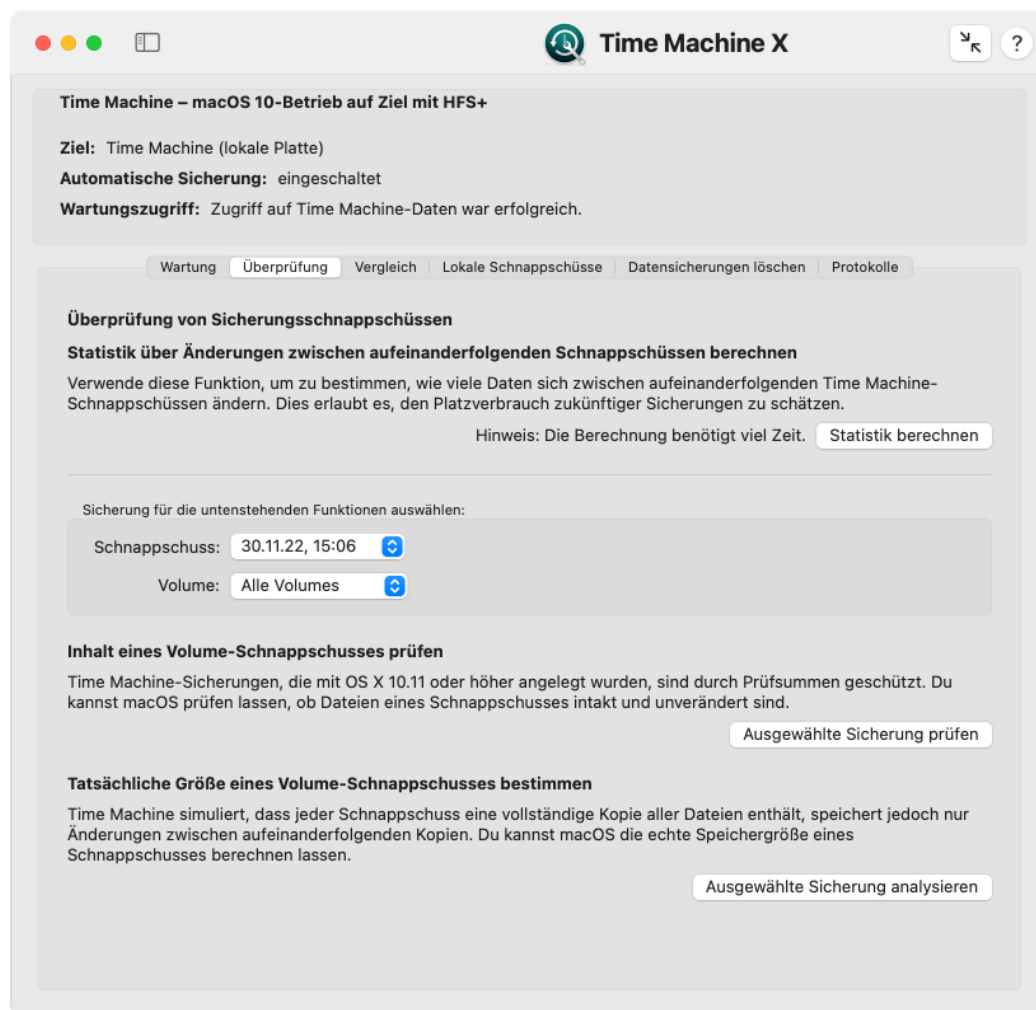


Abbildung 2.11: Funktionen zur Überprüfung und Statistik der Datensicherung

- **Keine Prüfung möglich:** die Datei konnte nicht erfolgreich überprüft werden, da die Prüfsumme nicht verfügbar war. Diese Anzeige bedeutet *nicht*, dass Sie der kopierten Datei nicht trauen können. Sie weist darauf hin, dass es im Moment unbekannt ist, ob die Datei in Ordnung ist oder nicht.

Mögliche Ursachen für Fälle, in denen keine Prüfung möglich ist, können sein:

- Der Schnappschuss wurde mit einem Betriebssystem vor Version 10.11 erstellt.
- Die Prüfsumme ist im Moment in Gebrauch, da ein anderer Time Machine-Vorgang (z.B. ein neuer Sicherungslauf) gerade im Hintergrund läuft. In diesem Fall sollten Sie den Test wiederholen, eventuell nach vorübergehendem Abschalten automatischer Sicherungen.

Die Liste möglicher Ursachen hängt von der Betriebssystemversion ab und ist möglicherweise nicht vollständig.

Den tatsächlichen Speicherbedarf eines Volume-Schnappschusses berechnen (macOS 10-Betrieb)

Zusätzlich zu den Änderungsraten aufeinanderfolgender Schnappschüsse kann es interessant sein, zu wissen, wie hoch der tatsächliche Speicherverbrauch eines Schnappschusses ist, der die Sicherungskopie eines Volumes enthält. Aufgrund der internen Optimierung von Time Machine kann sich diese Größe enorm von der simulierten Größe des entsprechenden Sicherungsordners unterscheiden, die vom Finder oder ähnlichen Programmen zum Auflisten von Dateien angezeigt wird.

Um Time Machine die tatsächliche Größe eines Volume-Schnappschusses berechnen zu lassen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Überprüfung** auf der Karte **Time Machine X**.
2. Verwenden Sie das Klappmenü **Schnappschuss**, um den Zeitpunkt der Sicherung auszuwählen, der ausgewertet werden soll.
3. Verwenden Sie das Klappmenü **Volume**, um das Volume in diesem Schnappschuss auszuwählen, das ausgewertet werden soll.
4. Drücken Sie den Knopf **Ausgewählte Sicherung analysieren**.

TinkerTool System fasst den Größenwert in einer Meldung zusammen, die angezeigt wird, sobald die Berechnung abgeschlossen ist.

Die tatsächliche Speichergröße kann bei Null liegen, falls sich das Volume zwischen aufeinanderfolgenden Sicherungsläufen nicht verändert hat.

2.4.3 Vergleich von Time Machine Sicherungsschnappschüssen (macOS 10-Betrieb)

Time Machine benötigt normalerweise keine Wartung solange Sie die Quell- oder Zielplatten nicht austauschen. Man definiert lediglich, welche Platten-Volumes in der Datensicherung berücksichtigt werden sollen, welches Ziellaufwerk benutzt wird, und schaltet Time Machine ein. Es kann allerdings bestimmte Fälle geben, in denen Time Machine nicht wie erwartet arbeitet, z.B. wenn es ein Dateisystemproblem auf einem der Quell-Volumes gibt,

oder wenn während einer Time Machine-Sicherung der Strom ausgefallen ist. TinkerTool System kann Ihnen dabei helfen, mögliche Probleme mit Datensicherungen zu erkennen, indem Sie eine der Diagnosefunktionen von Time Machine mit einfachen Mausklicks bedienen können.

Sie können zwei verschiedene Datensicherungssätze auswählen und alle enthaltenen Dateien miteinander vergleichen, wodurch der „wahre“, inkrementelle Inhalt der Time Machine-Sicherung angezeigt wird, nicht die simulierte Sicht des Finders oder der Time Machine-Bedieneroberfläche, die immer den gesamten, effektiven Datenbestand einer Datensicherung zu einem bestimmten Sicherungszeitpunkt zeigen. Falls ein Teil von Time Machine ausgefallen ist, bedeutet das, dass obwohl sich bestimmte Dateien verändert haben, diese nicht in die darauffolgende inkrementelle Datensicherung aufgenommen wurden, also diejenige Momentaufnahme bezieht, die unmittelbar nach der Änderungszeit lag. Bei typischen Time Machine-Problemen fehlen üblicherweise die Aktualisierungen in einem ganzen Ordner, was einfach erkannt werden kann, wenn man die beiden Sicherungen vor und nach der Änderung in dem betreffenden Ordner miteinander vergleicht.

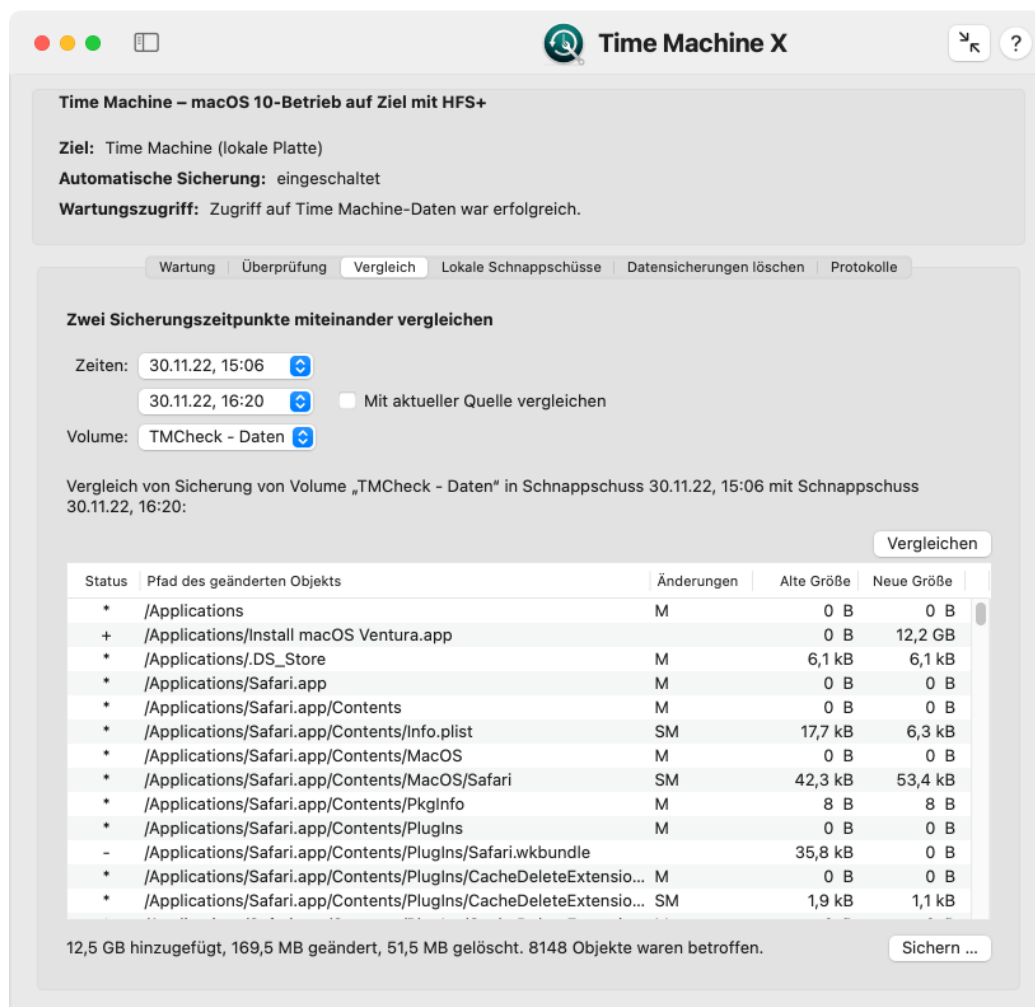


Abbildung 2.12: Time Machine prüfen

Als Nebenwirkung können Sie diese Funktion auch dazu verwenden, um zu ermitteln, welche Dateien sich auf Ihrem Computer zu einem bestimmten Zeitpunkt geändert haben,

oder um abzuschätzen, wie viele Dateien mit welchem Platzbedarf typischerweise jede Stunde gesichert werden.

In einer alternativen Betriebsart ist es außerdem möglich, die aktuellen Daten auf Ihrem Computer (genauer gesagt diejenigen Dateien, die zur Sicherung mit Time Machine ausgewählt sind) mit einer bestimmten Sicherungssitzung zu vergleichen. Diese Funktion ist hilfreich, um Implementationsfehler in Time Machine zu finden. Sie können sofort sehen, ob die Daten, die kopiert werden *sollten*, auch tatsächlich kopiert wurden. Beachten Sie, dass diese Art von Prüfvorgang eine erhebliche Zeit in Anspruch nimmt, da alle Dateien auf Ihrem Computer überprüft werden müssen.

Um den Vergleich zweier Time Machine-Sicherungen vorzunehmen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Vergleich** auf der Einstellungskarte **Time Machine X**.
2. Stellen Sie bei **Zeiten** die beiden Zeitpunkte ein, bei denen die Datensicherungen miteinander verglichen werden sollen. Die Reihenfolge der Zeitangaben spielt keine Rolle. Um die „Live“-Daten Ihres Computers zum Vergleich auszuwählen, kreuzen Sie den Punkt **Mit aktueller Quelle vergleichen** an.
3. Falls Time Machine dazu konfiguriert ist, Datensicherungen mehrerer Platten-Volumes anzulegen, wählen Sie die gewünschte Platte über das Aufklappmenü **Volume** aus. (Dies ist beim Vergleich der aktuellen Quelldaten nicht notwendig, bzw. möglich.)
4. Drücken Sie auf den Knopf **Vergleichen**.

Abhängig von der Größe Ihrer Datensicherung und der Datenmenge, die zwischen den beiden gewählten Sicherungen Unterschiede aufweisen, kann der Vergleichsvorgang wenige Sekunden, aber auch viele Minuten zur Fertigstellung benötigen. Die Ergebnisse werden danach in der Tabelle angezeigt.

- Die Spalte **Status** verwendet ein einzelnes Symbol, um den Gesamtstatus jeder gefundenen Differenz darzustellen. Die Symbole haben folgende Bedeutung:
 - +: Dieses Objekt wurde hinzugefügt.
 - -: Dieses Objekt wurde entfernt.
 - *: Dieses Objekt wurde verändert.
- **Pfad des geänderten Objekts** zeigt den UNIX-Pfad der Datei oder des Ordners an, bei dem ein Unterschied gefunden wurde. Der Pfad muss relativ zu dem Volume, das Sie zum Vergleich ausgewählt hatten, interpretiert werden.
- **Änderungen** gibt den exakten Typ der Veränderung an:
 - **A**: Die Zugriffssteuerungsliste (ACL) hat sich geändert.
 - **C**: Das Datum der Erstellung hat sich geändert.
 - **D**: Die Daten, die in dem Objekt gespeichert sind, haben sich verändert.
 - **G**: Der Gruppeneigentümer hat sich geändert.
 - **M**: Der Zeitpunkt der letzten Änderung (Modifikation) hat sich geändert.
 - **O**: Der Eigentümer hat sich geändert.
 - **P**: Die POSIX-Berechtigungen haben sich geändert.
 - **S**: Die Größe hat sich geändert.
 - **T**: Der Typ des Objekts hat sich geändert.

– **X**: Die Erweiterten Attribute haben sich geändert.

- Falls das Objekt eine Datei ist, die geändert wurde, gibt die Spalte **Alte Größe** den Speicherplatzbedarf an, den diese Datei bei dem älteren der beiden gewählten Zeitpunkte benötigt hat.
- Gleichermaßen gibt die Spalte **Neue Größe** den Speicherplatzbedarf für den späteren der beiden gewählten Zeitpunkte an.

Falls Sie den Mauszeiger über einen Eintrag in der Spalte **Änderungen** setzen, zeigt TinkerTool System einen kurzen Erläuterungstext an, so dass Sie die Abkürzungen nicht auswendig lernen müssen.

Aus Effizienzgründen können die Einträge in der Tabelle nicht umsortiert werden. TinkerTool System zeigt diese in der Reihenfolge an, in der Time Machine sie beim Sichern verarbeitet. Über den Knopf **Sichern ...** können Sie einen aufbereiteten Bericht in Textform erstellen lassen, der in eine Datei gespeichert wird.

2.4.4 Arbeiten mit lokalen APFS-Schnappschüssen (macOS 10-Betrieb)

Falls mindestens eines der Volumes, die Teil der Datensicherung sind, das moderne *Apple File System (APFS)* verwendet, schaltet Time Machine automatisch zusätzliche Funktionen ein:

- Jedesmal wenn ein Sicherungslauf stattfindet, legt Time Machine einen Schnappschuss für jedes APFS-Volume an, das zur Sicherung ansteht. Ein APFS-Schnappschuss stellt quasi ein eingefrorenes Abbild des Quell-Volumes dar, das angelegt wurde, als der Backup-Lauf begann. Auch wenn sich Dateien ändern während die Datensicherung läuft, stellt der Schnappschuss sicher, dass Time Machine nur ein unveränderliches Bild des Volumes „sieht“. Falls die Datensicherung später einmal zurückgeladen werden muss, wird das Ergebnis einen konsistenten Zustand des Volumes wiedergeben, ohne dass sich Dateien nur in einem vorübergehenden Zwischenstatus befinden.
- Jeder APFS-Schnappschuss wird vom Betriebssystem weiterhin auf dem entsprechenden Volume aufbewahrt, so lange dieses Volume genügend Speicherplatz hat. Der Schnappschuss ist während des Normalbetriebs unsichtbar und benötigt nur einen kleinen Betrag an zusätzlichem Speicherplatz. Er basiert auf der Strategie, die Blöcke eines Volumes, die von einer Datei belegt sind, niemals für neue Dateien wiederzuverwenden, sogar wenn die Datei gelöscht wurde oder sich der entsprechende Teil der Datei geändert hat.
- APFS-Schnappschüsse werden nicht nur dann angelegt, wenn die normalen Time Machine-Sicherungen laufen, das Betriebssystem legt sie auch an, wenn größere Änderungen im System erwartet werden, z.B. wenn ein Betriebssystem-Update zur Installation ansteht.
- Diese Schnappschüsse können als „Wiederherstellungspunkte“ verwendet werden, die es Ihnen erlauben, ein komplettes APFS-Volume sehr schnell wieder auf einen konsistenten Zustand in der Vergangenheit zu bringen. Dies wird von Time Machine erledigt (üblicherweise nach einem Start vom Wiederherstellungssystem aus), wobei das APFS-Volume selbst, nicht das Time Machine-Volume, als Quelle für die Wiederherstellung angegeben wird. Für weitere Informationen ziehen Sie bitte Apples offizielle Dokumentation zu macOS hinzu.

Dies heißt, dass ein APFS-Schnappschuss prinzipiell als lokaler Schnappschuss von Time Machine verwendet werden kann. Für die Nutzung solcher Schnappschüsse ist kein Zugriff auf das tatsächliche Time Machine-Sicherungs-Volume erforderlich.

Andere macOS-Bestandteile können die APFS-Schnappschussfunktion ebenso nutzen. Die Liste, die auf dem Tab **Lokale Schnappschüsse** angezeigt wird, berücksichtigt nur die APFS-Schnappschüsse, die von Time Machine genutzt werden. Wenn Sie mit der vollständigen Liste von APFS-Schnappschüssen arbeiten möchten, verwenden Sie bitte das Kapitel Die Einstellungskarte APFS (Abschnitt 3.7 auf Seite 228).

Es liegt im alleinigen Ermessen des Betriebssystems, wann APFS-Schnappschüsse angelegt oder entfernt werden. TinkerTool System gibt Ihnen jedoch zusätzliche manuelle Kontrolle über diese lokalen Schnappschüsse.

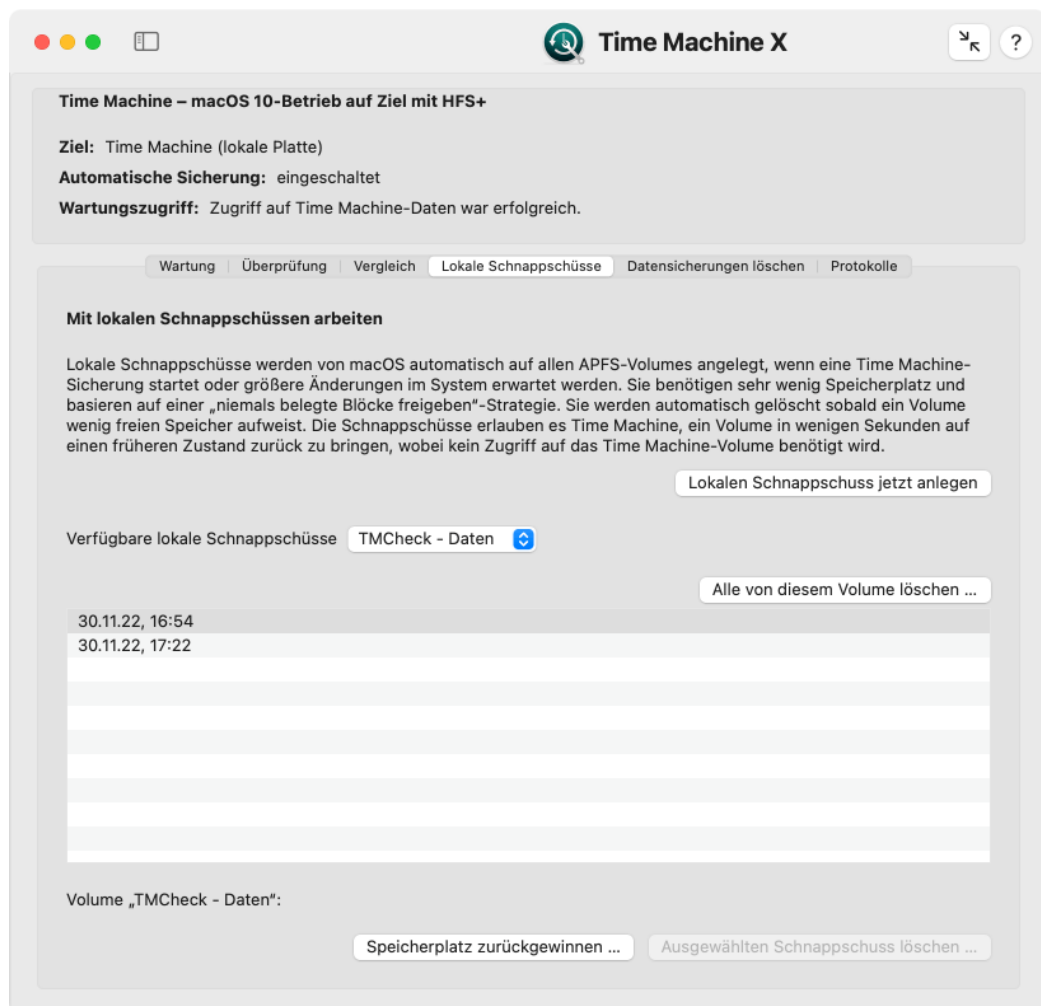


Abbildung 2.13: Arbeiten mit lokalen Schnappschüssen

- Sie können einen lokalen Schnappschuss sofort anlegen, wofür nur ein Knopfdruck nötig ist. Dies ist hilfreich, um einen wohldefinierten Wiederherstellungspunkt an-

zulegen, z.B. wenn Sie einen möglicherweise „gefährlichen“ Vorgang auf einem APFS-Volume ausprobieren möchten, der möglicherweise in naher Zukunft wieder rückgängig gemacht werden muss.

- Sie können einsehen, welche lokalen Schnappschüsse im Moment auf jedem APFS-Volume abgelegt sind.
- Sie können macOS dazu zwingen, seine lokalen Schnappschüsse sofort zu bereinigen, um den Zeitpunkt vorzuverlegen, an dem dies automatisch ablaufen würde. Dies geschieht dadurch, dass Sie eine geplante freizugebende Menge von Speicherplatz angeben, die durch die Bereinigung zurückgewonnen werden soll. macOS behält so viele Schnappschüsse wie möglich bei, während es versucht, dieses Ziel zu erfüllen.
- Sie können lokale Schnappschüsse Ihrer Wahl löschen.

Um einen neuen lokalen Schnappschuss auf allen APFS-Volumes anzulegen, die Teil der Time Machine-Sicherung sind, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Lokale Schnappschüsse** auf der Karte **Time Machine X**.
2. Drücken Sie den Knopf **Lokalen Schnappschuss jetzt anlegen**.

Das Anlegen eines lokalen Schnappschusses dauert typischerweise weniger als eine Minute.

Sie können alle Schnappschüsse über die Tabelle **Verfügbare lokale Schnappschüsse** auf der gleichen Karte einsehen. Die verfügbaren Zeitpunkte werden als einzelne Zeilen aufgelistet. Standardmäßig sehen Sie eine Liste für den gesamten Computer. Falls mehr als ein APFS-Volume genutzt wird, kann es aber interessant sein, die Liste der Schnappschüsse pro Volume anzuzeigen. Beachten Sie, dass die Menge der verfügbaren Schnappschüsse auf jedem Volume verschieden sein kann, da einige Volumes weniger freien Speicherplatz haben, so dass diese ihre Schnappschüsse früher bereinigen müssen, als andere. Um zwischen verschiedenen Volumes zu wechseln, verwenden Sie das Aufklappmenü über der Tabelle.

Um Speicherplatz auf einem bestimmte Volume wiederzugewinnen, wählen Sie das Volume mit dem Aufklappmenü über der Tabelle aus und drücken dann den Knopf **Speicherplatz zurückgewinnen**. TinkerTool System fragt in einem Dialogfenster, wie viele Bytes Sie mindestens zurückgewinnen möchten. Sie können einen niedrigen Wert (wie 1) angeben, um sicher zu stellen, dass nur die kleinstmögliche Zahl von Schnappschüssen gelöscht werden soll. Das Betriebssystem wird seine eigenen Standardverfahren verwenden, um automatisch diejenigen Schnappschüsse auszuwählen, die entfernt werden sollen. Am Ende des Vorgangs zeigt TinkerTool System eine Zusammenfassung an, wie viele Schnappschüsse verloren gegangen sind und wie viel Speicherplatz auf dem Volume frei geworden ist.

In manchen Fällen kann sich Time Machine entscheiden, den Aufräumvorgang für einige Zeit zu verschieben. In dieser besonderen Situation kann es sein, dass TinkerTool System sofort nach dem Anfordern einer Speicherwiedergewinnung nicht anzeigt, dass bereits Speicherplatz frei geworden ist.

Falls Sie so viel Speicher wie möglich von einem Volume freigeben möchten, wählen Sie das Volume bei **Verfügbare lokale Schnappschüsse** aus und betätigen Sie den Knopf **Alle**

von diesem Volume löschen. Time Machine wird dies als dringende Anforderung verstehen, den Höchstbetrag an Speicherplatz wiederzugewinnen, der im Moment für lokale Schnappschüsse genutzt wird.

Um von Hand einen lokalen Schnappschuss zu löschen, wählen Sie diesen in der Tabelle aus und drücken den Knopf **Ausgewählten Schnappschuss löschen**

2.4.5 Löschen von Time Machine-Sicherungsdaten (macOS 10-Betrieb)

Einen Sicherungsschnappschuss von der gerade aktuellen Time Machine-Platte entfernen (macOS 10-Betrieb)

Als Teil des täglichen Ablaufs räumt Time Machine seine Sicherungen regelmäßig auf, üblicherweise jede Stunde. Nachdem ein Sicherungslauf stattgefunden hat, werden veraltete Sicherungsschnappschüsse von der Sicherungsplatte entfernt. Manchmal möchten Sie vielleicht einen bestimmten Schnappschuss auch von Hand löschen, z.B. um Speicherplatz freizugeben. *Sie dürfen dies niemals über den macOS Finder machen. Dies könnte den Time Machine-Sicherungssatz und zusätzlich die Papierkorbfunktion des Finders beschädigen.* TinkerTool System bietet Ihnen einen sicheren Weg, eine Time Machine-Sicherung für einen bestimmten Zeitpunkt zu entfernen:

1. Öffnen Sie den Karteireiter **Datensicherungen löschen** auf der Karte **Time Machine X**.
2. Wählen Sie den Schnappschuss, der gelöscht werden soll, mit dem Klappmenü **Löschen** in der oberen Hälfte des Fensters aus.
3. Drücken Sie auf den Knopf **Löschen** ... daneben.

Dieser Vorgang entfernt Daten aus Time Machine „horizontal“: Alle Dateien und Ordner eines Schnappschusses werden gelöscht, so dass Sie nicht mehr länger „in die Vergangenheit reisen können“, um einen oder alle Dateien für diesen spezifischen Zeitpunkt wiederherstellen zu können. Alle andere Schnappschüsse bleiben jedoch intakt. Sie können zusätzlich Daten auch „vertikal“ entfernen, d.h. Sie löschen eine bestimmte Datei oder einen Ordner *aus allen Schnappschüssen* im Sicherungssatz. Diese Funktion ist bereits in die Bedienerschnittstelle von Time Machine eingebaut:

1. Verwenden Sie den Finder, um den Elternordner zu öffnen, der das zu löschende Objekt enthält.
2. Öffnen Sie die Bedieneroberfläche von Time Machine.
3. Wählen Sie das Objekt, das entfernt werden soll, im Finder-artigen Fenster von Time Machine aus.
4. Verwenden Sie das Kontextmenü (Rechtsklick), um das ausgewählte Objekt zu löschen.

Beliebige Time Machine-Daten von lokalen Sicherungsplatten im Format HFS+ entfernen (macOS 10-Betrieb)

Time Machine-Platten können von mehreren Computern genutzt werden. Im macOS 10-Betrieb können auch andere Daten auf Time Machine-Platten gespeichert werden, auch wenn dies definitiv nicht zu empfehlen ist, denn diese zusätzlichen Daten können nicht in die Time Machine-Sicherung eingeschlossen werden. (Bei einem Plattenausfall würden Sie gleichzeitig die Originaldaten und die Sicherung verlieren.) Falls Sie einige oder alle

Time Machine-Daten von solchen Platten entfernen möchten, z.B. wenn Sie Datensicherungen für einen ausgemusterten Computer nicht mehr benötigen, dürfen Sie auch hier den Finder nicht verwenden. Dies würde riskieren, dass das gesamte Dateisystem dieser Platte und der Papierkorb beschädigt werden.

TinkerTool System kann auch in diesem Fall helfen, wenn sich also Time Machine-Daten auf einer Platte befinden, die nicht notwendigerweise zur derzeit aktiven Datensicherung des lokalen Computers gehören. Sie können Daten aus inaktiven Datensicherungen oder von Sicherungen anderer Macs entfernen. Genauer gesagt können Sie löschen:

- alle Time Machine-Daten auf der Platte (wobei andere Dateien und Ordner unberührt bleiben),
- alle Time Machine-Sicherungen für einen bestimmten Computer auf einer bestimmten Platte,
- einen einzelnen Sicherungsschnappschuss für einen bestimmten Computer auf einer bestimmten Platte.

Falls Sie eine „reine“ Time Machine-Platte haben, die nur Datensicherungen für einen einzelnen Computer enthält und auf der keine anderen Daten gespeichert sind, ist die schnellste Lösung, diese Platte zu bereinigen, sie einfach mit dem Festplattendienstprogramm neu zu formatieren, indem Sie *Löschen* für deren Hauptpartition ausführen. Falls aber die Platte verschlüsselt war und später für neue, ebenso verschlüsselte Time Machine-Sicherungen wiederverwendet werden soll, könnte ein Löschvorgang über TinkerTool System insgesamt schneller sein, da die erforderliche Neuverschlüsselung (die beim manuellen Löschvorgang nicht nötig ist) sehr lange Zeit in Anspruch nehmen könnte.

1. Öffnen Sie den Karteireiter **Datensicherungen löschen** auf der Karte **Time Machine X**.
2. Treffen Sie in der unteren Hälfte des Fensters Ihre Auswahl für **Time Machine-Platte** und **Löschen**, um die Time Machine-Objekte auszuwählen, die entfernt werden sollen.
3. Betätigen Sie den Knopf **Löschen**

2.4.6 Auslesen von Time Machine-Protokollen (macOS 10-Betrieb)

macOS zeichnet jedes Mal ein Protokoll auf, wenn eine Time Machine-Datensicherung gelaufen ist und ein neuer Schnappschuss angelegt wurde. Diese Protokolle sind normalerweise unsichtbar, können aber von TinkerTool System für jeden Schnappschuss ausgelesen werden, falls nötig. Unter anderem enthält jedes Protokoll Daten darüber,

- wie lange der Sicherungslauf gedauert hat,
- ob eine volle oder inkrementelle Sicherung durchgeführt wurde,
- welche Speichermenge benötigt wurde,
- welche Dateien weggelassen wurden,
- ob während der Datensicherung ungewöhnliche Situationen aufgetreten sind, usw.

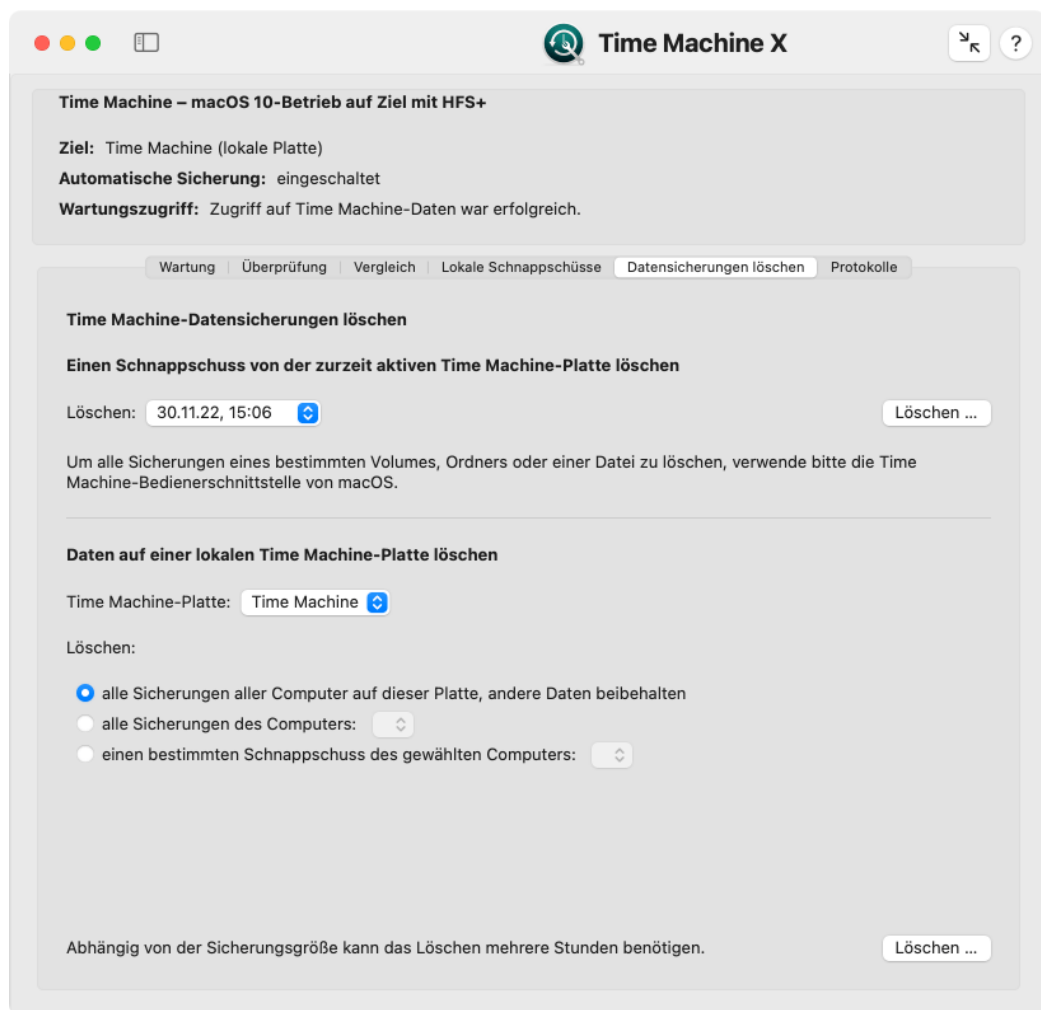


Abbildung 2.14: Löschen von Time Machine-Sicherungsdaten

Die Protokolle sind nur in englischer Sprache verfügbar, egal welche Sprache Sie für die Bedienerschnittstelle eingestellt haben. Die Berichte werden von macOS, nicht von TinkerTool System erstellt, so dass sich deren Inhalte ohne vorherige Ankündigung ändern können, je nach dem, welche Betriebssystemversion sie angelegt hat.

Um das Protokoll eines Schnappschusses aus einem Time Machine-Datensicherungssatz auszulesen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Protokolle** auf der Karte **Time Machine X**.
2. Wählen Sie mit dem Menüknopf **Schnappschuss** den Zeitpunkt der Datensicherung, der Sie interessiert.
3. Bestätigen Sie macOS, dass das Programm *authopen* die Berechtigung haben soll, das Protokoll zu lesen.

TinkerTool System zeigt den Inhalt des Protokolls im Textbereich **Sicherungsprotokoll (in englischer Sprache)** an.

2.5 Die Einstellungskarte Time Machine

Dieses Kapitel bezieht sich auf die Karte **Time Machine**. Wenn Sie Time Machine in der Betriebsart macOS 10 verwenden, was automatisch die Karte **Time Machine X** aktiviert, lesen Sie bitte stattdessen das vorhergehende Kapitel (Abschnitt 2.4 auf Seite 40).

TinkerTool System schaltet die Time Machine-Betriebsart nicht hin und her, während es läuft. Wenn Sie die Zielplatte von APFS zu HFS+ austauschen, während TinkerTool System gerade geöffnet ist, wird das Programm dies bemerken, wenn Sie einen Wartungsvorgang vorbereiten und eine entsprechende Fehlermeldung in diesem Fall anzeigen. Um diese Situation aufzulösen, reicht es einfach, das Programm zu beenden und wieder neu zu starten.

2.5.1 Wartung nach dem Austausch einer Datenquelle von Time Machine

Das inkrementelle Vorgehen bei der Datensicherung, das in der Einleitung erwähnt wurde, funktioniert nur dann, wenn Time Machine absolut sicher sein kann, welche Dateien sich zwischen zwei aufeinanderfolgenden Läufen geändert haben und welche nicht. Wenn es den kleinsten Zweifel daran gibt, dass eine Datei nicht mehr länger identisch mit dem Exemplar ist, das Time Machine beim vorhergehenden Lauf gesehen hat, muss die Datei im nächsten Lauf vollständig neu gesichert werden.

Wenn sich die Identität des Computers ändert, z.B. weil Sie einen neuen gekauft haben oder er bei einer Reparatur ausgetauscht werden musste, muss Time Machine annehmen, dass sich *alle* Dateien des Computers verändert haben, auch dann, wenn Sie ein fremdes Kopier- oder „Klon“-Programm eingesetzt haben, um alle Dateien des alten auf den neuen Computer zu kopieren. Dies hat zur Folge, dass beim nächsten Time Machine-Lauf alle Dateien noch einmal kopiert werden müssen, obwohl Sie selbst dafür gesorgt hatten, dass die Dateien die gleichen sind wie vorher. Nur wenn *Time Machine selbst* zum Einsatz

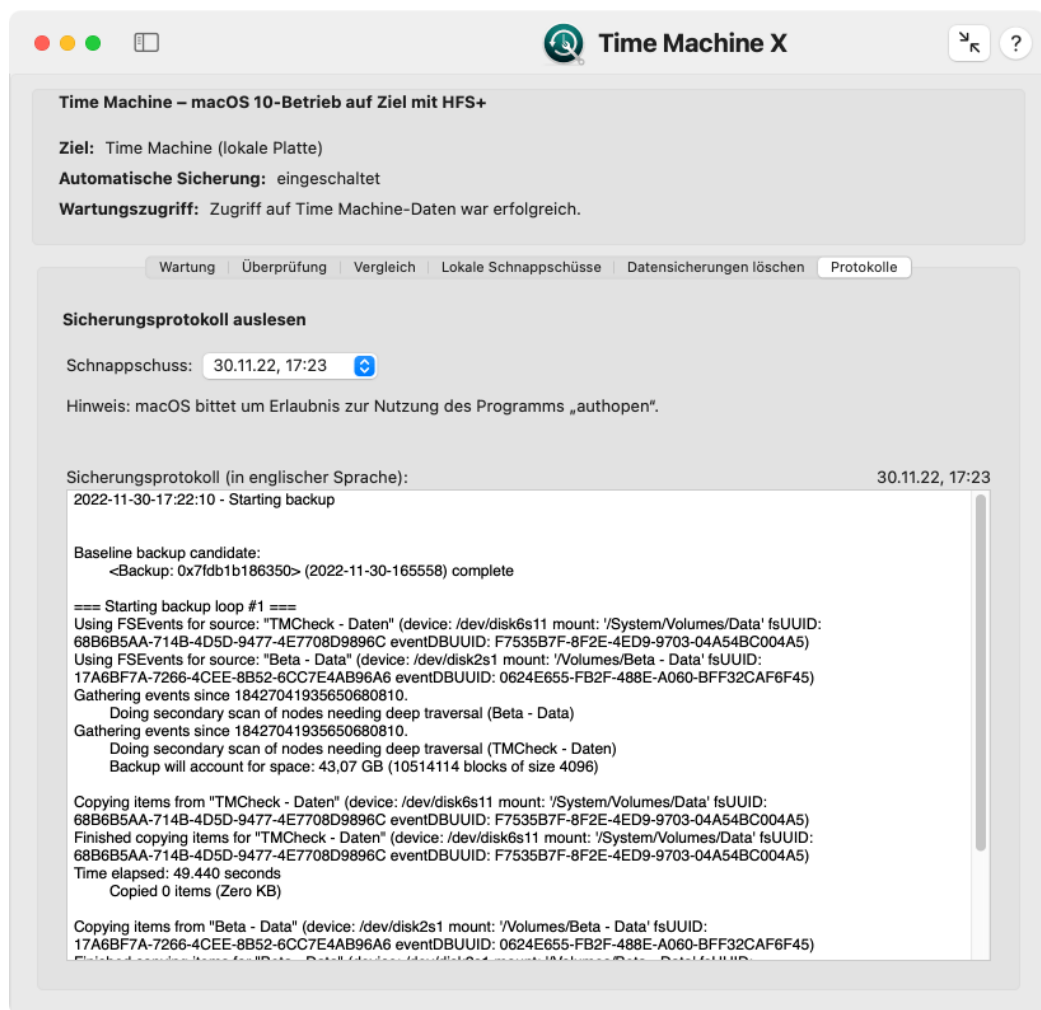


Abbildung 2.15: Zugriff auf Time Machine-Protokolle

gekommen ist, um eine vollständige Wiederherstellung des Computers aus der Datensicherung durchzuführen, „weiß“ Time Machine, dass es die vorige inkrementelle Sicherung problemlos weiter verwenden kann.

Genau das gleiche Problem tritt auf, wenn Sie ein Volume Ihres Mac ersetzen, aber nicht Time Machine, sondern ein fremdes Programm dazu genutzt haben, die Daten zurückzuspielen. Ersetzen eines Volumes kann bedeuten

- Sie haben ein Plattenlaufwerk physisch ausgetauscht,
- Sie haben eine Partition gelöscht oder neu formatiert,
- Sie haben ein Volume über ein Programm eines Drittanbieters geklont, aber das originale und das kopierte Volume waren vorübergehend gleichzeitig an den Computer angeschlossen, so dass das System gezwungen war, die Identität eines Volumes zu ändern, um nachverfolgen zu können, welches welches ist.

Nur dann, falls Sie ein Plattenlaufwerk oder eine Partition physisch kopiert haben (durch das Kopieren der rohen Datenblöcke, nicht Datei für Datei) und falls Sie sichergestellt haben, dass das Betriebssystem, auf dem Time Machine aktiv ist, nicht beide Volumes zur gleichen Zeit aktiviert hatte, kann Time Machine sein inkrementelles Vorgehen nahtlos fortsetzen. In allen anderen Fällen muss es annehmen, dass sich alle Dateien auf dem ganzen betroffenen Volume geändert haben, so dass diese noch einmal komplett kopiert werden müssen.

TinkerTool System kann in diesem Fall helfen, indem es Sie von Hand bestätigen lässt, dass ein Computer oder ein Volume immer noch als gleich anzusehen sind, obwohl sich deren Identität geändert hat. Auf diese Weise kann das neue Objekt die Rolle des ersetzten Objekts übernehmen, und dessen Historie in Time Machine kann fortgeführt werden, ohne dass eine komplett neue Datensicherung nötig ist.

Beachten Sie, dass in Fällen Voraussetzung ist, dass das Betriebssystem mit allen seinen Benutzer-Accounts identisch geblieben ist. Sie können diese Wartungsfunktionen zum Beispiel nicht nutzen, wenn Sie einen neuen Mac (mit einer anderen Installation von macOS) haben und Daten aus der Time Machine-Sicherung eines alten Mac übernehmen möchten. Auch wenn Systemversionen und Namen der Benutzer gleich sind, ist eine Übernahme einer Time Machine-Sicherung in diesem Fall nicht möglich, da in der Sicherung Zugriffsrechte für Benutzer-Accounts einer anderen Systeminstallation gespeichert sind. Sie können das Problem lösen, indem Sie die Accounts und Time Machine-Daten gleichzeitig über Apples Migrationsassistent kopieren.

Erben einer Time Machine-Datensicherung eines ersetzten Computers

Wenn Sie bestätigen müssen, dass Time Machine einen Sicherungssatz, der von einem anderen physischen Computer oder einer anderen Betriebssysteminstallation auf dem gleichen Computer erstellt worden ist, sicher übernehmen darf, können Sie den Sicherungssatz Ihrem aktuellen System neu zuweisen. Sie sollten dies nur dann tun, wenn die skizzierte Situation genau zutrifft und Sie die Dateien tatsächlich auf eine andere Weise (also nicht unter Kontrolle von Time Machine) auf die neue Systeminstallation kopiert haben. Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Wartung** auf der Karte **Time Machine**.
2. Betätigen Sie den Knopf **Fremde Sicherung diesem Mac zuweisen**

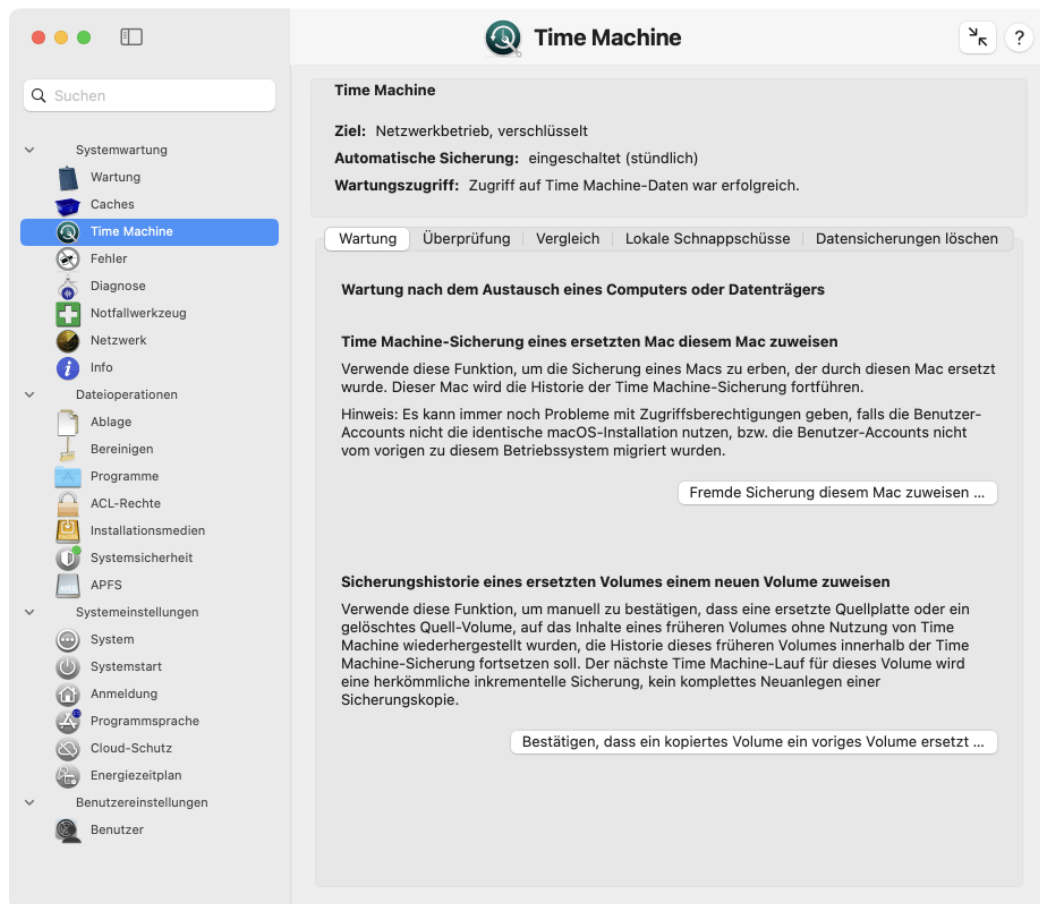


Abbildung 2.16: Wartung nach Austausch einer Time Machine-Datenquelle

TinkerTool System führt Sie dabei durch allen notwendigen Schritte. Sie müssen den Ort des fremden Datensicherungssatzes angeben, um den Vorgang abschließen zu können. Im Falle einer lokalen Time Machine-Platte handelt es sich dabei um den obersten Ordner dieser Datensicherung. Bei Verwendung von HFS+ trägt er den Namen des vorigen Computers und befindet sich im Ordner *Backups.backupdb* auf der Zielplatte. Bei Verwendung von APFS ist als Ordner das Sicherungs-Volume selbst anzugeben.

Abhängig davon wie Time Machine konfiguriert war, bevor die fremde Datensicherung zugewiesen wurde, müssen Sie möglicherweise Time Machine im Abschnitt **Allgemein** > **Time Machine** der **Systemeinstellungen** wieder einschalten und das Ziel für die Datensicherung neu einstellen.

Falls die lokalen Volumes des aktuellen Computers sich von denen des früheren Computers unterscheiden, *reicht die Neuuzuweisung der Datensicherung alleine nicht aus*. Sie müssen auch jedes Volume neu zuordnen, was im nächsten Abschnitt behandelt wird.

Neuzuweisung eines ersetzten Volumes mit einem Volume aus der Datensicherung

Wie in der Einleitung beschrieben, kann es ebenso Fälle geben, in denen Sie Time Machine bestätigen müssen, dass es die Historie eines Volumes in der Datensicherung ohne Risiko übernehmen kann, obwohl sich die Identität des originalen Quell-Volumes geändert hat. Sie können ein Volume in der Datensicherung (in allen Schnappschüssen, die von Time Machine aufgezeichnet wurden) einem Volume Ihrer jetzigen Konfiguration neu zuweisen, so dass diese übereinstimmen. Sie sollten dies nur in dem skizzierten Fall tun, wenn alle Dateien tatsächlich vom vorigen auf das neue Volume kopiert wurden (wobei nicht Time Machine zum Einsatz gekommen ist, so dass es hiervon nichts „weiß“). Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Wartung** auf der Karte **Time Machine**.
2. Drücken Sie den Knopf **Bestätigen, dass ein kopiertes Volume ein voriges Volume ersetzt**

Drei Dinge müssen angegeben werden:

- ein Schnappschuss im aktuellen Datensicherungssatz, der eine Sicherung dieses Volumes enthält,
- der Name dieses Volumes, wie er zum Zeitpunkt des ausgewählten Schnappschusses gelautet hat,
- der Name des neuen Volumes in Ihrer aktuellen Installation, das mit dem Volume in der Sicherung übereinstimmen soll.

TinkerTool System weist dieses Volume für die gesamte Zeitlinie, die im Datensicherungssatz aufgezeichnet wurde, neu zu, d.h. *für alle Schnappschüsse*. Es spielt keine Rolle wenn das frühere Volume während des aufgezeichneten Zeitabschnittes seinen Namen geändert hat. Time Machine identifiziert das Volume korrekt, indem die interne Historie nachverfolgt wird.



Missbrauchen Sie die beiden Wartungsfunktionen nicht, um die Datensicherung in anderen Fällen zu manipulieren, die hier nicht genannt wurden. Die Datensicherung könnte unbrauchbar werden.

2.5.2 Überprüfung der Datensicherung

Den Inhalt eines Volume-Schnappschusses überprüfen

Um absolut sicher zu sein, dass die Sicherungskopie eines Volumes für einen bestimmten Zeitpunkt ohne Probleme gelesen werden kann und vollständig intakt ist, können Sie Time Machine zwingen, seine internen Prüfsummen auszuwerten. Seit Version 10.11 des Betriebssystems schützt Time Machine jede Datei in der Datensicherung dadurch, dass eine Prüfsumme für den Inhalt jeder Datei berechnet und abgespeichert wird. Um einen Datensicherungslauf für ein Volume überprüfen zu lassen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Überprüfung** auf der Karte **Time Machine**.
2. Verwenden Sie das Klappmenü **Schnappschuss**, um den Zeitpunkt der Sicherung auszuwählen, der überprüft werden soll.
3. Verwenden Sie das Klappmenü **Volume**, um das Volume in diesem Schnappschuss auszuwählen, das überprüft werden soll.
4. Drücken Sie den Knopf **Ausgewählte Sicherung prüfen**.

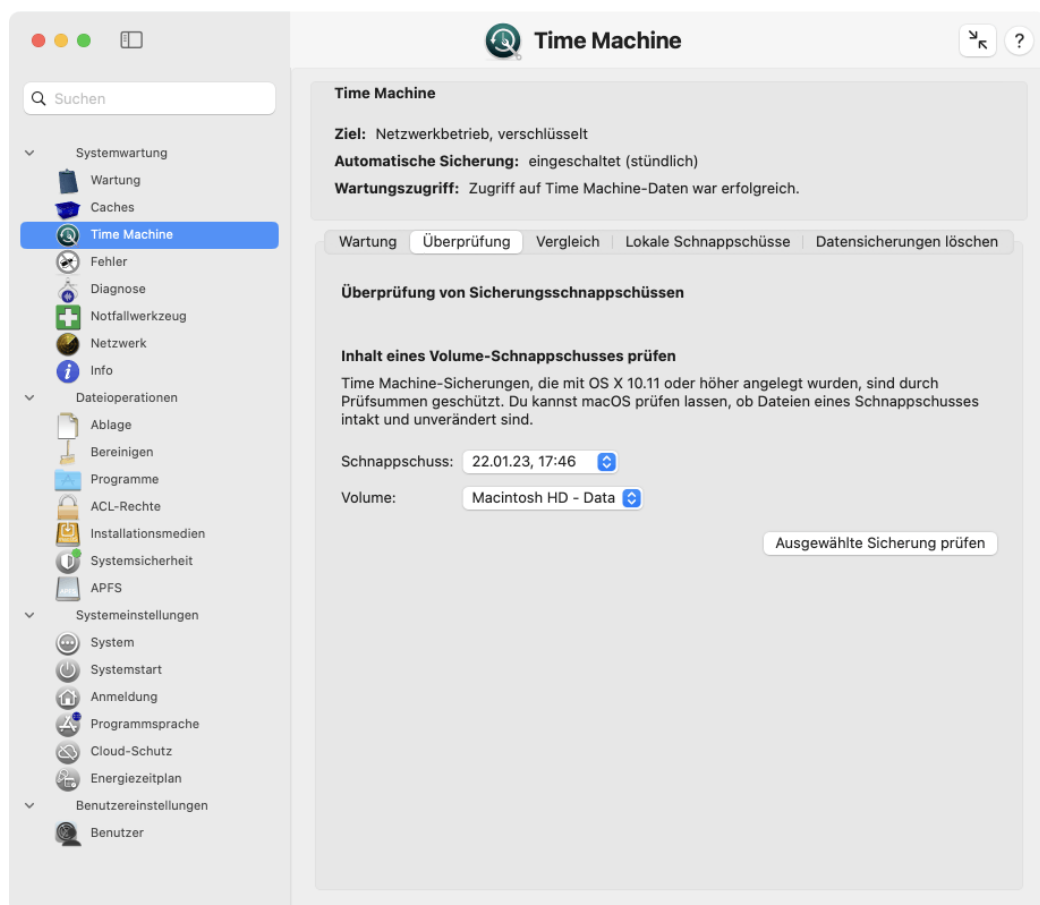


Abbildung 2.17: Funktion zur Überprüfung der Datensicherung

Die Prüfung wird einige Zeit in Anspruch nehmen. Wenn Probleme festgestellt werden, zeigt TinkerTool System eine Tabelle mit allen Auffälligkeiten an, nachdem der Prüflauf abgeschlossen ist. Die Tabelle listet die vollen Pfade der Dateien in der Datensicherung auf, bei denen ein Problem erkannt wurde. Es kann zwei Arten von Problemen geben, die wie folgt gekennzeichnet sind:

- **Datei verändert:** die Datei in der Datensicherung stimmt nicht mit ihrer Prüfsumme überein. Entweder konnte die Datei nicht korrekt gelesen werden oder der Inhalt hat sich unerwartet geändert.
- **Keine Prüfung möglich:** die Datei konnte nicht erfolgreich überprüft werden, da die Prüfsumme nicht verfügbar war. Diese Anzeige bedeutet *nicht*, dass Sie der kopierten Datei nicht trauen können. Sie weist darauf hin, dass es im Moment unbekannt ist, ob die Datei in Ordnung ist oder nicht.

Mögliche Ursachen für Fälle, in denen keine Prüfung möglich ist, können sein:

- Der Schnappschuss wurde mit einem Betriebssystem vor Version 10.11 erstellt.
- Die Prüfsumme ist im Moment in Gebrauch, da ein anderer Time Machine-Vorgang (z.B. ein neuer Sicherungslauf) gerade im Hintergrund läuft. In diesem Fall sollten Sie den Test wiederholen, eventuell nach vorübergehendem Abschalten automatischer Sicherungen.

Die Liste möglicher Ursachen hängt von der Betriebssystemversion ab und ist möglicherweise nicht vollständig.

2.5.3 Vergleich von Time Machine Sicherungsschnappschüssen

Time Machine benötigt normalerweise keine Wartung solange Sie die Quell- oder Zielplatten nicht austauschen. Man definiert lediglich, welche Platten-Volumes in der Datensicherung berücksichtigt werden sollen, welches Ziellaufwerk benutzt wird, und schaltet Time Machine ein. Es kann allerdings bestimmte Fälle geben, in denen Time Machine nicht wie erwartet arbeitet, z.B. wenn es ein Dateisystemproblem auf einem der Quell-Volumes gibt, oder wenn während einer Time Machine-Sicherung der Strom ausgefallen ist. TinkerTool System kann Ihnen dabei helfen, mögliche Probleme mit Datensicherungen zu erkennen, indem Sie eine der Diagnosefunktionen von Time Machine mit einfachen Mausklicks bedienen können.

Sie können zwei verschiedene Datensicherungssätze auswählen und alle enthaltenen Dateien miteinander vergleichen, wodurch der „wahre“, inkrementelle Inhalt der Time Machine-Sicherung angezeigt wird, nicht die simulierte Sicht des Finders oder der Time Machine-Bedieneroberfläche, die immer den gesamten, effektiven Datenbestand einer Datensicherung zu einem bestimmten Sicherungszeitpunkt zeigen. Falls ein Teil von Time Machine ausgefallen ist, bedeutet das, dass obwohl sich bestimmte Dateien verändert haben, diese nicht in die darauffolgende inkrementelle Datensicherung aufgenommen wurden, also diejenige Momentaufnahme bezieht, die unmittelbar nach der Änderungszeit lag. Bei typischen Time Machine-Problemen fehlen üblicherweise die Aktualisierungen in einem ganzen Ordner, was einfach erkannt werden kann, wenn man die beiden Sicherungen vor und nach der Änderung in dem betreffenden Ordner miteinander vergleicht.

Als Nebenwirkung können Sie diese Funktion auch dazu verwenden, um zu ermitteln, welche Dateien sich auf Ihrem Computer zu einem bestimmten Zeitpunkt geändert haben, oder um abzuschätzen, wie viele Dateien mit welchem Platzbedarf typischerweise jede Stunde gesichert werden.

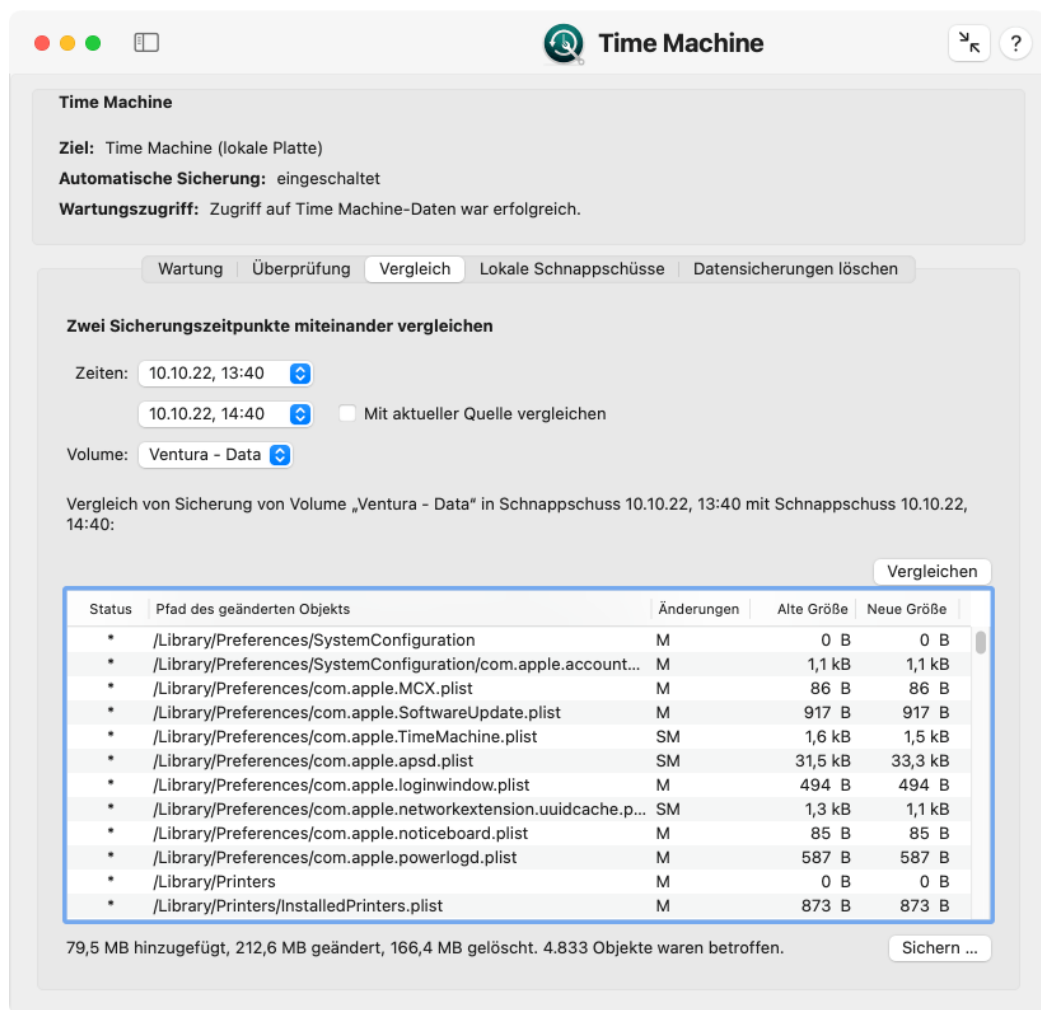


Abbildung 2.18: Time Machine prüfen

In einer alternativen Betriebsart ist es außerdem möglich, die aktuellen Daten auf Ihrem Computer (genauer gesagt diejenigen Dateien, die zur Sicherung mit Time Machine ausgewählt sind) mit einer bestimmten Sicherungssitzung zu vergleichen. Diese Funktion ist hilfreich, um Implementationsfehler in Time Machine zu finden. Sie können sofort sehen, ob die Daten, die kopiert werden *sollten*, auch tatsächlich kopiert wurden. Beachten Sie, dass diese Art von Prüfvorgang eine erhebliche Zeit in Anspruch nimmt, da alle Dateien auf Ihrem Computer überprüft werden müssen.

Um den Vergleich zweier Time Machine-Sicherungen vorzunehmen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Vergleich** auf der Einstellungskarte **Time Machine**.
2. Stellen Sie bei **Zeiten** die beiden Zeitpunkte ein, bei denen die Datensicherungen miteinander verglichen werden sollen. Die Reihenfolge der Zeitangaben spielt keine Rolle. Um die „Live“-Daten Ihres Computers zum Vergleich auszuwählen, kreuzen Sie den Punkt **Mit aktueller Quelle vergleichen** an.
3. Falls Time Machine dazu konfiguriert ist, Datensicherungen mehrerer Platten-Volumes anzulegen, wählen Sie die gewünschte Platte über das Aufklappmenü **Volume** aus. (Dies ist beim Vergleich der aktuellen Quelldaten nicht notwendig, bzw. möglich.)
4. Drücken Sie auf den Knopf **Vergleichen**.

Abhängig von der Größe Ihrer Datensicherung und der Datenmenge, die zwischen den beiden gewählten Sicherungen Unterschiede aufweisen, kann der Vergleichsvorgang wenige Sekunden, aber auch viele Minuten zur Fertigstellung benötigen. Die Ergebnisse werden danach in der Tabelle angezeigt.

- Die Spalte **Status** verwendet ein einzelnes Symbol, um den Gesamtstatus jeder gefundenen Differenz darzustellen. Die Symbole haben folgende Bedeutung:
 - +: Dieses Objekt wurde hinzugefügt.
 - -: Dieses Objekt wurde entfernt.
 - *: Dieses Objekt wurde verändert.
- **Pfad des geänderten Objekts** zeigt den UNIX-Pfad der Datei oder des Ordners an, bei dem ein Unterschied gefunden wurde. Der Pfad muss relativ zu dem Volume, das Sie zum Vergleich ausgewählt hatten, interpretiert werden.
- **Änderungen** gibt den exakten Typ der Veränderung an:
 - **A**: Die Zugriffssteuerungsliste (ACL) hat sich geändert.
 - **C**: Das Datum der Erstellung hat sich geändert.
 - **D**: Die Daten, die in dem Objekt gespeichert sind, haben sich verändert.
 - **G**: Der Gruppeneigentümer hat sich geändert.
 - **M**: Der Zeitpunkt der letzten Änderung (Modifikation) hat sich geändert.
 - **O**: Der Eigentümer hat sich geändert.
 - **P**: Die POSIX-Berechtigungen haben sich geändert.
 - **S**: Die Größe hat sich geändert.
 - **T**: Der Typ des Objekts hat sich geändert.
 - **X**: Die Erweiterten Attribute haben sich geändert.

- Falls das Objekt eine Datei ist, die geändert wurde, gibt die Spalte **Alte Größe** den Speicherplatzbedarf an, den diese Datei bei dem älteren der beiden gewählten Zeitpunkte benötigt hat.
- Gleichermäßen gibt die Spalte **Neue Größe** den Speicherplatzbedarf für den späteren der beiden gewählten Zeitpunkte an.

Falls Sie den Mauszeiger über einen Eintrag in der Spalte **Änderungen** setzen, zeigt TinkerTool System einen kurzen Erläuterungstext an, so dass Sie die Abkürzungen nicht auswendig lernen müssen.

Aus Effizienzgründen können die Einträge in der Tabelle nicht umsortiert werden. TinkerTool System zeigt diese in der Reihenfolge an, in der Time Machine sie beim Sichern verarbeitet. Über den Knopf **Sichern ...** können Sie einen aufbereiteten Bericht in Textform erstellen lassen, der in eine Datei gespeichert wird.

2.5.4 Arbeiten mit lokalen APFS-Schnappschüssen

Falls mindestens eines der Volumes, die Teil der Datensicherung sind, das moderne *Apple File System (APFS)* verwendet, schaltet Time Machine automatisch zusätzliche Funktionen ein:

- Jedesmal wenn ein Sicherungslauf stattfindet, legt Time Machine einen Schnappschuss für jedes APFS-Volume an, das zur Sicherung ansteht. Ein APFS-Schnappschuss stellt quasi ein eingefrorenes Abbild des Quell-Volumes dar, das angelegt wurde, als der Backup-Lauf begann. Auch wenn sich Dateien ändern während die Datensicherung läuft, stellt der Schnappschuss sicher, dass Time Machine nur ein unveränderliches Bild des Volumes „sieht“. Falls die Datensicherung später einmal zurückgeladen werden muss, wird das Ergebnis einen konsistenten Zustand des Volumes wiedergeben, ohne dass sich Dateien nur in einem vorübergehenden Zwischenstatus befinden.
- Jeder APFS-Schnappschuss wird vom Betriebssystem weiterhin auf dem entsprechenden Volume aufbewahrt, so lange dieses Volume genügend Speicherplatz hat. Der Schnappschuss ist während des Normalbetriebs unsichtbar und benötigt nur einen kleinen Betrag an zusätzlichem Speicherplatz. Er basiert auf der Strategie, die Blöcke eines Volumes, die von einer Datei belegt sind, niemals für neue Dateien wiederzuverwenden, sogar wenn die Datei gelöscht wurde oder sich der entsprechende Teil der Datei geändert hat.
- APFS-Schnappschüsse werden nicht nur dann angelegt, wenn die normalen Time Machine-Sicherungen laufen, das Betriebssystem legt sie auch an, wenn größere Änderungen im System erwartet werden, z.B. wenn ein Betriebssystem-Update zur Installation ansteht.
- Diese Schnappschüsse können als „Wiederherstellungspunkte“ verwendet werden, die es Ihnen erlauben, ein komplettes APFS-Volume sehr schnell wieder auf einen konsistenten Zustand in der Vergangenheit zu bringen. Dies wird von Time Machine erledigt (üblicherweise nach einem Start vom Wiederherstellungssystem aus), wobei das APFS-Volume selbst, nicht das Time Machine-Volume, als Quelle für die Wiederherstellung angegeben wird. Für weitere Informationen ziehen Sie bitte Apples offizielle Dokumentation zu macOS hinzu.

Dies heißt, dass ein APFS-Schnappschuss prinzipiell als lokaler Schnappschuss von Time Machine verwendet werden kann. Für die Nutzung solcher Schnappschüsse ist kein Zugriff auf das tatsächliche Time Machine-Sicherungs-Volume erforderlich.

Andere macOS-Bestandteile können die APFS-Schnappschussfunktion ebenso nutzen. Die Liste, die auf dem Tab **Lokale Schnappschüsse** angezeigt wird, berücksichtigt nur die APFS-Schnappschüsse, die von Time Machine genutzt werden. Wenn Sie mit der vollständigen Liste von APFS-Schnappschüssen arbeiten möchten, verwenden Sie bitte das Kapitel Die Einstellungskarte APFS (Abschnitt 3.7 auf Seite 228).

Es liegt im alleinigen Ermessen des Betriebssystems, wann APFS-Schnappschüsse angelegt oder entfernt werden. TinkerTool System gibt Ihnen jedoch zusätzliche manuelle Kontrolle über diese lokalen Schnappschüsse.

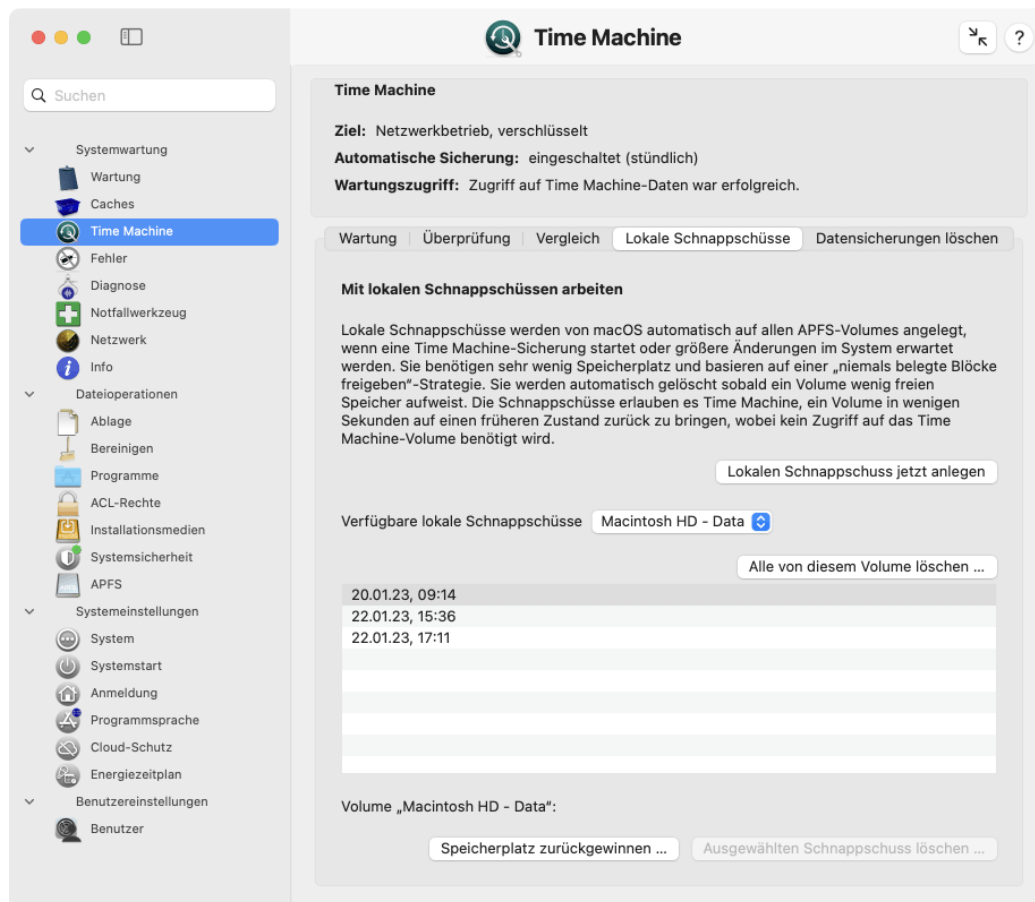


Abbildung 2.19: Arbeiten mit lokalen Schnappschüssen

- Sie können einen lokalen Schnappschuss sofort anlegen, wofür nur ein Knopfdruck nötig ist. Dies ist hilfreich, um einen wohldefinierten Wiederherstellungspunkt anzulegen, z.B. wenn Sie einen möglicherweise „gefährlichen“ Vorgang auf einem APFS-Volume ausprobieren möchten, der möglicherweise in naher Zukunft wieder rückgängig gemacht werden muss.
- Sie können einsehen, welche lokalen Schnappschüsse im Moment auf jedem APFS-Volume abgelegt sind.
- Sie können macOS dazu zwingen, seine lokalen Schnappschüsse sofort zu bereinigen, um den Zeitpunkt vorzuverlegen, an dem dies automatisch ablaufen würde.

Dies geschieht dadurch, dass Sie eine geplante freizugebende Menge von Speicherplatz angeben, die durch die Bereinigung zurückgewonnen werden soll. macOS behält so viele Schnappschüsse wie möglich bei, während es versucht, dieses Ziel zu erfüllen.

- Sie können lokale Schnappschüsse Ihrer Wahl löschen.

Um einen neuen lokalen Schnappschuss auf allen APFS-Volumes anzulegen, die Teil der Time Machine-Sicherung sind, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Lokale Schnappschüsse** auf der Karte **Time Machine**.
2. Drücken Sie den Knopf **Lokalen Schnappschuss jetzt anlegen**.

Das Anlegen eines lokalen Schnappschusses dauert typischerweise weniger als eine Minute.

Sie können alle Schnappschüsse über die Tabelle **Verfügbare lokale Schnappschüsse** auf der gleichen Karte einsehen. Die verfügbaren Zeitpunkte werden als einzelne Zeilen aufgelistet. Standardmäßig sehen Sie eine Liste für den gesamten Computer. Falls mehr als ein APFS-Volume genutzt wird, kann es aber interessant sein, die Liste der Schnappschüsse pro Volume anzuzeigen. Beachten Sie, dass die Menge der verfügbaren Schnappschüsse auf jedem Volume verschieden sein kann, da einige Volumes weniger freien Speicherplatz haben, so dass diese ihre Schnappschüsse früher bereinigen müssen, als andere. Um zwischen verschiedenen Volumes zu wechseln, verwenden Sie das Aufklappmenü über der Tabelle.

Um Speicherplatz auf einem bestimmte Volume wiederzugewinnen, wählen Sie das Volume mit dem Aufklappmenü über der Tabelle aus und drücken dann den Knopf **Speicherplatz zurückgewinnen**. TinkerTool System fragt in einem Dialogfenster, wie viele Bytes Sie mindestens zurückgewinnen möchten. Sie können einen niedrigen Wert (wie 1) angeben, um sicher zu stellen, dass nur die kleinstmögliche Zahl von Schnappschüssen gelöscht werden soll. Das Betriebssystem wird seine eigenen Standardverfahren verwenden, um automatisch diejenigen Schnappschüsse auszuwählen, die entfernt werden sollen. Am Ende des Vorgangs zeigt TinkerTool System eine Zusammenfassung an, wie viele Schnappschüsse verloren gegangen sind und wie viel Speicherplatz auf dem Volume frei geworden ist.

In manchen Fällen kann sich Time Machine entscheiden, den Aufräumvorgang für einige Zeit zu verschieben. In dieser besonderen Situation kann es sein, dass TinkerTool System sofort nach dem Anfordern einer Speicherwiedergewinnung nicht anzeigt, dass bereits Speicherplatz frei geworden ist.

Falls Sie so viel Speicher wie möglich von einem Volume freigeben möchten, wählen Sie das Volume bei **Verfügbare lokale Schnappschüsse** aus und betätigen Sie den Knopf **Alle von diesem Volume löschen**. Time Machine wird dies als dringende Anforderung verstehen, den Höchstbetrag an Speicherplatz wiederzugewinnen, der im Moment für lokale Schnappschüsse genutzt wird.

Um von Hand einen lokalen Schnappschuss zu löschen, wählen Sie diesen in der Tabelle aus und drücken den Knopf **Ausgewählten Schnappschuss löschen**

2.5.5 Löschen von Time Machine-Schnappschüssen

Als Teil des täglichen Ablaufs räumt Time Machine seine Sicherungen regelmäßig auf, falls notwendig jede Stunde. Nachdem ein Sicherungslauf stattgefunden hat, werden veraltete Sicherungsschnappschüsse von der Sicherungsplatte entfernt. Manchmal möchten Sie

vielleicht einen bestimmten Schnappschuss auch von Hand löschen, z.B. um Speicherplatz freizugeben. *Sie dürfen dies niemals über den macOS Finder machen. Dies könnte den Time Machine-Sicherungssatz und zusätzlich die Papierkorbfunktion des Finders beschädigen.* TinkerTool System bietet Ihnen einen sicheren Weg, eine Time Machine-Sicherung für einen bestimmten Zeitpunkt zu entfernen:

1. Öffnen Sie den Karteireiter **Datensicherungen löschen** auf der Karte **Time Machine**.
2. Wählen Sie den Schnappschuss, der gelöscht werden soll, mit dem Klappenmenü **Löschen** in der oberen Hälfte des Fensters aus.
3. Drücken Sie auf den Knopf **Löschen ...** daneben.

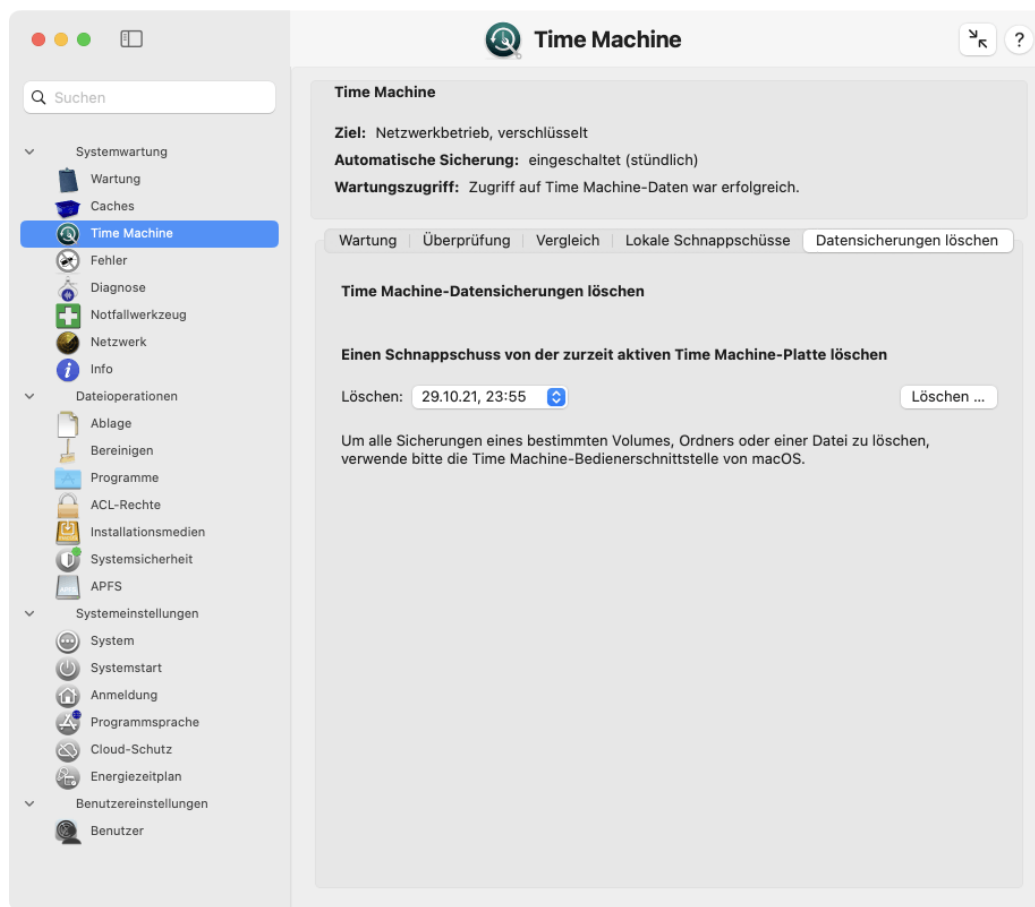


Abbildung 2.20: Löschen von Time Machine-Sicherungsdaten

2.6 Die Einstellungskarte Fehler

2.6.1 Beheben von Problemen mit der Softwareaktualisierung von macOS

Unter bestimmten Umständen, die von Ihrem lokalen Netz, Ihrem Internet-Dienstanbieter und vom Land, in dem Sie sich aufhalten, abhängen können, arbeitet die Funktion zum

Software-Update von macOS nicht immer so fehlerfrei wie man es erwarten kann. TinkerTool System kann dabei helfen, typische Probleme durch einzelne Mausklicks zu beheben.

Was ist die Softwareaktualisierung von macOS?

macOS verwendet zwei vollständig voneinander getrennte technische Funktionen um Softwareprodukte aktuell zu halten: Das Betriebssystem selbst und zusätzliche Komponenten, die als Erweiterungen des Betriebssystems angesehen werden können, werden durch eine Funktion aktualisiert, die sich *macOS-Software-Update* nennt. Sie basiert auf einer Architektur, die dem Abonnieren eines Nachrichtenkanals ähnelt, der macOS über die verfügbaren Updates informiert. Falls Sie an einem der *Beta-Software-Programme* teilnehmen, die Apple anbietet, kann der Standardnachrichtenkanal auf einen anderen umgelenkt werden, der zusätzliche Betaproducte enthält und der Allgemeinheit nicht zur Verfügung steht.

Für Apps, die aus dem App Store heruntergeladen wurden, egal ob diese von Apple oder von einem Drittanbieter entwickelt wurden, verwendet macOS einen anderen Mechanismus, der mit dem App Store selbst verbunden ist. Diese Funktion wird *App-Updates* genannt.

App-Updates werden im Programm **App Store** präsentiert, Unterpunkt **Updates**. Dagegen werden macOS-Software-Updates in **Systemeinstellungen** aufgelistet, Einstellungskarte **Allgemein > Softwareupdate**.

Apple liefert neue Betriebssysteme in Form einer App aus, die in Wirklichkeit ein Installationsprogramm für das jeweilige System ist. Das heißt, ein *Upgrade* von macOS (der Wechsel vom laufenden Betriebssystem zu einer neuen Generation mit einer anderen vorderen Versionsnummer) wird als App aus dem App Store geliefert, während jedes *Update* (Produktpflege, bei der sich nur die hintere Versionsnummer ändert) über die Funktion Software-Update ausgeliefert wird.

Eine hängende Suche nach Aktualisierungen zurücksetzen

Bei einigen der macOS-Updates, die Apple ab 2022 veröffentlicht hat, kann es passieren, dass die Funktion zum Softwareupdate nicht mehr richtig funktioniert. Wenn Sie nach den neuesten Aktualisierungen auf der Karte **Allgemein > Softwareupdate** in **Systemeinstellungen** suchen, dreht sich die Fortschrittsanzeige möglicherweise endlos und es findet keine tatsächliche Suche nach Updates statt. Ein ähnlicher Effekt tritt auf, wenn Sie den entsprechenden Suchbefehl im Terminal aufrufen. Dies kann ein kritisches Problem darstellen, da es die Möglichkeit blockiert, wichtige Sicherheits-Updates herunterzuladen. TinkerTool System kann die macOS-Komponente für Softwareupdates zurücksetzen, was dieses Problem üblicherweise sofort behebt. Führen Sie die folgenden Schritte aus, falls Ihre Version von macOS von diesem Problem betroffen ist:

1. Beenden Sie **Systemeinstellungen** oder den Befehl **softwareupdate** im Terminal, falls dieses Programme gerade laufen sollten.
2. Öffnen Sie in TinkerTool System den Unterpunkt **Softwareaktualisierung** auf der Karte **Fehler**.
3. Drücken Sie den Knopf **Laufenden Vorgang zurücksetzen**.

Wenn das Zurücksetzen erfolgreich war, können Sie sofort eine erneute Suche nach macOS-Updates starten.

Apple hat damit begonnen, diese Art von Wartung in allen Betriebssystemversionen zu sperren, die seit März 2024 veröffentlicht wurden. Falls Sie davon betroffen sein sollten, ist es nur dann möglich, diese Funktion zu nutzen, nachdem Sie den Systemintegritätsschutz abgeschaltet haben (eine Anleitung steht im entsprechenden Abschnitt unter Grundlegende Bedienungshinweise (Abschnitt 1.3 auf Seite 8) bereit.)

Erzwingen einer sofortigen Synchronisation der Liste verfügbarer Updates

Es kann passieren, dass macOS die Verfügbarkeit eines Updates nicht sofort bemerkt. Es kann eine Verzögerung von bis zu zwei Wochen auftreten, bevor ein Eintrag endlich auf dem lokalen System erscheint. Falls Sie aus einer anderen Quelle, z.B. einem Presseartikel oder einer Nachrichtenwebseite, erfahren haben, dass eine Aktualisierung verfügbar sein muss, die von Ihrem Computer aber noch nicht automatisch aufgelistet wurde, können Sie Ihren Mac zwingen, eine Verbindung zu Apple aufzubauen und die neueste Liste verfügbarer Updates sofort zu beziehen. Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Softwareaktualisierung** auf der Karte **Fehler**.
2. Drücken Sie den Knopf **Liste synchronisieren**.

Danach stellt macOS den Kontakt mit Apple über Ihre Internet-Verbindung her. TinkerTool System zeigt ein kleines Statusfenster, das live wiedergibt, was das Betriebssystem gerade macht. Das Beziehen und Auswerten der aktuellen Software-Liste kann mehrere Minuten in Anspruch nehmen. Falls neue Updates erhältlich sind, zeigt das Programm Systemeinstellungen diese automatisch an, sobald der Synchronisationsvorgang abgeschlossen ist.

Entfernen ungeeigneter Update-Benachrichtigungen

In einigen Spezialfällen kann das Gegenteil des Problems auftreten, das im vorigen Abschnitt behandelt wurde: macOS listet möglicherweise verfügbare Updates auf, an denen Sie kein Interesse mehr haben, es sind also „zu viele“ Einträge in der Liste der Aktualisierungen. Dies kann kurz nach einem Wechsel Ihrer persönlichen Quelle für Software-Aktualisierungen auftreten, beispielsweise wenn Sie sich dazu entschieden haben, nicht mehr länger an einem der Beta-Programme teilzunehmen. In diesem speziellen Fall zeigt das Programm Systemeinstellungen möglicherweise immer noch Beta-Updates an, obwohl Sie diese nicht mehr sehen möchten.

Um in einem solchen Fall die Liste der verfügbaren Aktualisierungen zu bereinigen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Softwareaktualisierung** auf der Karte **Fehler**.
2. Drücken Sie den Knopf **Update-Katalog bereinigen**.

Anwesenheit eines Cache-Servers prüfen

Wenn Sie viele Apple-Geräte in Ihrem lokalen Netz haben, kann es den Zugriff auf Updates enorm beschleunigen, wenn Sie einen *Inhaltscaching-Server* in Ihrem Netz einrichten. Hierzu müssen Sie die entsprechende Funktion nur auf einem Mac in Ihrem Netz einschalten, der möglichst kontinuierlich eingeschaltet ist. Der Server beobachtet den Datenverkehr für Updates und speichert alle heruntergeladenen Daten zwischen. Die anderen Computer im Netz stellen die Anwesenheit des Inhaltscaching-Servers fest und können Updates

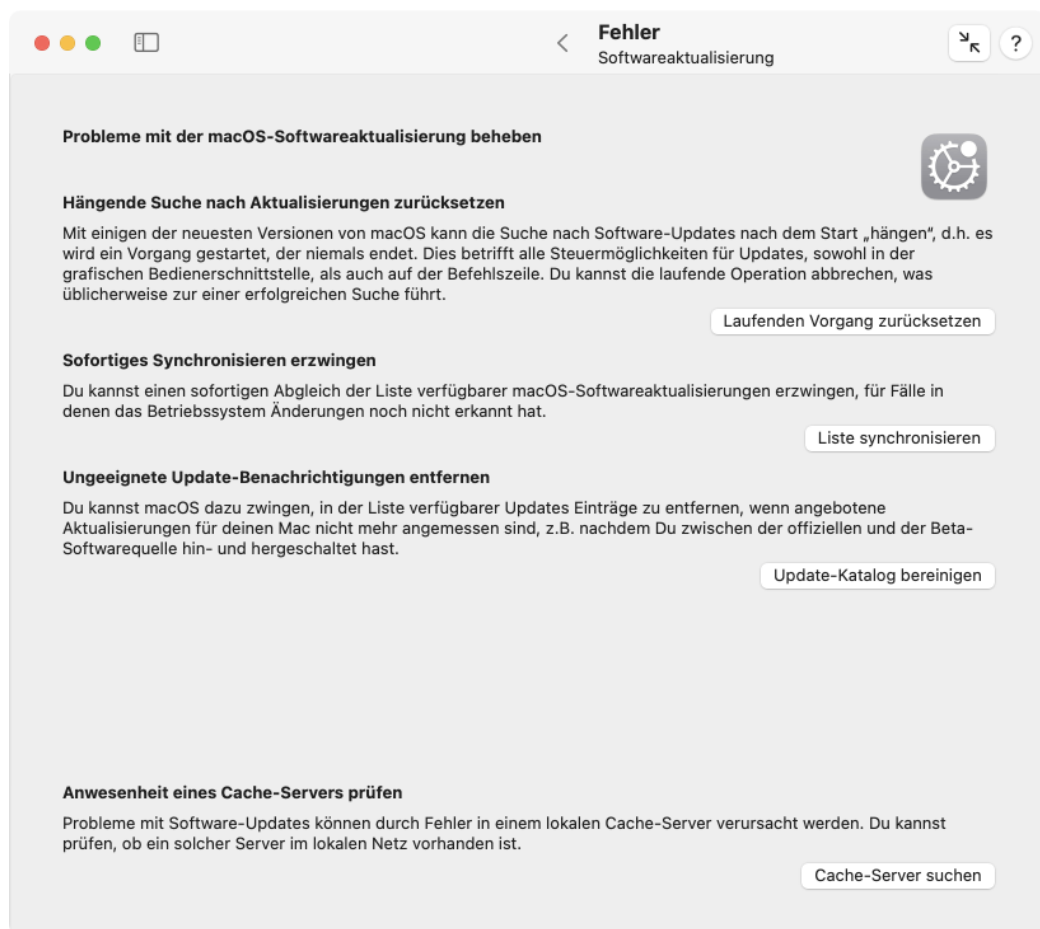


Abbildung 2.21: Beheben von Problemen mit der Softwareaktualisierung von macOS

nun über eine schnelle lokale Leitung von ihm laden. Die Update-Daten müssen nicht mehr erneut für jeden Computer über die langsamere Anbindung ins Internet heruntergeladen werden. Darüberhinaus kann der Inhaltscaching-Server auf Wunsch auch Lese- und Schreibzugriffe auf iCloud-Dienste beschleunigen, indem er dafür ebenso Daten lokal zwischenspeichert. Für sehr große Netze können auch mehrere Inhaltscaching-Server gleichzeitig eingesetzt werden.

Alle Aspekte eines Inhaltscaching-Servers arbeiten vollautomatisch. Außerdem dem Einschalten des Dienstes auf dem dafür ausgewählten Computer und der Auswahl der Optionen, welche und wie viele Daten maximal zwischengespeichert werden sollen, sind keine weiteren Aktionen erforderlich. Clients müssen nicht eingerichtet werden, sondern nutzen den Dienst automatisch, sobald er vorhanden ist.

Für bestimmte Kombinationen von Betriebssystemversionen der Clients und der Betriebssystemversion des Servers sind allerdings Fehler in macOS bekannt, in denen die Suche nach Updates nicht korrekt funktioniert, bzw. bestimmte Update-Pakete gar nicht oder stark verspätet angeboten werden. Aus diesem Grund ist es bei der Fehlerbehebung im Zusammenhang mit der Softwareaktualisierung erforderlich, zu wissen, ob sich ein oder mehrere Inhaltscaching-Server im Netz befinden. Dies ist nicht immer klar. Zum Beispiel könnte ein Benutzer eines mobilen Macs die Funktion Inhaltscaching-Server versehentlich (oder sogar böswillig) eingeschaltet haben und damit Probleme auslösen, wenn er sich im lokalen Netz aufhält.

TinkerTool System kann prüfen, ob Inhaltscaching-Server im lokalen Netz vorhanden sind und welcher davon im Moment bevorzugt von Ihrem Mac zum Beziehen von Updates verwendet wird. Die IP-Adressen eines Servers und die Liste der Detaildienste, die der Cache anbietet, können ebenso bestimmt werden.

1. Öffnen Sie den Unterpunkt **Softwareaktualisierung** auf der Karte **Fehler**.
2. Drücken Sie den Knopf **Cache-Server suchen**.

Sind ein oder mehrere Server vorhanden, werden diese in einem eigenen Dialogfenster aufgelistet. Das Fenster enthält folgende Daten:

- **Implementationsversion des Clients:** die Versionsnummer der Software, die die gerade laufende Version von macOS verwendet, um mit Inhaltscaching zu arbeiten
- **Öffentliche IPv4-Adresse:** die Netzwerkadresse, die vom Client im Moment beim Zugriff auf das Internet verwendet wird

In einer Tabelle sind alle lokalen Inhaltscaching-Server mit einer Kurzbeschreibung aufgeführt. Nach Auswahl einer Zeile erscheinen im unteren Bereich des Fensters die Details zu jedem Server:

- **Identifikation:** eine *UUID*-Angabe, mit der jeder Server weltweit eindeutig identifiziert wird
- **Netzwerkadresse und Port:** die IPv4-Adresse des Server im lokalen Netz und die Port-Nummer zum Zugriff auf den Cache-Dienst
- **Server ist bevorzugt:** eine Markierung, die angibt, ob dieser Server anderen vorhandenen Servern bevorzugt werden soll
- **Auswahlrang:** die Priorität, mit der auf diesen Server zugegriffen wird, falls mehrere Server im Netz vorhanden sind
- **Verbindungs-Timeout:** die Zeit, nach der ein Zugriffsversuch abgebrochen wird

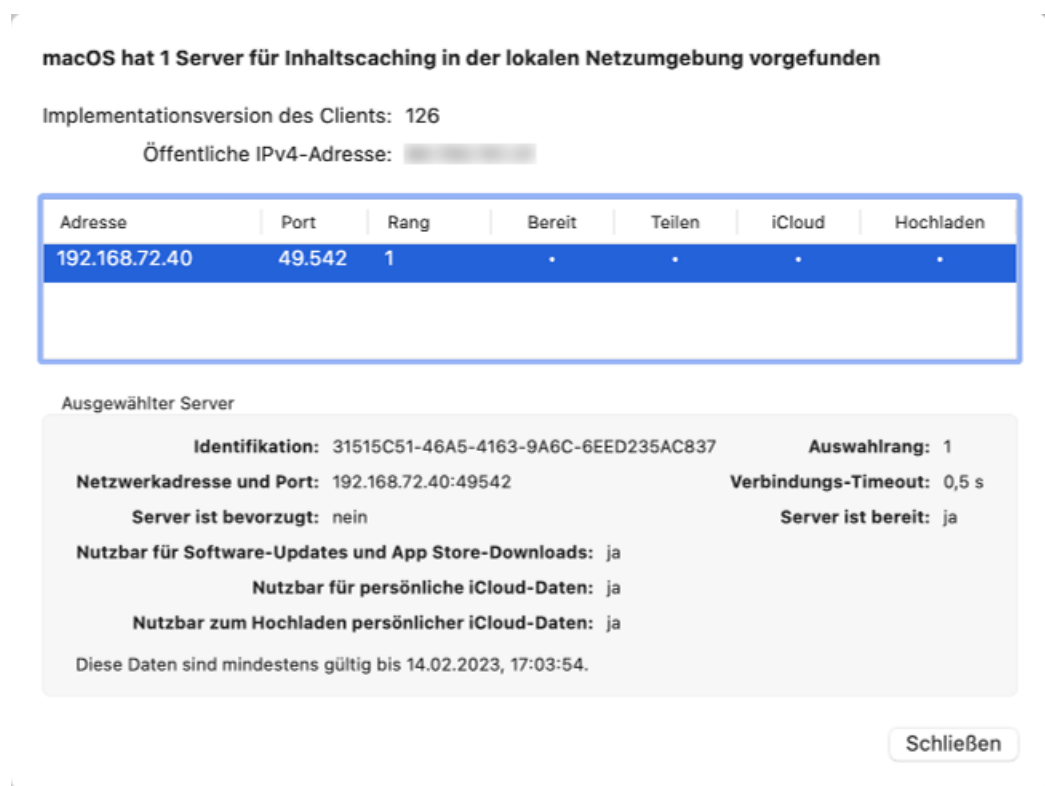


Abbildung 2.22: Sind Inhaltscaching-Server vorhanden, werden diese in einer Übersicht dargestellt

- **Server ist bereit:** eine Statusangabe, ob dieser Server im Moment betriebsbereit ist
- **Nutzbar für Software-Updates und App-Store-Downloads:** eine Statusangabe, ob dieser Server Softwareaktualisierungen und App-Updates zwischenspeichert
- **Nutzbar für persönliche iCloud-Daten:** eine Statusangabe, ob dieser Server zum Lesen von iCloud-Daten von Benutzern im lokalen Netz verwendet werden kann
- **Nutzbar zum Hochladen persönlicher iCloud-Daten:** eine Statusangabe, ob dieser Server zum Schreiben von iCloud-Daten von Benutzern im lokalen Netz verwendet werden kann

Zusätzlich ist eine Angabe aufgeführt, bis wann dieser Mac die angegebenen Daten als gültig ansieht. Spätestens zu diesem Zeitpunkt werden die Informationen wieder aufgefrischt.

2.6.2 App Store-Aktualisierungen

Das App Store-Programm führt ab macOS 11 ein ärgerliches Problem ein, bei dem Benutzer Update-Benachrichtigungen für Apps erhalten, die sie bereits aktualisiert haben, oft schon vor mehreren Monaten. Dies kann passieren, wenn Sie Ihren Mac mit mehreren Benutzern verwenden und nur einer von ihnen üblicherweise Aktualisierungen für Apps herunterlädt, oder falls Sie mehrere Macs haben, aber den App Store nur auf einem verwenden und dann die Apps von Hand auf die anderen kopieren.

Ein Zurücksetzen der App Store-Daten für den betroffenen Benutzer kann dieses Problem üblicherweise beheben. TinkerTool System bietet es an, entweder den aktuellen Benutzer-Account oder alle aktiven Benutzer-Accounts des Mac zurückzusetzen. In diesem Zusammenhang bezieht sich ein „aktiver“ Account auf einen Benutzer, der einen Privatordner an der Standardposition auf dem lokalen Mac hat (üblicherweise im Ordner `/Users`, bzw. **Benutzer:innen**).

Der Rücksetzvorgang löscht unter anderem die Übersichtsseite des App Store, die die kürzlich vorgenommenen Updates auflistet, die dieser Benutzer heruntergeladen hat. Die Liste der Käufe oder irgendwelche anderen Daten des Benutzers, der gerade im App Store angemeldet ist, sind jedoch nicht betroffen.

Um das App Store-Programm zurückzusetzen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **App Store** auf der Karte **Fehler**.
2. Verwenden Sie die Knöpfe bei **Benutzer-Accounts auswählen um den App Store zurückzusetzen**, um einzustellen, ob Sie das Rücksetzen für den aktuellen Benutzer oder für alle Benutzer dieses Mac ausführen möchten.
3. Drücken Sie den Knopf **Zurücksetzen**.

Sie sollten das App Store-Programm beenden, bevor Sie das Rücksetzen laufen lassen, und Sie sollten ebenso sicherstellen, dass im Hintergrund keine Lade- oder Aktualisierungsvorgänge aus dem App Store mehr laufen.

2.6.3 Xcode-Schlüsselbunde

Wenn Sie in den letzten Jahren im Programm Xcode versucht haben, Ihre geschützten, persönlichen Entwicklerdaten, d.h. die Apple-ID mit den zugehörigen Sicherheitszertifikaten zum digitalen Signieren von Programmen und Installern zu importieren oder exportieren, zum Beispiel um diese Daten auf einem zweiten Computer mit Xcode verwenden zu können, werden Sie danach ein fehlerhaftes Verhalten des Programms *Schlüsselbundverwaltung* bemerkt haben:

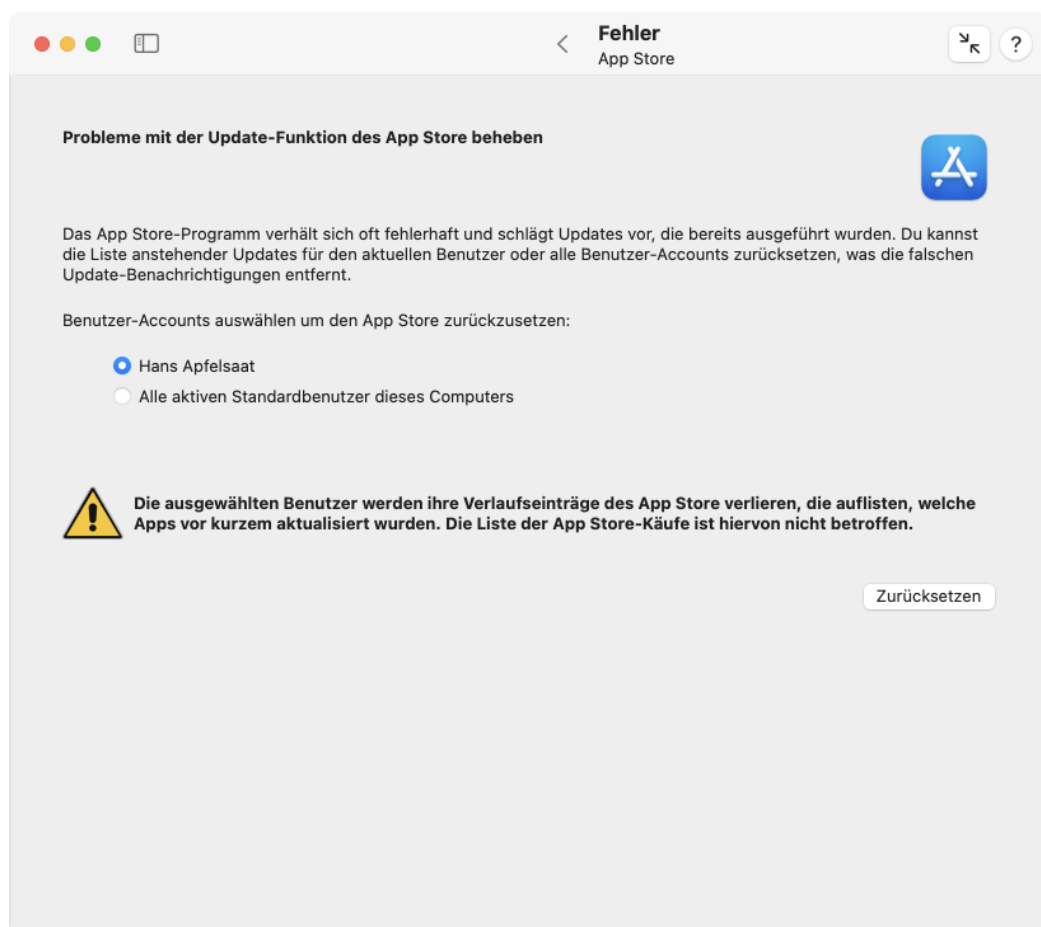


Abbildung 2.23: Das Zurücksetzen des App Store-Programms kann ungültige Update-Benachrichtigungen entfernen

- Es werden ein oder mehrere Schlüsselbunde mit dem Namensmuster **accountsKeychain...** im Programm aufgelistet. Diese Schlüsselbunde lassen sich weder nutzen, noch löschen.
- Je nach Version von macOS läuft das Programm Schlüsselbundverwaltung bei einigen Funktionen deutlich langsamer.

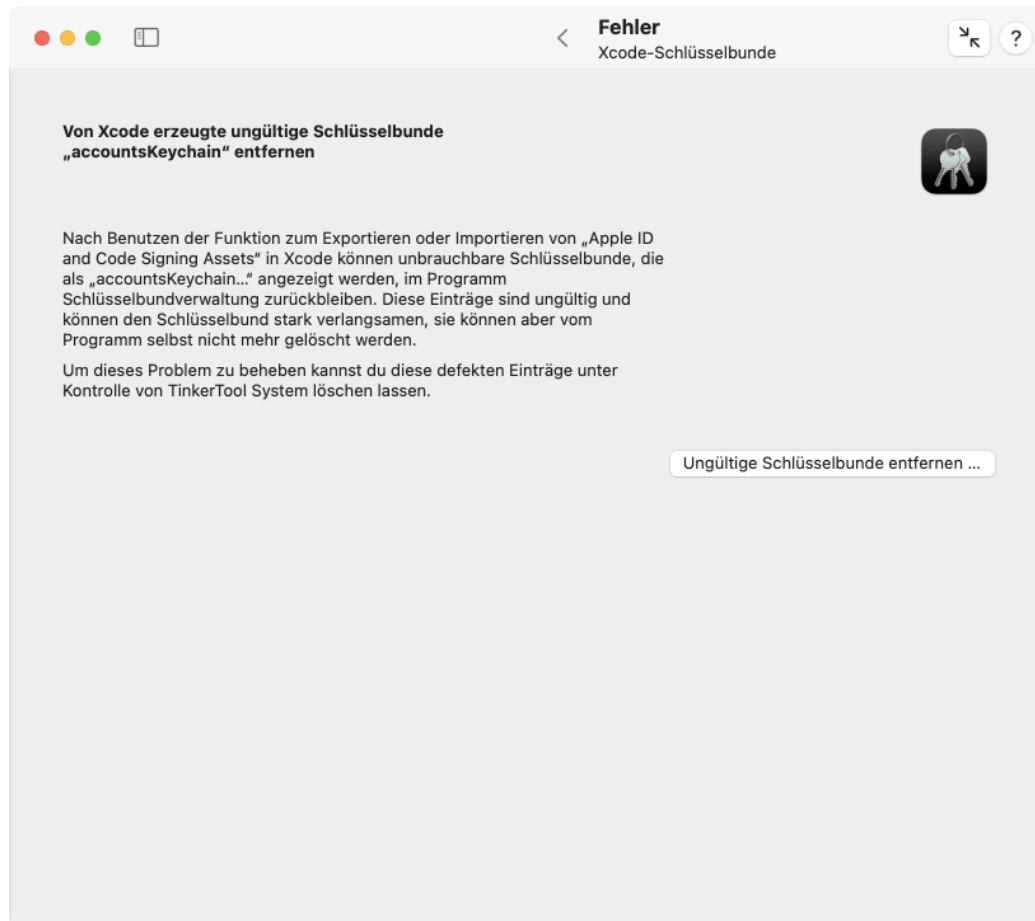


Abbildung 2.24: Von Xcode erstellte ungültige Schlüsselbunde können entfernt werden

In Xcode heißen die betreffenden Funktionen **Export**, bzw. **Import Apple ID and Code Signing Assets**. TinkerTool System kann prüfen, ob diese Funktionen die angesprochenen Fehler in der Schlüsselbundverwaltung ausgelöst haben. In dem Fall reicht ein einzelner Mausklick, um das Problem automatisch zu beheben. Die ungültigen Schlüsselbunde werden gelöscht:

1. Öffnen Sie den Unterpunkt **Xcode-Schlüsselbunde** auf der Karte **Fehler**.
2. Betätigen Sie die Schaltfläche **Ungültige Schlüsselbunde entfernen**.

2.6.4 Hintergrundobjekte

Mit macOS 13 Ventura hat Apple eine stark überarbeitete Fassung des Dienste-Managements in das Betriebssystem eingebaut. Die wichtigste Änderung ist, dass Hilfsprogramme, die

für „große“ Programme Dienste erbringen, jetzt nicht mehr in zentralen Ordnern des Betriebssystems (wie z.B. */Library/PrivilegedHelperTools/* für privilegierte Dienstprogramme) abgelegt werden müssen, sondern im zugehörigen Hauptprogramm liegen bleiben können. Dies hat den Vorteil, dass für neue Programme nichts mehr installiert oder deinstalliert werden muss. Wurde das Hauptprogramm auf den Mac kopiert, ist automatisch auch dessen eingebettetes Hilfsprogramm vorhanden, ohne dass es speziell eingerichtet werden musste. Wird das Programm später wieder gelöscht, wird damit automatisch auch das eingebettete Hilfsprogramm wieder entfernt. Dazu muss macOS im Hintergrund beobachten, ob die vorhandenen Programme Hilfsprogramme enthalten, die Dienste erbringen können. Anhand von Beschreibungsdateien, die sich versteckt im Hauptprogramm befinden, kann die Art jedes Dienstes festgestellt werden.

Sowohl diese neuen Hilfsprogramme, als auch die alten, wenn diese immer noch mit Betriebssystemen vor macOS 13 kompatibel sein möchten und deshalb die moderne Art der Einbettung ins Hauptprogramm noch nicht verwenden können, werden von Apple *Hintergrundobjekte* genannt. Alle erkannten Hilfsprogramme werden auf der Karte **Anmeldeobjekte** des Programms **Systemeinstellungen** aufgeführt, unter der Überschrift **Im Hintergrund erlauben**.

Der neue Begriff „Hintergrundobjekt“ und die Art der Darstellung sind für Benutzer leider sehr verwirrend. Es entsteht der falsche Eindruck, die aufgelisteten Objekte wären Programme, die macOS in jedem Fall automatisch starten würde. Hinzu kommt, dass auch die kurze Erklärung, die auf der Karte **Anmeldeobjekte** gegeben wird, die gleiche falsche Definition liefert.

In Wirklichkeit sind „Hintergrundobjekte“ nur die *Erlaubnis*, dass macOS ein Hilfsprogramm starten *darf*, falls das Hauptprogramm die Dienste seines Hilfsprogramms anfordern würde. Das kann im Einzelfall tatsächlich bedeuten, dass ein Hilfsprogramm von macOS bei jedem Systemstart automatisch gestartet wird, nämlich dann, wenn dies aufgrund der Funktion des Hilfsprogramms sinnvoll ist. Es kann aber genau so gut bedeuten, dass ein Hilfsprogramm niemals gestartet wird, z.B. weil der Benutzer dessen Dienste gar nicht benötigt. Unter welchen Bedingungen ein Hilfsprogramm gestartet werden soll, gibt das zugehörige Hauptprogramm in einer Beschreibung des Hilfsprogramms an.

Neben der irreführenden Beschreibung, was ein Hintergrundobjekt tatsächlich ist, kommt hinzu, dass das neue Dienste-Management in macOS Ventura alles andere als korrekt und zuverlässig arbeitet. Es sind eine große Menge interner Defekte und genereller Konstruktionsfehler vorhanden. Unter anderem gibt es folgende Probleme:

- Der Name eines Objekts wird oft falsch bestimmt und für verschiedene Benutzer unterschiedlich angezeigt.
- Das zugehörige Hauptprogramm eines Hintergrundobjekts kann oft nicht ermittelt werden.
- In manchen Fällen werden Objekte unter dem Namen des Software-Entwicklers in einer Gruppe zusammengefasst, für den Apple eines der zugehörigen Hauptprogramme beglaubigt („notarisiert“) hat. Dies ergibt keinen Sinn, da der Benutzer nun Objekte nicht mehr einzeln prüfen und abschalten kann.
- In vielen Fällen kann der Name des Software-Entwicklers nicht bestimmt werden.
- Der Name eines Software-Entwicklers erlaubt es in vielen Fällen nicht, darauf zu schließen, um welches Programm es sich handeln könnte.
- In manchen Fällen ruft ein Hauptprogramm ein Hilfsprogramm auf, das fest zum Lieferumfang von macOS gehört. Systemeinstellungen ist nicht in der Lage, „Apple“ als Entwickler anzuzeigen.

- Es wird nicht sauber unterschieden, ob der Name des Hilfsprogramms oder der Name des zugehörigen Hauptprogramms angezeigt wird.
- Es wird in manchen Fällen ein Knopf mit einem Info-Symbol angezeigt, um den Ort eines Hilfsprogramms ermitteln zu können. Dieser Knopf hat oft keine Funktion.
- In Fällen, in denen die Ortsangabe eines Hilfsprogramms funktioniert, kann der Benutzer dazu verleitet werden, das Hilfsprogramm einfach zu löschen. Das Löschen kann jedoch zu erheblichen Schäden im System führen.
- Der Hinweis, dass ein neu erkanntes Hintergrundobjekt genehmigt werden soll, erscheint oft viel zu spät. Manchmal erscheint er erst nach dem nächsten Neustart des Computers.
- Benutzer, die keinen lokalen Benutzer-Account, sondern einen Netzwerk-Account verwenden, können Hintergrundobjekte nicht genehmigen.
- Auch wenn der Benutzer ein Hintergrundobjekt genehmigt, startet macOS das zugehörige Hilfsprogramm oft nicht, selbst wenn das Hauptprogramm es dringend benötigt. Ein Neustart des Computers ist erforderlich.
- In manchen Fällen funktioniert das Genehmigen eines Hintergrundobjekts nicht dauerhaft. Nach jedem Neustart des Computers erhält der Benutzer Anfragen für alle vorhandenen Hintergrundobjekte erneut, oft mit Dutzenden von Benachrichtigungen.

Diese vielen Fehler und Konstruktionsmängel, die in den verschiedenen Versionen von macOS 13 unterschiedlich auftreten, kann TinkerTool System nicht grundsätzlich beheben, es kann jedoch zwei Funktionen anbieten, um in der Praxis zu einer brauchbaren Lösung zu kommen:

Sie können zum einen macOS dazu zwingen, das komplette Management von Hintergrundobjekten noch einmal zu löschen und mit der gerade laufenden Version noch einmal neu aufzubauen. Manche Mängel sind danach für einige Zeit behoben. Zum anderen können Sie eine Liste von Hintergrundobjekten von TinkerTool System erstellen lassen. Es versucht dabei, die Liste von macOS zu übernehmen, aber sie auf fehlerfreie Art darzustellen. Das kann dabei helfen, zu verstehen, warum macOS ein bestimmtes Hilfsprogramm als Hintergrundobjekt ansieht und was mit den oft zweifelhaften Einträgen in den Systemeinstellungen tatsächlich gemeint ist.

Wie oben erläutert, sind Hintergrundobjekte in Wirklichkeit Benutzereinstellungen, die steuern, welche Hilfsprogramme für Ihren Benutzer-Account bei Bedarf gestartet werden dürfen. Die Liste der Hintergrundobjekte kann deshalb für jeden Benutzer unterschiedlich sein.

Führen Sie die folgenden Schritte durch, um das Dienst-Management für Hintergrundobjekte in macOS zurückzusetzen:

1. Stellen Sie sicher, dass Sie den Computer neu starten können.
2. Öffnen Sie den Unterpunkt **Hintergrundobjekte** auf der Karte **Fehler**.
3. Betätigen Sie die Schaltfläche „**Hintergrundobjekte**“ **zurücksetzen**.
4. Folgen Sie den Anweisungen des Programms. Dabei wird TinkerTool System den Computer neu starten.

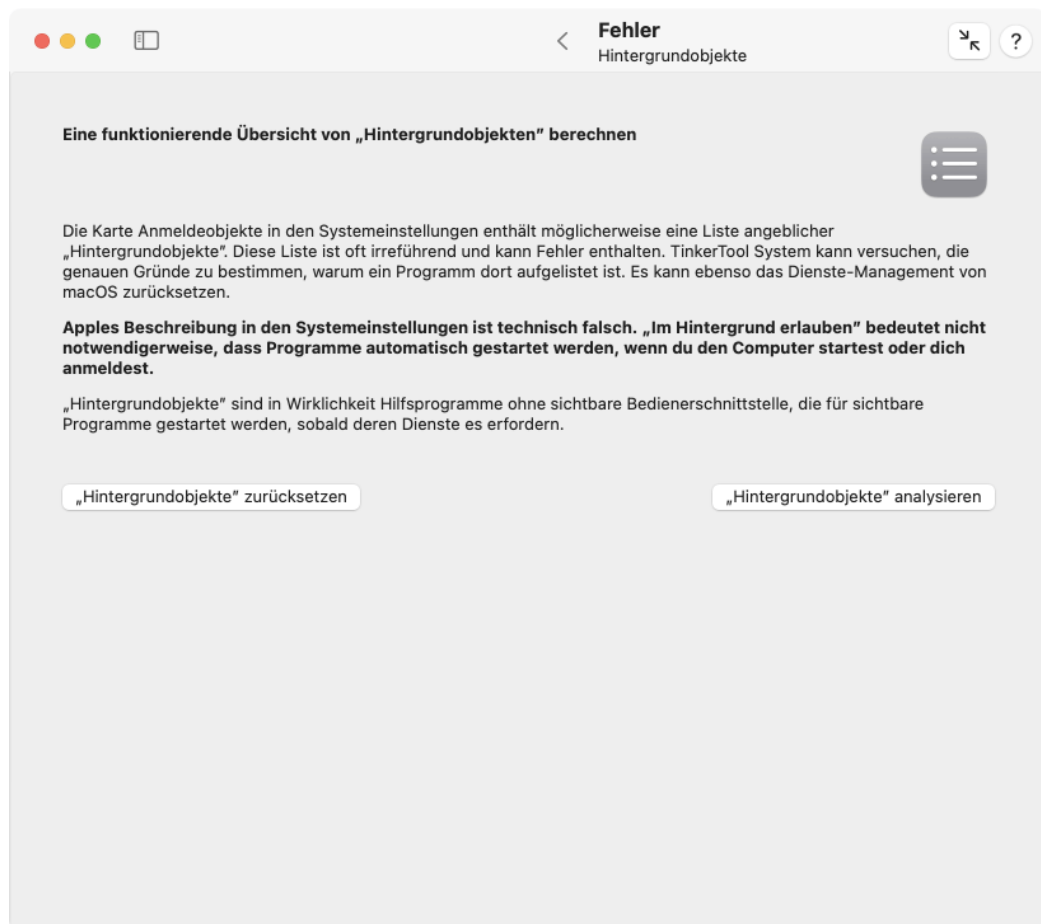


Abbildung 2.25: TinkerTool System hilft dabei, Probleme mit sogenannten „Hintergrundobjekten“ zu lösen und Apples mangelhafte Anzeige der Objekte besser zu verstehen

5. Melden Sie sich unter dem gleichen Benutzer-Account wieder am Computer an.
6. TinkerTool System startet automatisch erneut und bestätigt, dass das Rücksetzen abgeschlossen ist.

Führen Sie die folgenden Schritte durch, um die Liste der Hintergrundobjekte von TinkerTool System analysieren zu lassen. Das Programm zeigt danach eine ähnliche Liste so fehlerfrei wie möglich an. Sie können diese Liste mit der Liste vergleichen, die macOS in den Systemeinstellungen anzeigt.

1. Öffnen Sie den Unterpunkt **Hintergrundobjekte** auf der Karte **Fehler**.
2. Betätigen Sie die Schaltfläche „**Hintergrundobjekte**“ analysieren.

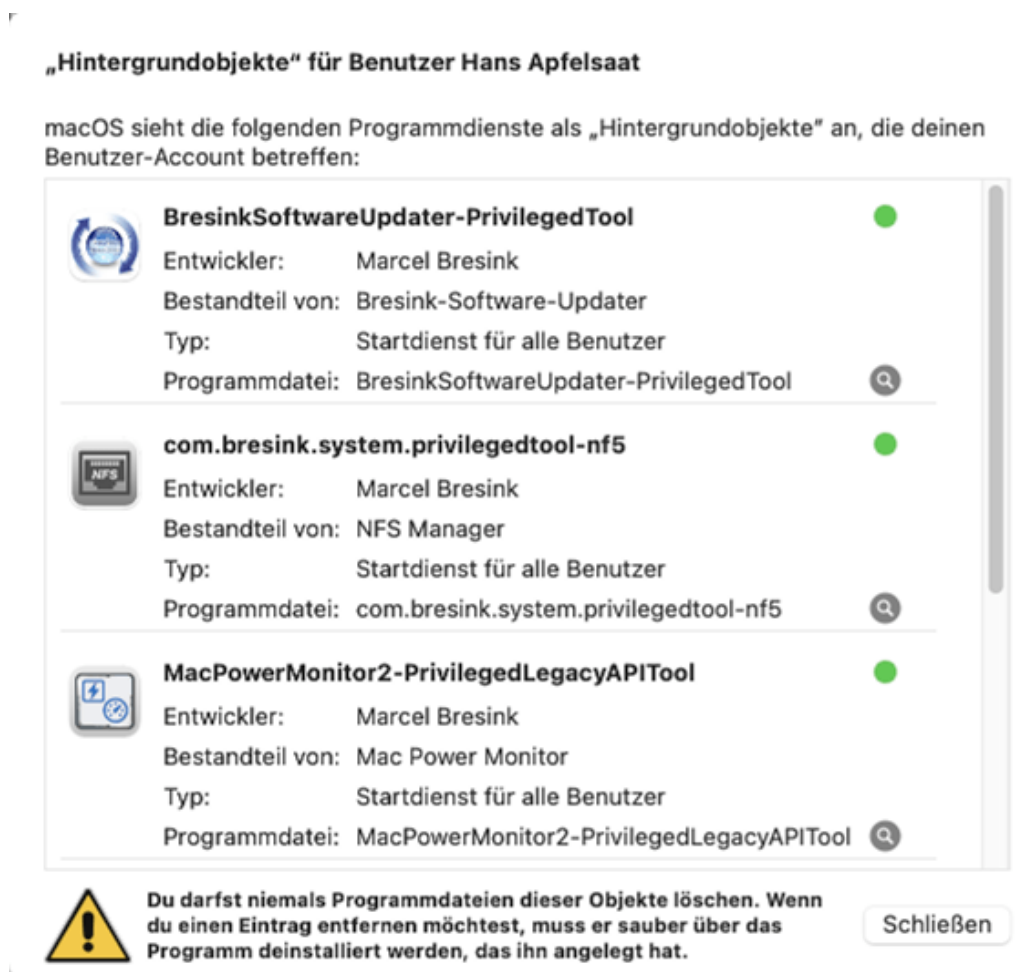


Abbildung 2.26: Die Liste der von macOS verwalteten Hintergrundobjekte kann verständlicher und mit so wenig Fehlern wie möglich angezeigt werden

Zu jedem Eintrag eines Hintergrundobjekts erhalten Sie die folgenden Informationen:

- ein Symbol und den Namen, unter dem das Objekt geführt wird
- eine Statusanzeige, ob das Hilfsprogramm bei Bedarf gestartet werden darf (grün), bzw. ob Sie den Start nicht genehmigen (rot)

- **Entwickler:** der Name des Entwicklers dieses Programms, falls dieser bestimmt werden kann
- **Bestandteil von:** der Name des Hauptprogramms, zu dem dieses Hilfsprogramm wahrscheinlich gehört. Bei älteren Programmen, die noch nicht an macOS 13 oder höher angepasst sind, ist es technisch nicht machbar, dies in jedem Fall exakt zu ermitteln.
- **Typ:** die Art des Hilfsprogramms, das gestartet wird (siehe unten)
- **Programmdatei:** der tatsächliche Dateiname des Hilfsprogramms, das gestartet wird
- ein Knopf zur Anzeige der Programmdatei im Finder

TinkerTool System unterscheidet zwischen den folgenden Typen von Hintergrundobjekten:

- **Startdienst für alle Benutzer:** das Hilfsprogramm darf wenn nötig gestartet werden, sobald macOS hochgefahren ist
- **Anmeldedienst für alle Benutzer:** das Hilfsprogramm darf wenn nötig gestartet werden, sobald sich irgendein Benutzer bei macOS angemeldet hat
- **Anmeldedienst für dich:** das Hilfsprogramm darf wenn nötig gestartet werden, sobald sich Ihr eigener Benutzer-Account bei macOS angemeldet hat
- **Eingebetteter Startdienst:** das Hilfsprogramm befindet sich im Hauptprogramm und darf wenn nötig gestartet werden, sobald macOS hochgefahren ist
- **Eingebetteter Anmeldedienst:** das Hilfsprogramm befindet sich im Hauptprogramm und darf wenn nötig gestartet werden, sobald sich irgendein Benutzer bei macOS angemeldet hat
- **Eingebettetes verstecktes Anmeldeobjekt:** das Hilfsprogramm befindet sich im Hauptprogramm und wird auf jeden Fall gestartet, sobald sich Ihr eigener Benutzer-Account bei macOS angemeldet hat. Es ähnelt dabei einem Anmeldeobjekt, wird aber vom zugehörigen Hauptprogramm und nicht in den sichtbaren Benutzereinstellungen eingerichtet.

Wenn Sie nicht den genauen Zweck eines Hintergrundobjekts kennen, ist es nicht empfehlenswert, den Start in den Systemeinstellungen zu sperren. Dies entspricht dem Verhalten aller macOS-Fassungen vor Version 13. Manche Hauptprogramme können nicht mehr arbeiten, wenn Sie deren Hilfsprogramme blockieren.



Warnung: Sie dürfen niemals die Programmdatei eines Hintergrundobjekts löschen. Bei eingebetteten Hilfsprogrammen wird hierbei das Hauptprogramm zerstört. Bei älteren Diensten kann dies dazu führen, dass macOS alle 10 Sekunden nach dem fehlenden Programm sucht. Dies führt dauerhaft zu zahlreichen Protokolleinträgen und Performance-Problemen. Falls Sie einen Eintrag für ein Hintergrundobjekt tatsächlich löschen möchten, müssen Sie in der Liste (bei **Bestandteil von**) prüfen, zu welchem Hauptprogramm es gehört. In der Dokumentation des Hauptprogramms finden Sie in der Regel Hinweise, wie Sie entweder nur das Hilfsprogramm, oder die komplette Software (Hauptprogramm und Hilfsprogramm) sauber vom Computer deinstallieren können.

2.6.5 Probleme mit automatischer Zeitsynchronisation beheben

In neueren Versionen von macOS gibt es einen bekannten Konstruktionsfehler: Fällt der Mac mitten im Betrieb aus, was zum Beispiel bei einem Stromausfall, bzw. bei tragbaren Macs bei einem leeren Akku passieren kann, so kann es sein, dass nach dem nächsten Wiedereinschalten Datum- und Uhrzeit nicht mehr stimmen, aber auch nicht mehr korrekt eingestellt werden können. macOS verändert in diesem speziellen Fall Datum und Uhrzeit selbständig immer wieder auf falsche Werte. Dies kann zu erheblichen weiteren Problemen bei der Kommunikation mit anderen Computern im Netz oder bei der Anmeldung von Benutzer-Accounts führen.

Sie sollten zunächst überprüfen, ob die Systemeinstellungen für automatische Zeitsynchronisation korrekt sind.

1. Öffnen Sie den Unterpunkt **Zeit** auf der Karte **Fehler**.
2. Klicken Sie auf **Einstellungen Datum & Uhrzeit**.

Der entsprechende Punkt in den Systemeinstellungen öffnet sich. Die normalen Einstellungen sind:

- **Datum und Uhrzeit automatisch einstellen:** eingeschaltet
- **Quelle:** Apple (time.apple.com.)
- **Zeitzone:** die für Ihren momentanen Standort gültige Zeitzone

Sind alle Einstellungen richtig, aber trotzdem Datum und Uhrzeit falsch, so können Sie versuchen, dieses Problem von TinkerTool System beheben zu lassen, indem der macOS-Dienst für Zeitsynchronisation zurückgesetzt und dabei fehlerhafte Daten gelöscht werden. Beachten Sie, dass es bei diesem Vorgang nötig ist, den Computer neu zu starten. Führen Sie zum Reparaturversuch die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Zeit** auf der Karte **Fehler**.
2. Klicken Sie auf **Zeitsynchronisierung zurücksetzen**
3. Folgen Sie den Anweisungen des Programms.

2.6.6 Hinzufügen von Farb-Tags auf Servern im Netzwerk

Seit der Einführung von macOS 13 Ventura (ab 2022) weist der Finder einen kritischen Defekt auf: Wenn man versucht, ein Tag für ein Objekt zu setzen, *das auf einem Dateiserver im Netzwerk gespeichert ist*, funktioniert dies in den meisten Fällen nicht mehr. Dabei spielt es keine Rolle, ob es sich bei dem Server um einen weiteren Mac handelt, oder um einen Computer eines anderen Anbieters mit einem fremden Betriebssystem. Auch die Wahl des Netzwerkprotokolls (wie SMB oder NFS) kann in der Regel nichts an diesem technischen Fehler ändern. Nur in wenigen Ausnahmefällen, mit speziellen serverseitigen Mount-Einstellungen für das Volume, auf dem die Freigabe liegt, funktioniert das Setzen von Tags manchmal. In der Regel schlägt das Einstellen von Tags mit folgenden Effekten fehl. Dies gilt für den Finder in macOS 13 und allen höheren Versionen:

- Der Finder zeigt eine unsinnige Aufforderung, den Vorgang mit einer Authentifizierung als Administrator erneut zu versuchen.
- Der Finder zeigt eine (sachlich falsche) Fehlermeldung, dass der Benutzer kein Zugriffsrecht hat, den Vorgang abzuschließen.

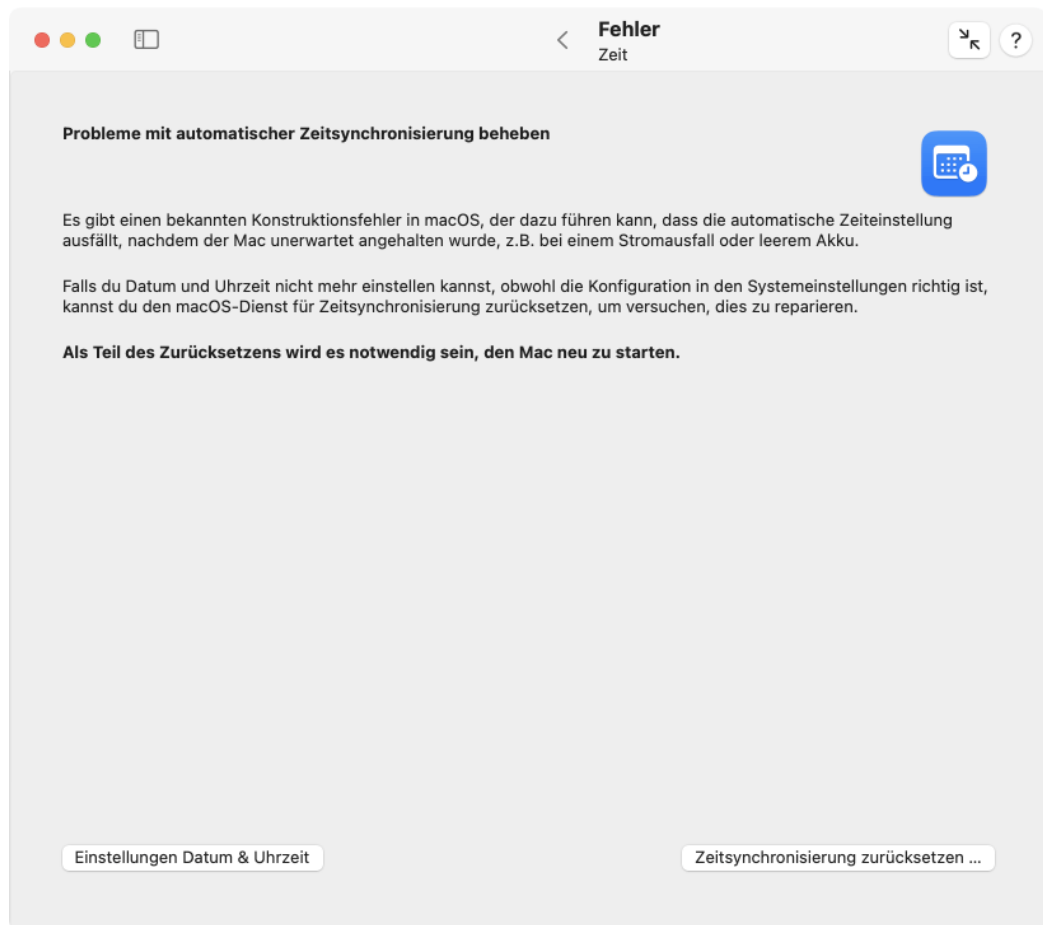


Abbildung 2.27: Der Ausfall der Datums- und Uhrzeiteinstellungen kann in vielen Fällen behoben werden

TinkerTool System ist in der Lage, auch ohne Finder ein Farb-Tag zu einer Datei oder einem Ordner hinzuzufügen, egal ob sich das Objekt im Netzwerk befindet oder nicht. Sobald einmal ein Farb-Tag für das Objekt vorhanden ist, *verhält sich der Finder danach für dieses eine Objekt fehlerfrei*. Sie können also im Anschluss weitere Tags, auch ohne Farbe, mit dem Finder zum gleichen Objekt hinzufügen oder sie löschen. Ähnliche Finder-Funktionen, wie das Einstellen eines Spotlight-Kommentars, sind dann ebenso fehlerfrei möglich.

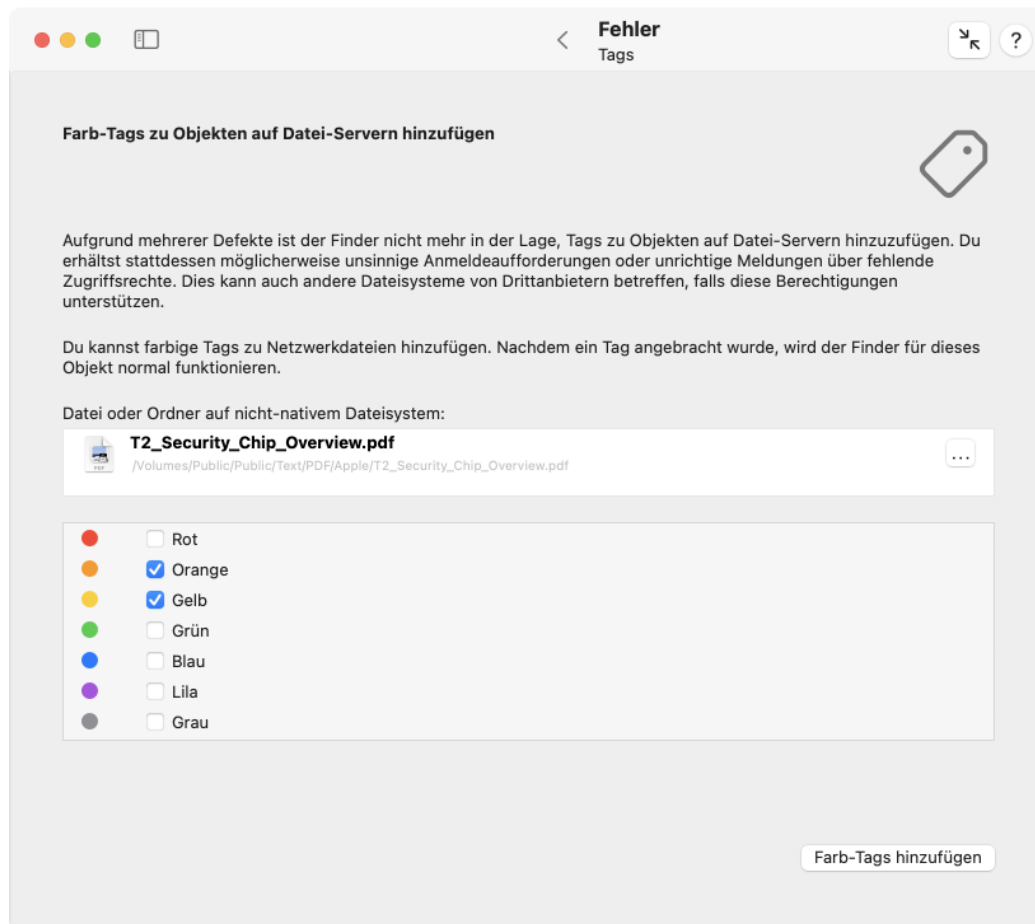


Abbildung 2.28: TinkerTool System kann Farb-Tags auch im Netzwerk hinzufügen

1. Öffnen Sie den Unterpunkt **Tags** auf der Karte **Fehler**.
2. Ziehen Sie eine Datei oder einen Ordner aus dem Finder in das Feld **Datei oder Ordner auf nicht-nativem Dateisystem**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Setzen Sie Häkchen für die gewünschten Tags, bzw. entfernen Sie diese.
4. Klicken Sie auf **Farb-Tags hinzufügen**.

Beachten Sie Folgendes:

- Sie können beliebige Objekte im Dateisystem, also Dateien, Ordner und dateiähnliche Einträge mit Tags versehen.

- Sie müssen Schreib- und Leserecht für den Ordner haben, in dem sich das betroffene Objekt befindet. Ebenso müssen Sie Leserecht für alle Attribute des Objekts haben. Sollte sich das Objekt auf einem Datenträger befinden, der Zugriffssteuerungslisten und Erweiterte Attribute unterstützt, benötigen Sie außerdem das Recht „Schreiben von Erweiterten Attributen“. Es ist nicht erforderlich, Eigentümer des Objekts zu sein.
- Sie dürfen Tags auch an einen Alias, oder ein alias-ähnliches Objekt wie einen symbolischen Link knüpfen. In dem Fall erhält der Alias das Tag, nicht das Objekt, auf das der Alias verweist.

Sie können nur Farb-Tags ändern. Haben Sie dies einmal für ein Objekt auf einem Netzwerk-Server erledigt, ist dieses Objekt danach „repariert“ und lässt sich in der Regel über den Finder weiter bearbeiten, ohne dass Fehler auftreten. Auf diese Weise können Sie im Anschluss weitere von Ihnen definierte nicht-farbige Tags dem Objekt hinzufügen.

Apple erlaubt nicht offiziell, dass Drittanbieterprogramme wie TinkerTool System Zugriff auf Ihre persönliche Liste verwendeter Tags bekommen. Deshalb lassen sich außer Farb-Tags keine anderen Tags im Programm verwenden. Sie können den im Finder eingestellten Text für ein Farb-Tag auch nur über den Finder ändern.

2.6.7 Löschen von Partitionierungsdaten auf Platten zur Lösung von Problemen mit dem Festplattendienstprogramm

Das *Festplattendienstprogramm*, wie es mit modernen Versionen von macOS ausgeliefert wird, ist von mehreren technischen Defekten betroffen. Eines dieser Probleme kann die Neuorganisation gebrauchter Platten verhindern: Abhängig vom Partitionierungsschema und dem früheren Inhalt lehnt es das Festplattendienstprogramm möglicherweise ab, eine Platte zu löschen, oder dies schlägt fehl, so dass Sie das Laufwerk nicht für neue Einsatzzwecke verwenden können. Alle Versuche, die früheren Dateisysteme zu entfernen, sind nicht erfolgreich. In diesem Fall kann TinkerTool System helfen, indem es die Partitionierungsdaten löscht, die im Festplattendienstprogramm Probleme verursachen.



Warnung: Löschen von Partitionierungsinformationen bedeutet, dass alle Dateisysteme auf der fraglichen Platte nicht mehr zugreifbar werden. Alle Daten in allen Volumes auf dieser Platte gehen verloren. Das Plattenlaufwerk wird sich ähnlich wie ein fabrikneues Gerät verhalten.

Um eine Platte zur erfolgreichen Wiederverwendung für das Festplattendienstprogramm vorzubereiten, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Plattenlaufwerke** auf der Karte **Fehler**.
2. Wählen Sie mit dem Menüknopf **Zu löschende Platte** das Laufwerk aus, das bereinigt werden soll.
3. Kontrollieren Sie das aktuelle Partitionierungslayout der ausgewählten Platte in der Übersicht **Betroffene Volumes**. TinkerTool System zeigt das Layout in hierarchischer

Reihenfolge, so wie es von macOS erkannt worden ist. Das Programm versucht, Namen und Größen aller vorgefundenen Volumes anzugeben, was Ihnen dabei hilft, die richtige Platte zu identifizieren. Beachten Sie, dass die Übersicht auch unsichtbare Systempartitionen enthalten kann, die vom Festplattendienstprogramm möglicherweise nicht gezeigt werden.

4. Drücken Sie den Knopf **Platte löschen**

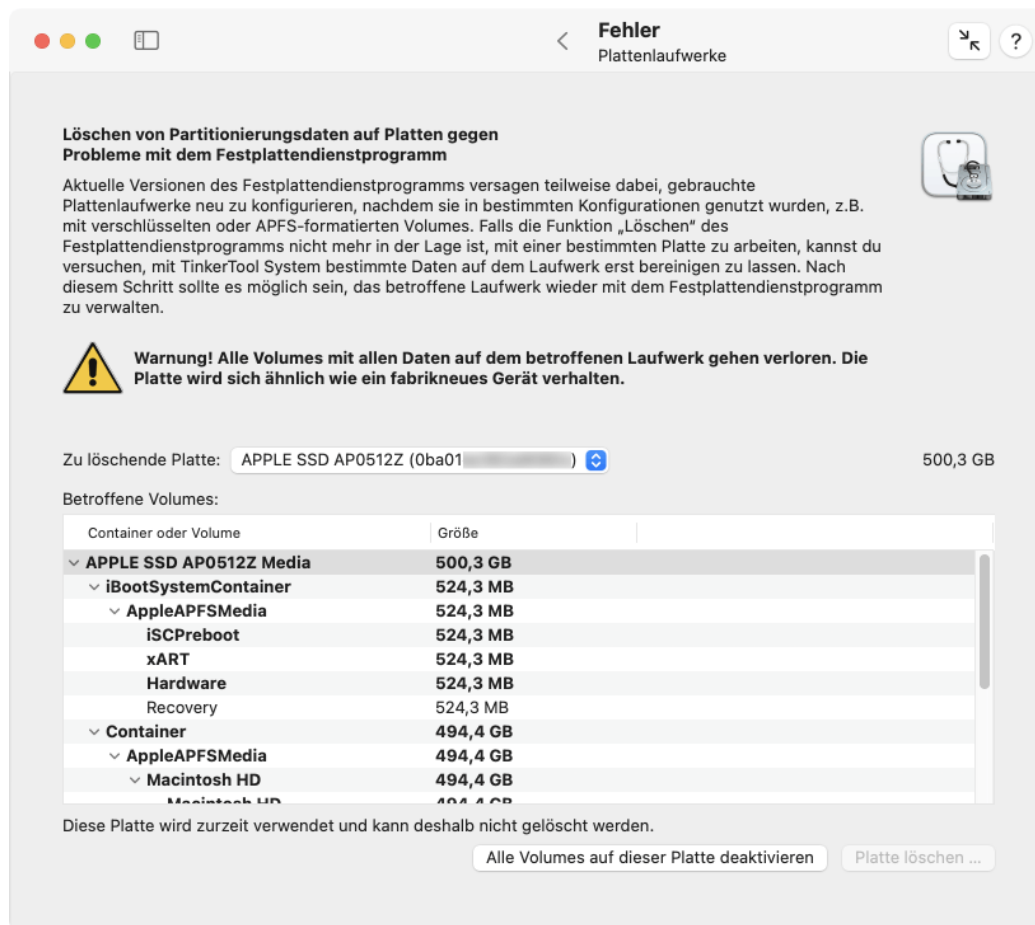
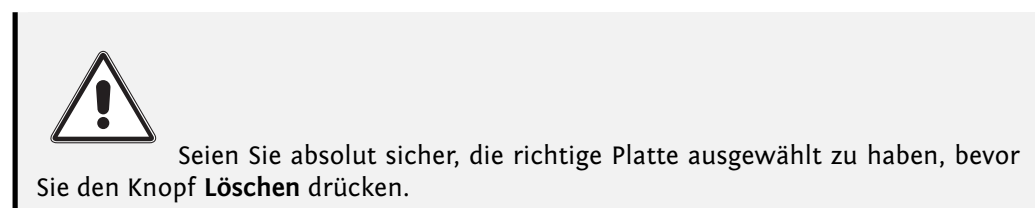


Abbildung 2.29: Bereinigen Sie Platten, die im Festplattendienstprogramm nicht mehr gehandhabt werden können



Die Platte selbst wird über ihren Gerätenamen dargestellt, oft ergänzt um eine Seriennummer oder Bus-Identifikation, was dabei hilft, zwischen ähnlichen Platten zu unterscheiden, wenn Sie mehrere Laufwerke des gleichen Modells haben. Auf Volumes, die im

Moment nicht aktiviert sind, kann nicht zugegriffen werden, was heißt, dass TinkerTool System vielleicht nicht die Volume-Namen anzeigen kann, die Sie gewohnt sind. Stattdessen werden interne Namen der jeweiligen Partitionen aufgeführt. Falls Sie sich über die Identität einer bestimmten Platte nicht ganz im Klaren sind, versuchen Sie diese im Festplattendienstprogramm zu aktivieren, um die Volume-Namen in TinkerTool System zu sehen, und deaktivieren Sie die Volumes dann wieder.

Sie können ein Laufwerk nur dann zur Löschung auswählen, wenn alle seine Volumes nicht aktiv sind. Falls eine Platte immer noch genutzt wird, deaktivieren Sie die diesbezüglichen Volumes durch Anklicken des Knopfes **Alle Volumes auf dieser Platte deaktivieren** unterhalb der Tabelle.

Nachdem TinkerTool System eine Löschung erfolgreich durchgeführt hat, können Sie versuchen, das Laufwerk im Festplattendienstprogramm wiederzuverwenden. Dessen eigene Funktion **Löschen** sollte jetzt korrekt funktionieren.

2.7 Die Einstellungskarte Diagnose

2.7.1 RAM-Größe auswerten

Einführung in virtuelle Speichertechnik

Die Menge an installiertem Hauptspeicher (*RAM, Random Access Memory*) eines Computers kann entscheidend für die damit erzielte Rechenleistung sein. Ist zu wenig Speicher vorhanden, kann die Geschwindigkeit des Computers stark herabgesetzt werden. Ist allerdings zu viel Speicher vorhanden, liegen Kapazitäten brach, die eigentlich nicht benötigt werden. Es entstehen also unnötige Kosten.

Welche Speichermenge optimal ist, hängt davon ab, wie Sie Ihren Computer verwenden, insbesondere welche Programme Sie einsetzen, welche Daten Sie mit diesen Programmen verarbeiten und in welchem Maße diese Programme gleichzeitig verwendet, also auch gleichzeitig im Speicher gehalten werden müssen. macOS führt intern sehr detaillierte Statistiken, wie die vorhandene Speichermenge von den einzelnen Programmen genutzt wird. TinkerTool System kann diese Statistiken auswerten, um zu beurteilen, ob die in Ihrem Computer installierte RAM-Größe für Ihre typische Arbeit angemessen ist. Sie haben somit eine wertvolle Entscheidungshilfe, um abzuschätzen, ob Sie mehr RAM für Ihren Computer kaufen sollten, bzw. ob zusätzlicher Speicher tatsächlich zu einer Erhöhung der Leistung führen würde.

Hintergrundwissen

Wie bei allen modernen Betriebssystemen hat kein laufendes Programm das Recht, direkt auf den Hauptspeicher zuzugreifen. Dies bleibt alleine dem innersten Kern (Kernel) des Betriebssystems vorbehalten. Für jedes laufende Programm (was als *Prozess* bezeichnet wird) wird jeweils ein eigener Speicherraum von der Hardware simuliert. Jeder Prozess läuft deshalb in einem komplett abgetrennten Bereich, der ihm scheinbar exklusiv zur Verfügung steht. Die Speicherbereiche der anderen Prozesse sind für den jeweils betrachteten Prozess völlig unsichtbar. Ein Prozess kann somit weder Daten aus anderen Prozessen ausspionieren, noch kann er absichtlich oder unabsichtlich Daten in den Speicherräumen fremder Prozesse überschreiben. Dies ist eine der wichtigsten Techniken, die dafür sorgen, dass ein Betriebssystem stabil und sicher läuft. Die Programme sind streng gegeneinander abgeschottet. Auch „schlechte“ Programme können fremde Prozesse oder gar das Betriebssystem nicht zum Absturz bringen.

Diese Technik wird *virtueller Speicher* genannt und im Wesentlichen von einer Hardware-Komponente im Prozessor verwaltet, der *Speichermanagementeinheit (Memory Manage-*

ment Unit, MMU). Bei jedem (virtuellen) Speicherzugriff eines Prozesses entscheidet diese MMU, auf welchen Speicher intern wirklich zugegriffen wird: Der virtuelle Speicher wird entweder auf tatsächlichen Hauptspeicher oder auf spezielle Dateien auf der Systemfestplatte, den sogenannten *Auslagerungsspeicher* abgebildet. Diese Abbildung von virtuellem Speicher auf realen Speicher erfolgt blockweise, in Organisationseinheiten, die *Seiten* genannt werden. Bei macOS ist eine Seite immer 4 KiB groß.

So lange es geht, versucht das System, den virtuellen Speicher auf echten Hauptspeicher abzubilden. Laufen jedoch viele Prozesse gleichzeitig oder werden sehr viele Daten gleichzeitig verarbeitet, reicht die Menge an vorhandenem Hauptspeicher irgendwann nicht mehr aus, um alle Seiten des virtuellen Speichers zu beherbergen. In diesem Fall wird eine Seite vom Hauptspeicher auf die Festplatte ausgelagert, um Platz zu schaffen. Hierbei wählt das System jeweils eine Speicherseite aus, die höchstwahrscheinlich in nächster Zukunft nicht von einem Prozess gebraucht wird. Der durch die Auslagerung frei gewordene Block im Hauptspeicher kann nun von einem anderen Prozess verwendet werden. Wird eine auf Platte ausgelagerte Seite später dann doch wieder von ihrem zugehörigen Prozess angesprochen, muss sie wieder in den Hauptspeicher eingelagert werden. Eine andere Seite wird nun zur Auslagerung ausgewählt und die beiden Seiten tauschen ihre Plätze.

Durch die unterschiedlichen Arbeitsgeschwindigkeiten von Hauptspeicher und Festplatte kann ein Zugriff auf ausgelagerten Speicher etwa 10.000 bis 100.000 mal langsamer sein als ein Zugriff auf Speicher, der sich im RAM befindet. Aus diesem Grund kann die Arbeitsgeschwindigkeit eines Computers drastisch sinken, wenn zu viele Auslagerungen stattfinden, also zu wenig Hauptspeicher vorhanden ist, um möglichst viele genutzte Speicherseiten im schnell zugreifbaren Bereich zu halten. Die theoretisch beste Nutzung des Speichers liegt genau dann vor, wenn der komplette Hauptspeicher genutzt wird (fast kein Speicher frei) und kein Auslagerungsspeicher benötigt wird. In diesem Fall befinden sich alle Daten im schnellen RAM und kein Teil des RAMs liegt brach.

Zusätzlich zu der Auslagerung von Speicherseiten auf die Systemfestplatte unterstützen die neuesten Versionen von macOS einen weiteren Ort zur Unterbringung von Seiten, die nicht mehr in den Standardspeicher passen: Da eine Festplatte so erheblich langsamer ist als RAM, kann sich das Betriebssystem dazu entscheiden, einen kleinen Teil des RAM zu opfern und diesen Teil zur Speicherung ausgelagerter Seiten zu verwenden, nachdem *Datenkompression* auf deren Inhalt angewendet wurde. Dies wird *komprimierter Speicher* genannt. Statt eine Speicherseite auf Platte zu schreiben, komprimiert das System die Seite und schreibt sie in einen speziellen Bereich des RAM, der dafür reserviert wurde. Das weitere Verkleinern der Hauptspeichermenge, die Anwendungen zur Verfügung steht, indem ein Teil davon für komprimierten Speicher reserviert wird, ist natürlich ein kritischer Schritt. Das System muss sorgfältig abwägen, ob der Gewinn durch das Komprimieren/Dekomprimieren im RAM statt des Lesens/Schreibens in Auslagerungsdateien die Effekte des Verlusts von verfügbarem RAM übersteigt.

Auswertung der vorhandenen Speichergröße

Wie erwähnt ist eine Beurteilung der Speichergröße nur im Zusammenhang mit der typischen Speichernutzung möglich, die beim täglichen Gebrauch Ihres Computers anfällt. Ob Sie genug Speicher haben, hängt davon ab, welche Programme Sie einsetzen und wie Sie diese verwenden. *Eine sinnvolle Beurteilung der Speichergröße ist deshalb nur dann möglich, wenn das Betriebssystem eine typische Nutzung des Speichers innerhalb eines gewissen Zeitraums beobachten konnte.* Gehen Sie wie folgt vor, um die Speichernutzungsstatistik von TinkerTool System auswerten zu lassen:

1. Wählen Sie den Unterpunkt **RAM-Größe** auf der Einstellungskarte **Diagnose**.

2. Drücken Sie auf die Schaltfläche **Werte aktualisieren**.

Die aktuellen Statistikwerte erscheinen nun in der oberen Box, die Auswertung in der unteren Box **Ergebnis**. Eine Auswertung ist erst dann möglich, wenn das System für mindestens 2 Stunden eingeschaltet war.

Die Betriebszeit von macOS, in der die Daten für die Statistik erfasst wurden, ist in der letzten Zeile der oberen Box aufgeführt. Sie müssen selber beurteilen, ob der Computer in dieser Betriebszeit „typisch“ genutzt wurde. War die Nutzung eher untypisch, z.B. weil Sie wesentlich mehr Programme als normal gleichzeitig eingesetzt haben, oder weil Sie in dieser Zeit mit einem unüblichen, „riesigen“ Dokument gearbeitet haben, das außergewöhnlich viel Speicher verbraucht hat, ist das Ergebnis nicht aussagekräftig.

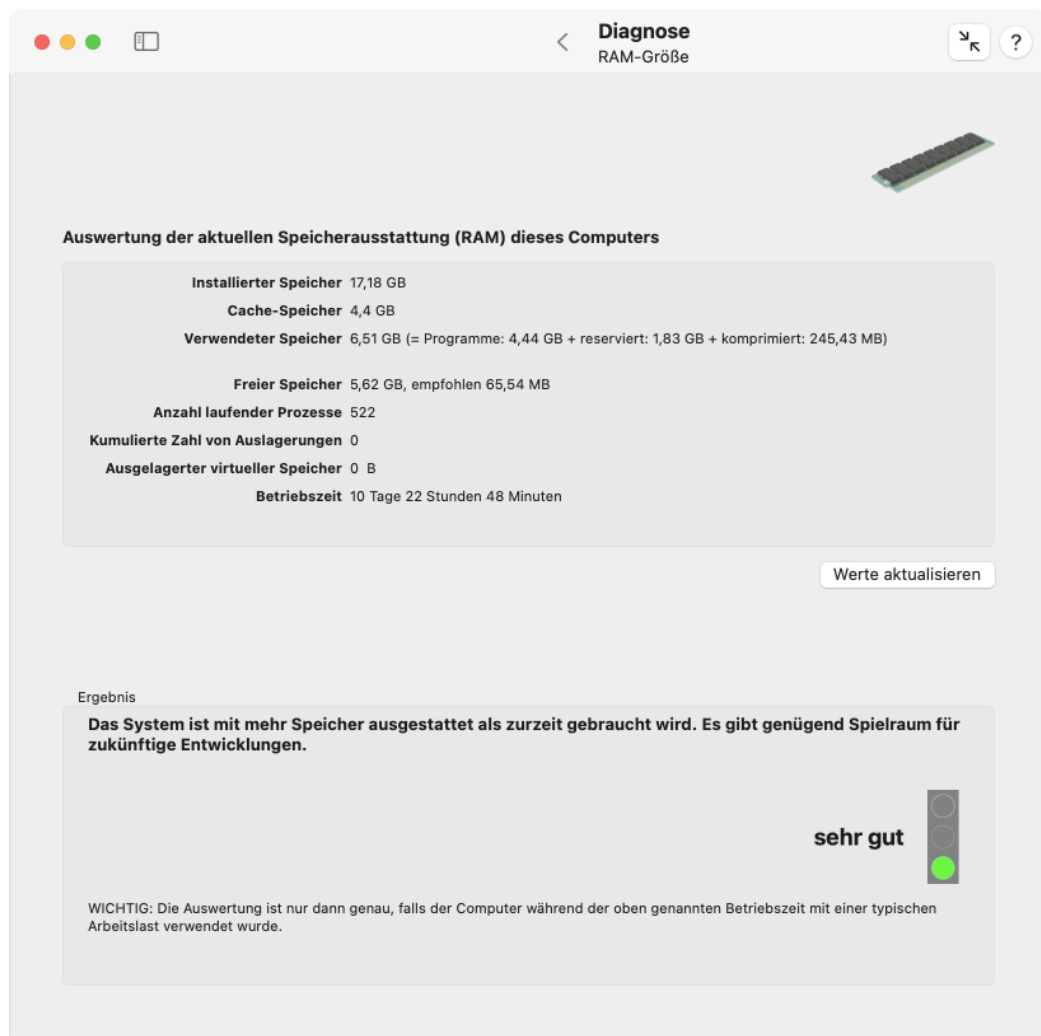


Abbildung 2.30: RAM-Größe auswerten

Erscheint Ihnen die Computernutzung innerhalb der angegebenen Betriebszeit nicht typisch genug, um eine aussagekräftige Beurteilung zu erlauben, führen Sie die folgenden

Schritte durch:

1. Starten Sie macOS neu.
2. Nutzen Sie den Computer für einen Zeitraum von mindestens zwei Stunden mit dem typischen Arbeitsumfang, für den dieser Computer angeschafft wurde.
3. Starten Sie TinkerTool System erneut und gehen Sie noch einmal zum Punkt **RAM-Größe auswerten**.

Die obere Box enthält ausgewählte Daten aus der Speichernutzungsstatistik, die von macOS geführt wird:

- **Installierter Speicher:** Die zur Verfügung stehende, tatsächliche Menge an Hauptspeicher, die von macOS und den laufenden Prozessen genutzt werden kann. Diese Größe entspricht normalerweise der Größe der im Computer installierten Speichermodule. In einigen Fällen kann die hier angezeigte Größe jedoch aufgrund von Einschränkungen der Hardware kleiner sein. Der Chipsatz des Computers oder die Funktion „gemeinsam verwendeter Speicher“ von Grafikchips kann die verfügbare Speichermenge auf bestimmten Computern reduzieren.
- **Cache-Speicher:** Hauptspeicher, der von macOS benutzt wird, um den Betrieb des Computers zu beschleunigen, insbesondere beim Zugriff auf Dateien und beim erneuten Start kurz zuvor genutzter Programme.
- **Verwendeter Speicher:** Die Größe des Hauptspeichers, der im Moment von den laufenden Prozessen und vom Systemkern genutzt wird. Der Speicher ist in drei Teile unterteilt, die ebenso in der folgenden Reihenfolge aufgelistet sind: Seiten, die von laufenden Prozessen benutzt werden (*Speicher für Programme*), Seiten, die nicht am Auslagerungsverfahren teilnehmen dürfen (manchmal *reservierter Speicher* genannt) und Seiten für komprimierten Speicher (*komprimierter Auslagerungsspeicher im RAM*).
- **Freier Speicher:** Die Größe des Hauptspeichers, der im Moment nicht auf virtuellen Speicher abgebildet wird. Dieser Speicher liegt brach und wird nicht genutzt. TinkerTool System gibt zusätzlich die empfohlene freie Speichergröße an. Das System läuft am besten, wenn fast das gesamte RAM in Nutzung ist und ein kleiner Teil für die laufende Verwaltung übrig bleibt. Die Empfehlung wird von macOS berechnet. Auf dem angegebenen Wert basiert die aktuelle Strategie der Speichervergabe, die vom System verwendet wird.
- **Anzahl laufender Prozesse:** Die Anzahl der zurzeit laufenden Prozesse. Jeder Prozess nutzt virtuellen Speicher.
- **Kumulierte Zahl von Auslagerungen:** Die Anzahl der gesamten Auslagerungsvorgänge in der Betriebszeit von macOS.
- **Auf Platte ausgelagerter virtueller Speicher:** Die Größe des Auslagerungsspeichers, der im Moment von laufenden Prozessen genutzt wird.
- **Betriebszeit:** Die Zeit seit dem letzten Start von macOS. In dieser Zeit wurden die aufgeführten Daten gesammelt.

In der Box **Ergebnis** finden Sie die aktuelle Beurteilung der in der oberen Box erfassten Statistik. Die Beurteilung besteht aus einem Erklärungstext und einer kurzen Gesamtbeurteilung wie „gut“, die zusätzlich durch ein Ampelsymbol grafisch dargestellt wird. Im einzelnen wird zwischen folgenden Bewertungen unterschieden:

- **sehr gut:** Das System ist mit genügend Hauptspeicher ausgestattet und besitzt im Moment sogar mehr Speicher, als eigentlich gebraucht wird. Mit dieser Ausstattung hat das System auch für die Zukunft noch genügend Leistungsreserven.
- **gut:** Die Menge an Hauptspeicher entspricht recht gut der Menge, die auch tatsächlich gebraucht wird. Eine Ausgewogenheit zwischen Preis und Leistung wurde erreicht. Wirtschaftlich gesehen ist dies die beste Lösung.
- **mittel:** Mit etwas mehr Hauptspeicher könnte das System geringfügig besser laufen. Die Speichermenge ist allerdings nicht so knapp, dass die Situation bereits kritisch wäre. Eine Erweiterung des Speichers wird die Leistung des Computers leicht erhöhen, allerdings nur in geringem Maße.
- **schlecht:** Das System ist mit zu wenig Hauptspeicher für das typische Nutzungsverhalten ausgestattet und wird deswegen ausgebremst. Falls es technisch möglich ist, sollten Sie den Speicher erweitern. Eine Speichererweiterung wird für spürbar mehr Leistung sorgen. Falls die Maximalausstattung bereits erreicht ist, sollten Sie auf einen größeren Computer wechseln oder die Arbeitslast reduzieren.

2.7.2 Finder Kopieren testen

Für das Programm Finder, das in macOS üblicherweise zum Arbeiten mit Dateien und Ordnern verwendet wird, ist bekannt, dass es bestimmte Konstruktionsfehler aufweist, die davon abhängen, welche Version Sie einsetzen. Besonders die Fehler, die Kopieroperationen von Dateien betreffen, sind kritisch, da Sie Daten verlieren können, wenn Sie annehmen, dass eine kopierte Datei hundertprozentig mit dem Original übereinstimmt. Dies gilt insbesondere dann, wenn Sie berücksichtigen, dass der Finder auch eine Rolle beim Betrieb von Time Machine, der Datensicherungslösung von macOS spielt.

TinkerTool System kann überprüfen, ob der Finder in der Lage ist, die folgenden Vorgänge korrekt auszuführen. Diese sind dafür bekannt, nicht zuverlässig zu arbeiten, wenn bestimmte Versionen des Finders und bestimmte Dateisystemtypen als Quelle und Ziel des Kopiervorgangs verwendet werden:

- Das Kopieren von Dateien mit emulierten Erweiterten Attributen (sogenannte *AppleDouble*-Dateien).
- Das Kopieren von symbolischen Links, die native Erweiterte Attribute besitzen.

Mit Dateisystemtyp ist das Format einer Platte oder Partition, bzw. das Übertragungsprotokoll beim Zugriff auf einen File Server im Netzwerk gemeint. Der Finder verhält sich unterschiedlich, wenn Sie z.B. zwischen zwei HFS-Festplatten, oder von einer HFS-Platte auf einen für Windows formatierten Speicher-Stick im FAT-Format von Windows kopieren. Sie können zwei gegebene Datenträger und Ihre Version des Finders von TinkerTool System überprüfen lassen. TinkerTool System kann den Finder fernsteuern und so testen, welche Operationen wie erwartet ablaufen und welche nicht. Zur Prüfung müssen Sie lediglich zwei Ordner angeben, zwischen denen Testdaten kopiert werden sollen.

- Beide Ordner müssen sich auf unterschiedlichen Datenträgern befinden, damit wirklich ein physischer Kopiervorgang stattfinden kann, nicht nur ein Verschieben von Daten.
- Sie müssen Lese- und Schreibrecht für beide Ordner haben, damit der unter Ihrem Account laufende Finder das Recht hat, den Kopiervorgang auszuführen.

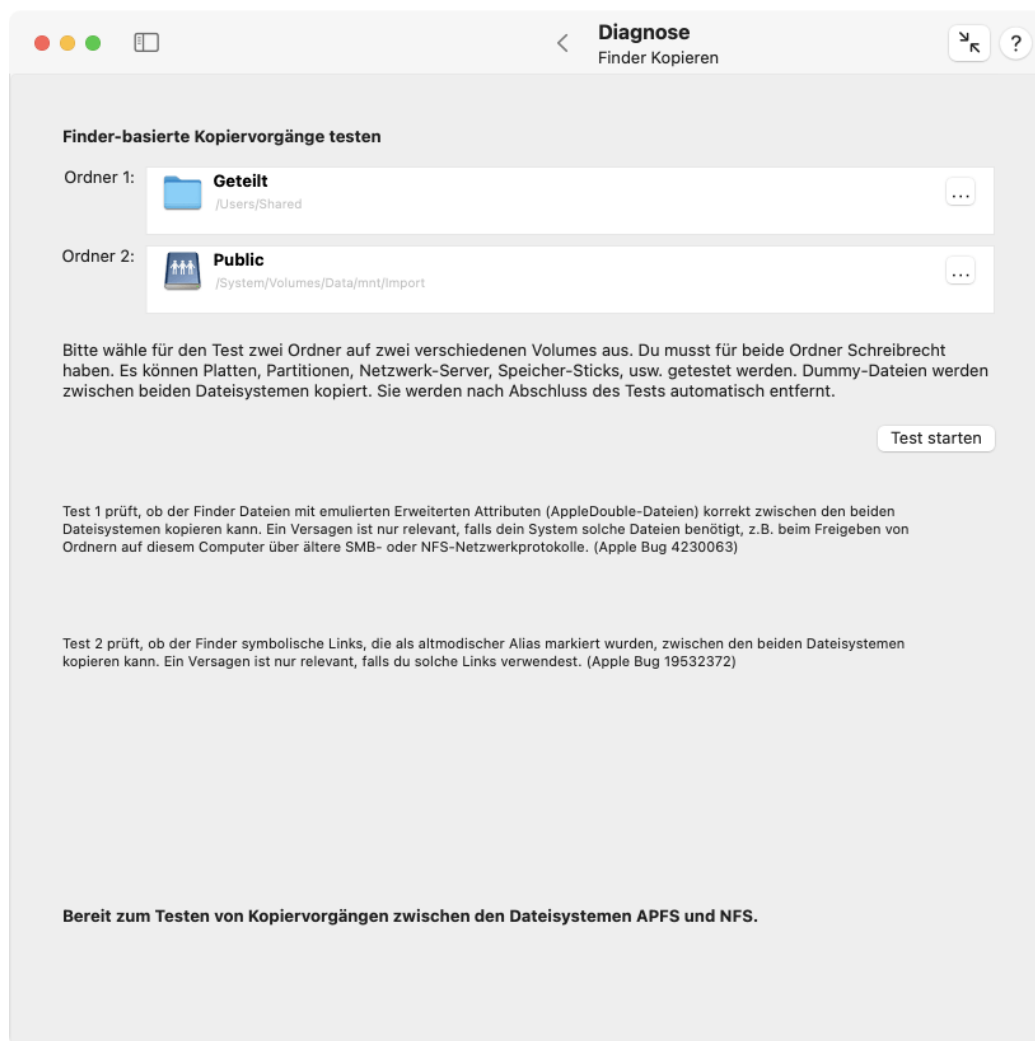


Abbildung 2.31: Dateikopiervorgänge überprüfen

Zum Durchführen der Tests benötigt TinkerTool System weniger als 200 kB Speicherplatz auf den beiden Datenträgern. Die während des Tests geschriebenen Daten werden nach Abschluss des Tests automatisch wieder gelöscht.

Beim Arbeiten mit Dateisystemtypen spielen nur die *Dateisystemfamilien* eine Rolle für das Verhalten des Finders, nicht die konkreten Untertypen. Die Meldungen, die von TinkerTool System während der Prüfung angezeigt werden, beziehen sich nur auf diese Familien. Beispielsweise werden die Dateisysteme „HFS“ und „HFS+ mit Journaling, Groß-/Kleinschreibung und Verschlüsselung“ beide durch die Familie „HFS“ repräsentiert.

TinkerTool System benötigt die Genehmigung, den Finder automatisieren zu dürfen, bevor Sie diese Funktion nutzen können. Weitere Informationen finden Sie im letzten Abschnitt des Kapitels Grundlegende Bedienungshinweise (Abschnitt 1.3 auf Seite 8).

Führen Sie die nachfolgenden Schritte durch, um den Finder zu testen:

1. Öffnen Sie den Unterpunkt **Finder Kopieren** auf der Einstellungskarte **Diagnose**.
2. Ziehen Sie einen Ordner, der sich auf dem ersten zu prüfenden Datenträger befindet, aus dem Finder in das Feld **Ordner 1**. Sie können auch den Knopf [...] drücken, um zum Ordner zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Ordners eingeben.
3. Wählen Sie nach dem gleichen Muster im Feld **Ordner 2** einen anderen Ordner, der sich auf dem zweiten zu prüfenden Datenträger befindet.
4. Drücken Sie nun auf den Knopf **Test starten**. Nach ein paar Sekunden erscheint das Testergebnis im unteren Bereich der Einstellungskarte.

Sie können den Knopf nur drücken wenn die oben genannten Voraussetzungen für die beiden Ordner erfüllt sind. Auf der Einstellungskarte können Sie vorher ablesen, ob der Test durchgeführt werden kann, bzw. welches mögliche Problem bei der Auswahl der Ordner vorliegt.

TinkerTool System testet Kopiervorgänge automatisch in beide Richtungen, d.h. für das Kopieren von Ordner 1 nach 2 und von Ordner 2 nach 1. Die Reihenfolge der ausgewählten Ordner spielt deshalb keine Rolle. Da TinkerTool System den Finder fernsteuert, hören Sie eventuell während des Tests mehrmals den Toneffekt, mit dem der Finder Kopiervorgänge begleitet.

Ein ordnungsgemäß bestandener Test wird mit einem grün markierten Häkchen, ein nicht bestandener Test mit einem rot markierten Kreuz dargestellt.

Ein Fehlschlagen von Test 1 zeigt an, dass der Finder nicht in der Lage ist, Erweiterte Attribute von Dateien und Ordnern zu kopieren, falls auf einem der Datenträger diese Attribute nicht nativ, also nicht auf einer Platte im Format „Mac OS Extended“ (HFS), „Apple File System“ (APFS), bzw. einem AppleShare-Dateiserver (AFPFS) gespeichert sind. *Ein Fehlschlagen des Tests ist möglicherweise für Sie nicht relevant.* Emulierte Erweiterte Attribute werden hauptsächlich dann benutzt, wenn Sie das System als Datei-Server verwenden, wobei Dateien mit alten Versionen der Netzwerkprotokolle SMB oder NFS freigegeben werden. Falls Sie Ihren Computer nicht in dieser Weise nutzen, ist es sehr wahrscheinlich, dass Ihre Installation von macOS niemals Dateien mit solchen Attributen angelegt hat.

Ein Fehlschlagen von Test 2 zeigt an, dass der Finder keine symbolischen Links kopieren kann, die mit Erweiterten Attributen verknüpft sind. Ein Fehlschlagen dieses Tests ist möglicherweise auch nicht für Sie relevant, aber eine solche Situation tritt häufiger auf, als

diejenige in Test 1. Beispielsweise können solche Objekte als Teil von Programmen auftauchen, in die ältere Software-Bibliotheken in Form von Frameworks eingebettet sind. Diese Frameworks könnten symbolische Links enthalten, die zusätzlich über ein Erweitertes Finder-Attribut als altmodischer Alias markiert sind. In der Praxis bemerken Sie ein solches Problem in Situationen, in denen der Finder unerwartet einen laufenden Kopiervorgang mit der Meldung abbricht, dass ein Objekt nicht gefunden wurde (*Fehler –36*), obwohl das Objekt da ist.

Beachten Sie, dass TinkerTool System nur prüft, ob der Finder wie erwartet funktioniert. Das Programm kann einen eventuell festgestellten Defekt im Finder nicht reparieren.

2.7.3 Optische Disks inspizieren

Ist Ihr Computer mit einem oder mehreren optischen Laufwerken mit Schreibfähigkeiten ausgestattet, können Sie TinkerTool System dazu verwenden, Detaildaten über eingelegte Diskmedien, wie CDs, DVDs oder Blu-ray Discs, abzurufen. Diese Funktion ist hilfreich, um zum Beispiel das tatsächliche Herstellerwerk eines Mediums herauszufinden oder Informationen über das Aufzeichnungsformat einer Disk abzurufen. Je nach Typ des eingelegten Mediums und dessen Aufzeichnungsformat kann sich die Menge der abrufbaren Daten sehr unterscheiden. TinkerTool System unterstützt bei passenden Medien unter anderem die folgenden Detaildaten:

- Laufwerksbezeichnung
- Firmware-Revisionsnummer des Laufwerks
- Typ des eingelegten Mediums
- Medienverhalten, d.h. Einhaltung einer Aufzeichnungsnorm
- Anzahl aufgezeichneter Sitzungen (Disk Sessions)
- Hersteller der Disk
- Anzahl der Aufzeichnungsschichten
- Durchmesser der Disk
- Unterstützte Rotationsgeschwindigkeiten für diese Kombination aus Medium und Laufwerk
- Speicherkapazität des Mediums

Neben den Eigenschaften des Mediums bestimmt auch die Frage, ob auf dem Medium bereits Daten aufgezeichnet sind, welche dieser Detailinformationen abrufbar sind und welche nicht.

Um Detailinformationen über ein optisches Diskmedium abzurufen, gehen Sie wie folgt vor:

1. Öffnen Sie den Unterpunkt **Optische Disks** auf der Einstellungskarte **Diagnose**.
2. Falls an Ihren Computer mehrere optische Laufwerke angeschlossen sind, wählen Sie das gewünschte Laufwerk mit dem Klappenmenü **Laufwerk**.
3. Stellen Sie sicher, dass das zu untersuchende Medium in dieses optische Laufwerk eingelegt ist. Sie können über den mit einem Auswurfsymbol markierten Knopf eine Disk auswerfen, bzw. ein eventuell vorhandenes Schubfach des Laufwerks öffnen oder schließen. Warten Sie, bis das Laufwerk und macOS die Disk erkannt haben.

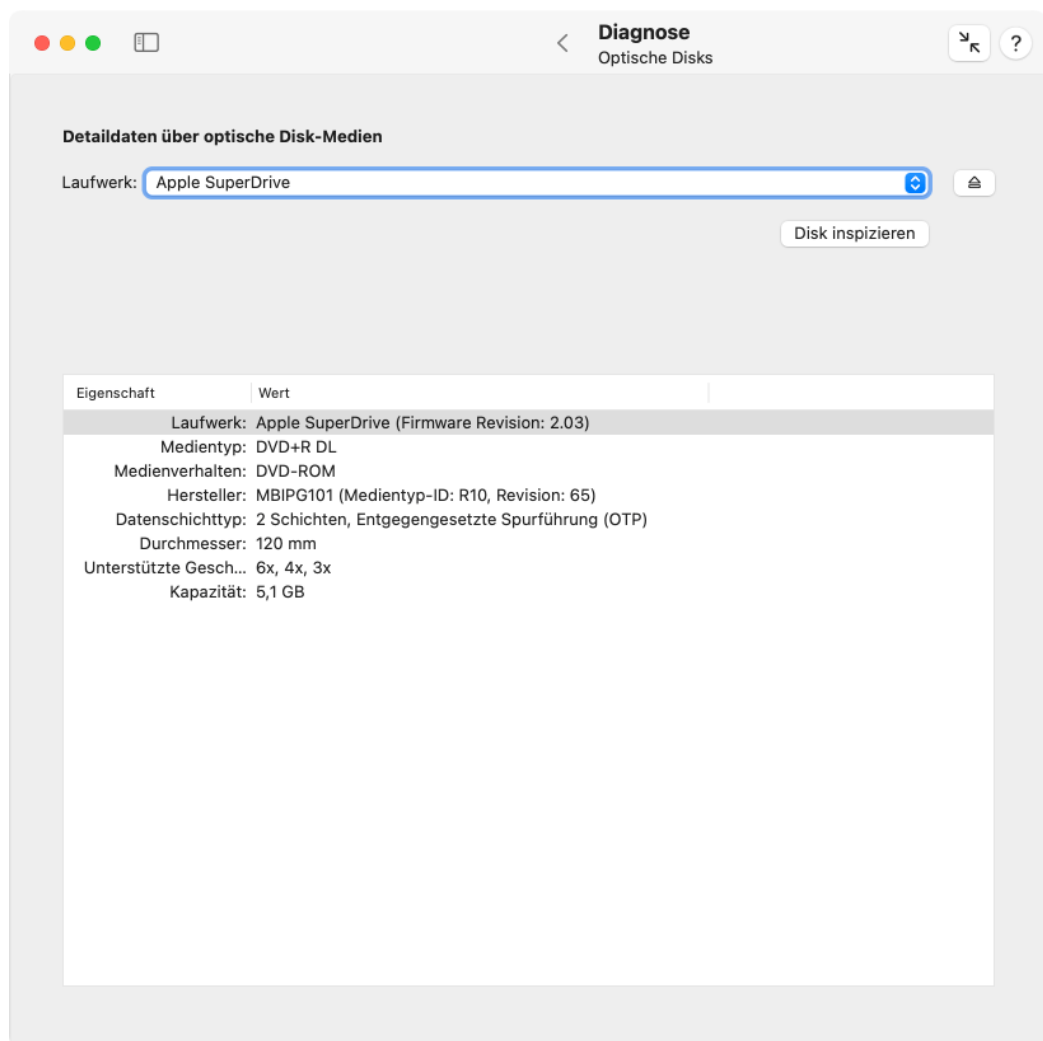


Abbildung 2.32: Optische Disks inspizieren

4. Drücken Sie den Knopf **Disk inspizieren**.

Das Untersuchungsergebnis wird daraufhin nach wenigen Sekunden in der Box **Ergebnis** angezeigt.

Beachten Sie den Unterschied zwischen den Angaben **Medientyp** und **Medienverhalten**: Wenn Sie beispielsweise ein Digitalvideo auf ein Medium des Typs DVD+R gebrannt und diese Aufzeichnung ordnungsgemäß abgeschlossen (finalisiert) haben, dann lautet der physische Medientyp **DVD+R**, die so erstellte Disk verhält sich jedoch wie eine **DVD-ROM**.

Falls Sie nicht die typischen „Superdrives“ von Apple verwenden, unterstützt das Programm nur optische Laufwerke, die sowohl lesen als auch schreiben können.

2.7.4 SSDs

Bevor wir über Solid-State-Laufwerke (SSD) sprechen, die in früheren Generationen von Macintosh-Systemen von Apple auch als „Flash-Speicher“ bezeichnet wurden, betrachten wir zunächst, wie konventionelle magnetische Festplatten die Löschung einer Datei handhaben. Bei Festplatten ist die Dateilöschung ein einfacher und schneller Vorgang. Das Betriebssystem entfernt den Eintrag der Datei aus deren Ordner und informiert das Dateisystem darüber, dass die Plattenblöcke, die von der Datei genutzt wurden, jetzt frei sind und zur erneuten Nutzung zur Verfügung stehen. Die alten Daten bleiben in den Blöcken liegen, bis das Plattenlaufwerk sie mit Daten für eine neue Datei überschreibt.

Aus technischen Gründen ist dies bei SSD-Speichermedien nicht so einfach. Obwohl aus Sicht des Betriebssystems ein SSD-Datenblock genau dasselbe ist wie ein Datenblock auf einer Festplatte, können diese nicht einfach mit neuen Daten überschrieben werden. Es ist notwendig, die Blöcke ausdrücklich zu löschen, bevor diese mit neuen Daten beschrieben werden können, was ein zeitaufwändiger Vorgang ist. Die Steuerung der SSD muss jedes einzelne Bit eines Datenblocks auf der physischen Ebene auf Null stellen, was intern durch Zurücksetzen aller Flash-Speicherzellen geschieht, die zu dem jeweiligen Block gehören. Ein Schreibvorgang auf einem Flash-basierten Speichermedium ist daher spürbar langsamer, falls das Laufwerk keine Reserve leerer Speicherblöcke vorrätig hat, die für die eingehenden Daten genutzt werden können. Das Betriebssystem muss möglicherweise darauf warten, dass das Laufwerk einen leeren Speicherblock zur Verfügung stellt, der für die anstehende Schreiboperation benötigt wird. Leer heißt dabei entweder ein brandneuer, noch nie genutzter Speicherblock, oder aber ein benutzter Block, der für einen neuen Schreibvorgang durch eine aufwändige Löschoperation vorbereitet wurde.

Falls große Datenmengen in der Vergangenheit auf eine SSD geschrieben wurden, wird die Wahrscheinlichkeit, dass entweder fabrikneue oder gelöschte Blöcke zur Verfügung stehen, geringer. Die Geschwindigkeit für Schreibvorgänge sinkt, je mehr Daten geschrieben werden. Um dieses Problem zu lösen, muss das Laufwerk versuchen, ungenutzte Blöcke so früh wie möglich zu löschen. Auf diese Weise ist die Chance, noch leere Blöcke in Reserve zu haben, die sofort für eingehende Schreibvorgänge verfügbar sind, viel höher. Aber wie soll das Laufwerk „erfahren“, welche Blöcke nicht mehr benötigt werden? Bei magnetischen Platten musste das Laufwerk das nicht „wissen“.

Um einen Speichermedium anzuzeigen, dass ein bestimmter Block vom Betriebssystem als frei angesehen wird, so dass dieser Block zur späteren Wiederverwendung vorbereitet werden kann, wurde der Befehl *Trim* eingeführt. Trim-Befehle sind Teil des Industriestandards ATA8-ACS2, der vorschreibt, wie Computer mit modernen Speicherlaufwerken kommunizieren sollen. Zusätzlich zur Aktualisierung seiner eigenen Dateisystemdaten, die angeben, welche Blöcke frei sind, kann das Betriebssystem per Trim nun auch das

Laufwerk informieren, welche Blöcke nicht mehr genutzt werden. Wenn eine SSD einen Trim-Befehl für einen bestimmten Speicherblock erhält, wird sie diesen Block auf ihre Merkliste zur Löschung setzen. Wenn das Laufwerk später Zeit für Aufräumarbeiten hat, wird es die jeweiligen Flash-Zellen in den betreffenden Blöcken löschen. Die Wahrscheinlichkeit, dass eingehende Schreibbefehle nun sofort nutzbare Blöcke finden, erhöht sich, so dass Schreibvorgänge jetzt so schnell wie möglich erledigt werden können.

In einer Standardkonfiguration sendet macOS Trim-Befehle nicht an alle SSDs, sondern nur an Flash-Speicherlaufwerke von Apple, da das System in diesem Fall sicher annehmen kann, dass die Trim-Befehle korrekt vom Laufwerk verarbeitet werden, diese also nicht zu Datenverlust oder Datenbeschädigung führen.

Sehr alte SSD-Laufwerke (aus einer Zeit bevor Trim genormt wurde) oder SSDs, die interne Konstruktionsfehler aufweisen, behandeln Trim-Befehle möglicherweise nicht richtig. Dies ist gefährlich, denn dies könnte zu Situationen führen, in der das Laufwerk einen *falschen* Block löscht, der immer noch vom Betriebssystem gebraucht wird. Dies würde typischerweise so aussehen, dass die eigentlichen Nutzdaten einer Datei mit 512 Bytes Nullen überschrieben werden. Um diese Gefahr zu umgehen, sendet macOS wie gesagt Trim-Befehle nur an SSDs von Apple; dort ist sicher, dass die Befehle korrekt umgesetzt werden.

Apple lässt Sie entscheiden, ob Sie Trim-Befehle mit allen Solid-State-Laufwerken von Drittanbietern nutzen möchten, genauer gesagt, SSDs, die an Ihr System über einen SATA-Bus und eine Busschnittstelle auf Basis des AHCI-Standards (Intel Advanced Host Controller Interface) angeschlossen sind. Das Umstellen der Betriebsart geschieht mit Apples Programm **trimforce**, das auf der UNIX-Befehlszeile aufgerufen werden muss. Der Systemintegritätsschutz stellt sicher, dass ausschließlich Software von Apple zum Ein- oder Ausschalten dieser Einstellung genutzt werden kann. Wir beschreiben die Nutzung von **trimforce** an dieser Stelle nicht. Ziehen Sie bitte Apples Dokumentation für weitere Informationen hinzu.

TinkerTool System kann die tatsächliche Betriebsart ermitteln, die in macOS ausgewählt ist, um mit Solid-State-Laufwerke zu kommunizieren. Öffnen Sie hierzu den Unterpunkt **SSDs** auf der Karte **Diagnose**.

SSDs mit SATA-Schnittstellen und AHCI-Protokoll sind veraltete Technik. Moderne Macs verwenden SSDs mit dem NVMe-Protokoll oder „rohe“ Flash-Speicher-Chips, die direkt an den Prozessor angeschlossen sind. Hier spielt die frühere Trim-Sperre für ältere SSDs keine Rolle mehr. TinkerTool System zeigt solche modernen Flash-Geräte nicht in der Tabelle an.

Die Tabelle auf dieser Karte zeigt alle relevanten SSDs, die an Ihren Mac angeschlossen sind, und listet ebenso auf, ob Trim-Befehle von macOS gesendet werden. Sie möchten wahrscheinlich den Status aller SSDs vor und nach der Umkonfigurierung des Betriebssystems durch trimforce überprüfen (nachdem der Computer neu gestartet wurde). Die Statuszeile unterhalb der Tabelle gibt an, ob die trimforce-Einstellung zurzeit im Betriebssystem eingeschaltet ist oder nicht.

2.7.5 Flash-Zustand

SSDs, bzw. die Flash-Speicherbausteine, aus denen solche Speichermedien aufgebaut sind, gelten genau wie magnetische Festplatten als Verschleißteile. Zwar gibt es hier keine mechanischen Bauelemente, die sich abnutzen können, aber jede Flash-Speicherzelle kann konstruktionsbedingt nur eine begrenzte Zahl von Löscho-, bzw. Schreiboperationen ausführen. Wird eine bestimmte Anzahl von Neuprogrammierungsvorgängen überschritten, kann die Speicherzelle irgendwann nicht mehr zuverlässig zwischen dem Zustand für 0 und 1

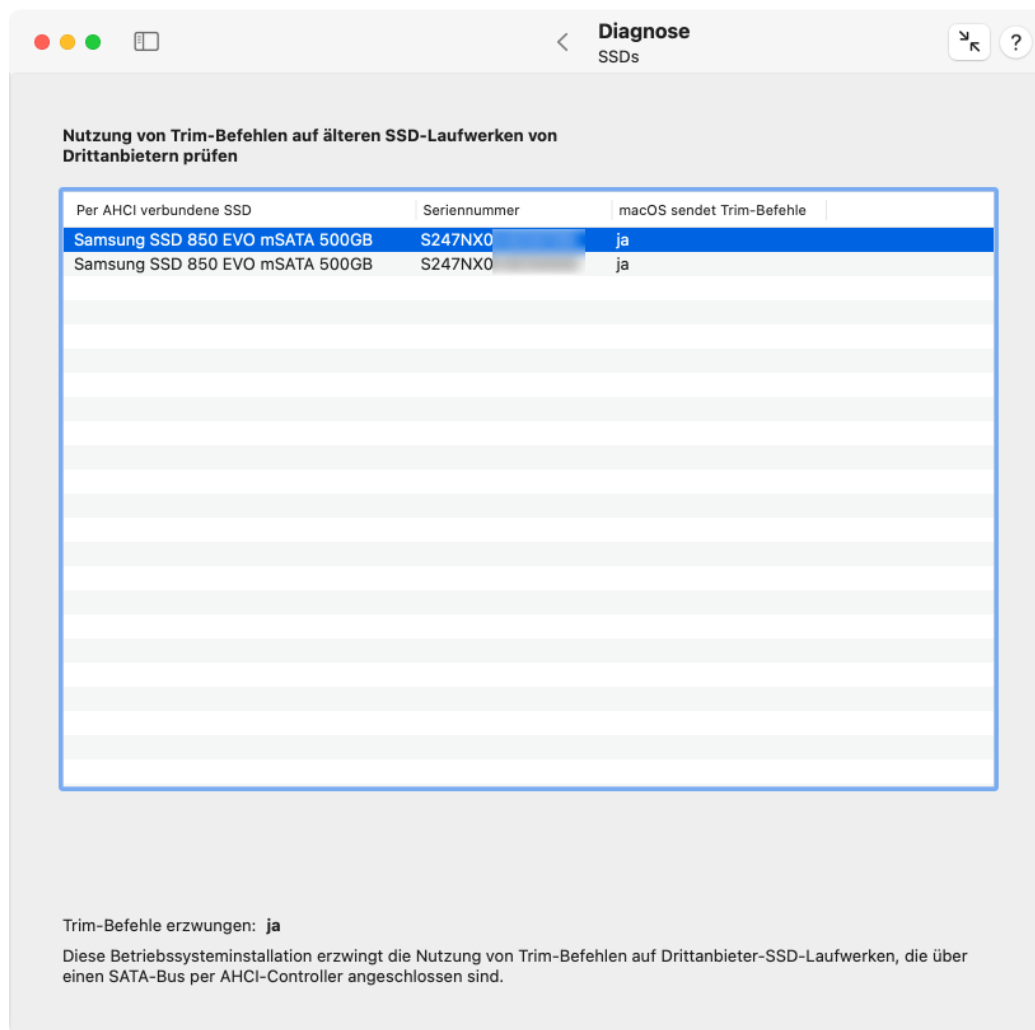


Abbildung 2.33: macOS kann Trim-Befehle an AHCI-verbundene SSDs von Drittanbietern senden

hin- und herschalten. Das betroffene Bit „bleibt hängen“ und der gesamte Speicherblock, in dem dieses Bit liegt, muss gesperrt werden, da der Block nicht mehr richtig funktioniert. Die Steuerung des Flash-Speichers ist auf solche Fälle vorbereitet und sorgt intern dafür, dass sich alle Blöcke möglichst gleichmäßig abnutzen. Außerdem ist der Speicherplatz überprovisioniert, d.h. es ist verdeckt mehr Speicherplatz vorhanden, als nach außen hin gemeldet wird. Der „zuviel“ vorhandene Speicher wird zum einen dafür verwendet, die langsame Geschwindigkeit von Löschvorgängen (siehe voriger Abschnitt) dadurch auszugleichen, dass immer genug im Voraus gelöschter Speicher als Reserve für Schreibvorgänge zur Verfügung steht, zum anderen wird er dafür verwendet, abgenutzte Speicherblöcke zu ersetzen.

Sie können den Gesundheitszustand des Flash-Speichers in Ihrem Mac mithilfe von TinkerTool System überprüfen lassen. Es lassen sich unter anderem statistische Daten abrufen, wieviele Schreib-/Lesevorgänge der Flash-Speicher bereits ausgeführt hat, wie lange er in Betrieb war, ob noch genug Reservespeicher zur Verfügung steht und wie stark der Speicher bereits abgenutzt ist. Hierbei spielt es keine Rolle, ob es sich um ein echtes SSD-Laufwerk handelt, oder ob es (wie bei allen modernen Macs üblich) um reine Flash-Speicherbausteine geht, bei denen ein Apple-Prozessor das Vorhandensein eines SSD-Laufwerks simuliert. Es muss sich allerdings um ein Originalbauteil von Apple für das jeweilige Mac-Modell handeln. SSD-Laufwerke von Drittanbietern werden von macOS nicht automatisch überwacht und deren Werte lassen sich daher nicht mit der Karte **Flash-Zustand** abrufen.

Genaue Daten werden nur garantiert, wenn die Kommunikation mit der Flash-Einheit auf *NVMe-Technik (Non-Volatile Memory Express)* basiert. Dies ist bei allen modernen Macintosh-Systemen der Fall, aber bei einigen älteren Macs, die AHCI-Kommunikation genutzt haben, unterstützt macOS nur eine sehr kleine Zahl von Gesundheitsmesswerten. TinkerTool System zeigt dies entsprechend an.

Es ist nicht notwendig, dass der Flash-Speicher benutzt wird oder ein aktiviertes Volume enthält, um ihn in der Übersicht erscheinen zu lassen. SSD-Einheiten, die Teil eines Apple Fusion Drive sind, werden ebenso automatisch in der Liste berücksichtigt.

Um TinkerTool System die Messwerte auslesen zu lassen, die macOS über Flash-Speicher von Apple ermittelt hat, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Flash-Zustand** auf der Einstellungskarte **Diagnose**.
2. Klicken Sie auf den Knopf **Aktualisieren** in der unteren rechten Ecke.

Alle erkannten Flash-Laufwerke von Apple werden nun in der oberen Tabelle angezeigt. Falls bei der Ermittlung der Daten ein Problem aufgetreten ist oder keine Originalteile von Apple vorhanden sind, bleibt die Tabelle leer und es erscheint die Meldung – **keine Einträge** –. Wenn Sie eine Zeile der Tabelle anklicken, werden die zugehörigen Messwerte für das ausgewählte Laufwerk in der unteren Hälfte des Fensters angezeigt.

Die Bedeutung der einzelnen Angaben ist wie folgt:

- **Modell:** Die offizielle Modellbezeichnung, unter der Apple die SSD (oder simulierte SSD) führt.
- **Revision:** Die Modellrevision der SSD, was sich auf Hardware- und Firmware-Version bezieht.
- **Seriennummer:** Die Seriennummer der SSD. Die Seriennummern von echten SSDs sind üblicherweise an der Verwendung von Großbuchstaben zu erkennen. Simulierte

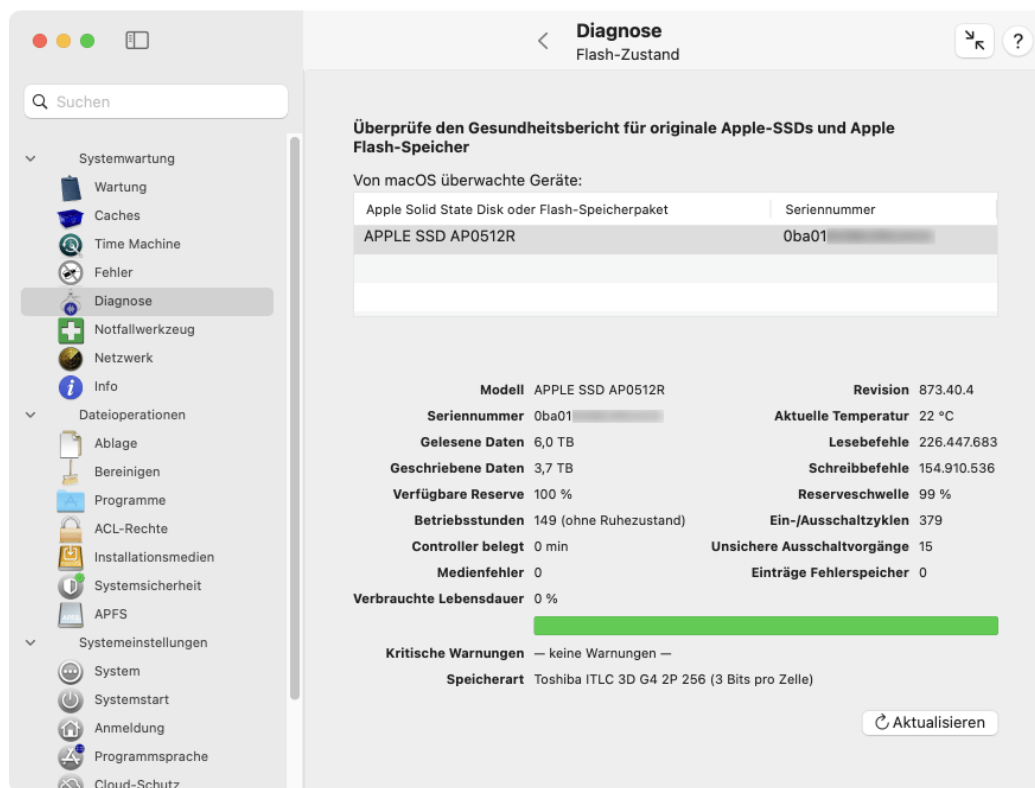


Abbildung 2.34: Überprüfen Sie den Zustand von originalem Apple-Flash-Speicher

SSDs tragen in der Regel nur einen festen Zufallscode aus den Ziffern 0 bis 9 und Kleinbuchstaben von a bis f.

- **Aktuelle Temperatur:** Die aktuell gemessene Betriebstemperatur des Flash-Speichers. Die Maßeinheit wird gemäß Ihrer persönlichen Landeseinstellungen bestimmt.
- **Gelesene Daten:** Die absolute Datenmenge, die während der bisherigen Lebensdauer der SSD aus dem Flash-Speicher gelesen wurde.
- **Lesebefehle:** Die Anzahl der Lesebefehle, die der angeschlossene Computer während der bisherigen Lebensdauer an die SSD gesendet hat.
- **Geschriebene Daten:** Die absolute Datenmenge, die während der bisherigen Lebensdauer der SSD in den Flash-Speicher geschrieben wurde.
- **Schreibbefehle:** Die Anzahl der Schreibbefehle, die der angeschlossene Computer während der bisherigen Lebensdauer an die SSD gesendet hat.
- **Verfügbare Reserve:** Die noch verfügbare Menge an Reservespeicher, die zur Verfügung steht, um defekte Flash-Speicherblöcke zu ersetzen. Die absolute Menge ist normalerweise ein Betriebsgeheimnis des Herstellers. Die Menge wird daher in Prozent seit der Herstellung angegeben. Sie beginnt bei 100% und sinkt dann mit fortschreitendem Alter.
- **Reserveschwelle:** Der vom Hersteller eingestellte Wert, bei dem die verbleibende Reserve als kritisch eingestuft wird. Fällt der Prozentwert für die Reserve unter diesen Wert, endet die Lebensdauer des Flash-Speichers in Kürze. Die SSD, bzw. die Hauptplatine des Mac sollte dann ausgetauscht werden.
- **Betriebsstunden:** Die Dauer in Stunden, in der die SSD vollständig eingeschaltet war. Der Ruhezustand von SSD oder Computer gilt nicht als Betriebszeit.
- **Ein-/Ausschaltzyklen:** Die Anzahl der Ein-/Ausschaltvorgänge während der bisherigen Lebensdauer der SSD.
- **Controller belegt:** Die Anzahl der Minuten, in der der Controller der SSD so beschäftigt war, dass er anstehende Befehle nicht sofort ausführen konnte. Dieser Wert kann dazu genutzt werden, um einzuschätzen, wie stark die SSD durch Aktivität belastet wird.
- **Unsichere Ausschaltvorgänge:** Die Anzahl von Situationen, in denen die SSD die Spannungsversorgung verloren hat, ohne dass der angeschlossene Computer vorher eine Benachrichtigung zum Herunterfahren gesendet hat. Die passiert beispielsweise bei einem unerwarteten Stromausfall. Der Controller der SSD sichert sich durch eine eigene Mini-Notstromversorgung gegen solche Vorfälle ab.
- **Medienfehler:** Die Anzahl der Fehler, die im Flash-Speicher über Prüfsummenverfahren erkannt und nicht behoben werden konnten. Es wurden fehlerhafte Daten gespeichert oder geliefert.
- **Einträge Fehlerspeicher:** Die Anzahl interner Fehlersituationen, die der Controller während der Lebensdauer der SSD intern beobachtet und aufgezeichnet hat.
- **Verbrauchte Lebensdauer:** Ein prozentueller Wert für die geschätzte Lebenszeit, die durch den Betrieb des Flash-Speichers bereits verbraucht wurde. Ein fabrikneuer Speicher trägt den Wert 0%. Hat die SSD die übliche „Laufleistung“ erreicht, die

vom Hersteller als normal angesehen wird, beträgt der Wert 100%. Hält der Speicher länger als erwartet, können Werte zwischen 100% und 255% angezeigt werden. Der nebenstehende Balken symbolisiert die geschätzte verbleibende Lebensdauer. Bei fabrikneuem Speicher ist der Balken vollständig grün. Durch Alterung wird der grüne Bereich kleiner und durch grau ersetzt. Die Schätzung wird vom Controller der SSD vorgenommen, nicht von macOS oder von TinkerTool System.

- **Kritische Warnungen:** Eine Liste von Warnungen, die die Gesundheit des Flash-Speichers betreffen und vom Controller im permanenten Fehlerspeicher festgehalten wurden. Übliche Warnungen sind:
 - die Menge an Reservespeicher ist unter die kritische Schwelle gesunken
 - die zulässige Betriebstemperatur wurde überschritten
 - es wurde eine hohe Zahl an Medienfehlern beobachtet
 - das Medium wurde per Hardware-Einstellung in den Nur-Lese-Betrieb versetzt
 - die interne Notstromversorgung des Controllers ist mindestens einmal ausgefallen
- **Speicherart:** Diese Angabe steht nur für bestimmte Modelle der neuesten Mac-Baureihen zur Verfügung. Sie bezieht sich auf Flash-Speicher, der unmittelbar an einen *Apple*-Prozessor angeschlossen ist. Falls möglich, wird versucht, Hersteller und Marketingname des Flash-Speichers auszulesen. Auch die Basistechnik der Flash-Speicherzellen, nämlich die Anzahl der Bits, die pro physischer Zelle speicherbar ist, kann angegeben sein. Flash-Speicher der Bauart *TLC (Triple Level Cell)* kann beispielsweise 3 Bits pro Zelle festhalten. Eine höhere Bit-Zahl bedeutet üblicherweise mehr Speicher zu niedrigerem Preis, gleichzeitig aber auch weniger Betriebssicherheit.

2.7.6 Schnelltest mit Kühlungslüftern durchführen

Viele Macs müssen ständig gekühlt werden, was durch ein oder mehrere Gebläse erledigt wird, die frische Luft in den Computer ziehen und heiße Luft nach außen drücken. Die meisten dieser Lüfter werden kontinuierlich überwacht und durch einen unabhängigen Hilfscomputer gesteuert, der in Ihren Mac eingebaut ist. In älteren Macs übernimmt dies der *System Management Controller (SMC)*, in späteren Modellen ein *Apple T2*-Prozessor, auf dem Apples BridgeOS-Betriebssystem läuft, und in modernen Macs mit Apple-Chips der M-Prozessor selbst. Lüfter sind mechanische Bauteile, die ständig in Betrieb sind, wenn der Computer läuft, so dass es sich um Komponenten handelt, die natürlichem Verschleiß unterliegen. Falls Sie ungewöhnliche Geräusche aus Ihrem Mac hören und Sie vermuten, dass einer seiner Lüfter nicht mehr richtig arbeitet, z.B. als Folge eines Lagerschadens, kann es hilfreich sein, schnell alle Lüfter selbst zu testen, ohne den Mac öffnen zu müssen. TinkerTool System kann dies erledigen, indem es einen Lüfter vorübergehend zwingt, auf sein zulässiges Maximum zu beschleunigen, wobei die aktuellen Drehzahlwerte angezeigt werden. Indem Sie das Antwortverhalten des Lüfters hören, können Sie leicht dessen Position finden und beurteilen, ob er normal zu arbeiten scheint.

Ab Dezember 2017 hat Apple damit begonnen, die Lüftersteuerungs-Hardware einiger Macintosh-Baureihen gegen den Zugriff durch Programme abzuschotten. In diesem Fall kann TinkerTool System die Bezeichnungen und Lagepositionen der Lüfter nicht ermitteln.

Um einen Test mit einem oder mehreren Lüftern laufen zu lassen, führen Sie die folgenden Schritte durch:

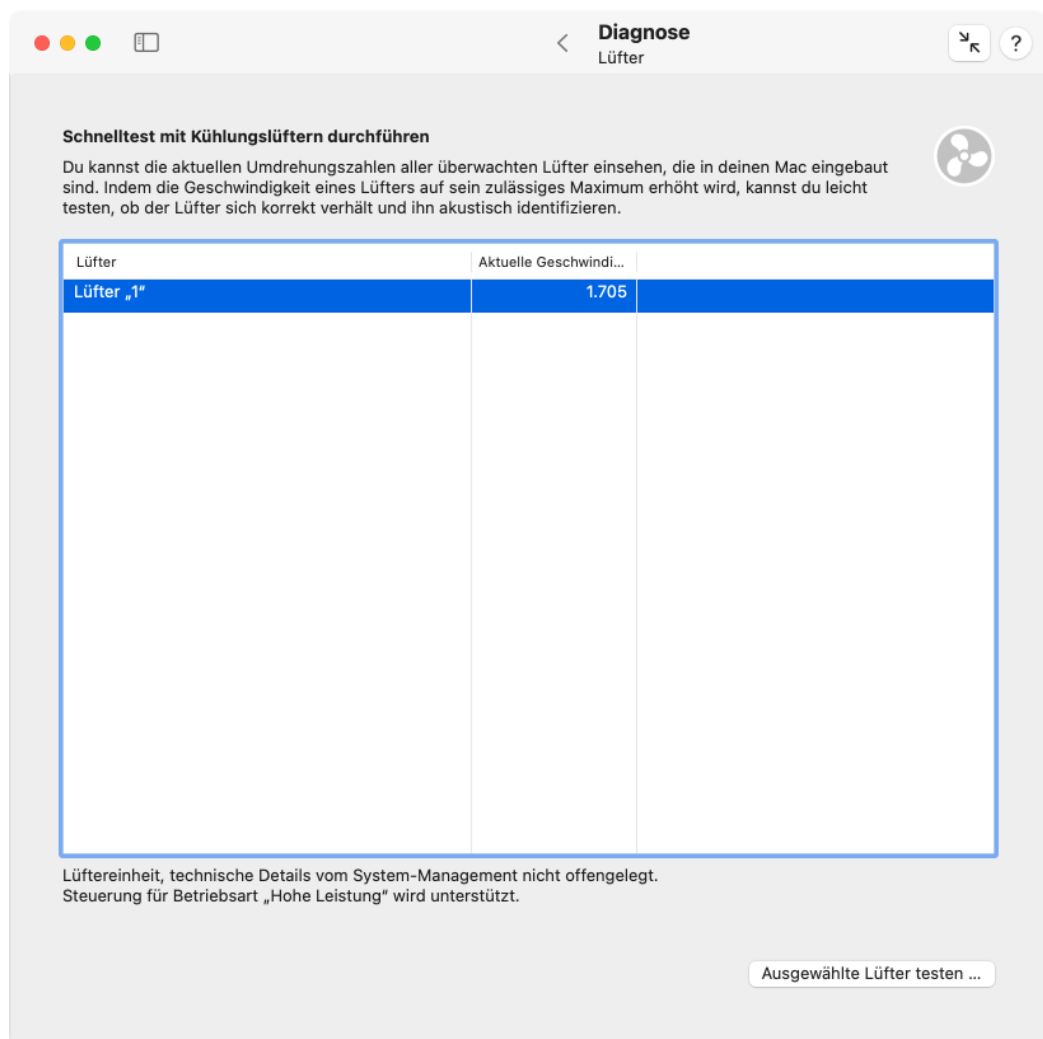


Abbildung 2.35: Kühllüfter des Macs überprüfen

1. Öffnen Sie den Unterpunkt **Lüfter** auf der Einstellungskarte **Diagnose**.
2. Wählen Sie einen oder mehrere Lüfter, die getestet werden sollen, in der Tabelle aus.
3. Drücken Sie den Knopf **Ausgewählte Lüfter testen**
4. Wenn Sie die Überprüfung der Lüfter abschließen möchten, drücken Sie den Knopf **Test beenden**.

Die aktuellen Geschwindigkeitswerte werden in der Tabelle angezeigt und laufend auf den neuesten Stand gebracht. Wenn Sie eine einzelne Zeile in der Tabelle auswählen, werden technische Details über den Lüfter und seine ungefähre Lage innerhalb des Gehäuses des Macs unter der Tabelle angezeigt.

Falls Sie ein Drittanbieterprogramm verwenden, um die eingebaute Standardlüftersteuerung des Mac zu manipulieren, wird TinkerTool System dieses Programm nicht beeinflussen und eine Fehlermeldung wird auf der Einstellungskarte angezeigt. Um Lüftertests laufen zu lassen, müssen Sie das andere Programm erst vorher deaktivieren und dann TinkerTool System neu starten.

Zusätzliche Überlegungen bei modernen Macs

Bei einigen Computermodeilen, die ab November 2023 oder später vorgestellt wurden (M3-Prozessoren oder höher), können die Lüfter und Lüftersteuerungseinheit vollständig ausgeschaltet sein, falls das System nicht warm genug ist, Kühlung zu benötigen. Im Unterschied zu früheren Hardware-Generationen, können Programme wie TinkerTool System dies nicht mehr übergehen. Die Lüfter bleiben abgeschaltet, als wären sie nicht vorhanden. Das Programm versucht, diese Situation zu erkennen und signalisiert diese besondere Situation mit einer Fehlermeldung, die unterhalb der Lüfertabelle angezeigt wird. Um die Lüfter in dieser Konstellation zu testen, führen Sie die folgenden Schritte durch:

1. Erzeugen Sie Rechenlast auf dem System, so dass die Prozessorkerne aktiv werden und Hitze erzeugen.
2. Warten Sie, bis die Anzeigen **Aktuelle Geschwindigkeit (RPM)** in der Tabelle von **0** auf einen höheren Wert wechseln. Dies zeigt an, dass die Lüfter-Hardware eingeschaltet wurde.
3. Beenden Sie TinkerTool System.
4. Starten Sie TinkerTool System erneut. Die Fehlermeldung bezüglich der Lüftersteuerung sollte nun nicht mehr angezeigt werden und Sie können die Lüfter wie vorher beschrieben testen.

Falls Sie kein Anwenderprogramm haben, das den Mac zwingt, eine dauernde Arbeitslast zu verarbeiten, können Sie unser kostenloses Hilfsprogramm **SystemLoad** herunterladen: <https://www.bresink.com/osx/SystemLoad-de.html>

2.7.7 Anmeldezeitabrechnung

macOS ist ein Unix-System und hat als solches seine Wurzeln im klassischen *Time-Sharing-Betrieb*, der in den 1950er-Jahren und danach genutzt wurde. Die Benutzer haben sich über eine Terminal-Leitung mit einem großen zentralen Computer verbunden, sich dort mit ihrem Account angemeldet, einige Programme laufen lassen und danach die Verbindung

wieder getrennt. Die Nutzung des Computers musste pro Minute bezahlt werden. Die Verbindungszeitstatistik, die für diese Art der Abrechnung notwendig ist, wird auch heute immer noch geführt. TinkerTool System erlaubt es Ihnen, Zugriff auf diese Daten zu erhalten. Sie können entweder die Gesamtverbindungszeit pro Benutzer abrufen oder die Gesamtzeit, an der der Mac pro Tag genutzt wurde.

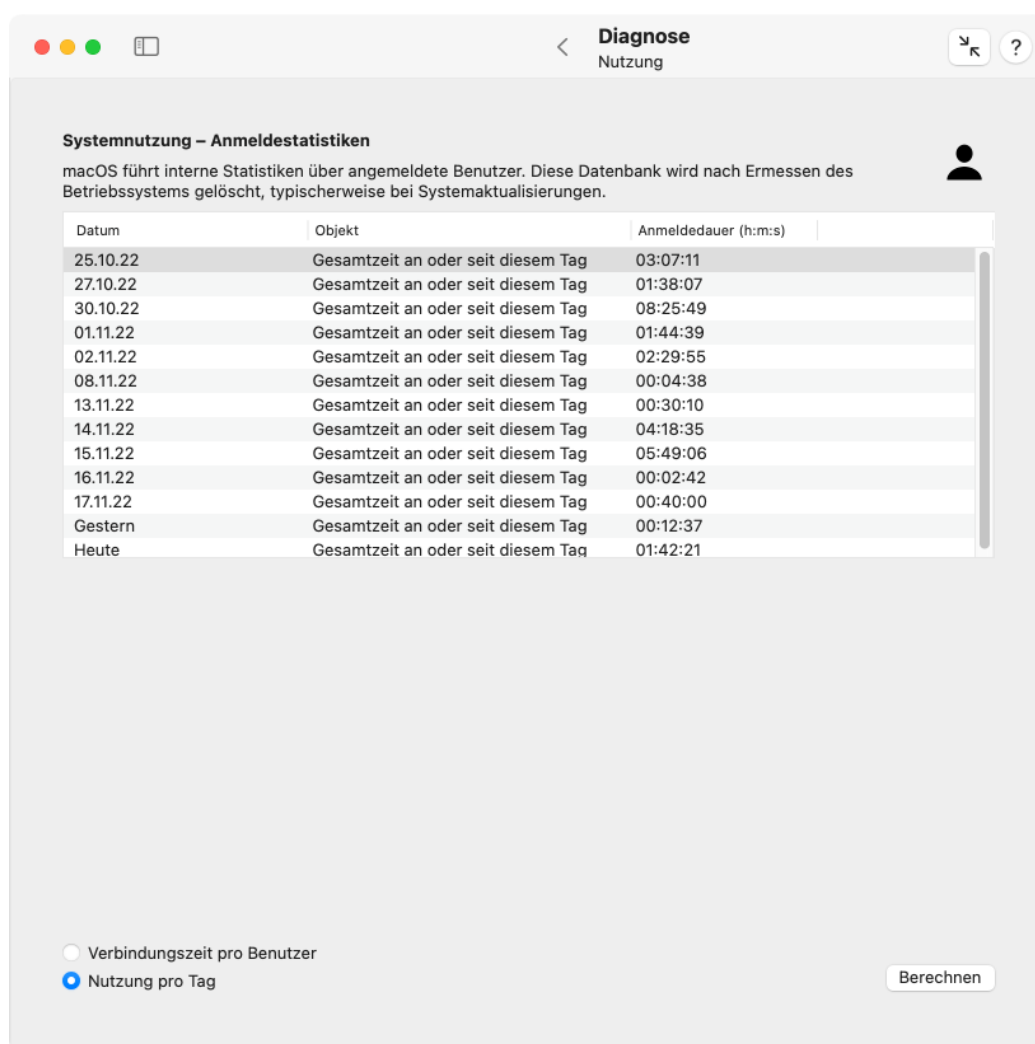


Abbildung 2.36: Rufen Sie die Statistik der Anmeldezeiten ab, die von macOS geführt wird

1. Öffnen Sie den Unterpunkt **Nutzung** auf der Einstellungskarte **Diagnose**.
2. Wählen Sie eine der Berichtsarten in der unteren linken Ecke.
3. Drücken Sie auf den Knopf **Berechnen**.

Das Ergebnis wird in der Tabelle angezeigt. Beachten Sie hierbei Folgendes:

- Die Anmeldedauer wird im Format Stunden/Minuten/Sekunden angegeben, getrennt durch Doppelpunkte (:). Falls ein Zeitintervall länger als einen Tag ist, wird die Anzahl der Tage zusätzlich mit der Einheit *d* (day) angezeigt.

- Die Aufzeichnungen der Verbindungszeit werden automatisch von macOS gesammelt. TinkerTool System hat keinen Einfluss auf die Genauigkeit der Daten. Das Betriebssystem kann die internen Statistiken nach eigenem Ermessen löschen. Dies geschieht üblicherweise während System-Upgrades.
- Die Anmeldezeit ist das Zeitintervall zwischen dem Punkt, an dem sich ein Benutzer angemeldet hat (entweder automatisch durch macOS bzw. FileVault, oder manuell durch Angabe seines Kennworts) und dem Punkt, an dem sich dieser Benutzer abmeldet (entweder automatisch wenn der Computer heruntergefahren wird, oder manuell).
- Alle Anmeldevorgänge werden berücksichtigt. Dies schließt die Arbeit am Bildschirm des Mac ein (was nach den Begriffen des Time-Sharing *Konsolenanmeldung* genannt wird), Schnelle Benutzerumschaltung, Anmeldung über eine Terminal-Sitzung, oder ferne Anmeldungen über ein Netzwerk. Die Nutzung von Dateifreigaben (File Server) wird jedoch üblicherweise *nicht* als Anmeldung gezählt. Dies kann vom File Server abhängen.
- Die Zeitintervalle werden auf Basis der echten Uhrzeit berechnet. Falls ein Benutzer angemeldet ist während sich der Computer im Ruhezustand oder Standby-Modus befindet, wird die Ruhezeit trotzdem als Anmeldezeit gezählt.
- Die Statistiken pro Benutzer werden über die *Kurznamen* der Benutzer verwaltet, die gültig waren, als diese Benutzer Zugang zum Computer hatten. Das heißt auch alte, umbenannte Accounts oder gelöschte Accounts können immer noch in der Liste auftauchen. Die kurzen Benutzernamen werden auf der Karte **Benutzer:innen & Gruppen** der Systemeinstellungen *Accountnamen* genannt und stimmen mit den Ordernamen der Privatordner jedes Benutzers überein.
- Die Auswertung kann Einträge für Benutzer mit den Namen *root* und *_mbsetupuser* enthalten. Es handelt sich hierbei um Accounts, die macOS intern während System-Updates nutzt.
- Obwohl kein privilegierter Vorgang notwendig ist, um diese Funktion zu nutzen, ist Leserecht für die Anmeldedaten erforderlich, da hier persönliche Daten Dritter betroffen sind. Sie müssen als Administrator angemeldet sein, um die Daten abrufen zu können.

2.7.8 Monitore testen

Je nach ihrer Qualitätsgüte können Bildschirme ab Werk bestimmte Fehler aufweisen: Einzelne Bildpunkte (Pixel) funktionieren gar nicht oder nicht immer zuverlässig. Auch Alterung des Gerätes kann zu solchen Bildfehlern führen. Abhängig von der verwendeten Display-Technik werden die einzelnen Farben der Bildpunkte dadurch erzeugt, dass sie entweder selbst zum Leuchten gebracht werden, oder indem weißes Licht von hinten auf ein Pixel gestrahlt wird, das dann bestimmte Farben ausfiltert und andere durchlässt. Der letztendliche Farbeindruck jedes Bildpunktes entsteht dadurch, dass eine bestimmte Menge rotes, grünes und blaues Licht, das auf diese Weise erzeugt oder gefiltert wird, miteinander gemischt wird.

Die technischen Vorrichtungen, die für rotes, grünes und blaues Licht in einem Bildpunkt verantwortlich sind, sind baulich voneinander getrennt. Liegt ein Defekt bei einem bestimmten Pixel vor, dann fällt üblicherweise der Mechanismus aus, der für das Erzeugen oder Ausblenden einer dieser drei Farben verantwortlich ist. Eine Grundfarbe eines Bildpunktes lässt sich dann entweder nicht mehr einschalten („totes Pixel“) oder nicht mehr abschalten („hängendes Pixel“).

Sie können mit TinkerTool System einen angeschlossenen Bildschirm testen, indem Sie alle Grundfarben und deren Mischungen gezielt für alle Pixel dieses Bildschirms ein- und ausschalten. Durch Auswählen von roten, grünen oder blauen Farbflächen lassen sich tote Pixel als schwarze Punkte erkennen. Durch Auswählen einer Mischfarbe oder Umschalten von Weiß auf eine Grundfarbe lassen sich hängende Pixel als weiße oder flimmernde Punkte erkennen. Sind alle Pixel in Ordnung, werden die Farben fehlerfrei über die ganze Bildfläche hinweg angezeigt.

Einige Macintosh-Systeme mit eingebautem Display sind außerdem dafür berüchtigt, dass die Glas- und Folienelemente, aus denen der Bildschirm besteht, nicht perfekt nach außen hin abgedichtet sind. Dadurch kann Staub und Feuchtigkeit eindringen und zu Schlieren, insbesondere an den Ecken des Bildes, führen. Solche Defekte lassen sich mit einem komplett weißen Bild leicht prüfen. Ein komplett schwarzes Bild kann dagegen nützlich sein, wenn Sie das Glas des Bildschirms reinigen möchten, ohne den Computer abschalten zu müssen. Schmutz auf der Glasoberfläche lässt sich dann gut erkennen.

TinkerTool System stellt die folgenden Testbilder bereit:

- schwarzes Bild
- rein weiße Farbfläche
- rein rote Farbfläche
- rein grüne Farbfläche
- rein blaue Farbfläche
- rein zyan-farbige Farbfläche („weiß ohne rot“)
- rein magenta-farbige Farbfläche („weiß ohne grün“)
- rein gelbe Farbfläche („weiß ohne blau“)
- vertikale Balken mit allen genannten Farben, ähnlich dem Testbild der Europäischen Rundfunkunion

Sie können die Testbilder wie folgt abrufen:

1. Öffnen Sie den Unterpunkt **Monitore** auf der Einstellungskarte **Diagnose**.
2. Drücken Sie auf den Knopf **Monitortest starten**.
3. Falls mehrere Bildschirme angeschlossen sind, werden Sie gefragt, auf welchem der Test durchgeführt werden soll. Wählen Sie den gewünschten Monitor aus und drücken Sie auf **OK**.
4. Sie können mit der Tastatur die einzelnen Testbilder auswählen (siehe unten). Der Test lässt sich mit der Taste **esc** beenden.

Wenn die Farbflächen eingeblendet sind, ist es zusätzlich möglich, ein pulsierendes schwarzes Gitterraster zu überblenden, das sich hin und her bewegt. Durch Drücken der Taste **1** wird ein Gitter mit einem Abstand von 1 physischen Pixel erzeugt, mit **2** ein Gitter mit dem Abstand 2. Sie sehen danach ein sehr feines Schachbrettmuster, dessen Felder stetig hin und her wechseln. Auf diese Weise werden fehlerhafte Pixel noch deutlicher sichtbar. Sie können diese Zusatzfunktion über die Taste **0** wieder ausschalten.

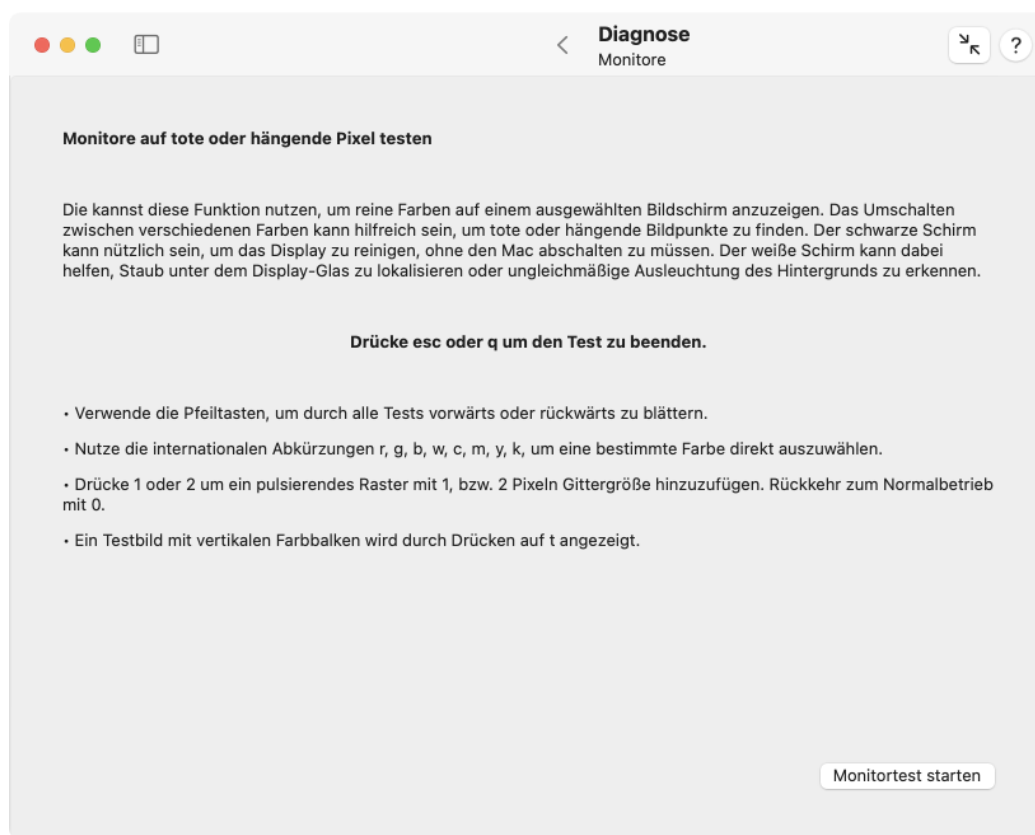


Abbildung 2.37: Angeschlossene Bildschirme können über Farbflächen getestet werden

Epilepsiehinweis für photosensitive Menschen: Das Programm sorgt dafür, dass der Wechseleffekt eine Frequenz von 2 Hz nicht überschreitet. Das hierdurch hervorgerufene Blinkmuster gilt als unbedenklich.
 Das Gitterraster ist bei der Anzeige der Farbbalken nicht aktiv. Beim Schwarzbild ist es naturgemäß nicht sichtbar.

Die Auswahl der Grundfarben mit Tasten entspricht den in der Drucktechnik üblichen internationalen Farbbabkürzungen.

Tabelle 2.1: Tasten zum Steuern der Testbilder

Taste	Funktion
oder	Test beenden
oder oder	nächstes Testbild
oder	voriges Testbild
	schwarz
	weiß
	rot
	grün
	blau
	zyan
	magenta
	gelb
	Testbild mit Farbbalken
	bewegendes schwarzes Gitterraster der Größe 1 hinzufügen
	bewegendes schwarzes Gitterraster der Größe 2 hinzufügen
	Funktion Gitterraster abschalten

2.8 Die Einstellungskarte Notfallwerkzeug

2.8.1 Einführung in das Notfallwerkzeug

In kritischen Fällen kann es dazu kommen, dass Ihre Installation von macOS aufgrund eines Festplattendefekts oder durch ein Drittanbieterprogramm, das Administratorrechte verwendet hat, so weit beschädigt wird, dass das Betriebssystem nicht mehr richtig oder gar nicht mehr startet. Wenn sich aufgrund eines solchen Problems das Betriebssystem nicht mehr bedienen lässt, können Sie auch Dienstprogramme wie TinkerTool System nicht mehr nutzen, um das Problem zu beheben.

Ebenso könnte es passieren, das macOS zwar noch läuft, jedoch eine wichtige Systemkomponente, die von TinkerTool System benötigt wird, beschädigt wurde. Selbst wenn TinkerTool System in der Lage ist, diese Komponente während des Normalbetriebs zu reparieren, so hilft Ihnen das in diesem speziellen Fall nicht weiter, wenn Sie TinkerTool System aufgrund der Beschädigung nicht mehr starten können.

TinkerTool System bietet Ihnen jedoch eine Lösung an, die Ihnen auch in diesen beiden kritischen Fällen weiterhelfen kann. Das Programm enthält eine Mini-Version, die Sie im speziellen Wiederherstellungs-Betriebssystem von macOS aufrufen können. Das

Wiederherstellungs-Betriebssystem ist auf einem speziellen Nur-Lese-Volume als Ergänzung jedes Betriebssystems installiert. Es sollte sich auch in Notfällen jederzeit aufrufen lassen. Die kleine, weitgehend auf sich alleine gestellte Version von TinkerTool System wird im Folgenden *TinkerTool System für macOS-Wiederherstellung* genannt, abgekürzt **ttsfrm** (*TinkerTool System for Recovery Mode*).

Beachten Sie, dass Sie sich *vorher*, also bevor ein kritisches Problem auftritt, darüber informieren sollten, wie man TinkerTool System für macOS-Wiederherstellung aufruft. Sie sind dann für den Notfall gerüstet. Die entsprechende Kurzanleitung lässt sich ausdrucken. **Sie kann für jeden Computer unterschiedlich sein.**

2.8.2 Ausdrucken der Anleitung

Um die Anleitung zum Aufruf von *TinkerTool System für macOS Wiederherstellung* zu drucken, führen Sie folgende Schritte durch:

1. Öffnen Sie die Karte **Notfallwerkzeug** aus der Rubrik **Systemwartung**.
2. Betätigen Sie den Knopf **Diese Anleitung drucken**

TinkerTool System passt die Ausgabe automatisch an die Papiergröße Ihres Druckers an.

2.8.3 Struktur des Startbefehls

Der für Ihren Computer gültige Startbefehl ist am Ende der Anleitung aufgeführt. Der Befehl unterscheidet sich je nach Ablageort der Software und der Benennung Ihrer Volumes, Ordner und Programm. Er könnte beispielsweise lauten:

```
"/Volumes/Macintosh HD - Daten/Applications/TinkerTool System.app/
Contents/SharedSupport/ttsfrm.app/Contents/MacOS/ttsfrm"
```

Der konkrete Aufruf, der als einzelne Zeile in das Programm **Terminal** eingetippt werden muss um das Programm zu starten, lässt sich nach folgendem Prinzip rekonstruieren:

1. Der Befehl beginnt immer mit **"/Volumes/**.
2. Es folgt der Name des Volumes, auf dem TinkerTool System gespeichert ist, gefolgt von einem Schrägstrich.
3. Es folgt der Pfad durch die Ordnerhierarchie, in der TinkerTool System auf diesem Volume gespeichert ist, jeweils getrennt durch Schrägstriche. Es muss der wahre Name der jeweils beteiligten Ordner verwendet werden, keine vom Finder in die Landessprache übersetzten Ordner. Der Ordner **Programme** heißt beispielsweise in Wirklichkeit **Applications**.
4. Es folgt der Name des Programms, in diesem Fall **TinkerTool System** gefolgt von der Angabe **.app** und einem Schrägstrich. Falls Sie das Programm umbenannt haben, müssen Sie den entsprechenden Namen austauschen.
5. Der Befehl endet immer mit **Contents/SharedSupport/ttsfrm.app/Contents/MacOS/ttsfrm"**.
6. Nach Ende des Befehls muss die Eingabetaste gedrückt werden.

Das Muster des Aufrufs lautet also

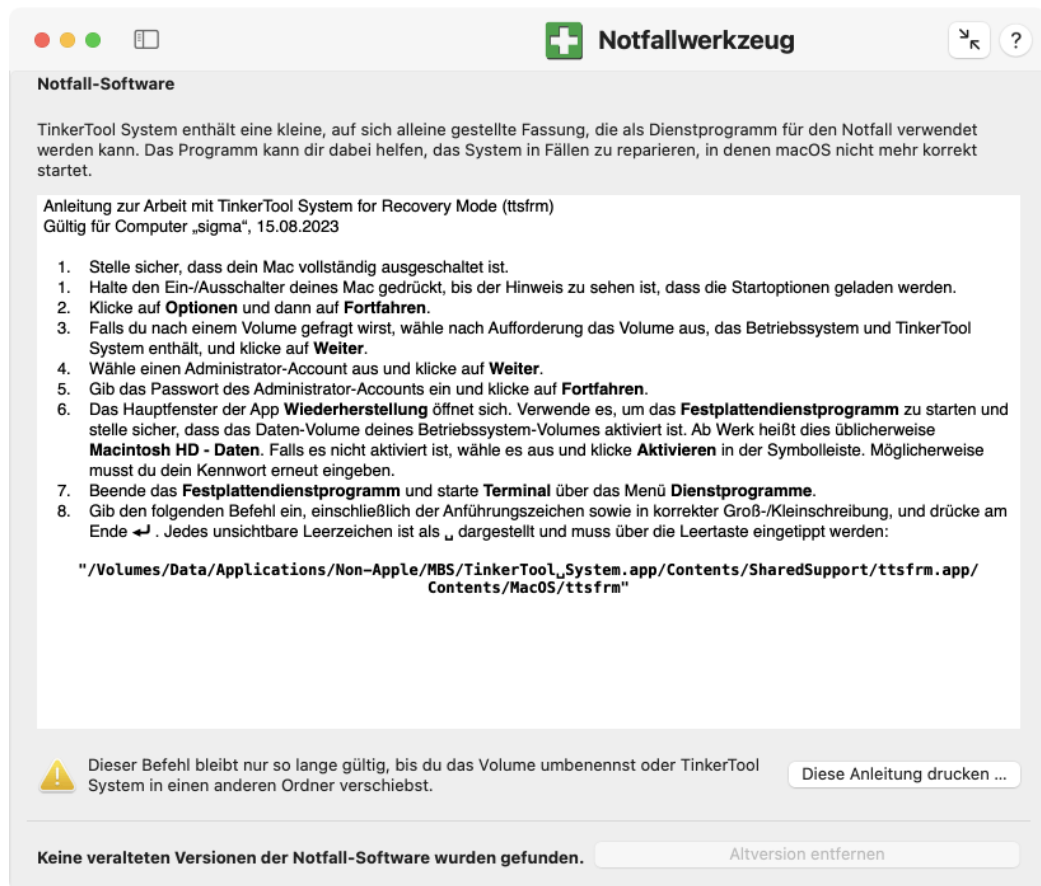


Abbildung 2.38: Notfallwerkzeug - Die im Bild gezeigte Anleitung ist individuell für jeden Computer und trifft auf Ihre Situation möglicherweise nicht zu.

```
"/Volumes/<volume>/<ordner1></...><ordnerX>/<programm>.app/  
Contents/SharedSupport/ttsfrm.app/Contents/MacOS/ttsfrm"
```

Hierbei müssen die mit spitzen Klammern gekennzeichneten Teile durch die Namen ersetzt werden, die auf Ihrem Computer gelten. Lassen Sie die Anführungszeichen nicht weg und ersetzen Sie diese nicht durch typografische Anführungszeichen. Drücken Sie die Eingabetaste erst am Ende, auch wenn der Befehl oben aus Platzgründen in mehreren Zeilen geschrieben ist. Damit Sie Leerzeichen besser erkennen können, sind diese in der Anleitung mit dem speziellen Zeichen `␣` markiert.

Zusammenhang zwischen Ablageort und Reparaturmöglichkeiten

Falls Sie mehrere Volumes mit Ihrem Mac verwenden oder sogar mehrere Betriebssysteme auf Ihrem Mac installiert sind, gibt es Einschränkungen, auf welches Volume Sie später im Wiederherstellungsmodus zugreifen können und welches Betriebssystem sich reparieren lässt. Es gilt folgende Grundregel:

TinkerTool System für macOS-Wiederherstellung arbeitet immer nur auf der Volume-Gruppe und dem dazugehörigen Betriebssystem, auf der das Programm selbst gespeichert ist.

Daraus ergeben sich folgende Konsequenzen:

- TinkerTool System sollte immer auf der Volume-Gruppe liegen, auf der auch das Betriebssystem gespeichert ist.
- Falls Sie mehrere Betriebssysteme einsetzen, sollte jeweils ein eigenes Exemplar von TinkerTool System auf jeder System-Volume-Gruppe liegen.

Eine Volume-Gruppe für macOS besteht aus dem System-Volume, dem zugehörigen Schnappschuss-Volume und dessen Daten-Volume. Sie können diese Gruppierung über die Karte APFS (Abschnitt 3.7 auf Seite 228) im Detail anzeigen lassen.

2.8.4 Verwenden des Notfallwerkzeugs

TinkerTool System für macOS-Wiederherstellung kann nur im Wiederherstellungsbetrieb von macOS verwendet werden. Detaillierte Informationen zur Bedienung erhalten Sie im Kapitel Arbeiten in der macOS-Wiederherstellung (Abschnitt 6 auf Seite 297).

2.8.5 Alte Versionen des Notfallwerkzeugs

Frühere Fassungen von TinkerTool System wurden mit einem anderen Werkzeug für den Notfall ausgeliefert, das für den sogenannten *Einbenutzerbetrieb* von macOS konzipiert war. Dieses Programm musste in einem besonderen Arbeitsschritt installiert werden. Apple unterstützt den Einbenutzerbetrieb von macOS nicht mehr offiziell und viele Macs sind so voreingestellt, dass der Einbenutzerbetrieb aus Sicherheitsgründen gesperrt wird. Hierdurch ist das alte Programm überflüssig geworden und sollte entfernt werden. TinkerTool System erkennt automatisch, ob eine alte Fassung der früheren Software im gerade laufenden Betriebssystem vorhanden ist und zeigt dies unten auf der Karte **Notfallwerkzeug** an. Drücken Sie in diesem Fall einfach auf den Knopf **Altversion entfernen** und folgen Sie den Anweisungen des Programms, um den Mac zu bereinigen.

2.9 Die Einstellungskarte Netzwerk

Die Einstellungskarte **Netzwerk** kann dazu genutzt werden, die weggefallenen Funktionen aus dem früheren **Netzwerkdienstprogramm** zu ersetzen, das in älteren Versionen von macOS Bestandteil des Betriebssystems war. TinkerTool System stellt einen ähnlichen Funktionsumfang zur Verfügung und enthält darüber hinaus zusätzliche, modernisierte Features, insbesondere zur Unterstützung des heute üblichen Protokolls IPv6.

2.9.1 Informationen über Netzwerkschnittstellen

Sie können technische Detaildaten und Statistiken über alle Netzwerkschnittstellen des Mac abrufen, die im Moment gerade aktiv sind. Aktiv bedeutet, dass dem Anschluss mindestens eine IPv4- oder IPv6-Adresse zugewiesen wurde, die zur Kommunikation mit anderen Geräten verwendet werden kann. Um die Daten abzurufen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie den Punkt **Info** auf der Karte **Netzwerk**.
2. Wählen Sie über den Menüknopf diejenige Schnittstelle aus, zu der Sie Informationen abrufen möchten.

Die Daten die im Fenster angezeigt werden, aktualisieren sich automatisch etwa alle 10 Sekunden.

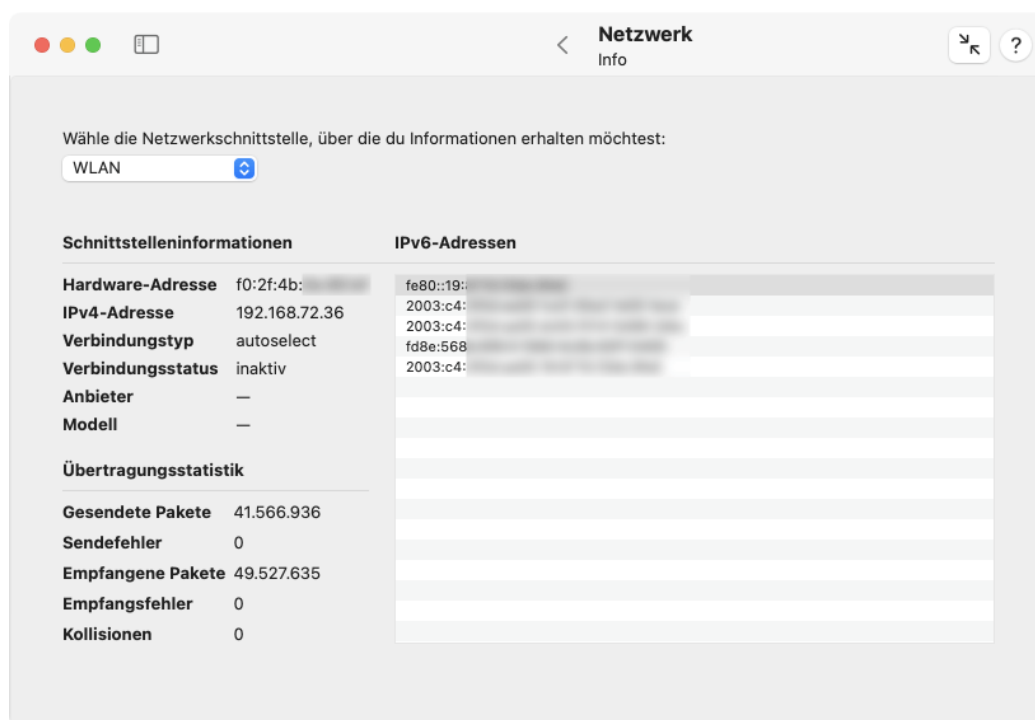


Abbildung 2.39: Detaildaten über jeden aktiven Netzwerkanschluss können ermittelt werden

Die folgende Details sind abrufbar:

- **Hardware-Adresse:** die in der Hardware vorgegebene Adresse des Anschlusses, die für die Kommunikation auf der Medienzugriffsebene standardmäßig verwendet wird. Diese Adresse wird auch *MAC-Adresse (Medium Access Control)* genannt.
- **IPv4-Adresse:** die im Moment zugewiesene Adresse für das Internet-Protokoll Version 4.
- **Verbindungstyp:** der Detailtyp der Netzwerkverbindung. Die genaue Bedeutung hängt von der Art des Anschlusses ab. In der Regel wird die momentan gewählte Datenübertragungsrate angegeben.
- **Verbindungsstatus:** der aktuelle Status des Netzwerkanschlusses im Betriebssystem.
- **Anbieter:** der Hersteller des physischen Anschlusses.
- **Modell:** Art des Anschlusses oder Bezeichnung des Hardware-Modells.
- **IPv6-Adressen:** die Liste der aktuell zugewiesenen Adressen für das Internet-Protokoll Version 6.
- **Gesendete Pakete:** die Anzahl der seit dem Start des Betriebssystems vom Computer gesendeten Datenpakete.
- **Sendefehler:** Anzahl der gesendeten Pakete, bei denen ein Fehler entdeckt wurde.
- **Empfangene Pakete:** die Anzahl der seit dem Start des Betriebssystems vom Computer empfangenen Datenpakete.
- **Empfangsfehler:** Anzahl der empfangenen Pakete, bei denen ein Fehler entdeckt wurde.
- **Kollisionen:** bei Netzwerktechniken, bei denen es technisch möglich ist, dass mehrere Geräte unsynchronisiert gleichzeitig Daten senden, wodurch diese sich gegenseitig stören, die Anzahl der Fälle, in denen solche Übertragungskollisionen aufgetreten sind.

2.9.2 Routing-Tabellen und Netzwerkstatistiken

Über den Punkt **Netstat** können Sie weitere Statistiken aus der Netzwerkverwaltung von macOS abrufen, die für alle Anschlüsse relevant sind.

1. Öffnen Sie den Punkt **Netstat** auf der Karte **Netzwerk**.
2. Wählen Sie über einen der Radioknöpfe denjenigen Punkt aus, zu dem Sie Daten abrufen möchten.
3. Betätigen Sie die Schaltfläche **Netstat**.

Die Daten werden daraufhin abgerufen und in einem weiteren Dialog angezeigt. Sie können das Ergebnis auch ausdrucken lassen oder als Textdatei abspeichern.

Bitte beachten Sie, dass macOS für einige Informationen mehrere Minuten Rechenzeit benötigen kann, bevor Daten angezeigt werden. Der Bericht wird in englischer Sprache direkt aus der UNIX-Ebene heraus erstellt.

Es lassen sich folgende Statistiken abrufen:

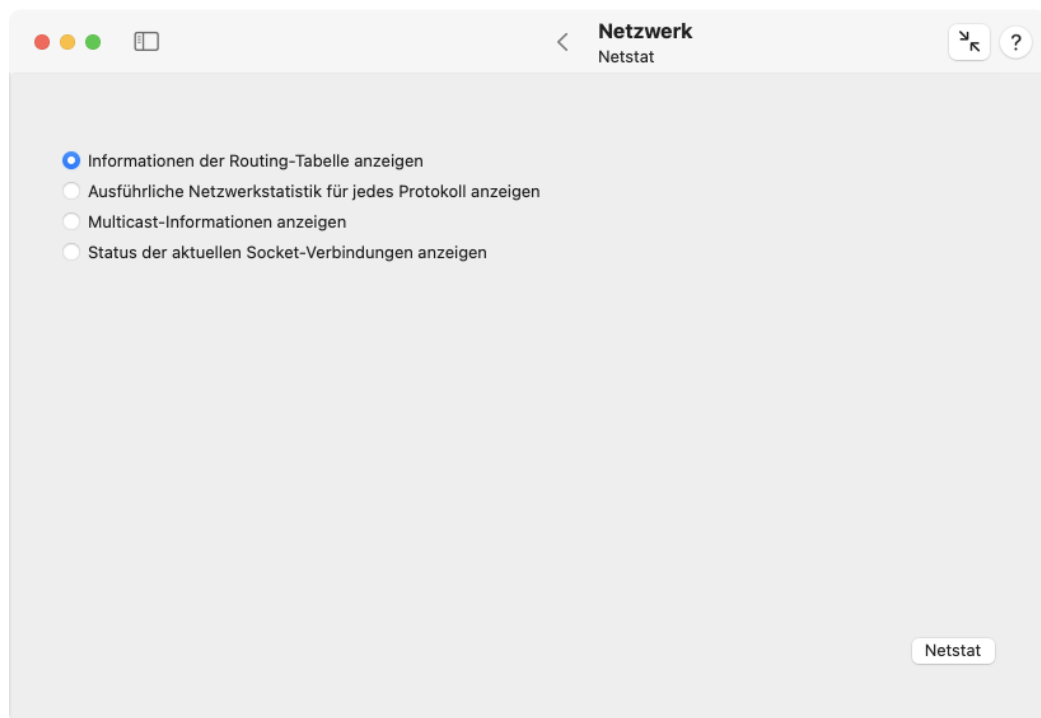


Abbildung 2.40: Statistiken und Routing-Tabellen lassen sich aus dem System auslesen

- die Routing-Tabelle des Betriebssystems: aus der Tabelle ist ersichtlich, über welche Schnittstelle Verbindungen mit welchen Zielen, bzw. Adressbereichen aufgenommen werden. Diese Tabelle entscheidet also darüber, über welchen Anschluss jedes ausgehende Netzwerkpaket gesendet wird.
- die Statistiken für Übertragungsprotokolle: Geordnet nach üblichen Protokollen wie unter anderem TCP, UDP, IPv4, ICMP, IGMP, IPsec, IPv6, ICMP6 und IPsec6 werden Statistiken zur Anzahl übertragener Pakete, Fehlern, Fragmentierung, Speicherbedarf und ähnlichem angezeigt.
- Statistiken bezüglich der Mitgliedschaft in Multicasts: Multicasts sind Übertragungen im Netzwerk, die von einer ganzen Gruppe von Geräten gleichzeitig empfangen wird.
- Statistiken bezüglich gerade aufgebauter logischer Netzwerkverbindungen (Sockets): hier wird in einer Tabelle dargestellt, zu welchen Endpunkten im Netzwerk gerade Verbindungen aufgebaut sind.

2.9.3 Netzwerkverbindung per Echosignal prüfen

Um die Verbindung zu einem anderen Gerät im Netzwerk zu prüfen, kann es nützlich sein, diesem Gerät eine Aufforderung zu senden, sich zu melden. Es wird ein Testpaket an das andere Gerät versandt, mit dem Wunsch, dies wie ein Echo wieder zurückzusenden. Aus der Techniksprache bei der Arbeit mit Echoloten wird das Hin- und Zurücksenden eines Prüfsignals als *Ping* bezeichnet.

Führen Sie die folgenden Schritte durch, um einen Kommunikationstest durchzuführen:

1. Öffnen Sie den Punkt **Ping** auf der Karte **Netzwerk**.
2. Geben Sie das gewünschte Ziel entweder per Adresse oder per Name in das Textfeld ein und drücken Sie die Eingabetaste.
3. Kreuzen Sie das Feld **IPv6-Protokoll verwenden** an, wenn der Vorgang nicht auf Basis von IPv4, sondern mit IPv6 durchgeführt werden soll.
4. Wählen Sie, ob eine bestimmte Anzahl an Testsignalen gesendet werden soll, oder ob der Test endlos laufen soll, bis Sie auf den Knopf **Stopp** klicken.
5. Klicken Sie auf den Knopf **Ping**.

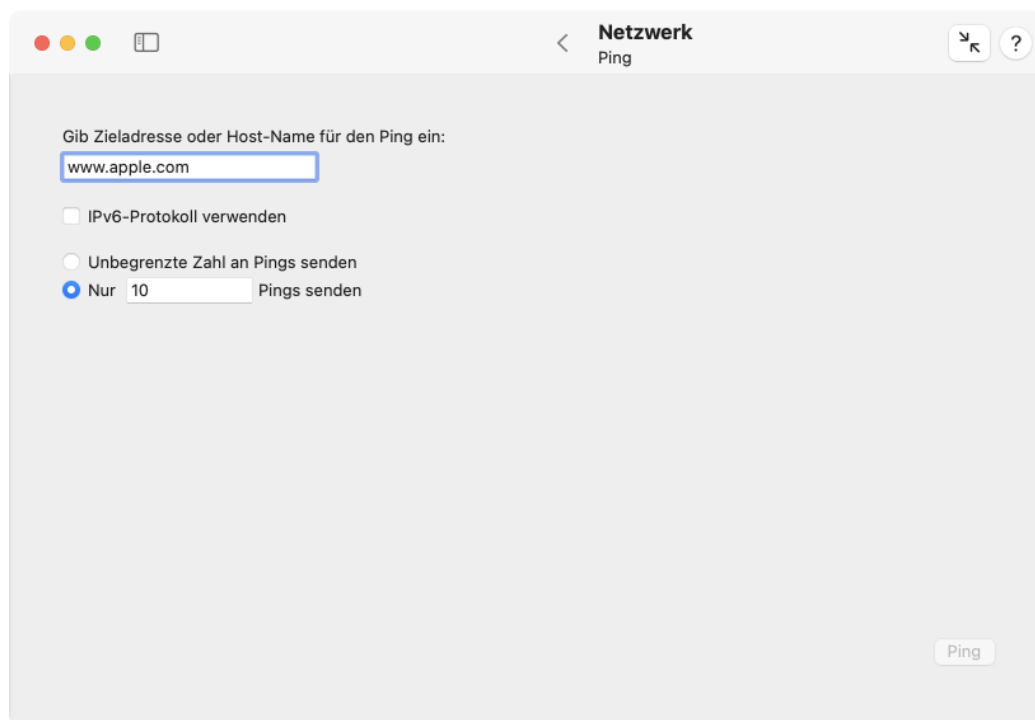


Abbildung 2.41: Um eine Verbindung zu prüfen, können Echo-Anforderungen versandt werden

Der Bericht, der während der einzelnen Ping-Signale angezeigt wird, gibt an, wie viele Bytes an welche Adresse versandt wurden, welche laufende Nummer (*icmp_seq*, *Internet Control Message Protocol Sequence Number*) der aktuelle Test hat, über wie viele Zwischenstationen die Pakete maximal laufen dürfen (*ttl*, *time-to-live*) und wie lange (in Millisekunden) es gedauert hat, bis das Echosignal wieder zurückgekommen ist (*time*). Am Ende des Vorgangs wird zusätzlich eine Zusammenfassung angezeigt, die unter anderem angibt, wie viele Testpakete verloren gegangen sind und wie die minimale, durchschnittliche und maximale Echozeit, sowie deren Standardabweichung während des gesamten Tests war.

Nicht alle Geräte beantworten Ping-Signale. Aus Sicherheits- oder Lastgründen können Geräte sich weigern, zu antworten. Dieser Fall kann nicht direkt von einem nicht erreichbaren Gerät unterschieden werden.

Sie können die normalen Funktionen von macOS zum Kopieren und Einsetzen oder Ziehen-und-Ablegen verwenden, wenn Sie Adressen oder Computernamen in das Textfeld übertragen möchten. Beachten Sie allerdings, dass ein Einsetzvorgang nicht angenommen wird, wenn Sie versuchen, einen Text zu übertragen, der Zeichen enthält, die laut Internet-Standard verboten sind, wie zum Beispiel ein Unterstrich (_). TinkerTool System führt keine volle Syntaxprüfung durch, aber lehnt möglicherweise ein Einsetzen von Text ab, der Zeichen enthält, die die Regeln von RFC 952 nicht einhalten.

Andere Felder der Netzwerkkarte zur Eingabe von Adressen oder Computernamen folgen ebenso dieser Vorgehensweise.

2.9.4 Zuordnung zwischen Host-Namen und Adressen ermitteln

Über den Dienst *DNS (Domain Name Service)* ist es möglich, andere Geräte im Netzwerk nicht nur über ihre Adresse, sondern auch über ihren Namen zu erreichen. Der Dienst sucht entweder zu einem Namen die gültigen Adressen heraus oder bestimmt umgekehrt zu einer Adresse den oder die zugeordneten Namen. Sie können jederzeit von Hand eine solche Anfrage an den Dienst stellen. Führen Sie dazu die folgenden Schritte durch:

1. Öffnen Sie den Punkt **Lookup** auf der Karte **Netzwerk**.
2. Geben Sie entweder den Namen des Geräts, oder seine IPv4-Adresse oder seine IPv6-Adresse in das Textfeld ein und drücken Sie die Eingabetaste. Dies wird als Aufforderung verstanden, die jeweils fehlenden Daten über den DNS-Dienst nachzuschlagen.
3. Falls Sie neben der reinen Bestimmung der DNS-Antwort noch sehr viel mehr Details über die interne Anfrage und die jeweilige Antwort des DNS-Dienstes erhalten möchten, kreuzen Sie das Feld **„dig“ für ausführlichere Informationen verwenden** an.
4. Falls Sie in Punkt 3 die ausführlichere Variante ausgewählt haben, können Sie zusätzlich noch festlegen, ob erzwungen werden soll, die Anfrage nur per IPv6-Protokoll zu versenden, bzw. neben den IPv4-Daten auch die IPv6-Daten heraussuchen zu lassen.
5. Klicken Sie auf den Knopf **DNS-Anfrage**.

In der Antwort ist jeweils festgehalten

- welcher Server (mit dessen Name und Adresse) die antwortet geliefert hat und
- wie die Antwort, also Name(n) und Adresse(n) lauten.

Es wird derjenige DNS-Server verwendet, der in der Netzwerkkonfiguration von macOS eingerichtet ist.

2.9.5 Weg von Datenpaketen nachverfolgen

In größeren Netzwerken wie dem Internet können Kommunikationsziele nur erreicht werden, indem die Datenpakete über mehrere Zwischenstationen zum Ziel gelangen. Die einzelnen Knotenpunkte des Netzwerks bestimmen für jedes Paket die zurzeit optimale Route, basierend auf Verbindungsplänen, Verbindungskosten und derzeitiger Auslastung der einzelnen Knoten. Es kann interessant sein, die im Moment gewählte Route zur Kommunikation mit einem bestimmten Ziel anzeigen zu lassen. Dies wird als *Paketverfolgung* oder *Traceroute* bezeichnet.

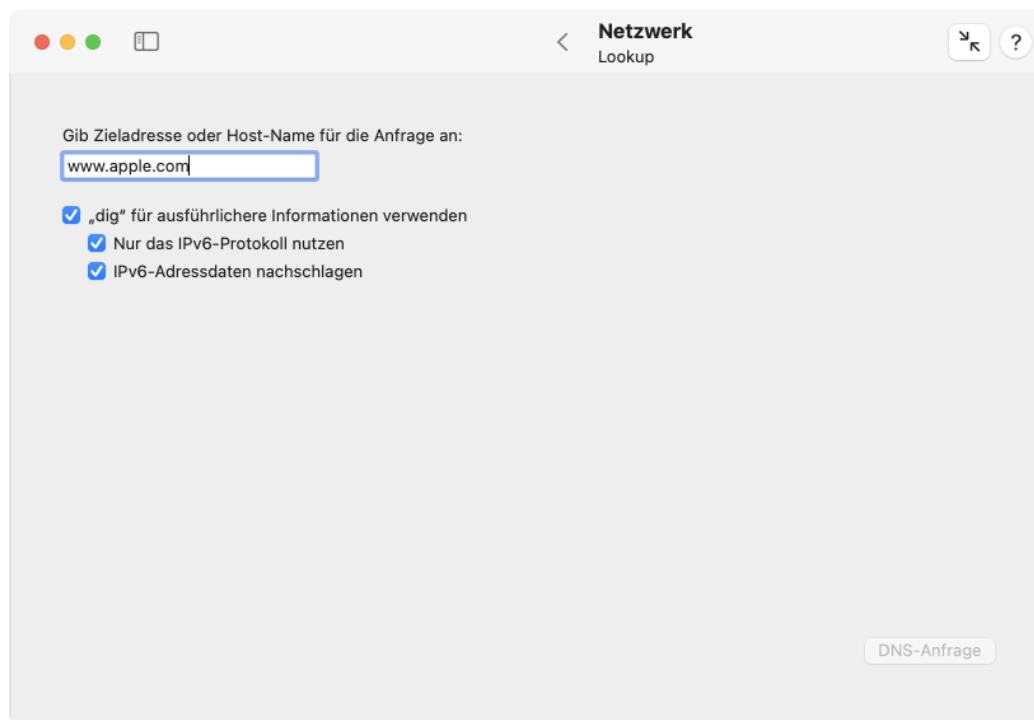


Abbildung 2.42: Die Beziehungen zwischen Namen und Adressen können abgerufen werden

Führen Sie die folgenden Schritte durch, um die derzeit gewählte Route für Datenpakete zwischen Ihrem Computer und einem anderen Computer bestimmen zu lassen:

1. Öffnen Sie den Punkt **Traceroute** auf der Karte **Netzwerk**.
2. Geben Sie entweder Name oder Adresse des Ziels in das Textfeld ein und drücken Sie die Eingabetaste.
3. Klicken Sie auf den Knopf **Verfolgen**.

Die derzeitige Route wird über eine Reihe von Testdatenpaketen (ähnlich wie bei Ping) bestimmt und ausgemessen. Sie erhalten pro Zwischenstation jeweils eine Zeile in der Ausgabe, die (falls verfügbar) Name, Adresse und Signalübertragungszeiten zum jeweils nächsten Knotenpunkt enthält. Die Bestimmung der Route kann einige Sekunden in Anspruch nehmen. Daten, die nicht abgerufen werden können, werden durch Sterne ersetzt.

2.9.6 Datenbanken des Whois-Dienstes abfragen

Im Internet werden die Namen der einzelnen Netzwerkgeräte, bzw. Schnittstellen nach einem hierarchischen Verfahren vergeben. Diese Namen können kostenpflichtig bei den jeweils zuständigen Vergabestellen angemeldet werden. Über den Dienst *whois* stellen die Vergabestellen den Zugriff auf Datenbanken her, in der die gerade vergebenen Namen verzeichnet sind. Sie können diese Datenbanken öffentlich abrufen und hiermit Informationen über den Eigentümer eines Namens, Ansprechpartner für Verwaltung, Ansprechpartner für Technik, Ansprechpartner für Namensmissbrauch, Anmelde- und Gültigkeitszeitraum, zuständige Registrierungsbehörde und zuständige Stelle für den DNS-Dienst heraussuchen lassen.

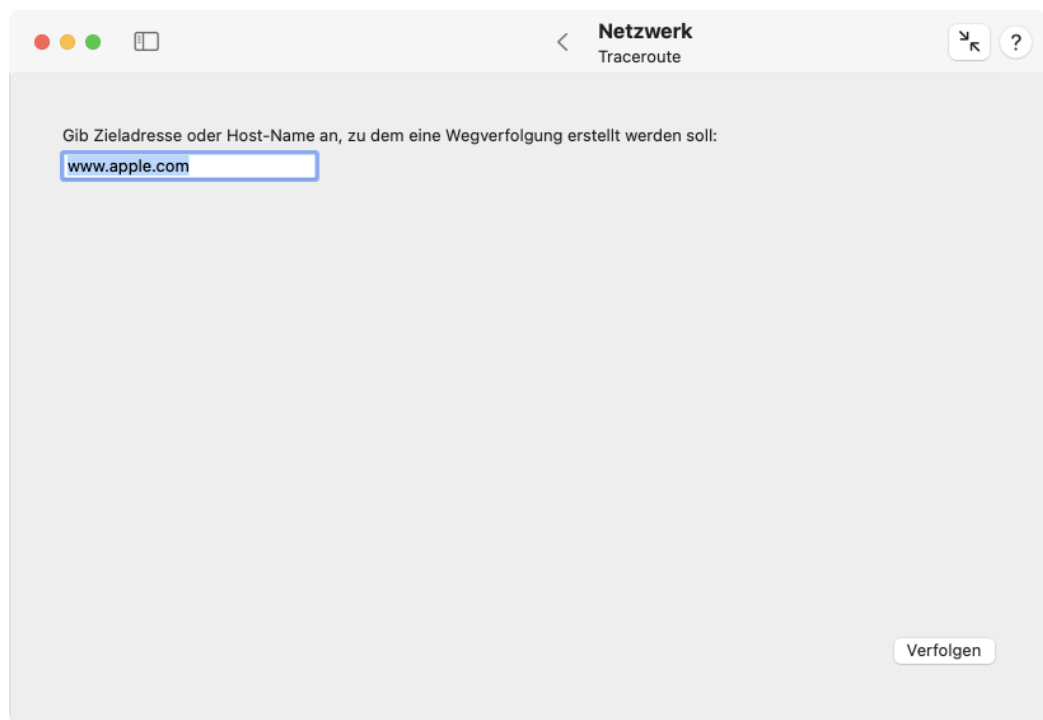


Abbildung 2.43: Der zurzeit gewählte Weg von Datenpaketen kann im Netz nachverfolgt werden

Aus Datenschutzgründen sind nicht mehr alle diese Daten in jedem Land, bzw. von jeder Registrierungsbehörde abrufbar. Die Menge der verfügbaren Daten kann sich je nach Domain-Name stark unterscheiden.

Um Daten über einen angemeldeten Domain-Namen herauszufinden, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Punkt **Whois** auf der Karte **Netzwerk**.
2. Geben Sie den Domain-Namen in das Textfeld ein und drücken Sie die Eingabetaste.
3. Wählen Sie aus der Übersicht der whois-Server den Dienst der vermutlich zuständigen Registrierungsbehörde aus oder geben Sie den DNS-Namen eines anderen whois-Servers an.
4. Klicken Sie auf den Knopf **Whois**.

Die jeweils öffentlich verfügbaren Daten, die der gewählte whois-Server geliefert hat, werden angezeigt. Wie immer können Sie das Ergebnis auch ausdrucken lassen oder als Textdatei abspeichern.

2.9.7 Nutzerinformationen per Finger-Dienst ermitteln

Das *Finger*-Protokoll beschreibt einen Auskunftsdienst, mit dem es möglich ist, Daten über Netzwerkbenutzer live abzurufen, hauptsächlich um festzustellen, wie und wo ein Benutzer innerhalb einer Firma oder ähnlichen Organisation erreicht werden kann. Neben Kontaktdaten wie beispielsweise Telefonnummer, Raumnummer oder E-Mail-Adresse kann

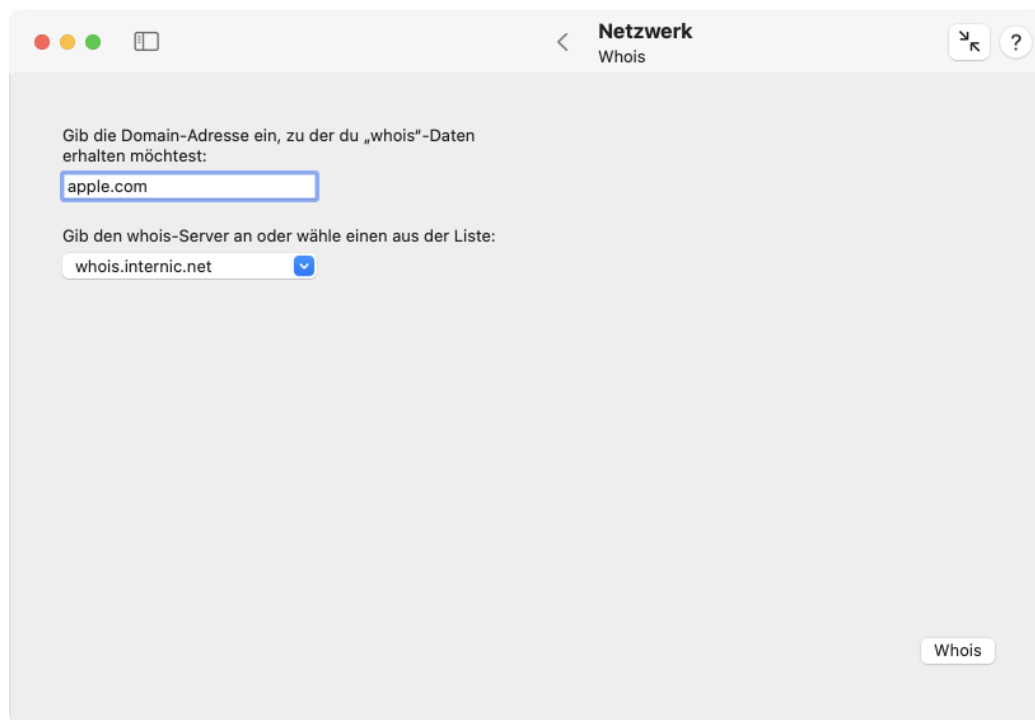


Abbildung 2.44: Der Whois-Dienst des Internet kann abgefragt werden

Finger bestimmen, an welchem Computer des Netzwerks eine Person gerade wie lange angemeldet ist. Die Anfrage an den Finger-Dienst erfolgt über ein ähnliches Muster, wie es bei E-Mail-Adressen verwendet wird, nämlich

`name@domain`

wobei *name* der Kurzname des Benutzers und *domain* der Domain-Name des Netzwerks ist.

Führen Sie die folgenden Schritte durch, um Finger-Daten über einen Netzwerkbenutzer abzurufen:

1. Öffnen Sie den Punkt **Finger** auf der Karte **Netzwerk**.
2. Geben Sie die Finger-Anfrage in das Textfeld ein und drücken Sie die Eingabetaste.
3. Klicken Sie auf den Knopf **Finger**.

Das Finger-Protokoll wurde in den Jahren 1971 bis 1977 entwickelt und gilt als veraltet. Aus Datenschutzgründen sowie aus arbeitsrechtlichen und Sicherheitsgründen kommt es heute nur noch selten zum Einsatz. Falls es zum Einsatz kommt, stehen die Daten in der Regel nur im lokalen Netz, aber nicht über das Internet hinweg zur Verfügung.

Steht der Finger-Dienst nicht zur Verfügung, erhalten Sie in der Regel nur einen Fehlerbericht, der unter anderem die Meldung

`finger: connect: Connection refused`

enthält.

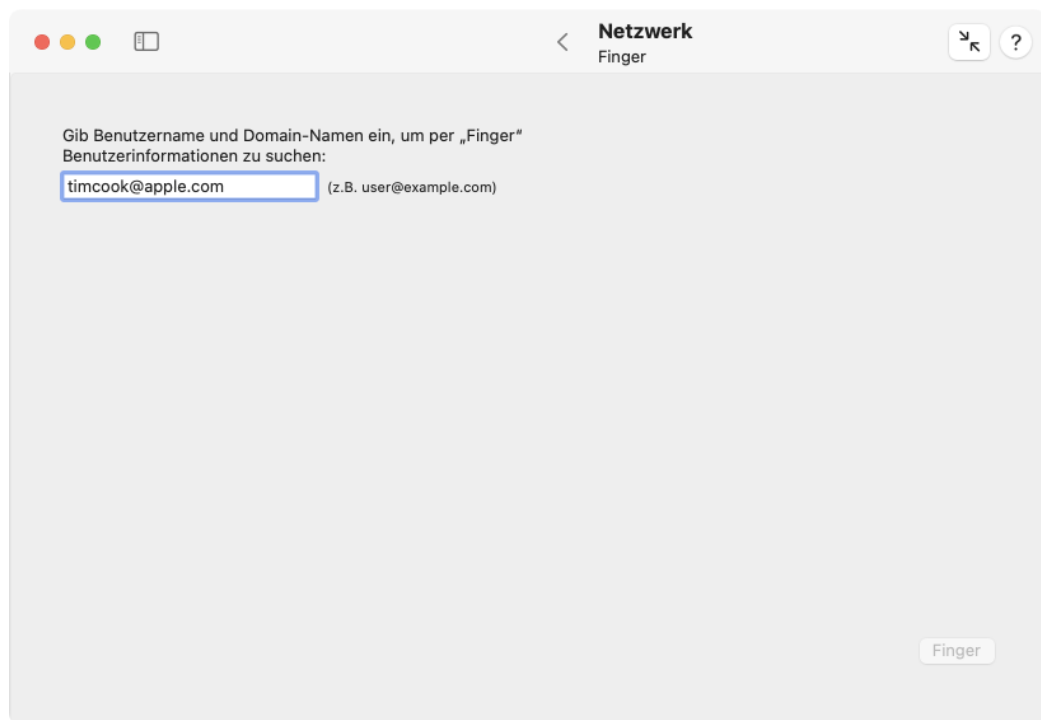


Abbildung 2.45: Daten über Netzwerkbenutzer kann der Finger-Dienst bereitstellen

2.9.8 Antwortverhalten

macOS enthält einen eingebauten Geschwindigkeitstest, der in der Lage ist, die Qualität ihres lokalen Netzes und dessen Internet-Anbindung einzuschätzen. Sie können den Test, der in der Regel weniger als eine halbe Minute beansprucht, durch einen einfachen Mausklick starten. Der Test beurteilt im Wesentlichen, wie gut Ihre Internet-Verbindung reagiert, wenn mehrere Geräte oder Apps diese gleichzeitig nutzen. Die Ergebnisse des Tests können insbesondere dann hilfreich sein, wenn Sie ein Internet-Gateway verwenden, dessen Leistung von Hand optimiert werden kann, beispielsweise durch Konfigurieren von Funktionen wie *Smart Queue Management (SQM)*. Sie können mehrere Tests unter ähnlichen Bedingungen durchführen, um damit zu experimentieren, welche Einstellungsänderungen sich positiv auswirken.

Bitte beachten Sie, dass sowohl das Netzwerk zwischen diesem Computer und Ihrem Internet-Gateway („Router“), das Netzwerk zwischen Gateway und Ihrem Internet-Provider, als auch die Anbindung Ihres Providers an das Internet in die Messung eingehen. macOS erfasst während des Tests die folgende Messgrößen:

- **Kapazität Upload:** der derzeitige Nettodurchsatz beim Senden von Daten ins Internet
- **Kapazität Download:** der derzeitige Nettodurchsatz beim Empfangen von Daten aus dem Internet
- **Gleichzeitige Uploads:** die maximale Anzahl gleichzeitig möglicher, typischer Internet-Sendeverbindungen, bis das Netz voll ausgelastet ist
- **Gleichzeitige Downloads:** die maximale Anzahl gleichzeitig möglicher, typischer Internet-Empfangsverbindungen, bis das Netz voll ausgelastet ist

- **Leerlaufzeit:** die typische Laufzeit der Daten zwischen diesem Computer und einem Server wenn die Kommunikationsverbindung nicht belastet ist
- **Antwortverhalten:** die maximale Anzahl an Paketumläufen pro Minute, die bei typischen Transaktionen zu erwarten ist, wenn mehrere Programme Anfragen absenden und auf Rückantworten aus dem Netz warten. Eine höhere Zahl bedeutet eine höhere Qualität des „gefühlten“ Netzwerkverhaltens.
- **Gesamtqualitätseinschätzung durch macOS:** eine Zusammenfassung des Ergebnisses als einfaches Schlagwort (siehe unten)

Während der Messung wird eine größere Menge an Testdaten zwischen Ihrem Computer und einem oder mehreren Internet-Servern von Apple übertragen. Um welche Server es sich handelt, kann von Apple dynamisch gesteuert werden und sich jederzeit ändern.

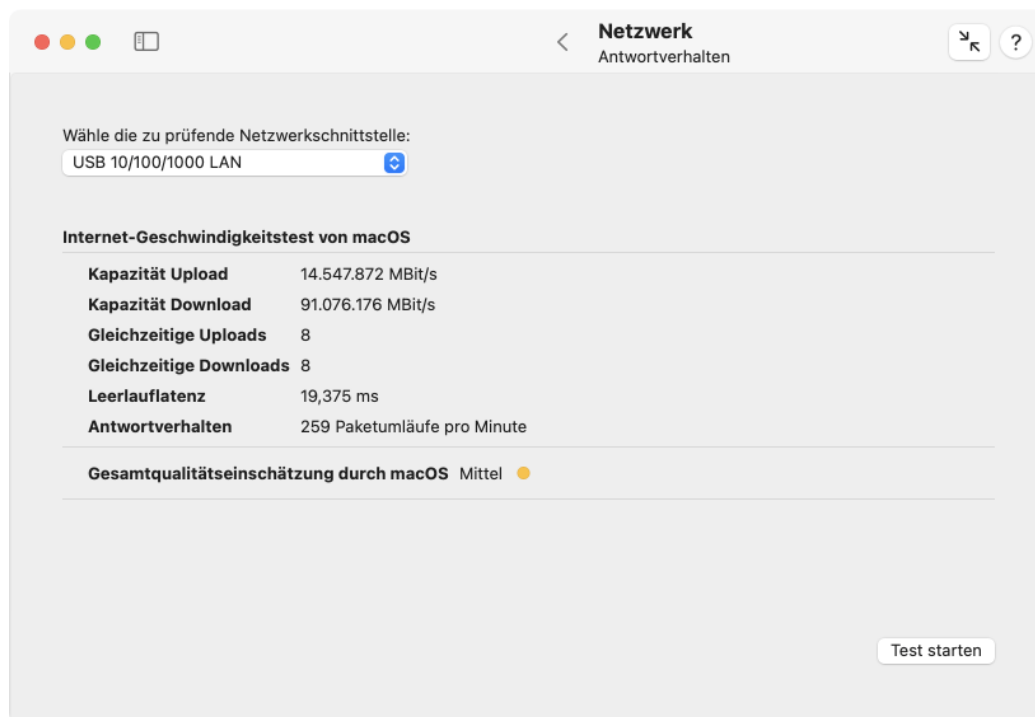


Abbildung 2.46: macOS kann das typische Antwortverhalten Ihres Netzwerks beurteilen und die Qualität einschätzen

Führen Sie die folgenden Schritte durch, um eine Einschätzung der Netzqualität zu erhalten:

1. Stellen Sie sicher, dass das Aufklappmenü **Wähle die zu prüfende Netzwerkschnittstelle** auf den gewünschten Wert eingestellt ist. TinkerTool System bietet alle physischen und virtuellen Netzwerkanschlüsse zur Auswahl an, die gerade eine aktive IP-Adresse verwenden. Beachten Sie, dass üblicherweise nicht alle Anschlüsse mit dem Internet verbunden sind und sich daher nicht für einen Test eignen. Üblicherweise reicht es aus, die Einstellung **Standardanschluss für Internet-Zugang** zu verwenden, wodurch macOS automatisch diejenige Schnittstelle wählt, die zurzeit für Internet-Zugriffe verwendet wird.
2. Klicken Sie auf den Knopf **Test starten**.

Der Test wird danach von macOS durchgeführt und das Endergebnis von TinkerTool System angezeigt. Die Gesamtbeurteilung liegt im Ermessen von macOS. Sie wird von TinkerTool System nicht beeinflusst. Zur Beurteilung des Endergebnisses stellt Apple die folgende Dokumentation bereit:

- **Niedrig:** Falls sich ein Gerät im selben Netzwerk befindet und beispielsweise einen Film lädt oder Fotos in iCloud sichert, ist die Verbindung in einigen Apps oder Diensten möglicherweise instabil, etwa bei FaceTime-Videoanrufen oder bei Spielen.
- **Mittel:** Wenn mehrere Geräte oder Apps auf das Netzwerk zugreifen, kommt es möglicherweise zu kurzen Pausen oder das Gerät/die App friert ein, etwa bei Audio- oder Videoanrufen in FaceTime.
- **Hoch:** Unabhängig von der Anzahl der Geräte und Apps, die auf das Netzwerk zugreifen, sollte die Verbindung in Apps und Diensten stabil bleiben.

2.10 Die Einstellungskarte Info

2.10.1 Mac-Systemdaten

Der Unterpunkt **Mac** listet technische Details über das aktuelle Computersystem auf. Dies schließt einige Daten ein, die über Apples Programm **Systeminformationen** von macOS nicht abrufbar sind.

Der Abschnitt **Computer** enthält den Namen des Systems, wie Sie ihn definiert haben (und der möglicherweise nicht mit dem Namen übereinstimmt, der diesen Computer im Netzwerk identifiziert), Apples offizielle Modellbezeichnung (auch als Marketing-Name bekannt), eine kurze Beschreibung, die Modellidentifikation von Apple, die den Code darstellt, den Apple und macOS intern zur Identifizierung dieser Baureihe verwenden, die Seriennummer des Computers, seine eindeutige Hardware-Identifikation und die Woche des Produktionsdatums. Falls Sie ein Macintosh-Modell einsetzen, das in verschiedenen Farben erhältlich ist, zeigt ein kleines Farbfeld neben der Zeile mit der Modellidentifikation die Gehäusefarbe an. Ein typisches Bild des Computermodells wird ganz oben über dem Text gezeigt.

Bei Apple-Geräten, die nach August 2021 gefertigt wurden, erlaubt Apple möglicherweise nicht mehr, dass das tatsächliche Herstellungsdatum ermittelt werden kann. In diesem Fall zeigt TinkerTool System dies mit einer entsprechenden Meldung an.

Falls Ihr Mac einen Prozessor auf Basis eines *Apple-Chips* enthält, fehlt Apples Kurzbeschreibungstext für die Baureihe. Stattdessen sind folgende Daten angegeben:

- die Apple-Bestellnummer dieses Macs,
- die Modellnummer des Gehäuses.

Der zweite Abschnitt **Prozessor** listet Details über die Prozessorkonfiguration auf, ebenso über die verfügbaren Cache-Größen. Dies beinhaltet die offizielle Angabe des Prozessormodells, die Anbieterkennung, die Anzahl der Prozessoren, sowie der verfügbaren und aktiven Prozessorkerne.

Für Intel-Prozessoren folgt die Information, ob das System dazu in der Lage ist, mehrere Befehlsstränge pro Kern abzuarbeiten (Simultanes Multithreading). In diesem Fall simuliert die Hardware die doppelte Anzahl an Prozessoren. Ebenso wird die Prozessorgeneration

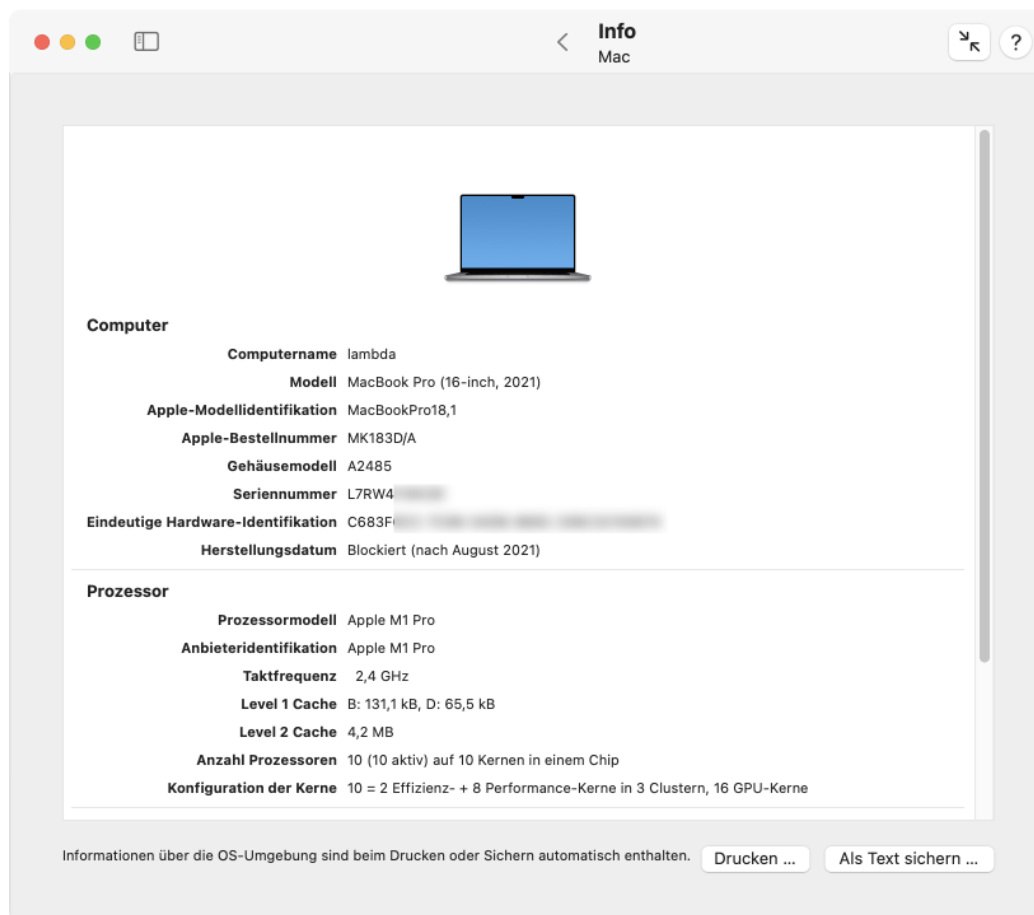


Abbildung 2.47: Systemdaten (Version für Macs mit Intel-Prozessor)

angegeben, was die Familiennummer, Modellnummer und Stepping-Nummer (Hardwareversion) einschließt, sowie die dezimale Signatur, die alle diese Identifikationscodes in eine einzelne Zahl vereinigt.

Daten über die Intel-Prozessorgeneration sind natürlicherweise für Macs mit Apple-Chip nicht verfügbar. Stattdessen wird hier die genaue Konfiguration der Prozessorkerne angegeben: Die Anzahl der Effizienzkerne, der Höchstleistungskerne, deren Verteilung auf Prozessor-Cluster und die Anzahl der Apple-GPU-Kerne.

Angegeben werden außerdem die Haupttaktfrequenz des Prozessors, die Größen der Level-1-Caches (B für Befehle, D für Daten) und die Größen der Level-2- und Level-3-Caches (nur Intel).

Der Abschnitt **Speicher** zeigt die Größe des physischen Speichers (RAM, Random Access Memory) an, der momentan in den Computer eingebaut ist, sowie die optimale Freispeichergröße. Dieser Wert gibt den kleinen Betrag des physischen Speichers an, den das Betriebssystem zum Erzielen der besten Leistung freihalten sollte. Das Optimum wird erreicht, wenn kein RAM verschwendet wird (fast alles ist in Gebrauch), aber ein kleiner Rest für die laufende Verwaltung zur Verfügung steht. Die Zeile **Adressierbarer Speicher** gibt die Größe des physischen und virtuellen Speichers an, den der Prozessor intern verwalten kann. Das bedeutet nicht, dass diese Menge tatsächlich in der Praxis verwendet werden könnte. Die Anzahl der verfügbaren Steckplätze für Speichermodule und andere Einschränkungen des verwendeten Chipsatzes limitieren diese theoretischen Werte. Weitere Informationen zur Speicherverwaltung finden Sie im Abschnitt Einführung in virtuelle Speichertechnik (Abschnitt 2.7 auf Seite 86).

Der vierte Abschnitt **Hauptplatine** enthält Detailangaben über die Hauptplatine (*Logic Board*) des Computers, nämlich die Anbieterkennzeichnung, die interne Modellnummer und ihre Seriennummer. Macs, die auf Apple-Chips aufbauen, verwenden keinen lesbaren Modellcode für die Hauptplatine, so dass die zugehörige Zeile in diesem Fall fehlt.

Weitere Daten für Intel-basierte Macs

Diese Daten sind nicht abrufbar, falls Sie einen Mac mit Apple-Chip verwenden. SMC und Bridge sind in den Hauptprozessor integriert, so dass sie nicht mehr als eigenständige Bauteile vorhanden sein müssen. Systemmanagementdaten nach dem SMBIOS-Standard werden nicht mehr unterstützt. Stattdessen sind Produktdaten verfügbar. Der nächste Abschnitt enthält nähere Informationen hierzu.

Im vierten Abschnitt wird ebenso die Versionsnummer des System Management Controllers (SMC), bzw. seiner Firmware angezeigt. Der SMC ist ein Hilfsprozessor, der die internen Sensoren des Computers und dessen Energieverteilung steuert. Er betreibt die „immer eingeschalteten“ Teile des Systems, die auch noch in Betrieb sind, wenn der tatsächliche Computer ausgeschaltet oder im Ruhezustand ist. Er ist ebenso dafür verantwortlich, den Computer als originales Apple-Produkt zu identifizieren und stellt damit die Hauptunterscheidungskomponente zwischen einem herkömmlichen Personal Computer (PC) und einem Macintosh dar.

Eine besondere Detailanzeige, die über den Knopf **Managementeinträge zeigen** zur Verfügung steht, listet technische Daten auf, die im Managementspeicher des Computers abgelegt sind. Dies beinhaltet:

- Daten über die Systemeinheit
- Detaildaten über jeden Prozessor
- Detaildaten über jede Cache-Einheit

- Detaildaten über jeden Speichersteckplatz oder die Speichermodule
- eine Beschreibung der System-Firmware
- Managementdaten über die Systemplatine
- Managementdaten über das Systemgehäuse
- Detaildaten über jeden Steckverbinder der Systemplatine oder des Systemgehäuses
- Detaildaten über jeden Erweiterungssteckplatz
- eine Liste der eingebauten Systemgeräte
- eine Liste von Steckbrücken und Schaltern auf der Systemplatine.

Diese Management-Datensätze werden nicht von TinkerTool System berechnet, sondern nur ausgelesen. Sie sind vom Hersteller des Computers im sogenannten *System Management BIOS*-Bereich der Firmware gespeichert worden, als der Computer gefertigt wurde. Einige Teile werden darüberhinaus dynamisch von macOS bestimmt, indem die entsprechenden Daten aus der Hardware gelesen werden.

Eine weitere herausgleitende Detailanzeige **BridgeOS-Info** ist verfügbar, falls Ihr Computer mit *Apple-BridgeOS-Prozessor*-Technik ausgestattet ist. Hierbei kann es sich entweder um das originale *iBridge*-System handeln, oder um den *Apple T2-Sicherheitsprozessor*. Das BridgeOS-System ist ein zweiter Computer, der in Ihren Mac eingebaut ist, und der Sicherheitsfunktionen wie den TouchID-Fingerabdrucksensor oder SSD-Verschlüsselung, je nach Modell, steuern kann. Dieses Hilffssystem verwendet ein eigenes Betriebssystem *Apple BridgeOS* und ist möglicherweise ständig eingeschaltet, wenn Stromversorgung vorhanden ist. Der Eintrag **Apple-BridgeOS-Prozessor** gibt an, ob solche Technik in Ihrem Mac zum Einsatz kommt. Falls ja, können Sie den Knopf **BridgeOS-Info** drücken, um mehr über deren Konfiguration zu erfahren.

Weitere Daten für Macs mit Apple-Chip

Statt SMBIOS-Daten speichern Macs mit Apple-Chip intern Apple-Produktinformationen. Die interessantesten Punkte werden nach Anklicken von **Produktdaten einblenden** angezeigt:

- der Typ des **System-On-a-Chip (SoC)**, der in diesem Mac zum Einsatz kommt,
- die **Macintosh-Kompatibilitätsstufe**, bei der es sich quasi um einen virtuellen Mac handelt, der einen bestimmten Funktionsumfang verkörpert. Zum Beispiel könnte ein Mac der „Generation 15“ mehr Funktionen unterstützen, als ein Mac der „Generation 14“, aber stattdessen gewisse veraltete Funktionen weglassen. Die Stufe, die durch die ersten Macs mit Apple-Chip aus dem Jahre 2020 definiert wird, wird „Generation 20“ genannt.
- die **Mobilgerät Kompatibilitätsstufe**: ähnlich wie beim vorherigen Punkt wird hierdurch ein Funktionsumfang definiert, den dieser Mac besitzt, wenn er auf eine Nutzung wie bei einem Apple-Mobilgerät zurückfällt, z.B. einem iPad Pro.
- die **Anzahl eingebauter Mikrofone**, die definiert, wie viele Audiosensoren in diesen Mac eingebaut sind,

- **Speicher aufrüstbar:** eine Angabe, ob RAM in diesem Mac aufgerüstet werden kann oder nicht.
- **Touch Bar Seriennummer:** falls dieser Mac eine Touch Bar oder einen Fingerabdrucksensor enthält, die Seriennummer dieser Baugruppe, die mit diesem Computer gekoppelt wurde.
- **Umgebungslichtsensor Seriennummer:** wie vor, jedoch mit Bezug auf den Lichtsensor.
- **Abdeckglas Seriennummer:** wie vor, jedoch für das Abdeckglas des Displays.
- **Bildschirmbaugruppe Teile- und Seriennummern:** falls dieser Mac ein eingebautes Display hat, die Seriennummern und/oder Teilenummern aller Komponenten, aus denen der Bildschirm sich zusammensetzt. Das Abdeckglas kann in dieser Liste enthalten sein.
- **Netzteildaten:** Bei bestimmten Mac-Baureihen lassen sich Daten über das eingebaute Netzteil abrufen. Falls Sie ein solches Mac-Modell verwenden, wird der Karteireiter **Netzteil** angezeigt, über den sich technische Details wie Hersteller, Modell und Seriennummer, sowie die nominelle Sekundärspannung, Maximalstrom und Leistung ablesen lassen. Diese Funktion ist typischerweise vorhanden, wenn der Mac intern wie ein „Mobilcomputer ohne Akku“ aufgebaut ist.

Es ist möglich, den Inhalt des Textbereichs entweder auszudrucken oder in eine HTML-basierte Textdatei zu speichern. Solche Dokumente können dazu benutzt werden, automatisch Inventarverzeichnisse für alle Ihre Computer zu erzeugen. Drücken Sie hierzu auf einen der Knöpfe **Drucken ...**, bzw. **Als Text speichern ...**. Die erzeugten Textdateien können mit jedem Web-Browser oder mit dem Programm TextEdit von macOS geöffnet werden. Neben den Daten aus dem Bereich **Mac** werden auch einige Daten aus dem Unterpunkt **Betriebsumgebung** (siehe nächster Abschnitt) in den gedruckten Bericht eingefügt.

Die Startzeit des Systems ist ein flüchtiger Wert, der nicht in die Textberichte mit aufgenommen wird.

2.10.2 Betriebsumgebung

Der Punkt **Betriebsumgebung** fasst die Versionsdaten über die Firmware des Computers, über das Darwin-Betriebssystem, auf dem macOS und iOS basieren, die Systemkernversion und dessen Revisionsnummern, sowie die Betriebssystemversion und Build-Nummer zusammen. Die Zeile **Systemupdatequelle** gibt an, ob Sie eine offiziell freigegebene Version des Betriebssystems verwenden oder ob das System dazu eingerichtet ist, Updates aus einem von Apples Vorabtestprogrammen (*Seeding Programs*) zu erhalten.

Beachten Sie, dass das Feld die Teilnahme an einem Programm für den Bezug von Updates angibt, nicht den Status des gerade laufenden Betriebssystems. In der Regel sind beide Angaben gleichwertig, aber falls Sie ein anstehendes Update noch nicht durchgeführt haben, kann es vorübergehend zu Unterschieden kommen.

Dieser Abschnitt zeigt außerdem die Hardware-Einstellung des Computers für den **Systemintegritätsschutz**, der im Moment für das Betriebssystem wirksam wird. (Für Informationen über den technischen Hintergrund dieser Funktion siehe das Ende des Kapitels

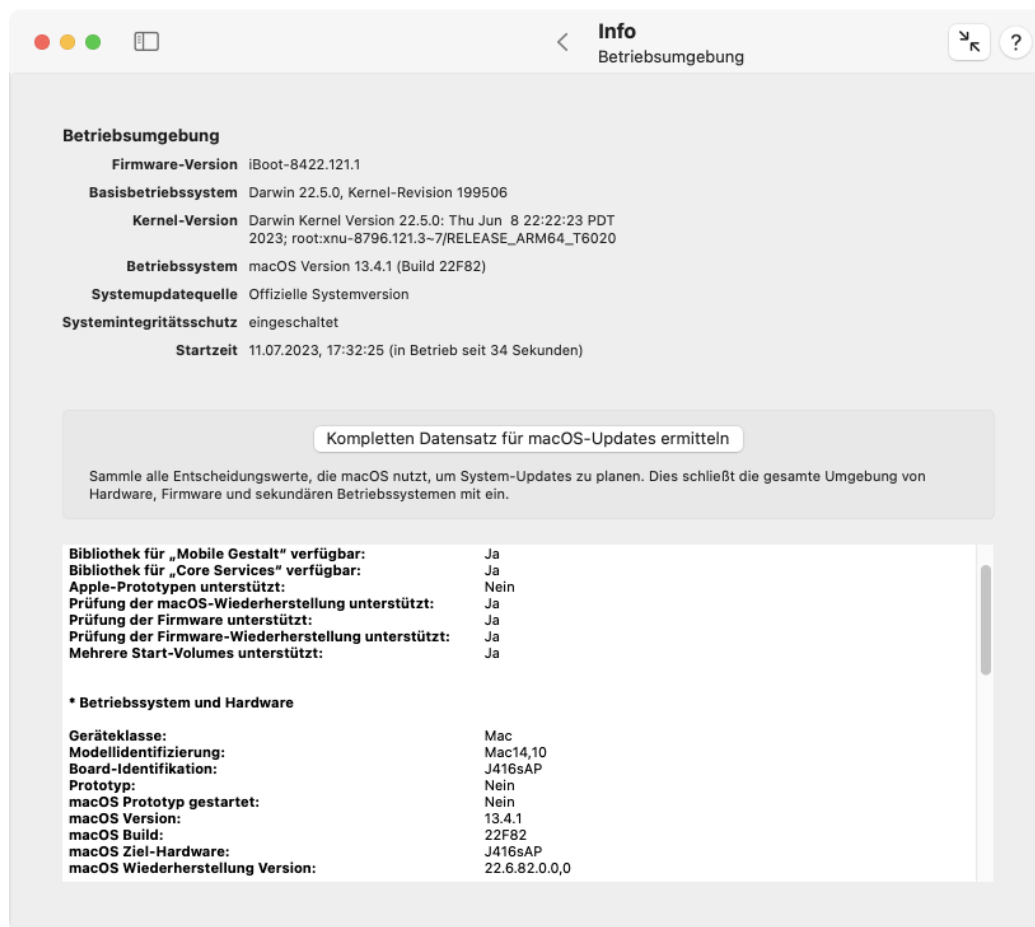


Abbildung 2.48: Betriebsumgebung

Grundlegende Bedienungshinweise (Abschnitt 1.3 auf Seite 8).) Die Funktion kann entweder voll eingeschaltet, komplett abgeschaltet oder teilweise aktiviert sein. Im teilweisen Fall verwendet TinkerTool System die folgenden Abkürzungen, um anzuzeigen, welche Vorgänge bei den gegenwärtigen Computereinstellungen zugelassen sind:

- **kext:** nicht vertrauenswürdige Kernel-Erweiterungen können in den Systemkern geladen werden.
- **fsac:** das System hat die Erlaubnis, Objekte im Dateisystem zu ändern oder zu löschen, für die das Attribut *restricted* eingeschaltet ist.
- **tpid:** das System hat die Erlaubnis, Funktionen zu nutzen, die ermitteln, welcher Prozess zu welcher Prozessidentifikationsnummer gehört.
- **kdbg:** Funktionen zur Fehlersuche im Kernel können genutzt werden.
- **appl:** das System hat die Erlaubnis, Funktionen zu nutzen, die als *Apple-intern* angesehen werden.
- **trac:** das System hat die Erlaubnis, Programmablaufverfolgung (basierend auf *dtrace*-Technik) ohne Einschränkungen nutzen zu dürfen.
- **pram:** das System hat die Erlaubnis, *alle* Einträge im nicht-flüchtigen RAM (NVRAM) ändern zu dürfen.
- **devc:** Gerätekonfiguration ist zugelassen.
- **reco:** der Computer hat die Erlaubnis, jedes beliebige der verfügbaren Wiederherstellungsbetriebssysteme nutzen zu dürfen.
- **akex:** das System darf vertrauenswürdige Kernel-Erweiterungen laden, die noch nicht von einem Administrator zugelassen wurden.
- **expo:** das System hat die Erlaubnis, die Sicherheitsrichtlinien für ausführbare Programme zu übergehen.
- **stur:** das Betriebssystem darf von einem nicht-autorisierten Stammdateisystem gestartet werden, das von Apple nicht kryptografisch versiegelt wurde.

Alle Schutzfunktionen, die *nicht* von TinkerTool System aufgelistet werden, sind voll wirksam. Die genaue Bedeutung dieser Einstellungen wird durch Apple definiert und kann sich jederzeit ohne Ankündigung ändern.

Die letzte Zeile der Übersicht zeigt die **Startzeit** des Betriebssystems, sowohl als absolute Zeitangabe, als auch als Zeitintervall, das seitdem vergangen ist, die sogenannte **Uptime**. Wenn Sie den Knopf **Kompletten Datensatz für macOS-Updates ermitteln** betätigen, sammelt TinkerTool System weitere Informationen, nämlich die Gesamtheit aller Entscheidungsdaten, die macOS heranzieht, wenn es nach System-Updates sucht. Hierbei gehen die Hardware, die Firmware, das laufende Betriebssystem und alle Hilfsbetriebssysteme, wie Bridge-Systeme, Startsysteme, Wiederherstellungssysteme ein. Die Daten werden tabellarisch in Textform gezeigt und sind in der Regel selbsterklärend.

Diese Daten sind möglicherweise nicht verfügbar, falls der Computer für längere Zeit ohne Neustart in Betrieb war. Ein Neustart behebt dieses Problem.

2.10.3 Malware-Schutz

macOS enthält mehrere eingebaute Schutzmaßnahmen gegen böswillige Software (*Malware*). Eine dieser Schutzvorrichtungen arbeitet wie ein Virens Scanner, der heruntergeladene Dateien anhand von bekannten Erkennungsmerkmalen (Signaturen) automatisch im Hintergrund überprüft. Apple bezeichnet diese Komponente als **Liste für sichere Downloads**. Diese Technik ist außerdem unter der Bezeichnung *XProtect* bekannt. Sie ist ab Werk eingeschaltet. Die Virensignaturen werden automatisch aktualisiert, wenn die Wahlmöglichkeit **Sicherheitsmaßnahmen und Systemdateien installieren** bei **Allgemein > Softwareupdate > Automatische Updates > i** in den **Systemeinstellungen** angekreuzt ist. Neben der Erkennung von Schadsoftware überwacht diese Vorrichtung auch die Versionsstände einiger im System installierter Internet-Plugins. Diese Plugins werden von Internet-Browsern verwendet, um zusätzliche Techniken, wie beispielsweise Adobe® Flash® oder Java™ unterstützen zu können.

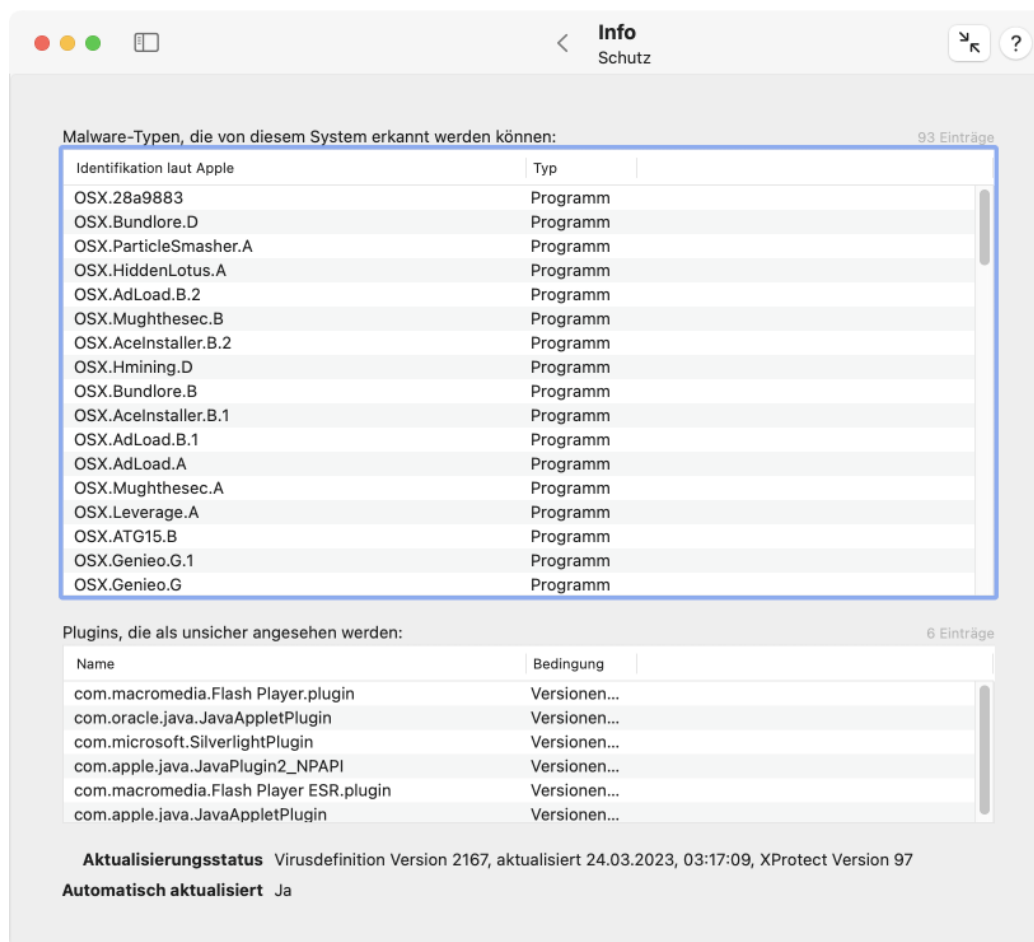


Abbildung 2.49: Malware-Schutz

Über den Unterpunkt **Schutz** können Sie sich den derzeitigen Inhalt der Liste für sichere Downloads anzeigen lassen. Die obere Tabelle zeigt dabei die Schadprogramme an, die vom Betriebssystem im Moment erkannt werden können. Der von Apple vergebene Name der Schadsoftware, sowie der Dateityp, unter dem diese Software auftritt, werden aufgelistet. Die untere Tabelle listet die Internet-Plugins auf, die vom Betriebssystem überwacht und

auf veraltete Versionen überprüft werden. Der jeweilige Name des Plugins, sowie die als kritisch einzustufenden Versionen werden angezeigt.

Unterhalb der beiden Tabellen führt TinkerTool System auf, wann Apple die Liste zum letzten Mal überarbeitet hat, wann diese Liste auf den Computer übertragen wurde, und ob das System automatisch überprüft, ob eine neue Version der Liste verfügbar ist. Bei den Versionsangaben wird zwischen den Malware-Definitionen und der Software XProtect zur Malware-Behandlung unterschieden.

Bitte beachten Sie die folgenden Punkte:

- Die Tabellen führen auf, welche Bedrohungen das Betriebssystem potenziell erkennen kann. Sie geben keine Auskunft darüber, ob dieser Computer eine solche Schadsoftware irgendwann einmal vorgefunden oder entfernt hat. Falls es also einen Eintrag *abc* in einer der beiden Tabellen gibt, heißt das nur, dass macOS die Komponente *abc* erkennen würde, aber nicht, dass sich *abc* zurzeit auf Ihrem System befindet.
- Einträge in den Tabellen können sich mit gleicher Bezeichnung mehrmals wiederholen, falls die Malware unter verschiedenen Varianten mit unterschiedlichen Signaturen auftritt, Apple aber darauf verzichtet hat, jeder Variante einen eigenen Namen zu geben.

2.10.4 Sperrliste Programme

Nachdem Sie den Unterpunkt **Sperrliste Programme** öffnen, zeigt Ihnen TinkerTool System die aktuelle Liste des Betriebssystems für Programme an, die von der Nutzung bestimmter Funktion ausgeschlossen werden oder deren Start generell verhindert soll. Auch diese Liste wird aktualisiert, wenn die Wahlmöglichkeit **Sicherheitsmaßnahmen und Systemdateien installieren** in den **Systemeinstellungen** eingeschaltet ist.

Drei unterschiedliche Typen von Sperrlisten werden auf der Karte angezeigt:

- Die obere Tabelle listet Programme auf, die die Funktion **App Nap** standardmäßig nicht nutzen sollen. App Nap ist eine Apple-Technologie zum Energiesparen auf Programmebene: Wenn das Betriebssystem erkennt, dass ein laufendes Programm für den Benutzer zurzeit weder sichtbar noch hörbar ist (alle Fenster sind verdeckt und das Programm spielt im Moment keine Töne ab) und es außerdem keine Hintergrunddienste (wie das Herunterladen einer Datei) erbringt, wird dieses Programm automatisch abgebremst, indem es quasi in eine besondere Art von Ruhezustand versetzt wird. Aus dem Ruhezustand wird es nur nach längeren Warteperioden geweckt, um zu prüfen, ob es etwas zu tun gibt. Einige ältere Softwareprodukte sind für diese Technik noch nicht vorbereitet und arbeiten nicht mehr richtig, wenn App Nap aktiv wird. macOS „kennt“ die betreffenden, hier aufgelisteten Programme und sperrt automatisch App Nap für sie.
- Die mittlere Tabelle listet Programme auf, bei denen bekannt ist, dass sie mit der Funktion **Hohe Auflösung** von macOS, auch unter dem Namen *HiDPI* (*High number of Dots Per Inch*) bekannt, nicht korrekt funktionieren. Falls Sie mit einem Macintosh-System arbeiten, das mit einem *Retina*-, *4k*- oder *5k-Bildschirm* ausgestattet ist, skaliert macOS automatisch alle Grafiken neu, um den scharfen, hoch aufgelösten Bildschirm ausnutzen zu können. Einige ältere Programme arbeiten in dieser Betriebsart nicht korrekt. Wenn diese hier aufgelistet sind, schaltet macOS keine Retina-Funktionen für sie ein.
- Die untere Tabelle listet Programme, für die bekannt ist, dass sie überhaupt nicht mit der aktuellen Version des Betriebssystems zusammenarbeiten oder sogar technische

Probleme verursachen. macOS wird sich weigern, die Programme zu starten oder zu migrieren, wenn diese auf Ihrem System erkannt werden.

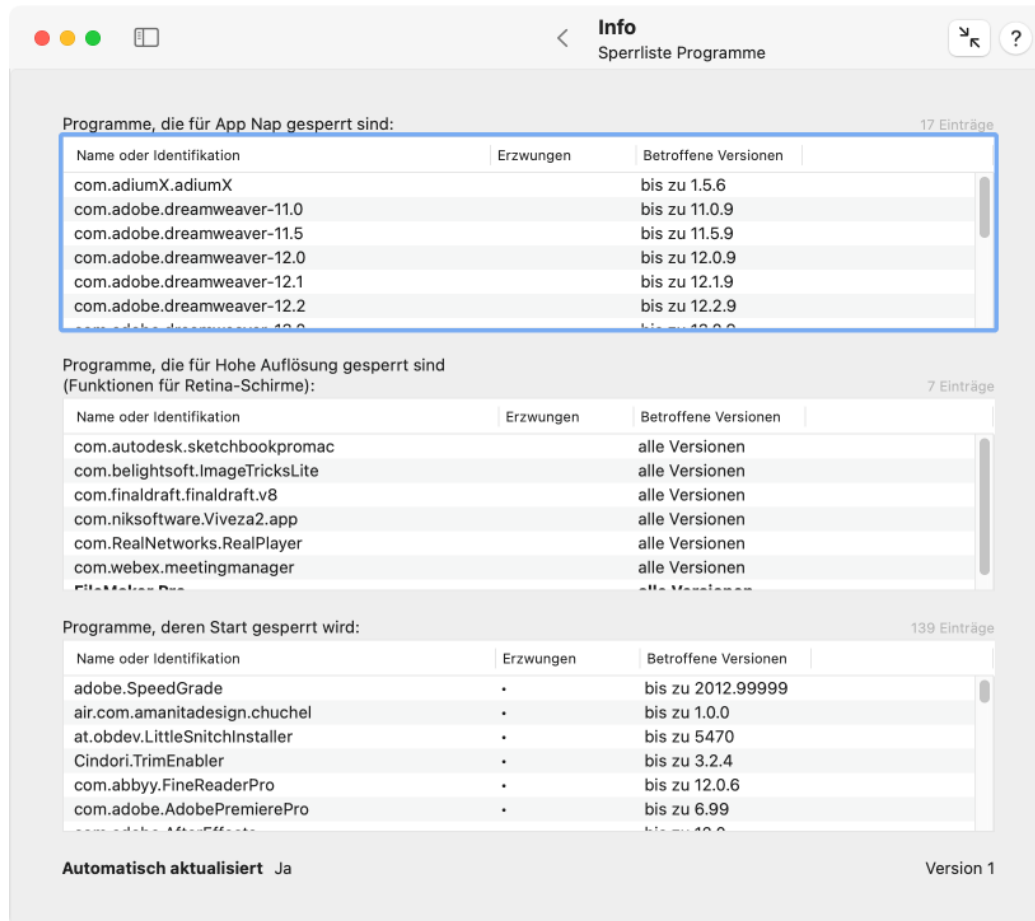


Abbildung 2.50: Sperrliste Programme

Jede Tabelle hat drei Spalten mit der folgenden Bedeutung:

- **Name oder Identifikation:** die Bezeichnung oder der interne Identifikationscode des Programms, das gesperrt wird. Falls das betroffene Programm auf Ihrem Computer vorhanden ist, versucht TinkerTool System, den Namen dieses Software-Produkts in Ihrer bevorzugten Sprache anzuzeigen. In diesem Fall erscheint der gesamte Eintrag außerdem in Fettschrift. Programme, die auf Ihrem System nicht vorgefunden wurden, werden nur über deren eindeutige Identifikation angezeigt.
- **Erzwungen:** Falls in dieser Spalte ein Punkt gezeigt wird, wird macOS das Sperren des entsprechenden Programms strikt einhalten. Der Benutzer kann diese Entscheidung nicht übergehen.
- **Betroffene Versionen:** Diese Spalte gibt die exakten Programmversionen an, für die ein Sperreintrag wirksam werden soll. In einigen Fällen sind nur alte, ausgelaufene Versionen eines Software-Produkts von einer Sperre betroffen.

2.10.5 Klassische Protokolle und Berichte

Nach Auswahl des Unterpunktes **Klassische Protokolle & Berichte** haben Sie direkten Zugriff auf eine hohe Zahl von Protokollaufzeichnungen, die von macOS vorgehalten wird. Das Betriebssystem sammelt Benachrichtigungs-, Warnungs- und Fehlermeldungen in solchen Dateien, insbesondere für diejenigen Komponenten des Systems, die keine direkte grafische Oberfläche haben. Systemverwalter können diese Daten auswerten, um Systemprobleme nachzuverfolgen, die in der Vergangenheit aufgetreten sind. Die klassischen Protokolle sind einfache Textdateien, die sich über die Zeit hinweg Zeile für Zeile füllen. Die meisten Dienste notieren zusätzlich Datum und Uhrzeit in jeder Zeile, so dass es einfacher wird, die Abfolge der Ereignisse zu verstehen, die aufgetreten sind.

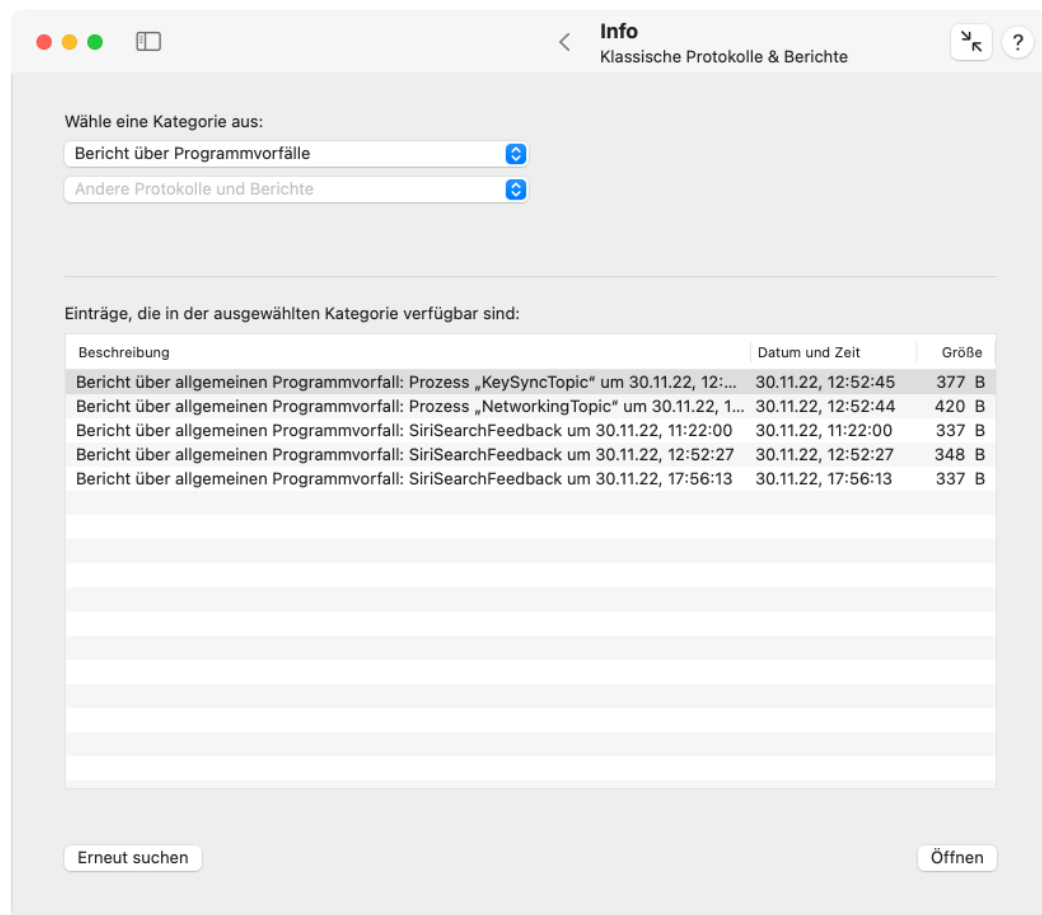


Abbildung 2.51: Protokolle und Berichte

Die möglicherweise verfügbaren Protokolle und Berichte können über zwei Aufklappmenüs abgerufen werden. Der obere Knopf **Standardprotokolle und Berichte** erlaubt es Ihnen, die wichtigsten Protokolldateien zu öffnen, die von macOS geführt werden:

- **Systemprotokolle:** das Hauptsystemprotokoll, das alle Warnungen und Fehlermeldungen aller laufenden Programme aufzeichnet.
- **Programmabsturzberichte:** Detailinformationen über alle Ereignisse, bei denen ein Programm unerwartet beendet werden musste, da ein ernster interner Fehler aufgetreten ist.

- **Programmabsturzberichte (iOS-Stil):** Ab 2022 hat Apple damit begonnen, Absturzberichte für alle Plattformen zu vereinheitlichen. Auch macOS ist davon betroffen, das Absturzberichte nun in der Regel in einer Variante erzeugt, die ursprünglich für iPhones entwickelt wurde. Intern sind diese Daten nicht mehr als sofort lesbarer Bericht, sondern in einer maschinenlesbaren Form gespeichert. TinkerTool System versucht, diesen Bericht so gut wie es geht lesbar zu machen.
- **Programmstillstandsberichte:** Details über Vorkommnisse, bei denen ein Programm in einen nicht mehr antwortenden Zustand getreten ist. Das betroffene Programm „hing“, d.h. es führte nur noch interne Verarbeitung durch, konnte aber nicht mehr auf Benutzeraktivität, wie z.B. Mausklicks, reagieren.
- **Systemabsturzberichte:** technische Informationen über Ereignisse, bei denen ein ernster Fehler im inneren Kern („Kernel“) des Betriebssystems entdeckt wurde, so dass der gesamte Computer sofort heruntergefahren werden musste, um Beschädigung von Daten zu verhindern. In älteren Versionen von macOS wurde hierfür auch der Begriff *Kernel Panic* verwendet.
- **System-Not-Aus:** hierbei handelt es sich um Berichte über Vorgänge, bei denen der Benutzer die „Not-Aus“-Funktion des Mac verwendet hat, d.h. die erzwungene Abschaltung über langes Halten des Ein-/Aus-Knopfes.
- **Apple-Chip-Problem Basisbericht:** technische Informationen über Ereignisse, bei denen das sekundäre Betriebssystem des „Immer an“-Teils von Macintosh-Computern mit Apple-Chip ein Problem entdeckt hat, für das ein Hardware-Neustart erforderlich war. Die kann Hardware- und Systemmanagement-Probleme mit einschließen.
- **Apple-Chip-Problem Voller Bericht:** Eine fortgeschrittenere Variante des vorherigen Punktes.
- **Berichte über starke Prozessoraktivität:** Diese Berichte führen Buch über Vorfälle, bei denen macOS entdeckt hat, dass ein Programm eine große Menge Prozessorleistung verbraucht hat, wobei ein oder mehrere Prozessoren über einen längeren Zeitraum belegt wurden. Solche Ereignisse sind für bestimmte Typen von Programmen normal, so dass diese Berichte nicht auf ein abnormes Verhalten hinweisen müssen. Die Berichte können dabei nützlich sein, auf Programme aufmerksam zu werden, die mehr Energie als andere benötigen, was bei akkubetriebenen Mobilcomputern interessant sein kann.
- **Berichte über starke Programmaktivität:** Die Berichte über starke Programmaktivität beziehen sich auf Ereignisse, bei denen ein Programm innerhalb eines kurzen Zeitraums sehr häufig geweckt wurde. Ganz ähnlich wie bei hoher Prozessoraktivität sind diese Berichte unkritisch, können aber dabei helfen, den Energieverbrauch besser zu verstehen.
- **Berichte über hohen Speicherverbrauch:** Falls dies sinnvoll ist, können Software-Entwickler das typische Speichernutzungsverhalten ihrer Programme definieren. Wenn ein solches Programm sich dann ungewöhnlich verhält, d.h. mehr Speicher als erwartet verbraucht, kann dieses Problem gemeldet werden, oder Gegenmaßnahmen können eingeleitet werden. Zum Beispiel könnte das Programm versuchen, seinen Platzbedarf zu reduzieren oder es könnte heruntergefahren werden. Diese Berichte verfolgen solche Ereignisse nach und enthalten die zugehörigen Speicherstatistiken.

- **Bericht über Plattenschreibaktivität:** Da die meisten Macintosh-Computer Flash-basierten Speicher verwenden, der immer einer Abnutzung unterliegt, sammelt Apple Statistiken über die Anzahl von Schreibvorgängen auf bestimmten Speichereinheiten. Dies erlaubt es, die verbleibende Lebensdauer von Flash-Speicherzellen abzuschätzen.
- **Berichte über langsames Antwortverhalten** macOS beobachtet, ob Programme auf Benutzeraktionen, wie einen Tastendruck oder ein Mausklick, innerhalb einer akzeptablen Zeit antworten. Falls ein Programm im Moment zu beschäftigt ist, um schnell genug auf ein Ereignis zu antworten, oder von einem technischen Problem betroffen ist, zeigt macOS einen rotierenden Cursor an. Zusätzlich wird diese Art von Bericht angelegt.
- **Bericht über langsames Herunterfahren:** Eine besondere Art von langsamem Antwortverhalten liegt bei einem Computer vor, der eine ungewöhnlich lange Zeit zum Herunterfahren braucht. Um die Ursache für solche Probleme zu finden, legt macOS einen Bericht über langsames Herunterfahren an, sobald einen solcher Effekt beobachtet wird.
- **„Differential Privacy“-Einsendungen:** Apple-Geräte sammeln Informationen darüber, wie die verschiedenen Produkte, Programme und Dienstleistungen genutzt werden. Falls Ihre Datenschutzeinstellungen es Apple erlauben, werden solche Daten von Zeit zu Zeit an Apple versandt, wobei diese mit einer Technik namens *Differential Privacy* anonymisiert werden. Jeder Sendevorgang an Apple wird protokolliert.
- **Apple-Bericht „Drahtlos-Diagnose“:** Wenn das Betriebssystem bestimmte Probleme beim WLAN-Betrieb beobachtet, protokolliert es automatisch Diagnosedaten über jeden Vorfall. Die Daten können private Informationen über Netzwerke in der Nachbarschaft enthalten. Aus diesem Grund sind die Protokolle üblicherweise verschlüsselt und können nur von autorisierten Apple-Service-Ingenieuren verarbeitet werden.
- **Bericht über iCloud-Dienste:** Diese Protokolle enthalten Diagnose- und Statistikdaten über die Kommunikation mit Apples iCloud-Diensten.
- **Bericht über Baseband-Verarbeitungsvorfälle:** Aus technischen Gründen werden alle Vorgänge, die Radiosignale in digitale Daten oder umgekehrt wandeln, als *Baseband-Verarbeitung* bezeichnet. Diese Protokollkategorie wird verwendet, um besondere Ereignisse aufzuzeichnen, die im Zusammenhang mit einer funkbasierten Komponente des Mac, wie WLAN oder Bluetooth aufgetreten sind.
- **Bericht über Telefonieüberwachung:** Diese Protokolle enthalten Informationen, die von den Telefoniefunktionen von macOS gesammelt werden.
- **Bericht über Vertrauensprüfungen:** Vertrauensprüfungen werden von macOS verwendet, um die Echtheit und Unversehrtheit einer Software-Komponente festzustellen. Dies beruht üblicherweise auf der Prüfung einer digitalen Signatur ausführbaren Codes und von deren Zertifikatskette.
- **Bericht über iPhone-Aktualisierungen:** Das System erstellt einen Bericht, jedes Mal wenn Sie macOS verwenden, um iOS auf einem angeschlossenen iPhone zu aktualisieren.
- **Bericht über iPad-Aktualisierungen:** Der gleiche Typ von Bericht wird für jedes Betriebssystem-Update eines iPad erstellt.

- **Bericht über proaktive Ereignisse:** macOS zeichnet statistische Daten pro Tag darüber auf, wie oft Siri etwas neues über den Benutzer „erlernt“ hat, um das Verhalten als persönlicher Assistent zu verbessern. Zum Beispiel könnte Siri erfolgreich eine familiäre Beziehung zwischen dem Benutzer und einer anderen Person identifiziert haben.
- **Bericht über Programmvorfälle:** dies sind allgemeine Diagnoseberichte, die einzelne Programme auslösen können, wenn sie intern besondere Ereignisse feststellen, beispielsweise eine übermäßig große Anzahl an Schreibvorgängen auf Datenträger. Es liegt im Ermessen des jeweiligen Programms, was als besonderes Ereignis anzusehen ist.

Der zweite Knopf sammelt **Andere Protokolle und Berichte**. Dies beinhaltet bekannte Aktivitätsberichte von macOS, z.B. bezüglich des App Store, des Festplattendienstprogramms, der Resume-Funktion, Überwachung des Abschaltvorgangs, usw. sowie außerdem unbekannte Protokolle, die von Drittanbieterprogrammen angelegt werden. Im letzteren Fall kann TinkerTool System den exakten Inhalt und die Bedeutung der Protokolldateien nicht im Voraus ermitteln, so dass die entsprechenden Menüpunkte mit ihrem rohen Dateinamen im Menü aufgeführt werden.

Aus Sicherheitsgründen dürfen Protokolle, die potenziell vertrauliche oder sicherheitskritische Daten enthalten könnten, nicht von jedem Benutzer geöffnet werden. Sie müssen als Benutzer mit Verwalterberechtigung angemeldet sein, um sicher zu stellen, dass Sie die vollständige Menge von Protokolldateien sehen und öffnen können. TinkerTool System zeigt eine dementsprechende Warnung an, falls Sie keinen Administrator-Account verwenden.

Nachdem Sie eine Protokollkategorie mit einem der zwei Knöpfe ausgewählt haben, gibt Ihnen die Tabelle einen Überblick über die vorhandenen Protokolle. Jedes wird mit einer kurzen Beschreibung, Datum und Uhrzeit, die üblicherweise mit dem letzten Eintrag, der in einem Protokoll aufgezeichnet wurde, zusammenfällt, sowie Dateigröße aufgeführt. Doppelklicken Sie entweder einen aufgelisteten Eintrag oder drücken Sie den Knopf **Öffnen**, um das entsprechende Protokoll zu öffnen. Ein Textfenster wird Ihnen den Inhalt der betreffenden Protokolldatei zeigen. Beachten Sie, dass Sie so viele Fenster gleichzeitig öffnen können, wie Sie möchten. Die Protokolle können außerdem gedruckt oder in Textdateien gespeichert werden, indem Sie die entsprechenden Knöpfe in der rechten unteren Ecke jedes Fensters betätigen.

Bei manchen Protokollen wird der zusätzliche Knopf **Mit „Konsole“ öffnen** angezeigt. Dies gilt für Protokolle, die macOS nicht als lesbarer Klartext, sondern in einer maschinenlesbaren Form speichert. TinkerTool System bemüht sich immer, auch diese Protokolle so gut es geht lesbar zu machen, es gibt aber ein paar Fälle, in denen das Programm **Konsole** (aus dem Ordner **Dienstprogramme**) internes Spezialwissen von Apple verwendet, um dies noch besser gestalten zu können. Sie können testweise ein Protokoll zusätzlich in der Konsole öffnen, um zu prüfen, ob es dort anders aufbereitet wird. In einigen Fällen liefert Konsole, in anderen TinkerTool System die besseren Ergebnisse.

Falls Sie annehmen, dass macOS neue Berichte angelegt hat, während TinkerTool System lief, drücken Sie den Knopf **Erneut suchen** in der unteren linken Ecke, um die Klappmenüs zu aktualisieren.

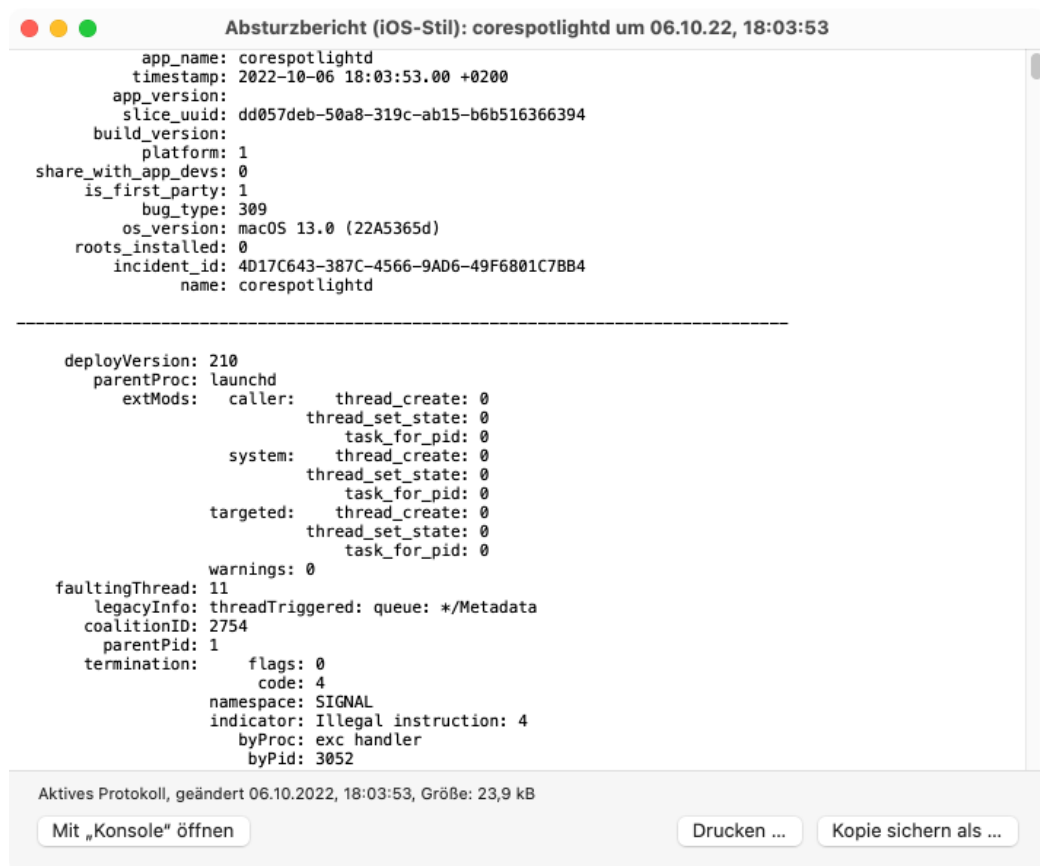


Abbildung 2.52: Der Inhalt eines Protokolls oder Berichts wird in einem getrennten Fenster angezeigt.

2.10.6 Moderne Protokollierung und Ablaufverfolgung

Zusätzlich zur klassischen Protokollführung, bei der Meldungszeilen an das Ende einiger Textdateien angehängt werden, verwendet macOS eine moderne Protokolltechnik, die auf Datenbanken beruht. Diese enthalten strukturierte, komprimierte Datensätze, die je nach Fall zwischen Dateien und Hauptspeicher verteilt werden.

Apple bezeichnet das moderne Verfahren auch als *Vereinheitlichte Protokollierung (Unified Logging)*. Es ist dazu gedacht, aller bisherigen Protokolltechniken (wie Textprotokolle, syslog oder ASL - Apple System Log) zu ersetzen.

Die Struktur heutiger Programme stellt neue Herausforderungen:

- Programme werden in verschiedene Prozesse getrennt, z.B. um Privilegien auf eine sicherere Art zu verwalten.
- Prozesse werden auf verschiedene Handlungsstränge (Threads) aufgeteilt, um die Arbeit auf mehrere Prozessorkerne zu verteilen.
- Threads werden parallel oder in zufälliger Reihenfolge abgearbeitet, was im Vorhinein unbekannt ist.

Wenn man versucht, Probleme mit Programmen über altmodische Textberichte zu identifizieren, kann es schwierig oder gar unmöglich werden, miteinander in Beziehung stehende Ereignisse in verschiedenen Prozessen und Threads nachzuverfolgen. Die Problemnachrichten können in chaotischer Reihenfolge aufgezeichnet worden sein und es ist möglicherweise nicht klar, wie sie miteinander verbunden sind. Das Erzeugen von Textzeilen mit detaillierten Diagnosedaten (die vielleicht unter normalen Umständen niemals gebraucht werden) setzt Programme und das Betriebssystem unnötigem Stress aus.

macOS versucht, diese Probleme dadurch zu lösen, dass Technik eingeführt wird, die für aktuelle Anwendungen geeigneter erscheint:

- Statt in Textdateien werden Protokoll- und Ablaufverfolgungsdaten in Hochleistungsdatenbanken aufgezeichnet.
- Programme müssen komplexe Textzeilen nicht mehr selber erzeugen (beispielsweise indem die Textdarstellung einer Netzwerkadresse berechnet wird, die Teil einer Fehlermeldung werden soll). Sie können solche Daten in roher Form an eine zentrale Protokolleinheit schicken. Diese Komponente kann den Text dann später *auf Wunsch, nur falls und wenn er wirklich benötigt wird*, berechnen. Auf diese Weise wird die Entscheidung, Text zu erzeugen und Diagnosedaten aufzubereiten, so lange wie möglich aufgeschoben. In vielen Fällen können diese Daten nach einiger Zeit einfach wieder verworfen werden, ohne dass sie jemals verarbeitet werden mussten.
- Die gleiche Technik kommt auf allen Ebenen des Systems zum Einsatz. Der innere Systemkern verwendet genau die gleiche Technik wie eine Anwendung mit grafischer Oberfläche auf hoher Ebene.
- Es gibt systemweite Schweregrade, die definieren, wie wichtig eine Nachricht sein wird. Unwichtige Meldungen, die nur zum Debugging benötigt werden, können für eine kurze, begrenzte Zeit im Hauptspeicher gehalten werden, statt sie permanent in Dateien abzulegen. Das Verwerfen, Archivieren und Bereinigen der Protokolle kann viel präziser gesteuert werden.

- Meldungen können mit einem sogenannten **Aktivitätsbezeichner** versehen sein. Diese machen es einfacher, nachzuverfolgen, welche Meldungen zu einem bestimmten Vorgang im System gehören, auch wenn die Berechnungen, die für diesen Vorgang erforderlich sind, auf mehrere Prozesse und Threads verteilt sind.
- Die Protokolleinträge in der Datenbank können mit zusätzlichen Daten angereichert werden. Wenn Protokolldaten dazu gebraucht werden, ein Problem zu beheben, können Datenbankfilter dazu verwendet werden, die nötigen Informationen zu finden und nicht relevante Daten auszublenden. Sogenannte **Subsystembezeichner** und **Kategoriebezeichner** können dazu genutzt werden, Protokolleinträge entsprechend zu organisieren.
- Bezüge auf Benutzerdaten, die kritisch für die Privatsphäre der Benutzer sind, können entfernt werden, bevor diese in der Protokolldatenbank verarbeitet und gespeichert werden. Das macht es einfacher, Protokolldaten an Techniker weiterzugeben, ohne dass das Risiko besteht, dass private Informationen oder Firmengeheimnisse unbeabsichtigt an Unbefugte übertragen werden.

Aktivitäten enthalten eine kurze Klartextbeschreibung mit einem numerischen Bezeichner. TinkerTool System zeigt Aktivitätsbezeichner als 16-stellige hexadezimale Zahl an. Was als separate Aktivität angesehen und wie sie beschrieben wird, ist dem Autor des Programms überlassen, das einen Aktivitätseintrag anlegt.

Subsystem- und Kategoriebezeichner sind ebenso durch die jeweiligen Anwenderprogramme festgelegt. Falls Sie also Protokollnachrichten herausfiltern möchten, die mit einer bestimmten Software-Komponente verknüpft sind, benötigen Sie Daten des Software-Entwicklers, welche Bezeichner hier zum Einsatz kommen. Subsystembezeichner sollen dafür verwendet werden, den Ort innerhalb eines Programms anzugeben, z.B. ein bestimmtes Modul. Kategoriebezeichner sollen dazu genutzt werden, eine bestimmte Betriebsart zu definieren, z.B. „Testmodus“ oder „netzwerkbezogen“.

TinkerTool System analysiert automatisch das laufende Betriebssystem und versucht, einige der wichtigsten Subsystembezeichner zu „erraten“. Die Namen erscheinen in der Kombobox **Filtern nach macOS-Protokollsystembezeichner** und können als Menüpunkte ausgewählt werden. Sie können das Eingabefeld aber auch überschreiben und irgendeinen anderen gültigen Namen eingeben, der hier nicht aufgeführt ist.

macOS verwendet fünf verschiedene Grade, um die Rolle oder Schwere einer Protokollnachricht festzulegen:

- **Fehler:** eine Meldung, die auf eine Fehlersituation hinweist, die sich auf das gesamte Betriebssystem oder mehrere Komponenten eines Software-Produkts bezieht.
- **Problem:** eine Meldung für eine Angelegenheit, die sich nur auf eine einzelne Software-Komponente bezieht.
- **Standard:** eine Meldung, die kein abnormes Verhalten anzeigt, aber immer noch so wichtig ist, dass sie im Protokoll festgehalten werden sollte.
- **Info:** eine Meldung rein informatorischer Natur. Solche Meldungen werden standardmäßig nicht permanent gespeichert. Sie werden für gewöhnlich nur auf besondere Anforderung abgerufen.

- **Debugging:** eine Meldung, die nur für Software-Entwickler von Interesse ist, um das Verhalten eines Programms auf Quellcode-Ebene nachverfolgen zu können. Solche Einträge werden im Normalbetrieb unterdrückt und können mit sehr hoher Frequenz auftreten, z.B. mehrere hundert Einträge pro Sekunde.

TinkerTool System kann genutzt werden, um entweder

- ausgewählte Einträge aus der Live-Protokolldatenbank oder aus einem exportierten Archiv zu extrahieren und in lesbaren Text umzuwandeln, der angezeigt oder gesichert werden kann, oder um
- ausgewählte oder alle Einträge aus der Protokolldatenbank zu exportieren, so dass sie auf einem anderen Computer ausgewertet werden können.

Apple hat ein bestimmtes Dateiformat, das **macOS-Protokollarchiv** mit der Namensendung **logarchive**, definiert, um Protokoll- und Ablaufverfolgungsdaten zwischen verschiedenen macOS-Systemen auszutauschen. Diese Archive können mit früheren Systemgenerationen (OS X oder Mac OS X) nicht direkt verwendet werden.

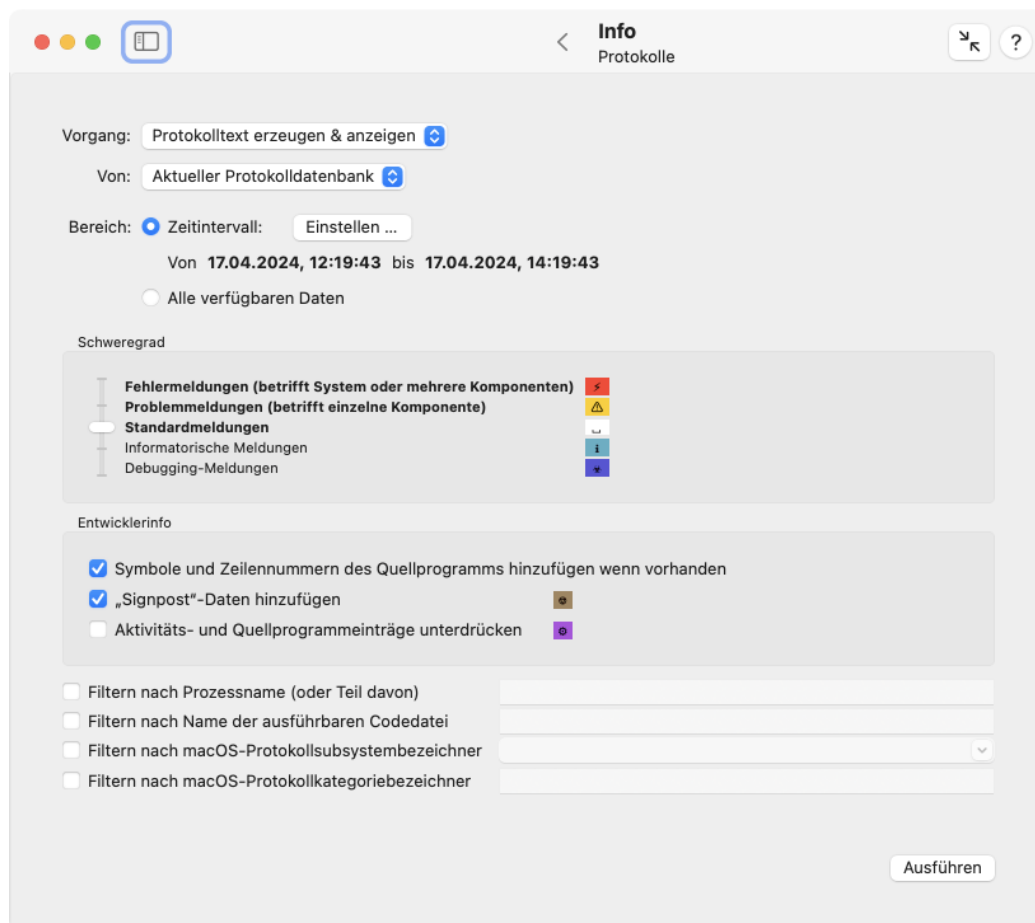


Abbildung 2.53: Arbeiten mit modernen Protokollen

Um mit modernen macOS-Protokollen zu arbeiten, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Protokolle** auf der Karte **Info**.

2. Wählen Sie den **Vorgang** aus, der ausgeführt werden soll. Sie können entweder **Protokolltext erzeugen und anzeigen** oder **Protokolldaten exportieren**.
3. Wählen Sie bei **Von** die Quelle für den Vorgang (falls zutreffend) aus. Dies kann entweder die **aktuelle Protokolldatenbank** des lokalen Computers oder **importierte Protokolldaten** sein.
4. Wählen Sie über die Knöpfe bei **Bereich** das Zeitintervall aus, das erfasst werden soll. Sie können entweder ein bestimmtes Intervall über den Knopf **Einstellen** angeben oder **Alle verfügbaren Daten** wählen. Das Zeitintervall kann mit den Kalender-/Uhr-Elementen bei **Von** und **Bis** eingestellt werden. Sie können entweder die Uhrzeiger bewegen oder die Zeit als Text eingeben. Der Knopf **+12h** kann dazu genutzt werden, um schnell zwischen vor- und nachmittags, bzw. umgekehrt, umzuschalten. Sie können auch ein **vorberechnetes Zeitintervall** verwenden, was weiter unter beschrieben wird.
5. Wählen Sie den **Schweregrad** mit dem Schieberegler. Eine niedrige Ebene enthält auch alle Meldungen der höheren Ebenen, was durch Fettschrift wiedergegeben wird.
6. Falls Sie Diagnosedaten für Software-Entwickler hinzufügen möchten falls verfügbar, kreuzen Sie die entsprechenden Punkte bei **Entwicklerinfo** an.
7. Schalten Sie alle Filteroptionen ein oder aus, die Sie brauchen.
8. Drücken Sie auf den Knopf **Ausführen**.

Im Standardfall wählt TinkerTool System ein Zeitintervall, das die letzten zwei Stunden bevor das Programm gestartet wurde, umfasst. Wenn Sie das Protokoll nicht weiter durch Filter einschränken, kann dieses Zeitintervall zu groß sein, denn oft werden in dieser Zeit mehr als 2 Millionen Ereignisse protokolliert. Wenn Sie wissen, wann ein besonderes Ereignis aufgetreten ist, für das Sie sich interessieren, können Sie im Dialog für das Zeitintervall den Abschnitt ... **oder verwende die vorberechnete Zeit** verwenden.

Dort können Sie Datum und Uhrzeit eines Ereignisses von Hand einstellen und ein Fenster zwischen 1 Sekunde und 999 Minuten um dieses Ereignis herum von TinkerTool System als Intervall automatisch einstellen lassen. Die charakteristische Zeit kann wahlweise am Anfang, am Ende oder in der Mitte des Intervalls liegen. Als Zeitpunkt kann außerdem die **Systemstartzeit** oder die aktuelle Zeit (Knopf „Jetzt“) automatisch eingestellt werden.

Um einen Filter zu nutzen, setzen Sie ein entsprechendes Häkchen und geben Sie den Namen oder den Bezeichner für den jeweiligen Filter im Feld rechts daneben an.

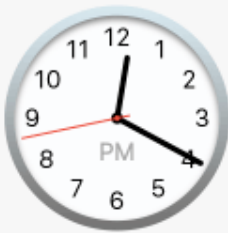
Es wird nicht empfohlen, TinkerTool System sehr große Protokolltexte erzeugen zu lassen. Das System könnte sonst Probleme haben, einen solch langen Text in einem Standardfenster innerhalb einer erträglichen Zeit anzuzeigen. Aus diesem Grund beschränkt das Programm die Textberichte automatisch auf 500 Megabyte verarbeitete Rohdaten.

TinkerTool System verwendet die kleinen Symbole und die Farbhinterlegungen, die neben den Einstellmöglichkeiten zu sehen sind, auch, um Meldungen mit dem entsprechenden Schweregrad, bzw. Aktivitätseinträge im Ergebnistext zu markieren. Die Symbole befinden sich am Anfang der jeweiligen Zeile. Sie können alle Farbmarkierungen durch Drücken des Knopfes **Farben entfernen** ausblenden. Dies kann nicht rückgängig gemacht werden.

Stelle das Zeitintervall manuell ein:

Von

Apr. 2024 ◀ ● ▶
M D M D F S S
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 1 2 3 4 5
6 7 8 9 10 11 12

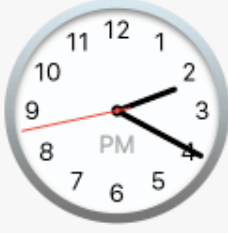


+12h

Heute, 12:19:43 12:19:43 ▲▼

Bis

Apr. 2024 ◀ ● ▶
M D M D F S S
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 1 2 3 4 5
6 7 8 9 10 11 12



+12h

Heute, 14:19:43 14:19:43 ▲▼

... oder verwende die vorberechnete Zeit:

17. 4.2024, 12:08:14 ▲▼

Systemstartzeit „Jetzt“

als Startzeit mit Endzeit ▲▼

2

Sekunden ▲▼ später.

Zeitintervall ändern

Einstellen

Abbildung 2.54: Der Zeiteingabedialog hilft Ihnen dabei, das Intervall auszuwählen, das von Interesse ist

```

17.04.2024, 12:19:43 [33579]-(0x2cba77) imagent: (CoreData) [:] CoreData: XPC: Unable to connect to server with options {
  NSPersistentHistoryTrackingKey = 1;
  NSReadOnlyPersistentStoreOption = 0;
  NSXPCStoreServerEndpointFactory = "<ONCDRemotePersistentStoreEndpointFactory: 0x1352049c0>";
  skipModelCheck = 1;
}
17.04.2024, 12:19:43 [33579]-(0x2cba77) imagent: (CoreData) [:] CoreData: XPC: Unable to load metadata: Error Domain=NSCocoaErrorDomain
Code=134068 "Ein CoreData-Fehler ist aufgetreten." UserInfo={Problem=Unable to send to server; failed after 8 attempts.}
17.04.2024, 12:19:43 [33579]-(0x2cba77) imagent: (libxpc.dylib) [com.apple.xpc:connection] [0x135038f80] activating connection: mach=true
listeners=false peer=false name=com.apple.contactsd.persistence
17.04.2024, 12:19:43 [0]-(0x2d6b12) kernel: (Sandbox) [:] 1 duplicate report for Sandbox: searchpartyuseragent(33574) deny(1) mach-lookup
com.apple.contactsd.persistence
17.04.2024, 12:19:43 [0]-(0x2d6b12) kernel: (Sandbox) [:] Sandbox: imagent(33579) deny(1) mach-lookup com.apple.contactsd.persistence
17.04.2024, 12:19:43 [1]-(0x2d6b12) launchd: [gui/501 [102923]:] denied lookup: name = com.apple.contactsd.persistence, requestor =
imagent(33579), error = 159: Sandbox restriction
17.04.2024, 12:19:43 [1]-(0x2d6733) launchd: [:] Last log repeated 1 times
17.04.2024, 12:19:43 [33579]-(0x2cba77) imagent: (libxpc.dylib) [com.apple.xpc:connection] [0x135038f80] failed to do a bootstrap look-up:
xpc_error=159: Unknown error: 159
17.04.2024, 12:19:43 [33579]-(0x2cba77) imagent: (libxpc.dylib) [com.apple.xpc:connection] [0x135038f80] invalidated after a failed init
17.04.2024, 12:19:43 [33579]-(0x2d6da0) imagent: (ContactsPersistence) [com.apple.contacts:persistence] Persistent store service connection
invalidated: failed at lookup with error 159 - Sandbox restriction
17.04.2024, 12:19:43 [33579]-(0x2d6da0) imagent: (ContactsPersistence) [com.apple.contacts:persistence] Error communicating with persistent
store service proxy: Error Domain=NSCocoaErrorDomain Code=4099 "The connection to service named com.apple.contactsd.persistence was invalidated:
failed at lookup with error 159 - Sandbox restriction." UserInfo={NSDebugDescription=The connection to service named
com.apple.contactsd.persistence was invalidated: failed at lookup with error 159 - Sandbox restriction.}
17.04.2024, 12:19:43 [33579]-(0x2cba77) imagent: (ContactsPersistence) [com.apple.contacts:persistence] Error connecting to remote
endpoint: (null)
17.04.2024, 12:19:43 [33579]-(0x2cba77) imagent: (CoreData) [com.apple.coredata:error] fault: Unable to create token NSXPCConnection.
NSXPCStoreServerEndpointFactory 0x1352049c0 -newEndpoint returned nil
17.04.2024, 12:19:43 [33579]-(0x2cba77) imagent: (CoreData) [com.apple.coredata:error] CoreData: Unable to create token NSXPCConnection.
NSXPCStoreServerEndpointFactory 0x1352049c0 -newEndpoint returned nil
17.04.2024, 12:19:43 [33579]-(0x2cba77) ***Activity 0x000000000005f356*** imagent: (libsystem_trace.dylib) [:] Activity for state dumps
17.04.2024, 12:19:43 [33579]-(0x2cba77) imagent: (CoreData) [com.apple.coredata:error] error: Failed to create NSXPCConnection
17.04.2024, 12:19:43 [33579]-(0x2cba77) imagent: (libxpc.dylib) [com.apple.xpc:connection] [0x135038f80] activating connection: mach=true
listeners=false peer=false name=com.apple.contactsd.persistence
17.04.2024, 12:19:43 [33579]-(0x2cba77) imagent: (libxpc.dylib) [com.apple.xpc:connection] [0x135038f80] failed to do a bootstrap look-up:
xpc_error=159: Unknown error: 159
17.04.2024, 12:19:43 [33579]-(0x2cba77) imagent: (libxpc.dylib) [com.apple.xpc:connection] [0x135038f80] invalidated after a failed init
17.04.2024, 12:19:43 [33579]-(0x2d6da0) imagent: (ContactsPersistence) [com.apple.contacts:persistence] Persistent store service connection
invalidated: failed at lookup with error 159 - Sandbox restriction

```

Abbildung 2.55: Anzeige eines macOS-Protokolls

Ein schwarzer Balken im Protokolltext zeigt an, dass das macOS-Protokollsubsystem eine Information aus der Ausgabe entfernt hat, da das Programm, das die Nachricht protokolliert hatte, nicht ausdrücklich bestätigt hat, dass der Text als öffentlich anzusehen ist. Der entfernte Teil könnte Daten enthalten, die der Privatsphäre eines Benutzers unterliegen oder anderweitig unter den Datenschutz fallen. Diese Vorgehensweise stellt sicher, dass Protokollauszüge an Dritte weitergegeben werden können, wobei die nationalen Datenschutzbestimmungen eingehalten werden. Tinker-Tool System kann diese „zensierten“ Teile nicht sichtbar machen. Falls Sie die Farben entfernen, werden die schwarzen Bereiche mit dem Text **private** dargestellt.

Falls Sie die Funktion **Symbole und Zeilennummern des Quellprogramms hinzufügen wenn vorhanden** eingeschaltet haben und die entsprechenden Daten bei einem Protokolleintrag vorhanden sind, werden diese mit der Markierung

```
>>> source:
```

an das Ende des Eintrags angehängt. Zum leichteren Verständnis für Entwickler wird der Begriff „source“ nicht ins Deutsche übersetzt. „Signpost“-Meldungen werden mit einer braunen Markierung hinterlegt. Sie enthalten neben dem eigentlichen Text eine Angabe nach dem Muster

```
[spid 0x123456789, ABC, DEF]
```

wobei die Zahl hinter **spid** der hexadezimale Signpost-Bezeichner ist, gefolgt von einem Gültigkeitsbereich (*Scope*) und einer Typangabe.

Sie können den erzeugten Protokolltext speichern, indem Sie den Knopf **Sichern ...** im Anzeigefenster betätigen. Er wird im *Rich Text Format (RTF)* abgelegt, so dass er von jedem professionellen Texteditor wie z.B. **TextEdit** geöffnet werden kann. Um nach Text in den Protokollen zu suchen, verwenden Sie die Menüpunkte bei **Bearbeiten > Suchen** oder drücken Sie + .

Falls der Protokolltext sehr lang ist, Sie aber in etwa wissen, wonach Sie suchen, können Sie neben der reinen Suche auch einen nachträglichen, textbasierten Filter verwenden, um sich auf bestimmte Meldungszeilen zu konzentrieren und alle anderen auszublenden. Drücken Sie hierzu auf den Knopf mit dem Filtersymbol unten links. Sie können nun einen Suchbegriff in einem Dialog definieren und anwenden. Es werden danach nur noch diejenigen Zeilen angezeigt, die dieses Suchwort enthalten. Ein weiterer Klick auf den Filterknopf lässt die ausgeblendeten Zeilen wieder erscheinen.

Mithilfe des Knopfes **Prozesse trennen...** ist es möglich, Einträge für einzelne Prozess exemplare, die von besonderen Interesse sind, aus dem Gesamtfenster zu isolieren und in jeweils getrennten Fenstern anzuzeigen. Nach Anklicken erscheint ein Dialog, in dem Sie die erkannten Prozess exemplare wählen können. Es wird jeweils der Programmname, gefolgt von der Prozessidentifikation (PID) in runden Klammern angegeben. Nach Auswahl der anzuzeigenden Prozesse erscheint jedes Exemplar in einem eigenen Fenster. Um macOS nicht zu überlasten, wird die gleichzeitige Anzeige auf maximal 40 Fenster begrenzt.

Kapitel 3

Dateioperationen

3.1 Die Einstellungskarte Ablage

3.1.1 Link

Ein *Link* im Dateisystem ist eine zusätzliche Darstellung einer existierenden Datei, oder – in manchen Fällen – eines Ordners. Diese Darstellung kann dazu benutzt werden, um an einem anderen Ort einen weiteren Bezug auf die Datei herzustellen, d.h. in einem anderen Ordner oder auf einem anderen Plattenlaufwerk, oder unter einem anderen Namen. macOS unterstützt drei Arten von Links:

- **Alias:** ein Objekt, das sich auf eine andere Datei oder einen anderen Ordner bezieht, und in der Lage ist, das Originalobjekt nachzuverfolgen, falls dieses an eine andere Stelle verschoben oder umbenannt werden sollte. Ein Alias wird ungültig, sobald das Originalobjekt gelöscht wird.
- **Symbolischer Link:** ein Objekt, das sich auf eine andere Datei oder einen Ordner über dessen UNIX-Pfadangabe bezieht. Wenn das Originalobjekt verschoben oder umbenannt wird, geht der Link mit Absicht kaputt. Wird versucht, eine solches Objekt über den defekten Link zu öffnen, erhalten Sie eine Fehlermeldung.
- **Fester Link:** ein zusätzlicher Eintrag in einem Ordner, der sich auf eine Datei bezieht. Weder der Benutzer noch das Betriebssystem können einen festen Link vom „ersten“ Eintrag einer Datei unterscheiden, so dass wir hier nicht mehr von einem Originalobjekt sprechen können. Feste Links sind lediglich ein oder mehrere zusätzliche Namen, die auf die gleiche Datei zeigen. Hierbei sind feste Links auf Dateien beschränkt, sie können nicht für Ordner benutzt werden. Ebenso ist es nicht möglich, die Grenzen von Volumes zu überschreiten. Die Datei, auf die sich ein fester Link bezieht, muss also auf dem gleichen Volume liegen, wie der Link.

Der macOS-Finder ist nur in der Lage, Aliase anzulegen. Wenn der Finder einen symbolischen Link anzeigt, wird er ebenso als Alias dargestellt, um die Situation für unerfahrene Benutzer zu vereinfachen. Solche Objekte werden mit einem runden Pfeil zusätzlich zu ihrem normalen Symbol gekennzeichnet. Aliase stellen eine Technik dar, die aus dem klassischen Mac OS übernommen wurde, und in bestimmten Fällen müssen Programme die Alias-Technik ausdrücklich unterstützen, um auf das Originalobjekt zuzugreifen, auf das der Alias verweist. Links dagegen werden vom Betriebssystem selbst ausgewertet, sollten daher also in allen Programmen funktionieren.

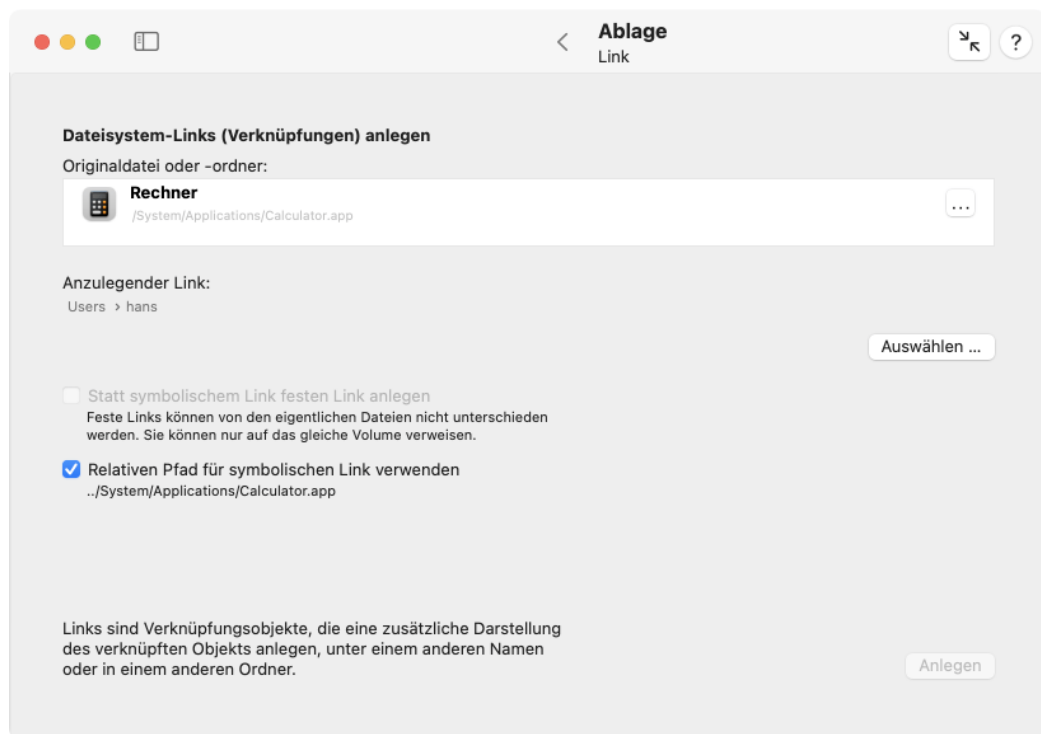


Abbildung 3.1: Link

Genauer betrachtet unterscheiden moderne Versionen von macOS zwischen klassischen Mac OS-Aliasen, die inzwischen als veraltet und missbilligt gelten, und modernen Aliasen, die auf sogenannten *Bookmarks* basieren.

Da der Finder keine symbolischen Links oder feste Links anlegen kann, fügt TinkerTool System diese fehlenden Funktionen hinzu. Führen Sie die folgenden Schritte durch, um Links anzulegen:

1. Öffnen Sie den Unterpunkt **Link** auf der Einstellungskarte **Ablage**.
2. Ziehen Sie die Originaldatei- oder ordner aus dem Finder in das Feld **Originaldatei oder -ordner**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Drücken Sie den Knopf **Auswählen ...**, um den Ort anzugeben, an dem Sie den Link anlegen lassen möchten.
4. Normalerweise wird ein symbolischer Link angelegt. Falls Sie stattdessen einen festen Link anlegen möchten, kreuzen Sie die Wahlmöglichkeit **Statt symbolischem Link festen Link anlegen** an. Denken Sie daran, dass feste Links auf Dateien auf dem gleichen Platten-Volume beschränkt sind.
5. Falls Sie einen symbolischen Link gewählt haben, entscheiden Sie über die Option **Relativen Pfad für symbolischen Link verwenden**, ob er mit einem absoluten oder einem relativen Pfad angelegt werden soll. Ein relativer Pfad bleibt in solchen Fällen gültig, in denen Sie eine ganze Ordnerhierarchie später an einen anderen Ort bewegen, und sowohl der Link als auch das Link-Ziel beide in dieser Hierarchie enthalten

sind. Der relative Pfad, der hierbei entsteht, wird zur Kontrolle unterhalb der Option angezeigt.

6. Drücken Sie den Knopf **Anlegen**.

3.1.2 Schutz

macOS unterstützt ein spezielles Schutzattribut, mit dem Dateien oder Ordner versehen werden können. Wenn Sie ein Objekt als geschützt markieren, ist es nicht mehr möglich, dieses zu verändern oder zu löschen. Jede Änderung erfordert, dass der Schutz vorher entfernt wird. Der macOS-Finder verwendet ein Schlosssymbol, das zusätzlich zum normalen Symbol angezeigt wird, um ein geschütztes Objekt darzustellen. Aus diesem Grund verwendet man manchmal auch die Sprechweise, ein solches Objekt wäre „geloct“, also mit einem Schloss versehen (engl. *lock* heißt Schloss). In der Fachsprache bezeichnet Lock aber auch etwas anderes, nämlich die Markierung eines Objektes mit der Bedeutung, dass dieses gerade von einem Programm exklusiv benutzt wird. Dies ist hier jedoch nicht gemeint.

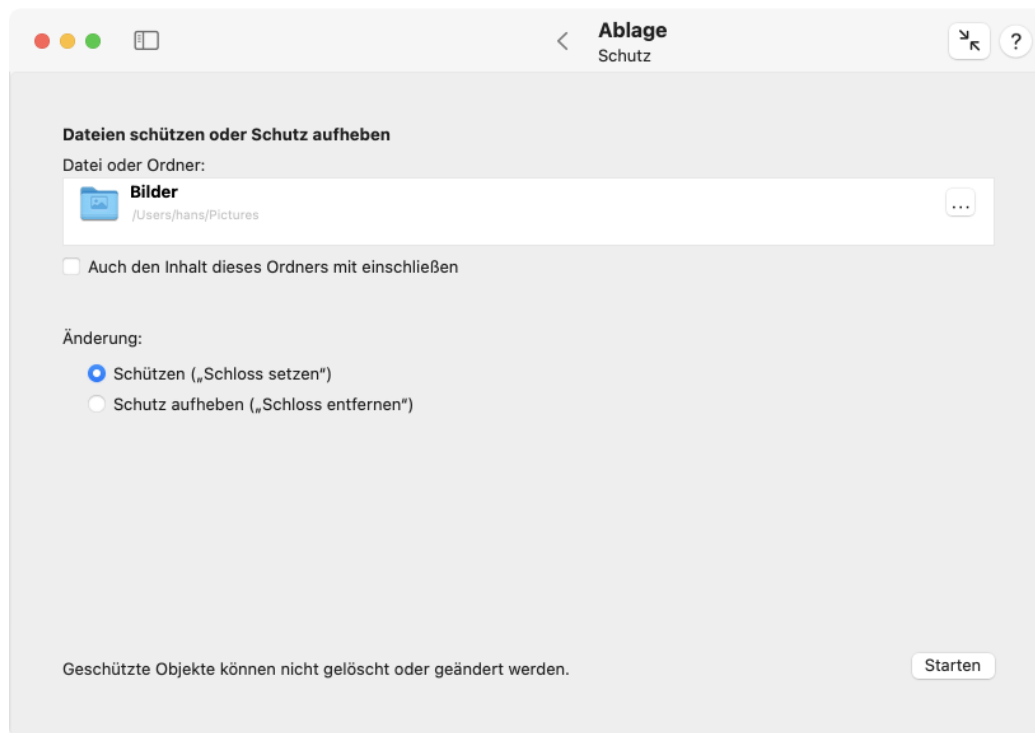


Abbildung 3.2: Schutz

TinkerTool System bietet an, die Schutzmarkierung nicht nur für einzelne Objekte, sondern für eine ganze Hierarchie von Dateien oder Ordnern, die sich in einem zuoberst liegenden Ordner befinden, zu setzen oder zu entfernen. Um mit Schutzattributen zu arbeiten, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Schutz** auf der Einstellungskarte **Ablage**.
2. Ziehen Sie eine Datei oder einen Ordner aus dem Finder in das Feld **Datei oder Ordner**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.

3. Falls Sie einen Ordner ausgewählt haben, entscheiden Sie, ob der Schutz nur auf den Ordner selbst, oder auch auf dessen vollständigen Inhalt angewendet werden soll. Markieren Sie das Feld **Auch den Inhalt des Ordners mit einschließen** entsprechend.
4. Drücken Sie auf einen der Knöpfe **Schützen** oder **Schutz aufheben** unter **Änderung**.
5. Drücken Sie auf den Knopf **Starten**.

Einige Nicht-Macintosh-Dateisysteme sind nicht in der Lage, die Schutzattribute zu unterstützen. In diesem Fall bestätigt das Betriebssystem eventuell, die Schutzmarkierung wäre erfolgreich gesetzt worden, obwohl sich das Objekt immer noch im ungeschützten Zustand befindet.

3.1.3 Attribute

In Ergänzung zur Schutzmarkierung, die auch auf der UNIX-Ebene von macOS unterstützt wird, unterstützt das Betriebssystem auch einige Attribute auf hoher Systemebene, die aus dem klassischen Mac OS übernommen wurden.

- Eine Datei kann mit einem **HFS-Typcode** versehen sein. Der Typcode ist dazu gedacht, anzuzeigen, welche Art von Dokument eine Datei darstellen soll. Mithilfe des Typcodes kann das System schnell bestimmen, was in einer gegebenen Datei gespeichert sein soll, ohne dass spezielle Markierungen im Dateinamen (wie Dateinamenserweiterungen) nötig sind, und ohne dass der Inhalt der Datei analysiert werden muss.
- Eine Datei kann auch mit einem **HFS-Erzeugercode (Creator Code)** versehen sein. Erzeugercodes waren dafür vorgesehen, schnell zu bestimmen, welches Programm der Benutzer zum Öffnen eines gegebenen Dokumentes bevorzugt. Erzeugercodes hatten eine höhere Priorität als Typcodes. Sie konnten dazu verwendet werden, die Verbindung zwischen dem Dateityp und dem damit verknüpften Standardprogramm zum Öffnen von Dokumenten dieses Typs zu überschreiben, so dass eine feste Bindung zwischen einem bestimmten Dokument und einem Programm hergestellt wurde. Heutzutage sind Erzeugercodes ein Ding der Vergangenheit. TinkerTool System kann Erzeugercodes immer noch anzeigen oder ändern, aber sie werden in macOS nicht mehr verwendet.
- Dateien oder Ordner können mit einer **Sichtbarkeitsmarkierung** versehen sein: Wenn ein Objekt als unsichtbar markiert ist, werden der Finder und alle Dialogfenster **Öffnen** dieses Objekt nicht mehr anzeigen. Sie können sich auf das Objekt nur noch über dessen volle UNIX-Pfadangabe beziehen oder über ein Programm, welches das Sichtbarkeitsattribut nicht beachtet. Unsichtbare Objekte werden auch als **versteckt** bezeichnet.

Obwohl wir die Typ- und Erzeugercodes als HFS-Codes bezeichnen, sind sie nicht auf die Dateisysteme HFS und HFS+ beschränkt. macOS kann diese Attribute auf fast jedem Dateisystem emulieren.

Um diese Attribute höherer Systemebene zu ändern, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Attribute** auf der Einstellungskarte **Ablage**.

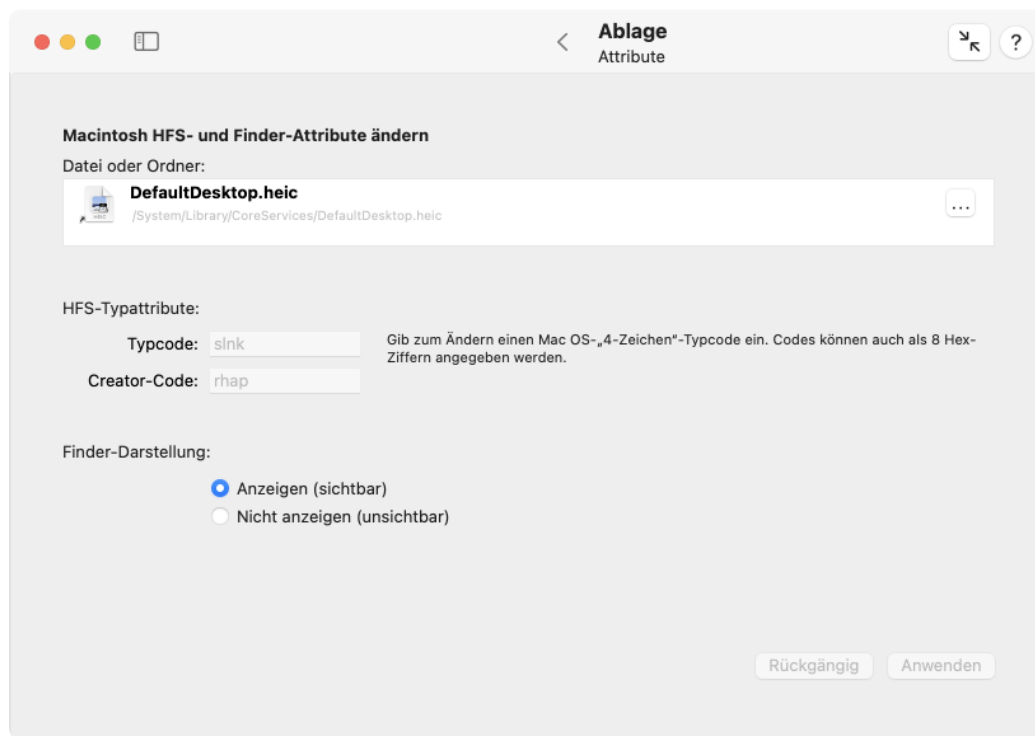


Abbildung 3.3: Attribute

2. Ziehen Sie eine Datei oder einen Ordner aus dem Finder in das Feld **Datei oder Ordner**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Ändern Sie die Attribute, indem Sie neue Werte in die Code-Felder eingeben oder einen der Knöpfe **Finder-Darstellung** betätigen.
4. Drücken Sie den Knopf **Anwenden**, um die neuen Attribute zu setzen. Sie können auch den Knopf **Rückgängig** drücken, um Ihre Änderungen zu verwerfen und die aktuellen Attribute des ausgewählten Objektes wieder neu einlesen zu lassen.

Typcodes und Erzeugercodes müssen entweder durch vier Zeichen aus dem Zeichenvorrat ASCII eingegeben werden, oder über vier beliebige Bytes, die über acht Hexadezimalziffern (die Ziffern 0 bis 9 und die Buchstaben a, b, c, d, e, f oder A, B, C, D, E, F) angegeben werden müssen. Das Programm erkennt automatisch an der Länge Ihrer Eingabe, was Sie meinen. Bitte beachten Sie, dass bei Codes, die per ASCII eingegeben werden, Groß- und Kleinschreibung eine Rolle spielt. Beispiele für gültige Codes sind:

- PREF
- ilge
- 8BPS
- A4B7C1D1

Um einen Typ- oder Erzeugercode von einer Datei zu entfernen, löschen Sie den Eintrag im entsprechenden Code-Feld vollständig und drücken Sie **Anwenden**. TinkerTool System

kann Ihnen nicht dabei helfen, Typ- oder Erzeugercodes von bekannten Dokumenten oder bekannten Programmen auszuwählen. Sie müssen die richtigen Codes im Vorhinein wissen.

Auch wenn es technisch möglich ist, HFS-Typattribute für Ordner zu speichern, war die Bedeutung hiervon im klassischen Mac OS undefiniert und Apple hat dies nie offiziell unterstützt. Aus diesem Grund lässt es TinkerTool System ebenso nicht zu, diese Attribute an Ordner zu knüpfen.

Bitte beachten Sie, dass Sie kein Ziehen-und-Ablegen oder Dateidialoge mehr für Objekte verwenden können, die unsichtbar sind. Sie müssen den vollen UNIX-Pfad des Objektes angeben, um es von einem Programm aus nutzen zu können. Dies schließt auch TinkerTool System ein. Sie können jedoch im Finder die Tastenkombination  +  +  betätigen, um unsichtbare Objekte einzublenden. Ein nochmaliger Aufruf dieser Tastenkombination im Finder schaltet diese Funktion wieder aus.

3.1.4 Zeitattribute ändern

Zu den vielen Attributen, die bei jeder Datei und jedem Ordner gespeichert sind, gehören auch verschiedene Zeitangaben:

- Zeit der Erstellung
- Zeit der letzten Änderung
- Zeit des letzten Zugriffs
- Zeit der letzten Datensicherung
- Zeit der letzten Statusänderung

Die Zeit der letzten Änderung und des letzten Zugriffs sind Pflichtangaben. Ob auch weitere Zeiten gespeichert sind, hängt vom jeweiligen Dateisystem ab. So ist HFS+ beispielsweise in der Lage, die Zeit der letzten Datensicherung zu speichern, während APFS das nicht kann. Nicht verfügbare Angaben werden von TinkerTool System in abgeblendeter Schrift markiert.

macOS und andere UNIX-Systeme verwenden das Datum **01.01.1970** um anzugeben, dass noch keine gültige Zeitangabe gespeichert wurde.

Es kann verschiedene Gründe geben, die Zeitangaben von Hand anzupassen oder zu korrigieren, beispielsweise wenn eine Datei das digitale Bild einer Kamera enthält, bei der die Uhr falsch eingestellt war. TinkerTool System erlaubt es, die vorhandenen Zeitangaben mit anderen Werten zu überschreiben.

Die Zeit der letzten Statusänderung nimmt im Betriebssystem eine Sonderrolle ein und wird von Programmen wie dem Finder üblicherweise auch nicht angezeigt. Diese Zeitangabe wird unter anderem dazu verwendet, die interne Verwaltung des Dateisystems zu steuern und lässt sich *nicht* ändern, um Fehler im System zu vermeiden.

Um eine oder mehrere Zeitattribute eines Objekts zu ändern, führen Sie folgende Schritte durch:

1. Öffnen Sie den Unterpunkt **Zeiten** auf der Einstellungskarte **Ablage**.

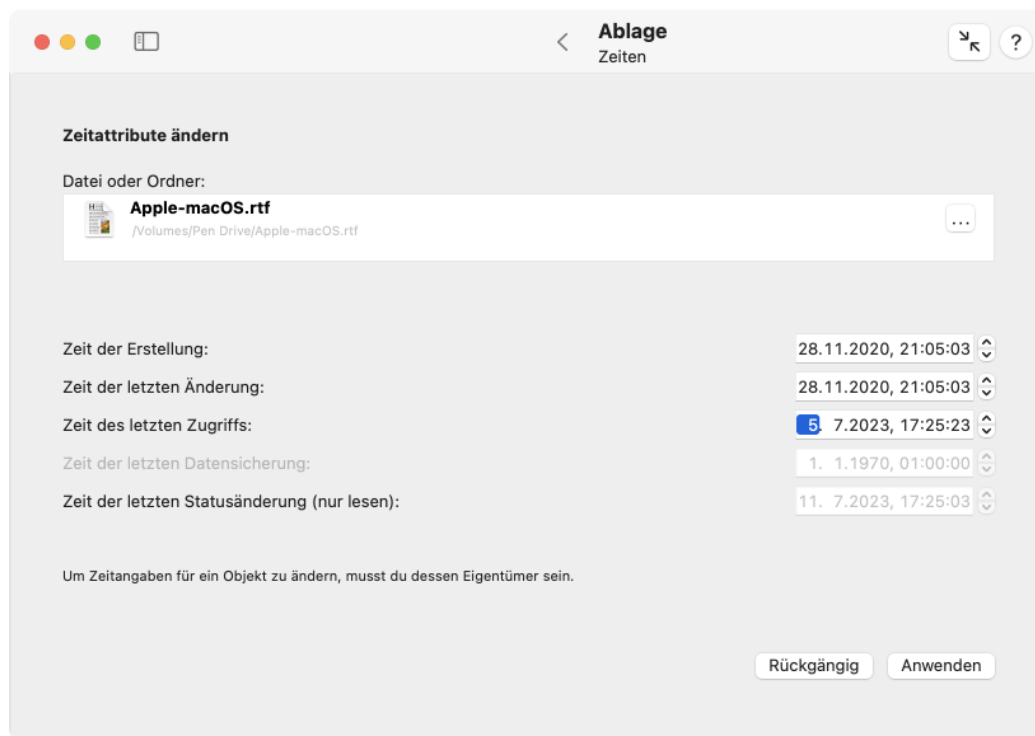


Abbildung 3.4: Gespeicherte Zeitangaben eines Objektes lassen sich ändern

2. Ziehen Sie eine Datei oder einen Ordner aus dem Finder in das Feld **Datei oder Ordner**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Ändern Sie die Zeitangaben wie gewünscht, indem Sie neue Werte in die Felder eingeben, bzw. deren Pfeiltasten anklicken.
4. Klicken Sie auf **Anwenden**.

Sie können jederzeit den Knopf **Rückgängig** verwenden, um wieder zu den Werten zurückzukehren, die im Moment abgespeichert sind.

Durch Aktivitäten des Betriebssystems kann sich der Wert für **Zeit des letzten Zugriffs** unerwartet wieder ändern, nachdem TinkerTool System ihn gespeichert hat. Dies liegt hauptsächlich an der Funktionsweise der Vorschaufunktionen des Finders und lässt sich nicht verhindern.

Der Finder zeigt auch eine Zeit für **Zuletzt geöffnet** an. Hierbei handelt es sich nicht um ein Attribut, das tatsächlich im Dateisystem abgespeichert ist, sondern um einen Wert, der von Spotlight berechnet wird. Er ist deshalb in der Liste der Zeitangaben nicht enthalten.

3.1.5 Quarantäne

Ein wichtiger Teil der in macOS eingebauten Sicherheitsinfrastruktur liegt darin, möglicherweise gefährliche Dateien, die aus nicht vertrauensvollen Quellen stammen oder die

über unsichere Datenkanäle wie das Internet übertragen wurden, nachzuverfolgen. Wenn Sie eine solche Datei oder ein Programm öffnen, erhalten Sie eine Warnmeldung, die nach einer Rückbestätigung fragt, ob Sie der Datei tatsächlich vertrauen. Die Quelle der Datei und die Zeitangabe, wann diese auf Ihren Computer geladen wurde, sind in der Meldung angegeben.

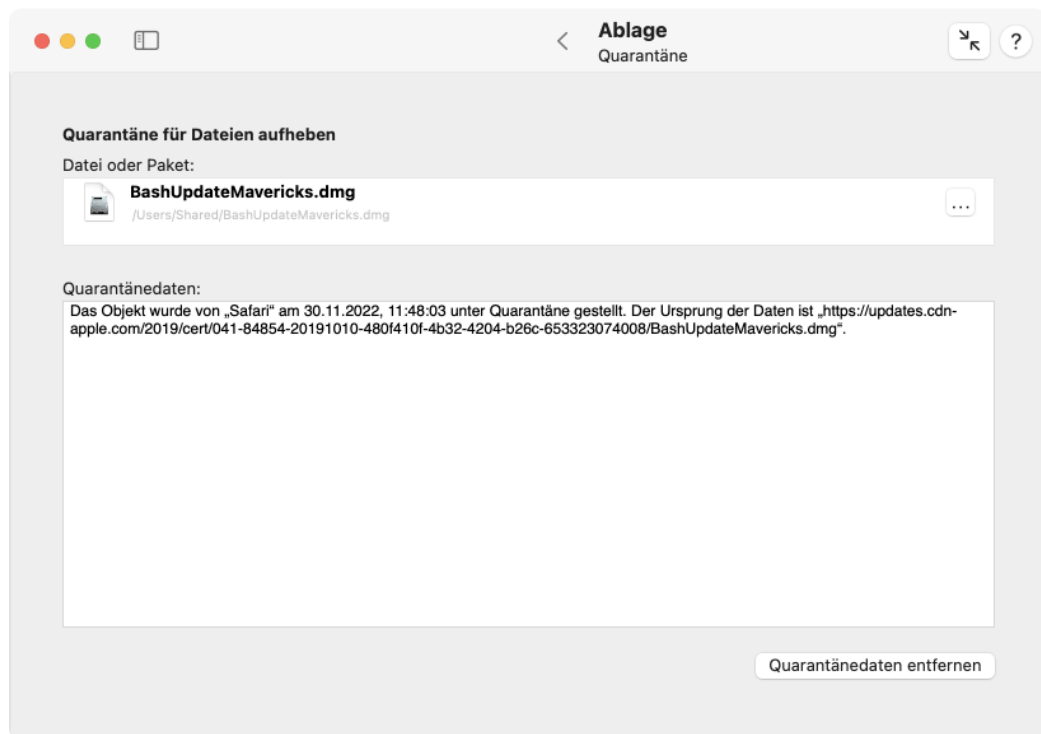


Abbildung 3.5: Quarantäne

Dieses Feature wird technisch realisiert, in dem spezielle Quarantäne-Attribute an die Datei angefügt werden. TinkerTool System kann diese Daten anzeigen und Ihnen die Möglichkeit geben, das entsprechende Attribut zu entfernen und damit die Dateien aus der Quarantäne zu nehmen. Dies kann hilfreich sein, wenn Sie wissen, dass die Datei aus einer vertrauensvollen Quelle stammt und Sie die Datei in Ihrer eigenen Umgebung „öffentlich“ machen, z.B. bevor Sie diese in den Ordner **Benutzer:innen > Geteilt (/Users/Shared)** auf Ihrer Platte speichern oder sie auf Ihrem lokalen Dateiserver ablegen. Auf diese Weise können Sie vermeiden, dass andere Benutzer mit der Warnmeldung konfrontiert werden. Diese sind möglicherweise nicht in der Lage, erfolgreich zu bestätigen, dass sie den Dateien vertrauen, da sie eventuell nicht die notwendige Schreibberechtigung für den gemeinsam genutzten Ordner haben.

Das Entfernen der Quarantänedaten aus einem Programm schaltet auch die Sicherheitsfunktion „Gatekeeper“ für dieses Programm ab. macOS erkennt nicht mehr, dass das Programm aus dem Internet heruntergeladen wurde, so dass dessen Dateien irrelevant für Gatekeeper werden.

Um die Quarantänedaten von einem einzelnen Objekt zu entfernen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Quarantäne** auf der Einstellungskarte **Ablage**.

2. Ziehen Sie eine Datei oder ein Paket aus dem Finder in das Feld **Datei oder Paket**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Prüfen Sie den aktuellen Status, der im Feld **Quarantänedaten** angegeben wird.
4. Drücken Sie den Knopf **Quarantänedaten entfernen**.

3.1.6 Inhalt

Sie erhalten manchmal möglicherweise Dateien unbekannten Ursprungs oder mit unbekanntem Dokumententyp. In anderen Fällen haben Dateien möglicherweise ungültige Typmarkierungen oder Dateinamenserweiterungen, z.B. eine Datei, die vom Finder als PNG-Bild angezeigt wird, obwohl die Datei eigentlich ein JPEG-Bild enthält. Um herauszufinden, was tatsächlich in einer Datei enthalten ist, können Sie macOS in die Datei hineinschauen lassen, um zu analysieren, was deren Inhalt sein könnte. Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Inhalt** auf der Einstellungskarte **Ablage**.
2. Ziehen Sie eine Datei aus dem Finder in das Feld **Zu analysierende Datei**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Das Ergebnis der Analyse wird im Feld **Ergebnis (in englischer Sprache)** angezeigt.

Die Analyse wird vom zugrundeliegenden Betriebssystem durchgeführt, nicht von TinkerTool System. Aus diesem Grund können die Ergebnisse in verschiedenen Betriebssystemversionen leicht voneinander abweichen. Der Bericht wird grundsätzlich auf Englisch angezeigt, egal welche Sprache Sie in Ihren persönlichen Voreinstellungen ausgewählt haben.

Sie können nur eine Datei gleichzeitig auswählen. Es ist nicht möglich, Programme oder andere Pakete zu analysieren. Diese werden einfach als **Directory** dargestellt, dem technischen Fachbegriff für einen Ordner. Diese Analyse ist richtig, da Pakete in der Tat Ordner darstellen, die eine große Menge von unterschiedlichen Dateien beinhalten können, auch wenn der Finder diese als ein einzelnes Dateisymbol darstellt. Um eine der Dateien in einem Paket auszuwählen, wählen Sie dieses im Finder aus und verwenden Sie dann die Finder-Funktion **Paketinhalt zeigen**, um das Paket als Ordner darzustellen. Ziehen Sie dann eine der enthaltenen Dateien in das Feld von TinkerTool System.

In manchen Fällen kann es auch hilfreich sein, zu wissen, welche Metadaten die Spotlight-Suchmaschine über ein bestimmtes Objekt gespeichert hat. Um zusätzlich die Spotlight-Daten anzuzeigen, drücken Sie den Knopf **Auch Spotlight-Metadaten zeigen** unterhalb des Felds **Ergebnis**. Eine Tabelle wird erscheinen, die die vollständige Liste aller Spotlight-Attribute für das ausgewählte Objekt enthält.

3.1.7 Aliasobjekte analysieren

Im Jahr 1991 führte Apple im damaligen Betriebssystem Mac OS 7 ein neues Dateisystemobjekt ein, den *Alias*. Über den Menüpunkt **Alias erzeugen** kann man einen Verweis auf eine bereits bestehende Datei oder einen Ordner anlegen und somit ein und dasselbe Objekt über verschiedene Namen, bzw. an verschiedenen Orten ansprechen, ohne dass es

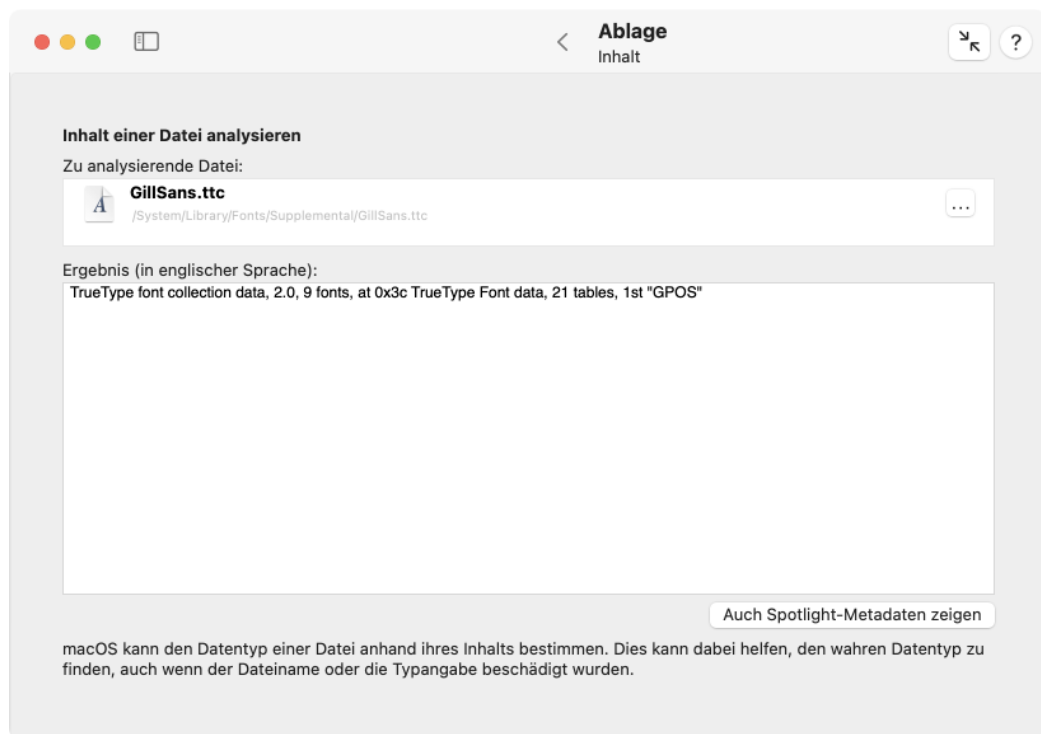


Abbildung 3.6: Inhalt

doppelt gespeichert werden muss. In anderen Betriebssystemen werden Aliase auch als Verknüpfung bezeichnet.

Aliase gibt es auch im heutigen macOS noch. Sie werden jedoch technisch anders realisiert, da die ursprüngliche Art, Aliase zu speichern, nach heutigen Maßstäben zu unsicher ist und gewisse Nachteile aufweist. Da die Basis des Betriebssystems auf das professionelle UNIX umgestellt wurde, sind außerdem weitere Arten von alias-ähnlichen Objekten hinzugekommen, da es in UNIX Dateiverweise schon sehr viel länger gab. Alle diese verschiedenen Arten, Dateien zu verknüpfen werden vom Finder der Einfachheit halber als Alias dargestellt, obwohl oft Detailunterschiede in den Eigenschaften und Fähigkeiten dieser Verweise bestehen. Mit TinkerTool System können Sie bestimmen, um welche Art von Verweis es sich bei einem Alias handelt. Außerdem lässt sich prüfen, auf welches Zielobjekt der Alias verweist und wieviel Speicherplatz er benötigt.

macOS verwendet im Moment die folgenden Arten von Aliasobjekten:

- **Klassischer Mac OS Alias:** Dies war der ursprüngliche Dateityp, um Aliase zu speichern. Es handelte sich um eine spezielle Beschreibungsdatei, in der eine Art Suchvorgabe für das Zielobjekt gespeichert war. Neben Name und Ablageordner waren auch Dinge wie ungefähre Dateigröße und Dateien in der Umgebung angegeben. Wenn ein Programm ein Alias-Objekt öffnen wollte, musste es selbst spezielle Schritte unternehmen, nämlich das Objekt an den *Mac OS Alias Manager* zur Auswertung weitergeben. Dieser hat eine Art Suchanfrage an das Betriebssystem geschickt, die Originaldatei anhand der vorhandenen Beschreibungsdaten wiederzufinden. Auf diese Weise blieb ein Alias oft auch noch dann funktionsfähig, selbst wenn die Originaldatei umbenannt oder verschoben wurde. Dies war recht komfortabel, hatte aber den Nachteil, dass jedes Programm aktiv das Arbeiten mit Aliasen unterstützen musste. Nach heutigen Maßstäben ist außerdem die Idee, das Original im Zweifels-

Beschreibung	Daten
Angabe, ob das Dateisuffix ausgeblendet ist	Nein
Angabe, ob die Datei sichtbar ist	Nein
Anzahl an Dateien und Ordnern innerhalb des Ordners	1254028
Art des Objekts	TrueType®-Schriftsammlung
Baum der uniformen Typbezeichner	public.truetype-collection-font, public.truetype-font, public.font, public.data,...
Benutzer-ID von Dateieigentümer:in	0
Datum von Interesse (nur für Sortierung)	07.05.2024, 02:00:00
Datum, an dem das Objekt zuletzt bewegt wurde	07.05.2024, 09:01:44
Datum, an dem der Dateinhalt zuletzt geändert wurde	07.05.2024, 09:01:44
Datum, an dem der Inhalt dieses Objekts erstellt wurde	13.05.2024, 21:01:05
Datum, an dem der Inhalt dieses Objekts erstellt wurde (nur für Sortierung)	13.05.2024, 02:00:00
Datum, an dem der Inhalt dieses Objekts geändert wurde	07.05.2024, 09:01:44
Datum, an dem die Datei erstellt wurde	07.05.2024, 09:01:44
Dokumenten-Identifikation	0
FOND-Name	GillSans, GillSans-Bold, GillSans-BoldItalic, GillSans-Italic, GillSans-Light, Gil...
Finder-Attribute	0
Finder-Etikett, das der Datei zugeordnet ist	0
Gruppen-ID von Dateieigentümer:in	0
Hat die Datei ein eigenes Symbol?	Nein
In diesem Objekt verwendete Schriften	Bold, Bold Italic, Gill Sans, Gill Sans Bold, Gill Sans Bold Italic, Gill Sans Italic,...
Informationen zum Copyright für dieses Objekt	Copyright © 2012 The Monotype Corporation. All rights reserved. This font s...
Ist die Datei ein Formularblock?	Nein
Logische Größe der Datei auf der Festplatte in Byte	1254028
Logische Größe des Objekts in Byte	1254028
Lokalisiert angezeigter Name der Datei	GillSans.ttc
Mac OS Creator-Code	0
Mac OS Typcode	0
Name der Datei	GillSans.ttc
Name der Schriftfamilie	Gill Sans
Name des Schriftstils	Bold, Bold Italic, Italic, Light, Light Italic, Regular, SemiBold, SemiBold Italic,...
Personen, die dieses Objekt erstellt haben	Eric Gill
Physische Größe des Objekts in Byte	684032
PostScript-Name	GillSans, GillSans-Bold, GillSans-BoldItalic, GillSans-Italic, GillSans-Light, Gil...
Präsentierter Dateiname mit Suffix	GillSans.ttc
Uniformer Typbezeichner	public.truetype-collection-font
Veröffentlicher des Dokuments	Monotype Imaging Inc.
Versionsnummer dieses Objekts	16.0d1e1
Voller Schriftname	Gill Sans, Gill Sans Bold, Gill Sans Bold Italic, Gill Sans Italic, Gill Sans Light,...
com_apple_ats_names	16.0d1e1, Bold, Bold Italic, Copyright © 2012 The Monotype Corporation. All r...

Spotlight hat die aufgeführten Daten für diese Datei gespeichert.

OK

Abbildung 3.7: Auch die Liste der Spotlight-Metadaten, die macOS über diese Datei führt, kann angezeigt werden

fall durch einen Suchvorgang wiederzufinden, zu gefährlich: Ein Angreifer könnte eine Originaldatei durch eine Fälschung ersetzen, die dem Original so ähnlich ist, dass der Alias Manager das manipulierte Exemplar statt das Original als Ziel des Alias ansieht. Dadurch könnte der Benutzer veranlasst werden, mit seinen Rechten eine Datei zu öffnen, die Schadfunktionen auslöst. Moderne Versionen von macOS legen solche klassischen Aliase nicht mehr an. Aus Kompatibilitätsgründen können diese Aliase aber immer noch geöffnet werden. Sie unterliegen jedoch dann speziellen Sicherheitseinschränkungen.

- **macOS-Bookmark:** Wenn Sie einen Alias über den Finder anlegen, speichern aktuelle Versionen von macOS den Alias als eine *macOS-Bookmark-Datei*. Diese verhält sich ähnlich wie ein Lesezeichen in einem Web-Browser und speichert das Ziel über eine dateibezogene URL („Internet-Adresse“), die zusätzlich mit Sicherheitsinformationen geschützt sein kann. Wenn Sie das Originalobjekt an einen anderen Ort verschieben, wird der Verweis aus Sicherheitsgründen absichtlich ungültig und der Alias kann nicht mehr aufgelöst werden. Beim Arbeiten mit Dateien und Ordnern über die üblichen Öffnen-Dialogfenster von macOS wird das Auswerten von Bookmarks vollautomatisch von den höheren Ebenen von macOS unterstützt, so dass Programme sich darum nicht kümmern müssen.
- **absoluter symbolischer Link:** auf der UNIX-Ebene von macOS können Verweise noch einfacher realisiert sein: Man speichert den absoluten Dateipfad des Ziels in einer Textdatei und fügt eine Markierung an, dass es sich um einen Verweis, in diesem Fall einen *symbolischen Link* handelt. Das Arbeiten und Anlegen von symbolischen Links wurde bereits im ersten Abschnitt dieses Kapitels beschrieben. Auch hier wird der Link gewollt ungültig, wenn das Originalobjekt umbenannt oder verschoben wird. Symbolische Links werden vom Betriebssystem vollautomatisch aufgelöst, ohne dass das öffnende Programm das „wissen“ muss. Nur wenn ein Programm aktiv angibt, dass es Fälle, in denen ein symbolischer Link vorliegt, ausdrücklich *nicht* ausgewertet haben will, kann es einen symbolischen Link als solchen erkennen.
- **relativer symbolischer Link:** dies ist eine spezielle Variante eines symbolischen Links, bei dem der Dateipfad nicht als absolute Ortsangabe, sondern relativ zum Ort des Alias gespeichert wird (z.B. als „einen Ordner höher gehen, dann im Unterordner X das Objekt Y“). In diesem Fall kann eine ganze Unterordnerhierarchie an einen neuen Ort verschoben werden und der Link bleibt trotzdem gültig.

Führen Sie die folgenden Schritte durch, um den tatsächlichen Typ eines Objekts zu bestimmen, das vom Finder als Alias dargestellt wird:

1. Öffnen Sie den Unterpunkt **Alias** auf der Einstellungskarte **Ablage**.
2. Ziehen Sie einen Alias in das Feld **Zu analysierender Alias**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.

Die Auswertung wird in der Box **Ergebnis** dargestellt. Über das Lupensymbol können Sie das Originalobjekt im Finder anzeigen lassen.

3.1.8 Zwangslöschung

Schlecht geschriebene Programme oder Installationsprogramme, die Berechtigungen nicht sauber beachten, hinterlassen oft Dateien oder Ordner auf Ihrem System, die nicht einfach

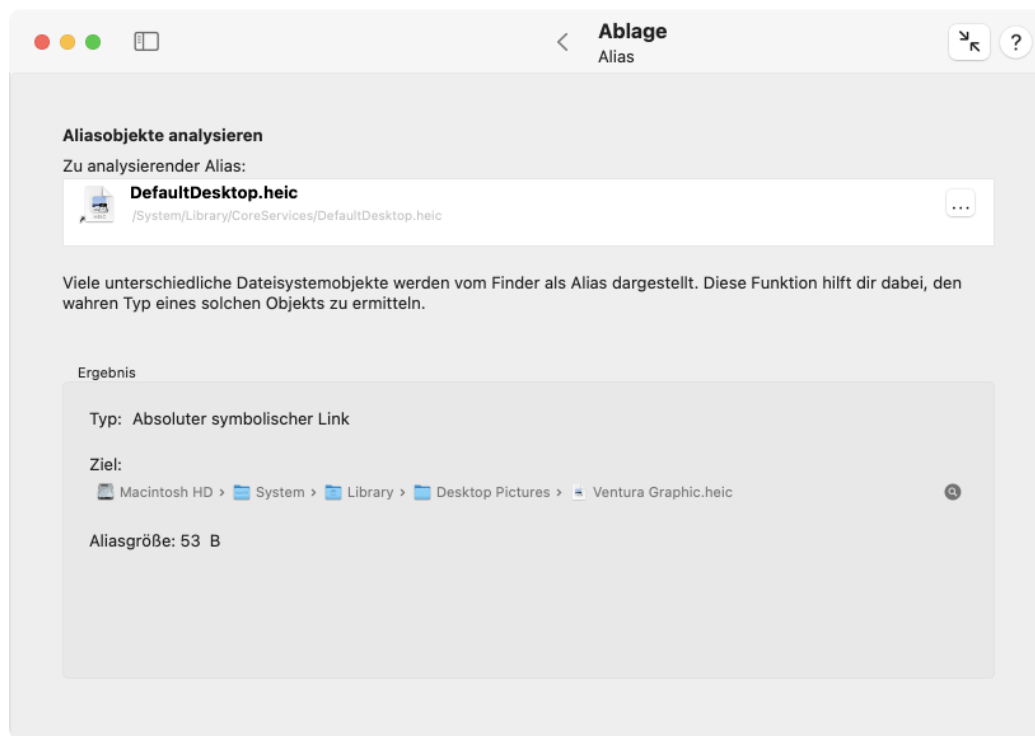


Abbildung 3.8: Der Finder verwendet für verschiedene Arten von Objekten den Oberbegriff Alias

in den Papierkorb geworfen werden können. In anderen Fällen legen Programme möglicherweise eine große Zahl von Dateien mit Schreibschutz an, die ebenso nicht einfach entfernt werden können. Falls Sie die Entfernung einer großen Menge von geschützten Dateien erzwingen möchten, oder falls Sie eine Datei oder einen Ordner mit unpassenden Berechtigungseinstellungen entfernen möchten, können Sie dies mit der Funktion **Zwangslöschung** durchführen:

1. Öffnen Sie den Unterpunkt **Zwangslöschung** auf der Einstellungskarte **Ablage**.
2. Ziehen Sie eine Datei oder einen Ordner in das Feld **Zu entfernende Datei oder Ordner**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Falls Sie einen Ordner zur Löschung ausgewählt haben und dieser Ordner enthält Objekte, müssen Sie zusätzlich bestätigen, dass der Ordner zusammen mit den enthaltenen Objekten gelöscht werden soll. Kreuzen Sie in diesem Fall den Punkt **Löschung nicht-leerer Ordner erlauben** an.
4. Drücken Sie den Knopf **Löschen**.

3.1.9 Verschachtelung

Grenzwerte des lokalen Betriebssystems

Moderne Betriebssysteme und Dateisysteme haben keine Einschränkungen, wie tief Ordner verschachtelt werden können. Es gibt jedoch ein technisches Limit bei den Pfaden,

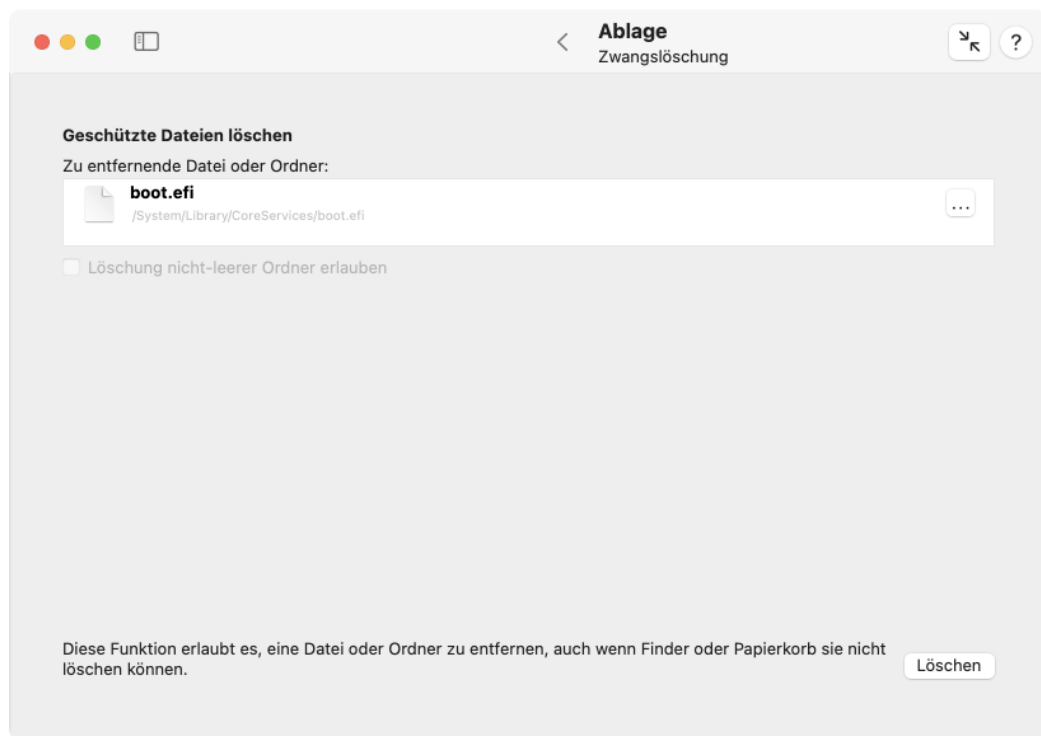


Abbildung 3.9: Zwangslöschung

die benutzt werden, um sich auf diese Ordner oder auf die Dateien, die sie enthalten, zu beziehen. In Übereinstimmung mit dem POSIX-Industriestandard muss ein Betriebssystem Dateizugriffspfade ab einer bestimmten Länge nicht mehr unterstützen, wenn auf ein Dateisystemobjekt in einem Programm, einem Befehl oder irgendeiner Funktion, die mit Dateinamen arbeitet, verwiesen wird.

In der Praxis bedeutet das, dass der Zugriff auf eine Datei in einer Hierarchie sehr tief verschachtelter Ordner mit langen Namen einfach fehlschlagen kann, wenn das Betriebssystem den *absoluten Pfad* dieser Datei nicht akzeptiert, weil er zu lang ist. Objekte in solchen Ordnern können auf der grafischen Oberfläche unsichtbar werden, z.B. im Finder oder in Dialogfenstern zum Öffnen/Sichern, da das System deren überlange Pfade nicht mehr verarbeiten kann.

Beachten Sie, dass Pfade von der Umgebung und der gegenwärtigen Situation abhängen. Wenn sich eine Datei auf Ihrem System-Volumen mit dem Namen „Macintosh HD“ befindet, kann diese einen absoluten Zugriffspfad wie

```
/Users/MeinName/Documents/Ein/Verschachteltes/Ordner/Beispiel/Dokument.txt
```

haben. Falls diese Platte nun als externes Laufwerk von einem anderen Mac aktiviert wird, kann genau die gleiche Datei nun unter dem Pfad

```
/Volumes/Macintosh HD/Users/MeinName/Documents/Ein/Verschachteltes/Ordner/Beispiel/Dokument.txt
```

angesprochen werden, so dass sich die Länge des Pfades um den Teil vergrößert hat, der für „/Volumes/Macintosh HD“ benötigt wird, was der andere Mac nutzt, um sich auf die externe Platte zu beziehen. Pfade für identische Objekte können sich also unterscheiden, je nach dem, wie mehrere Platten miteinander kombiniert werden, um die gesamte Dateisystemhierarchie des laufenden Computers aufzubauen. In Firmennetzwerken können

Objekte auf Datei-Servern in beliebigen Ordnern eingeblendet werden, die der Netzadministrator zu diesem Zweck auf den Klienten-Computern vorgesehen hat. In diesem Fall werden die Pfade zur Laufzeit auch einfach aneinandergehängt. Sie sind nirgendwo gespeichert.

Solche tiefen Ordnerhierarchien mit überlangen Zugriffsnamen können angelegt werden, indem man *relative* Pfade verwendet. Wir wollen an dieser Stelle nicht tiefer ins Detail gehen, aber das Betriebssystem unterstützt alternativ den Begriff des *aktuellen Arbeitsordners*. Sie können das System anweisen, in den Ordner bei

/Users/MeinName

zu „gehen“, dann in den Unterordner **Ein** zu navigieren, dort in dessen Unterordner **Verschachteltes**, und so weiter, wobei nur *relative* „Navigations“-Anweisungen mit kurzen Pfaden gegeben werden, anstatt die gesamte Ortsposition der Datei in eine einzige Pfadangabe zu packen.

Wenn von Pfadlängen die Rede ist, spielt nicht die reine Zahl der Zeichen die entscheidende Rolle, sondern die Speichergröße, die belegt wird, um den Pfad anzugeben. Alle modernen Betriebssysteme verwenden die Kodierung Unicode UTF-8 bei der Verarbeitung von Dateipfaden. Bei diesem Kodierungssystem werden lateinische Schriftzeichen, einschließlich Zeichen mit Akzenten für viele europäische Sprachen üblicherweise mit einem Byte pro Zeichen gespeichert. Zeichen vieler asiatischer Sprachen werden mit zwei Bytes gespeichert. Hochspezialisierte Zeichen wie Emojis benötigen vier oder noch mehr Bytes.

TinkerTool System kann ermitteln, welche Maximalzahl von Bytes die gerade laufende Version von macOS garantiert unterstützt, wenn auf Dateien per Pfad Bezug genommen wird. Es kann auch prüfen, ob alle Dateien in einer Ordnerhierarchie, die bei einem angegebenen obersten Ordner beginnt, im Moment adressiert werden können, ohne dieses Limit zu überschreiten.

- Die Prüfung kann mit jedem Ordner durchgeführt werden, egal ob er sich auf dem System-Volume, auf einer externen Platte oder auf einem Dateiserver befindet.
- Um Probleme mit dem Datenschutz zu vermeiden, wird die Prüfung auf die Dateien und Ordner beschränkt, die Sie öffnen dürfen.
- Die Suche wird automatisch auf das Volume eingeschränkt, auf dem der oberste Ordner liegt. Wenn Sie alle Platten testen möchten, müssen Sie getrennte Prüfungen laufen lassen, indem Sie jedes Mal deren oberste Ordner auswählen.
- Objekte, die als *datenlose Dateien* markiert sind, was sich auf synchronisierte Daten in iCloud oder Cloud-Lösungen anderer Anbieter bezieht, sind von der Verarbeitung automatisch ausgeschlossen. Andernfalls würde macOS automatische Downloads für die betroffenen Dateien auslösen, sobald deren Ordner durchsucht werden.

Sie können eine zusätzliche Wahlmöglichkeit einschalten, nicht nur die Pfade zu testen, so wie sie im Moment sind, sondern auch *mögliche* Pfade zu überprüfen, die entstehen könnten, falls ein Programm versucht, die überprüften Dateien auf ein anderes Volume zu kopieren, unter der Annahme, dass es hierzu absolute Pfade nutzt. Wie wir bereits oben erwähnt hatten, müsste der Pfad des Einblendungspunkts (Mount Point) für das Ziel-Volume zu den bereits vorhandenen Pfaden hinzugefügt werden, falls ein Programm versucht, einen „Klon“ eines Volumes zu erstellen, indem es dessen Inhalt Datei für Datei auf ein anderes kopiert.

Führen Sie die folgenden Schritte durch, um eine Ordnerhierarchie nach überlangen Zugriffspfaden abzusuchen:

1. Öffnen Sie den Unterpunkt **Verschachtelung** auf der Einstellungskarte **Ablage**.



Abbildung 3.10: Suche nach absoluten Pfaden, die für viele Programme zu lang sein könnten

2. Ziehen Sie den Ordner, bei dem der Test starten soll, in das Feld **Oberster Ordner zur Prüfung**. Sie können auch den Knopf [...] drücken, um zum Ordner zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Ordners eingeben.
3. Entscheiden Sie, ob Sie die Pfade der ausgewählten Objekte so überprüfen möchten, wie sie gerade sind, oder ob Sie die Pfade unter der Annahme testen lassen möchten, dass jedes Objekt auf alle gerade angeschlossenen Volumes kopiert werden würde. Im letzteren Fall kreuzen Sie das Feld **Auf theoretische Pfadlängenüberschreitung prüfen falls Objekte auf lokale angeschlossene Volumes geklont wurden** an.
4. Drücken Sie den Knopf **Ausgewählten Ordner prüfen**.

Danach wird die Suche gestartet. Sie kann jederzeit abgebrochen werden, indem Sie den Knopf **Stopp** im Statusfenster klicken. Nachdem alle Prüfungen abgeschlossen sind, wird das Ergebnis in einem weiteren Dialogfenster angezeigt. Falls bei allen Objekten ein problemloser Zugriff zu erwarten ist, wird ein grünes Symbol mit Häkchen angezeigt. Falls ein oder mehrere Probleme gefunden wurden, zeigt das Ergebnisfenster an:

- eine Liste aller Dateien und Ordner, die möglicherweise nicht für alle Programme zugreifbar sind, (bzw. die sich nicht auf ein gerade lokal angeschlossenes Volume kopieren lassen),
- die Anzahl der Bytes, die genutzt wird, um den Pfad jedes potenziell unzugänglichen Objekts zu speichern,
- ein Öffnen-Knopf für jedes Objekt, um zu dem jeweils problematischen Ordner im Finder zu navigieren,

- eine getrennte Tabelle, die alle Ordner auflistet, die aufgrund von Berechtigungsproblemen nicht überprüft werden konnten.

Bei der Verwendung eines Öffnen-Knopfes zeigt der Finder möglicherweise *nicht* das jeweilige Dateisystemobjekt, da er selbst ja auch von dem Pfadproblem betroffen ist, den Ort des Objekts also nicht mehr richtig verarbeiten kann. Stattdessen gibt TinkerTool System dem Finder die Anweisung, den „tiefsten“ Ordner in der Hierarchie zu öffnen, der immer noch sicher dargestellt werden kann.



Obwohl der angezeigte Ordner noch vom Finder verarbeitet werden kann, können einige oder alle Inhalte dieses Ordners im Finder-Fenster bereits unsichtbar sein, da der Finder nicht in der Lage ist, die Namen der Objekte an dieser tiefen Ebene der Hierarchie zu bewältigen. Falls Sie den vermeintlich leeren Ordner löschen, könnten Sie Daten verlieren!

Sie sollten den Ordner an dieser oder einer höheren Ebene umbenennen, so dass er einen kürzeren Namen erhält, um das Problem zu beheben. Alternativ können Sie den Ordner stattdessen auch an eine höhere Position in der Hierarchie bewegen. Es wäre nicht angemessen, dies automatisch durchzuführen, so dass Ihnen TinkerTool System hierbei nicht weiterhilft. Die Neuorganisation der Ordner sollte vom Eigentümer der Dateien durchgeführt werden, der die verschachtelte Hierarchie angelegt hat.

Beliebige Grenzwerte anderer Systeme

In einigen Fällen betrifft die Frage, wie lang der Pfad eines Dateisystemobjekts sein darf, um korrekt verarbeitet werden zu können, nicht das lokale System, sondern die Zusammenarbeit mit anderen Systemen. Beispielsweise haben Sie vielleicht einen Ordner eingerichtet, der automatisch mit einem fernen Ordner im Netz synchronisiert werden soll, aber der Netzwerk-Server verwendet andere Limits für akzeptierte Pfadangaben.

Zusätzlich zu der lokalen Prüfung bietet TinkerTool System einen einfachen Schnelltest, der eine ausgewählte Ordnerhierarchie gegen eine Pfadlängengrenze prüft, die Sie selbst angeben können. Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Verschachtelung** auf der Einstellungskarte **Ablage**.
2. Ziehen Sie den Ordner, bei dem der Test starten soll, in das Feld **Oberster Ordner zur Prüfung**. Sie können auch den Knopf [...] drücken, um zum Ordner zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Ordners eingeben.
3. Drücken Sie auf den Knopf **Lange Pfade suchen**
4. Wählen Sie aus, ob Sie **absolute** Pfade prüfen möchten (wie sie im Moment auf dem Volume des lokalen Computers vorliegen) oder **relative** Pfade (wie vom ausgewählten obersten Ordner aus gesehen) und geben Sie das Limit in Bytes an. Drücken Sie **OK**.

TinkerTool System überprüft nun den Ordner und alle seine Unterordner auf dem gleichen Volume, in denen Sie Leserecht haben, und sammelt alle Dateisystemobjekte in einer Liste, bei denen die angegebenen Pfadlänge überschritten ist. Das Ergebnis wird am Ende des Suchvorgangs angezeigt, wobei die Pfade und deren jeweilige Längen angegeben werden.

Durch Auswählen von Zeilen können Sie den jeweiligen Pfad in voller Länge einblenden lassen und auf Wunsch auch (soweit technisch machbar) im Finder öffnen. Der minimale Grenzwert, den Sie angeben können, liegt bei 200 Bytes, das Maximum entspricht dem lokalen Limit des laufenden Betriebssystems.

3.1.10 Erweiterte Attribute

Viele der bereits in diesem Kapitel genannten Dateiergänzungen wie HFS-Attribute oder Quarantänemarkierungen stellen Zusatzinformationen dar, die zusätzlich zu einer Datei oder einem Ordner gespeichert sein können. Hierzu gehören auch noch einige weitere Elemente wie beispielsweise Finder-Tags, Spotlight-Kommentare, Sicherungsmarkierungen von Time Machine und vieles andere mehr. Alle modernen Versionen von macOS fassen diese Zusatzdaten unter dem Stichwort *Erweiterte Attribute* zusammen. Jedes Erweiterte Attribut trägt einen bestimmten Namen, der von dem Programm frei vergeben werden kann, das dieses Attribut anlegt und verwendet. Mit jedem Namen ist dann eine gewisse Folge von Bytes verknüpft, die den Wert oder Inhalt des Attributs darstellt. Was als Inhalt gespeichert wird, liegt im Ermessen des jeweiligen Programms. Die Anzahl der Erweiterten Attribute, die an ein Dateisystemobjekt geknüpft werden kann, ist theoretisch unbegrenzt. Ältere Versionen von macOS oder dem klassischen Mac OS haben ein ganz ähnliches Konzept genutzt, nämlich sogenannte *benannte Zweige* einer Datei (engl. *named forks*). Hier spielte insbesondere der *Ressourcenzweig* (*resource fork*) eine wichtige Rolle. Der Vorteil von Erweiterten Attributen, bzw. Dateizweigen besteht darin, dass sich die Zusatzdaten *zusammen* mit dem eigentlichen Inhalt der Datei (dem sogenannten *Datenzweig*) unter einem einzelnen Symbol und Dateinamen verwalten und transportieren lassen. Der Nachteil besteht darin, dass nicht alle Dateisysteme (z.B. das FAT-Format von MS-DOS) solche Attribute speichern können. Wenn eine mit vielen Attributen versehene Datei auf eine Platte kopiert wird, die nicht darauf vorbereitet ist, solche Funktionen zu unterstützen, können die zusätzlichen Datenströme einfach verlorengehen. Auch ist es nicht mehr so einfach, die benötigte Speicherplatzgröße einer Datei anzugeben, wie im simplen Fall.

In modernen Versionen von macOS wird der Ressourcenzweig intern als Erweitertes Attribut gespeichert, das den Namen **com.apple.ResourceFork** trägt.

Es kann verschiedene Gründe geben, Erweiterte Attribute von Dateien zu entfernen. Hier zwei Beispiele aus der Praxis:

- Sie haben eine große Menge von Bilddateien erhalten, die ursprünglich mit dem klassischen Mac OS erstellt wurden. Die Dateien enthalten Ressourcenzweige, in denen Dateisymbole gespeichert sind, die jeweils ein Vorschaubild („Thumbnail“) für das jeweilige Bild enthalten. Diese Ressourcen benötigen sehr viel unnötigen Speicherplatz, denn heutige Computer mit Mehrkernprozessoren sind so schnell, dass der Finder die Vorschau direkt aus dem Bildinhalt errechnet, parallel während er die Dateien auflistet. Die im Voraus berechneten Vorschaubilder werden nicht mehr benötigt. In diesem Fall können Sie für den ganzen Ordner voller Bilddateien alle Erweiterten Attribute mit dem Namen **com.apple.ResourceFork** löschen.
- Sie haben in einem Notfall Daten aus einer Time Machine-Datensicherung wiederhergestellt, indem Sie die Dateien über die Befehlszeile direkt von der Time Machine-Platte auf die Systemplatte kopiert haben, ohne den Finder oder die Time Machine-Oberfläche zu verwenden. In dem Fall sind versehentlich die internen Bearbeitungsvermerke, mit denen Time Machine festhält, welche Versionsstände zu welchen Zeitpunkten vorhanden sind, nun auf der Originalplatte gelandet. Um spätere Sicherun-

gen nicht zu behindern, möchten Sie die jeweiligen Attribute der wiederhergestellten Dateien löschen. Hierzu sind alle Erweiterten Attribute zu entfernen, die mit der Bezeichnung **com.apple.TimeMachine** beginnen.

Sie können in TinkerTool System eine Datei oder einen ganzen Ordner voller Dateien angeben und sich dort alle vorkommenden Erweiterten Attribute anzeigen lassen. Sie können danach auswählen, eines oder alle Attribute mit einem bestimmten Namen aus der gesamten Menge der Dateiobjekte zu löschen. Bitte beachten Sie, dass Sie zur Anzeige Lese-recht für die betroffenen Ordner und Erweiterten Attribute benötigen. Zum Löschen wird entsprechend Schreibrecht benötigt.

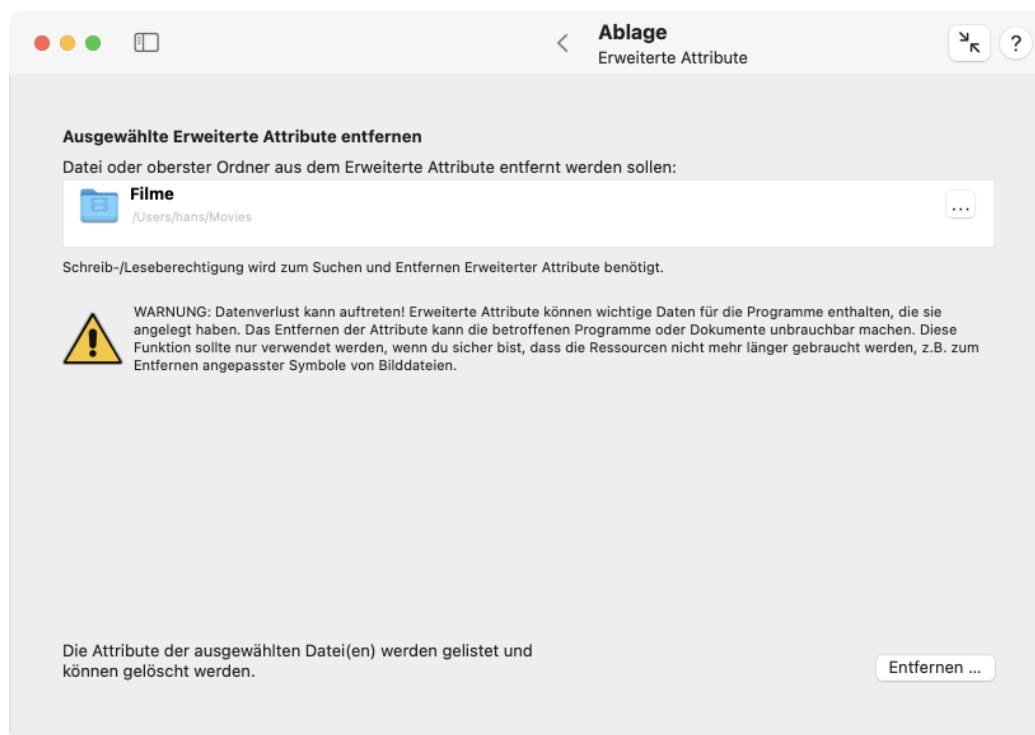


Abbildung 3.11: Erweiterte Attribute entfernen

Führen Sie die folgenden Schritte durch, um Erweiterte Attribute anzuzeigen, bzw. zu löschen:

1. Öffnen Sie den Unterpunkt **Erweiterte Attribute** auf der Einstellungskarte **Ablage**.
2. Ziehen Sie eine Datei oder einen Ordner in das Feld **Datei oder oberster Ordner aus dem Erweiterte Attribute entfernt werden sollen**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Drücken Sie den Knopf **Entfernen ...** um die Erweiterten Attribute der ausgewählten Objekte zu prüfen.

Bevor tatsächlich Attribute gelöscht werden, zeigt TinkerTool System ein herausgleitendes Dialogfenster an, in dem alle vorgefundenen Attribute und die dazugehörigen Dateisystemobjekte aufgelistet werden:

- Der obere Teil des Fensters listet die Namen aller vorkommenden Attribute und die Anzahl der Objekte (Dateien oder Ordner), die mit dem jeweiligen Attribut versehen sind. Durch Löschen oder Setzen eines Häkchens bei **Entfernen?** können Sie bestimmen, ob das Attribut gelöscht werden soll.
- Wählen Sie in der oberen Hälfte des Fensters ein Attribut aus, so werden in der unteren Hälfte alle Pfade der Objekte angezeigt, die das jeweilige Attribut enthalten. Beachten Sie, dass die ausgewählten Erweiterten Attribute aus *allen* Objekten gelöscht werden, die jeweils aufgelistet sind. Möchten Sie den Vorgang auf einzelne Dateien beschränken, müssen Sie das Objekt einzeln in das Feld **Datei oder oberster Ordner aus dem Erweiterte Attribute entfernt werden sollen** ziehen.

Die Löschung findet statt, sobald Sie den Knopf **Löschen** im Dialogfenster betätigen. Alle Objekte bleiben unberührt, wenn Sie den Knopf **Abbrechen** drücken.



Sie sollten diese Funktion nur dann verwenden, wenn Sie genau wissen, was Sie tun, insbesondere welche Attribute zu welchem Zweck gebraucht werden. Möglicherweise können bestimmte Dokumente nicht mehr geöffnet werden, wenn deren Attribute entfernt wurden.

3.2 Die Einstellungskarte Bereinigen

3.2.1 Allgemeine Hinweise zum Löschen von Dateien

Die Einstellungskarte **Bereinigen** ist dazu gedacht, Dateien von Ihrem Computer zu entfernen, die möglicherweise nicht mehr länger gebraucht werden. Beachten Sie, dass TinkerTool System Sie nicht von der Entscheidung entbinden kann, ob gewisse Dateien in der Tat noch gebraucht werden oder doch besser behalten werden sollten. Um zu verhindern, dass das Programm Dateien ohne Ihre ausdrückliche Erlaubnis bereinigt, wird empfohlen, die Wahlmöglichkeit **Vor jeglicher Löschung Analyse anzeigen**, die jeweils am unteren Rand jedes Unterpunktes angeboten wird, in der eingeschalteten Einstellung zu belassen. Dieser Punkt ist standardmäßig eingeschaltet, wenn Sie die Einstellung **Vor jedem Löschvorgang immer Bericht erstellen** im Einstellungsfenster des Programms (Abschnitt 1.3 auf Seite 8) angekreuzt haben.

Ist diese Funktion eingeschaltet, zeigt TinkerTool System immer einen Bestätigungsdialog mit einer Liste aller Dateien und Ordner, die zur Löschung vorgesehen sind, an, bevor der eigentliche Löschvorgang stattfinden wird. Sie haben damit eine letzte Chance, die Liste der Daten durchzugehen. Durch Abwählen bestimmter Dateien aus der Liste können Sie diese auch einzeln vom Löschvorgang ausnehmen. Jeder Eintrag hat außerdem einen „Im-Finder-zeigen“-Knopf, der angeklickt werden kann, um den betroffenen Ordner mit Darstellung des jeweiligen Objekts in einem Finder-Fenster zu öffnen.

3.2.2 Versteckte Hilfsdateien

macOS verwendet mehrere Typen versteckter Unterstützungsdateien, um bestimmte Aufgaben zu erfüllen. Wenn Sie einen Datenträger an Benutzer von Betriebssystemen weiterleiten, auf denen diese versteckten Daten sichtbar werden könnten, z.B. wenn Sie eine Dateien auf einem gemeinsam benutzten Server hochladen, oder wenn Sie mit externen

Laufwerken zum Datentransport arbeiten, könnten diese Dateien Verwirrung auslösen oder als störend empfunden werden. Einige versteckte Dateien enthalten wichtige Informationen, während andere auf fremden Systemen nutzlos sein können. TinkerTool System unterstützt die Entfernung zweier bestimmter Arten von versteckten Dateien:

- **Desktop Services Store-Dateien:** Diese Dateien tragen immer den Namen **.DS_Store**. Der Finder legt eine **.DS_Store**-Datei in jedem Ordner an, der jemals mit dem Finder geöffnet wurde, unter der Bedingung, dass der jeweilige Benutzer Schreibrecht für den in Frage kommenden Ordner hatte. Eine **.DS_Store**-Datei enthält alle Darstellungseinstellungen, die der Finder verwendet hat, als er den Ordner, der die Datei enthält, zum letzten Mal geöffnet hat. Zu den Darstellungseinstellungen gehört die Größe des Anzeigefensters des Finders, dessen Darstellungsart (Symbol, Liste, Spalten oder Galerie), die Position der Symbole, die Sortiereinstellungen, Hintergrundbilder und vieles Andere mehr. Die Ansichtseinstellungen des Finders werden entweder indirekt bestimmt, durch das Öffnen eines neuen Standardfensters, das gewisse Ansichtseinstellungen hat, oder ausdrücklich, über den Menüpunkt **Darstellung > Darstellungsoptionen einblenden** im Finder. Wenn eine **.DS_Store**-Datei entfernt wird, wird deren Ordner auf Standardeinstellungen für die Darstellung zurückfallen. Eine neue **.DS_Store**-Datei wird erstellt, wenn der Ordner mit dem Finder das nächste Mal geöffnet wird.
- **AppleDouble-Dateien:** Diese Dateien werden auch „Punkt-Unterstrich-Dateien“ genannt, denn Sie tragen immer Dateinamen, die mit „_“ beginnen. Der macOS-Systemkern legt diese Dateien automatisch an, wenn es notwendig ist, gewisse Mac-spezifische Attribute auf Dateisystemen zu speichern, die solche Attribute nicht von Hause aus speichern können. Beispiele für diese Zusatzattribute sind Typcodes, die Sichtbarkeitsmarkierungen, Quarantänedaten oder Ressourcenzweige, die bereits im Kapitel Die Einstellungskarte Ablage (Abschnitt 3 auf Seite 145) erwähnt wurden. Solche Dateien werden nur dann angelegt, wenn es notwendig ist, diese Attribute auf einem fremden Dateisystem zu emulieren, z.B. wenn ein klassisches Mac-Programm auf einer MS-DOS-Diskette gespeichert wird. Aus diesem Grund werden Sie solche Dateien selten auf HFS-Platten finden. Sie können nichtsdestotrotz auf solchen Platten vorhanden sein, z.B. nachdem eine Dokumentendatei mit emulierten Attributen über ein anderes Betriebssystem als macOS auf eine HFS-Platte zurückkopiert wurde. Die Verbindung zwischen Hauptdatei und der damit zusammenhängenden AppleDouble-Datei wird über Dateinamen hergestellt, die einem einfachen Namensmuster folgen: Wird eine AppleDouble-Datei angelegt, um die Mac-Besonderheiten einer Datei „Beispiel“ zu speichern, so wird macOS dafür den Namen „_Beispiel“ verwenden.

TinkerTool System kann im Vorhinein nicht verhindern, dass solche Dateien angelegt werden (Dies würde ansonsten dazu führen, dass der Finder keine Darstellungseinstellungen mehr speichern könnte und würde bei AppleDouble-Dateien zu Datenverlust führen.) Der Finder enthält jedoch eine erweiterte Einstellung „für Profis“, die dazu genutzt werden kann, zumindest die Anlage neuer **.DS_Store**-Dateien zu unterdrücken, wenn der Finder Ordner auf Netzwerk-Fileservern öffnet. Diese Einstellung ist über das Schwesterprogramm TinkerTool zugreifbar.

TinkerTool System kann diese beiden Arten versteckter Dateien entfernen, wobei auch eine ganze Hierarchie von Ordnern bereinigt werden kann, falls gewünscht. Der Benutzer, der die Entfernung anstößt, muss Leseberechtigung für die betroffenen Dateien und Ordner besitzen. Um versteckte Dateien zu löschen, führen Sie die folgenden Schritte durch:

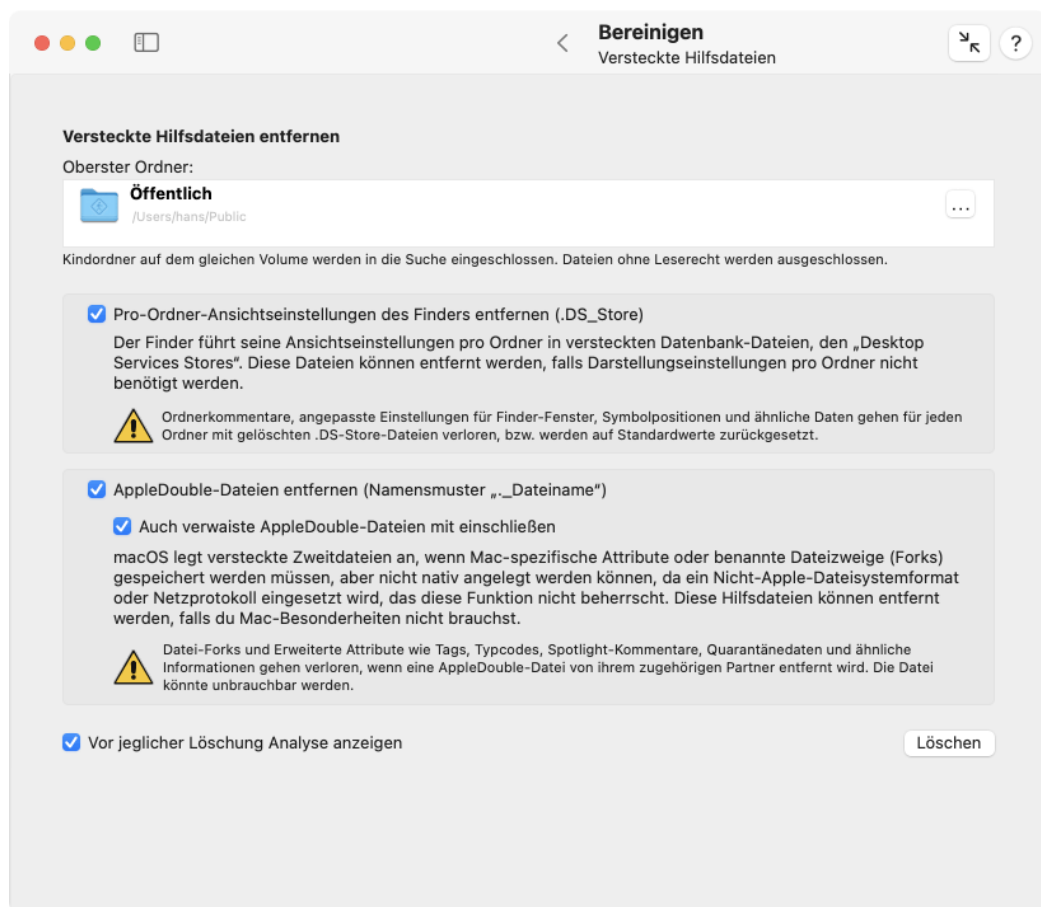


Abbildung 3.12: Versteckte Hilfsdateien

1. Öffnen Sie den Unterpunkt **Versteckte Hilfsdateien** auf der Einstellungskarte **Bereinigen**.
2. Ziehen Sie den obersten Ordner, der bearbeitet werden soll, vom Finder in das Feld Oberster Ordner. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Falls Sie alle Desktop Services Store-Dateien aus diesem Ordner und allen seinen Unterordnern entfernen möchten, kreuzen Sie **Pro-Ordner-Ansichtseinstellungen des Finders entfernen (.DS_Store)** an.
4. Falls Sie alle AppleDouble-Dateien entfernen möchten, die sich auf vorhandene Dateien in diesem Ordner und seinen Unterordnern beziehen, kreuzen Sie die Wahlmöglichkeit **AppleDouble-Dateien entfernen (Hilfsdateien nach dem Namensmuster „_Dateiname“)** an. Falls Sie auch Dateien einschließen möchten, die nur wie AppleDouble-Dateien aussehen, egal, ob es damit zusammenhängende Dateien gibt oder nicht, setzen Sie ein zusätzliches Häkchen bei **Auch verwaiste AppleDouble-Dateien mit einschließen**.
5. Drücken Sie den Knopf **Löschen**.



Entfernen Sie nur dann versteckte Dateien, wenn Sie sicher sind, dass deren Inhalt nicht wichtig ist. Andernfalls könnte ernster Datenverlust auftreten.

3.2.3 Protokollarchive

Wie im Kapitel Die Einstellungskarte Info (Abschnitt 2.10 auf Seite 122) skizziert, verwaltet macOS eine große Anzahl an Protokolldateien, die Meldungen über Ereignisse und Fehlerbedingungen sammeln, die während des Betriebs des Computers aufgetreten sind. Wenn Protokolldateien ein gewisses Alter oder eine bestimmte Größe (abhängig von der Protokollart) erreicht haben, werden diese von macOS automatisch entfernt und die Protokollierung mit leeren Dateien neu begonnen. Einige Protokolldateien werden allerdings als wichtig angesehen, und alte Exemplare nicht einfach gelöscht, sondern sie werden komprimiert und in einen Archivbereich gelegt. Abhängig von der Wichtigkeit der jeweiligen Daten hält macOS mehrere Generationen dieser Archivexemplare vor, bis diese endgültig gelöscht werden.

Falls Ihr Computer mit sehr wenig Plattenspeicherplatz läuft, möchten Sie möglicherweise die archivierten Protokolldateien sofort entfernen. Die aktuelle Generation der Protokolle wird bei diesem Vorgang nicht berührt. Um archivierte Protokolldateien zu löschen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Protokollarchive** auf der Einstellungskarte **Bereinigen**.
2. Drücken Sie den Knopf **Löschen**.

3.2.4 Absturzberichte

Jedesmal wenn ein Programm abstürzt, erstellt macOS automatisch einen sogenannten Absturzbericht, der Software-Entwicklern dabei helfen kann, die genaue technische Ursache herauszufinden, warum das Programm sofort beendet werden musste. Programmabstürze werden normalerweise von Programmierfehlern entweder im Programm selbst

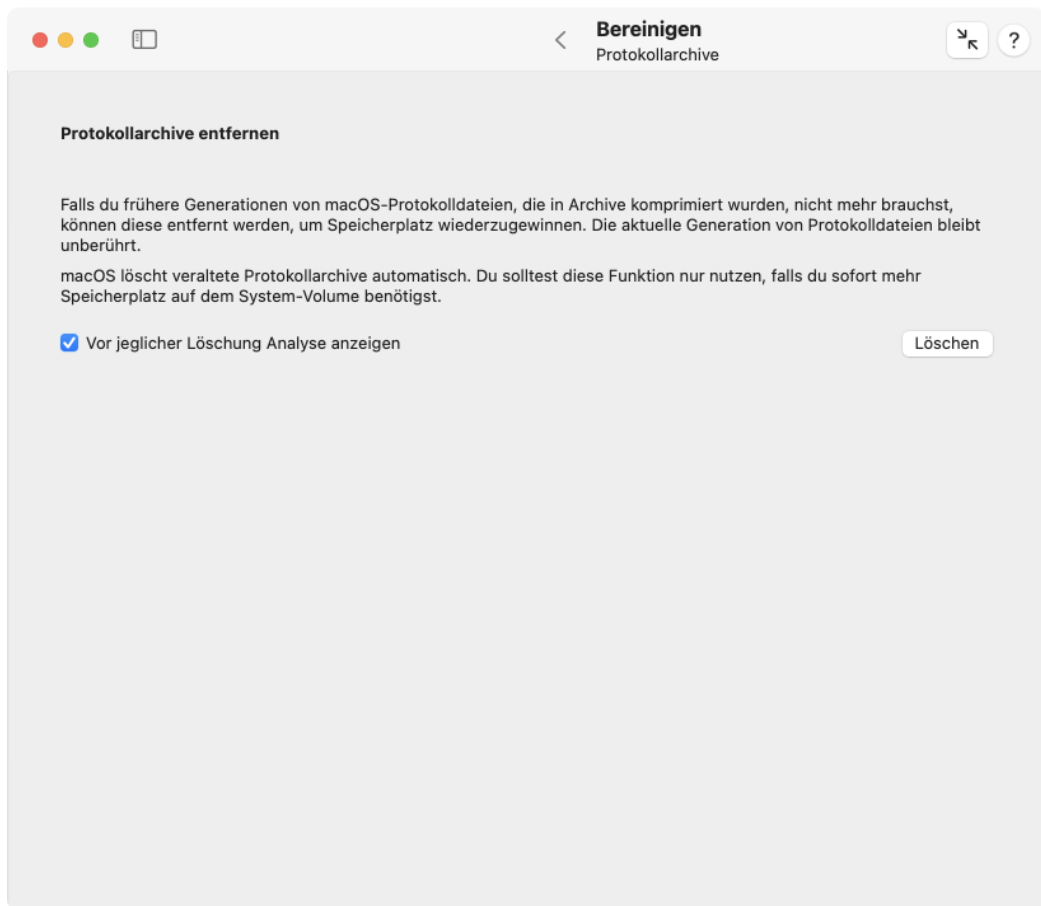


Abbildung 3.13: Protokollarchive

oder im Betriebssystem verursacht. Wenn Sie einen Absturzvorfall an den Herausgeber eines Programms melden, wird der zuständige Software-Ingenieur üblicherweise den Absturzbericht zur genaueren Analyse von Ihnen anfordern.

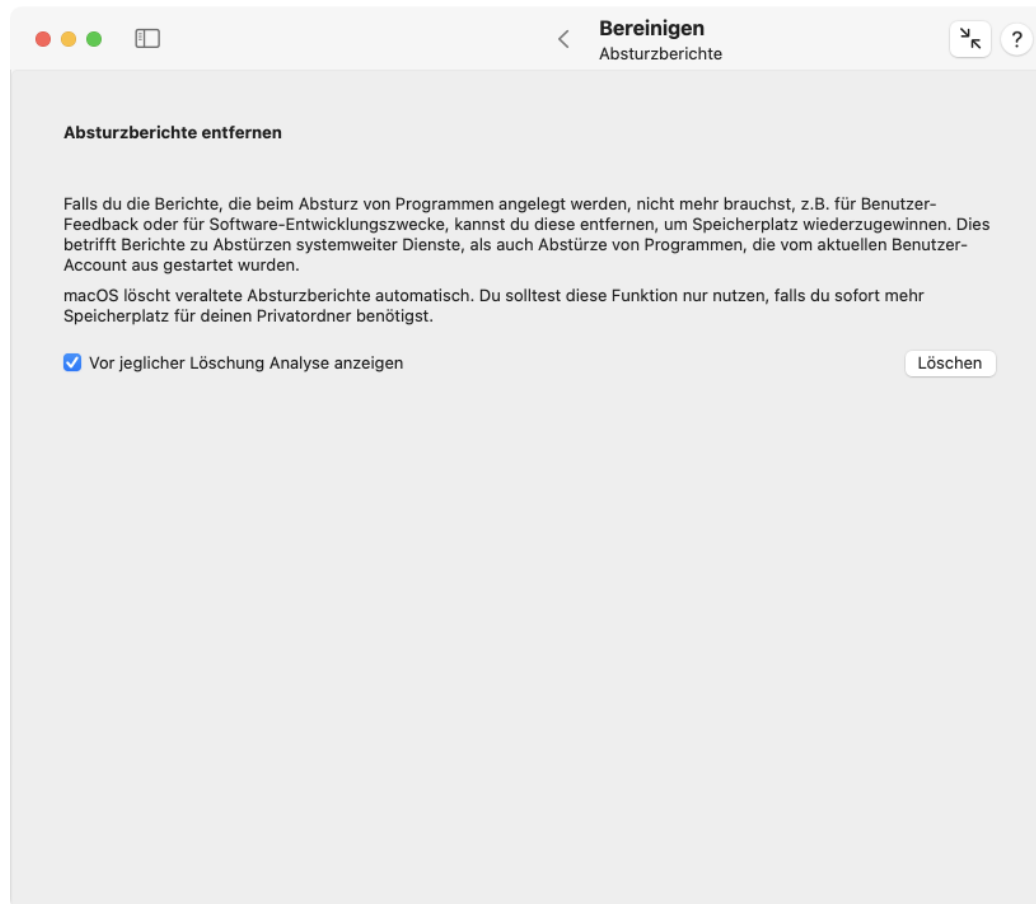


Abbildung 3.14: Absturzberichte

Für den Fall, dass Sie bestimmte Absturzberichte nicht mehr zur Kommunikation mit einem Software-Anbieter brauchen, können Sie diese löschen, um Speicherplatz wiederzugewinnen. TinkerTool System kann Absturzberichte automatisch finden, die sich auf Programme beziehen, die den gesamten Computer betreffen (üblicherweise Systemdienste), oder auf Programme, die vom aktuellen Benutzer-Account aus gestartet wurden. (Absturzberichte, die anderen Benutzern gehören, werden nicht angezeigt.) Die Liste der Absturzberichte kann auch Abstürze mit einschließen, die auf mobilen Apple-Geräten aufgetreten sind, die ihren Bericht nicht direkt an Apple senden konnten, z.B. einem iPod touch.

macOS entfernt automatisch überzählige und abgelaufene Absturzberichte, d.h. zum einen sich wiederholende Berichte für die gleiche Art von Vorfall, die keine neuen Erkenntnisse bringen, und zum anderen Berichte, die so alt sind, dass sie nicht mehr nützlich erscheinen. Die automatische Löschung abgelaufener Absturzberichte findet in der Regel nach 30 Tagen statt.

Um nicht benötigte Absturzberichte zu löschen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Absturzberichte** auf der Einstellungskarte **Bereinigen**.
2. Drücken Sie den Knopf **Löschen** und warten Sie, bis das Programm alle Berichte gesammelt hat.
3. Falls die Einstellung **Vor jeglicher Löschung Analyse zeigen** eingeschaltet ist, erscheint eine Liste der verfügbaren Absturzberichte. Die Tabelle enthält die folgenden Daten: der Name des Gerätes, auf dem der Absturz aufgetreten ist, eine Markierung, ob es sich um ein Mobilgerät gehandelt hat, der Prozessname des abgestürzten Programms, der genaue Zeitpunkt, zu dem der Absturz aufgezeichnet wurde, und die Dateigröße des Berichts. Durch Wählen oder Abwählen von Häkchen in der Spalte **Entfernen?** können Sie bestimmen, welche Berichte gelöscht und welche aufbewahrt werden sollen.
4. Drücken Sie den Knopf **Löschen** im Dialogfenster, um die ausgewählten Berichte zu löschen oder drücken Sie **Abbrechen**, um keinen Vorgang auszulösen.

3.2.5 Verwaiste Dateien

Wird ein Computer von vielen Personen verwendet, so wird es hin und wieder vorkommen, dass Benutzer-Accounts nach einiger Zeit der Nutzung wieder gelöscht werden. Bei einem Firmencomputer wird dies beispielsweise dann der Fall sein, wenn eine Mitarbeiterin die Firma verlässt, bei einem Schulcomputer, wenn ein Schüler seinen Abschluss macht. Typischerweise wird das Programm **Systemeinstellungen** zur Löschung eines Accounts verwendet, wobei das Programm anbietet, gleichzeitig auch den kompletten Privatordner des betroffenen Benutzers zu löschen. In der Regel werden dabei alle Daten, die dieser Benutzer angelegt hatte, sauber vom Computer entfernt.

Probleme kann es jedoch geben, wenn einem Benutzer die Berechtigung erteilt wurde, auch *außerhalb* seines Privatordners Dateien anzulegen oder dort Programme zu speichern. In diesem Fall werden *verwaiste* Dateien, Ordner und Programme auf dem Computer zurückbleiben, auch wenn der Benutzer-Account und der Privatordner sauber gelöscht wurden. TinkerTool System kann Ihnen dabei helfen, solche Objekte zu finden und diese auf Wunsch löschen. Alternativ können die Objekte auch einem neuen Eigentümer zugewiesen werden. Dieser Vorgang muss für jedes Volume einzeln durchgeführt werden und beschränkt sich auf Volumes, auf denen Eigentümerangaben gespeichert werden. Ein Dateisystemobjekt gilt dann als verwaist, wenn es einen Eigentümereintrag hat, der keinem vorhandenen Benutzer mehr zugeordnet werden kann. Das Informationsfenster des Finders zeigt in diesem Fall nur **Laden ...** als Eigentümer eines solchen Objekts an. Die Karte **ACL-Rechte** (Abschnitt 3.4 auf Seite 192) in TinkerTool System zeigt bei den Zugriffsrechten in der POSIX-Eigentümerzeile nur noch die Bezeichnung **ID x** (also keinen lesbaren Namen mehr) an, wobei **x** eine numerische Kennung ist.



Warnung: Falls der Computer Teil eines verwalteten Netzes ist, so werden in der Regel Benutzer-Accounts nicht nur von diesem Computer selbst, sondern auch von einem oder mehreren anderen Computern im Netz gespeichert. Diese netzweiten Accounts sind dazu in *Verzeichnisdiensten* abgelegt. Bevor Sie mit dieser Funktion arbeiten, sollten Sie sicherstellen, dass der Computer gerade mit allen für Ihr Netzwerk relevanten Verzeichnisdiensten verbunden ist und dass diese Verzeichnisse ordnungsgemäß arbeiten. Ansonsten ist es nicht zuverlässig möglich, zu entscheiden, welche

Benutzer-Accounts vorhanden und welche nicht vorhanden sind. Dateien, die Netzbenutzern gehören, könnten so fälschlicherweise als verwaist eingestuft werden.

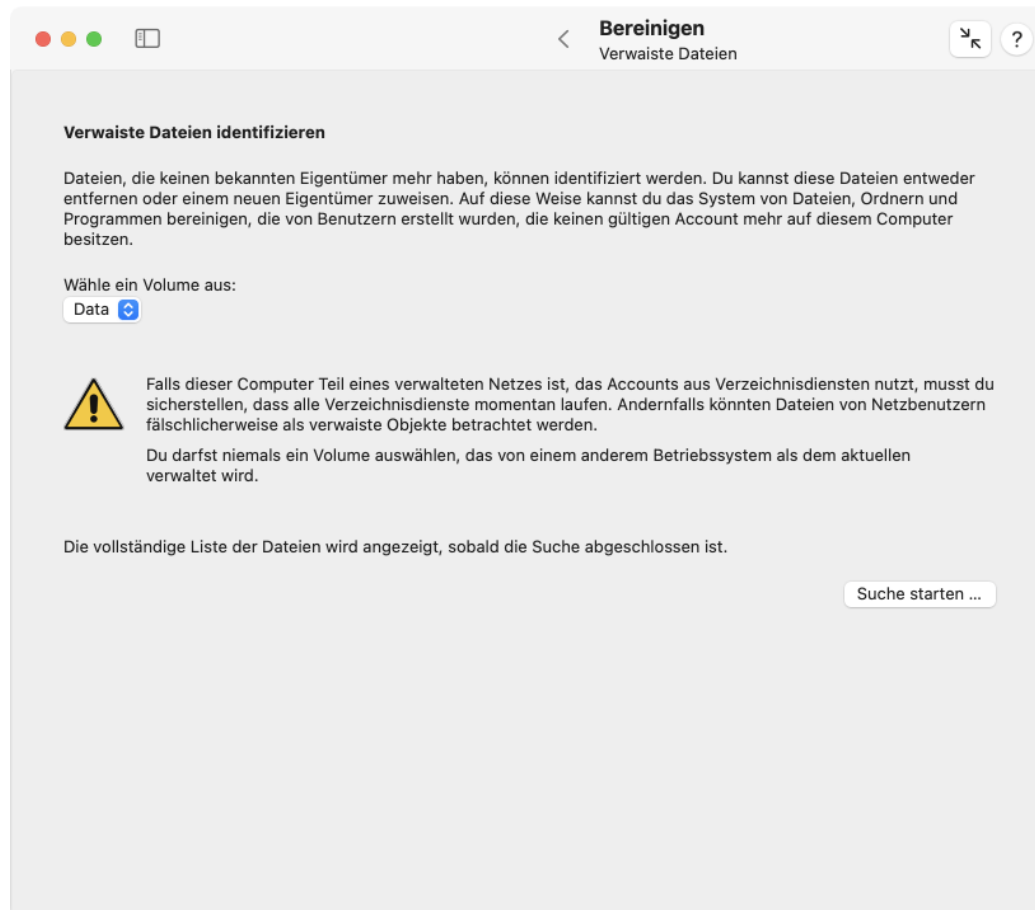


Abbildung 3.15: Verwaiste Dateien



Warnung: Sie dürfen diese Funktion nicht auf einem Volume verwenden, das von einem anderen als Ihrem aktuellen Betriebssystem verwaltet wird. Das andere System verwendet höchstwahrscheinlich eine andere Benutzer-Account-Datenbank, so dass die Information, welche Benutzer noch vorhanden und welche nicht mehr verfügbar sind, sehr unterschiedlich sein könnte.

Um verwaiste Dateien zu identifizieren, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Verwaiste Dateien** auf der Einstellungskarte **Bereinigen**.
2. Drücken Sie den Knopf **Suche starten ...** und beantworten Sie die Fragen des Programms.

3. Wenn eine Suche nach verwaisten Dateien notwendig ist, warten Sie, bis das Programm alle entsprechenden Dateien gefunden hat.
4. Die Liste aller betroffenen Dateien und Ordner wird angezeigt. Durch eine entsprechende Auswahl in der Spalte **Vorgang** können Sie bestimmen, wie mit jedem Objekt verfahren werden soll. Sie können auch mehrere oder alle Zeilen in der Tabelle markieren, über das Aufklappmenü unter der Tabelle den gleichen Vorgang für die gewählten Objekte auswählen und dann **Einstellen** drücken, um eine Einzelbehandlung zu vermeiden.
5. Drücken Sie den Knopf **Ausgewählte Aktionen durchführen** im Dialogfenster, um die entsprechende Behandlung der verwaisten Objekte einzuleiten.

Im Detail bedeuten die Vorgänge:

- **Ignorieren:** das Objekt bleibt, wie es ist
- **Löschen:** das Objekt wird vom Volume entfernt und geht verloren
- **Neuzuweisen:** das Objekt wird einem neuen Eigentümer „geschenkt“

Sie können in einem Durchlauf nur einen einzigen neuen Eigentümer zuweisen. Falls Sie Objekte eines Volumes unterschiedlichen Benutzern zuweisen möchten, müssen Sie die entsprechenden Einträge zunächst **ignorieren** und dann in erneuten Durchläufen dem jeweils gewünschten Benutzer zuordnen.

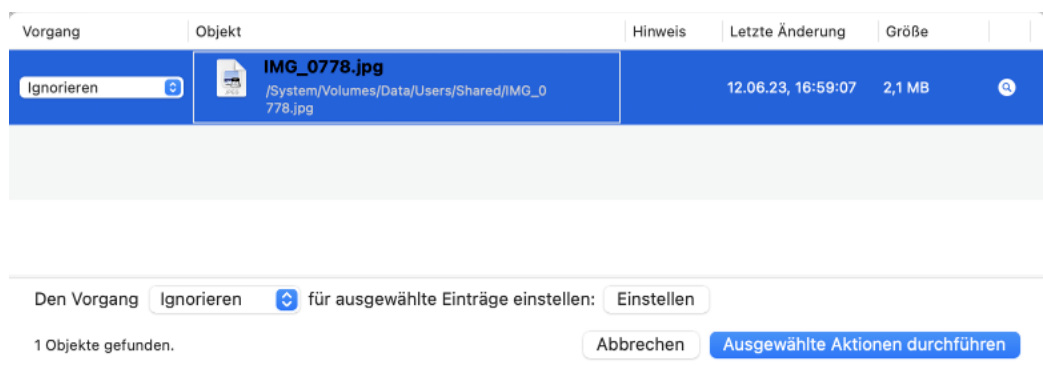


Abbildung 3.16: Bei jedem einzelnen verwaisten Objekt können Sie entscheiden, was zu tun ist.

Einige verwaiste Objekte können mit dem Hinweis **falsche Eigentümereinstellung wahrscheinlich** versehen sein. In diesem Fall ist der Eigentümer des Objekts tatsächlich unbekannt (so dass die Datei verwaist ist), es gibt aber jedoch Anzeichen dafür, dass es sich nur um eine falsche Eigentümereinstellung handelt, nicht um ein Objekt, das von einem gelöschten Benutzer-Account zurückgelassen wurde. Einige Software-Anbieter (inklusive Apple) liefern manchmal Programme und andere Komponenten mit fehlerhaften Berechtigungseinstellungen aus, was zu solch einem Effekt führen kann. In diesem Fall sollten Sie die betroffenen Dateien *nicht* löschen,

sondern Kontakt mit den Anbietern aufnehmen, die die Dateien verteilt haben, so dass diese von den Paketierfehlern in Kenntnis gesetzt werden.

Verwaiste Ordner werden nur dann zur Löschung angeboten, wenn auch deren Inhalt vollständig verwaist ist. In diesem Fall wird darauf verzichtet, die in dem betroffenen Ordner enthaltenen Objekte einzeln aufzulisten und TinkerTool System summiert auch deren Größe nicht auf. Ein solcher Ordner kann also mit einer kleinen Größe aufgelistet werden, obwohl er möglicherweise große Dateihierarchien beherbergt.

3.2.6 Aliase

Aliase sind ein Funktionsmerkmal, das vom klassischen Mac OS nach macOS übernommen wurde (siehe auch die Karte Ablage (Abschnitt 3 auf Seite 145)). Es handelt sich um Objekte im Dateisystem, die auf andere Objekte im Dateisystem verweisen, wobei das originale Objekt unter einem anderen Namen oder in einem anderen Ordner verfügbar gemacht wird. Wenn das Originalobjekt wegbewegt oder umbenannt wird, können Programme immer noch versuchen, das Originalobjekt wiederzufinden, falls sie das wollen, wobei Objekte durch kompetentes Raten nachverfolgt werden, ähnlich wie bei einer smarten Suchfunktion. Ist das Originalobjekt allerdings gelöscht worden, so sind die Aliase, die auf es verweisen, nicht mehr aktuell und werden defekt. Sie können TinkerTool System verwenden, um solche veralteten Aliase zu finden und zu löschen.

Der Vorgang, ein Objekt zu suchen, auf das sich ein Alias bezieht, wird als *Auflösen des Alias* bezeichnet. Es ist wichtig zu wissen, dass die aktuelle Umgebung, in der ein Alias aufgelöst wird, eine Rolle spielt, um zu entscheiden, ob ein Alias veraltet ist oder nicht. Ein Alias verweist möglicherweise auf ein Objekt, das sich auf einem gerade nicht aktivierten Datenträger befindet, z.B. ein gemeinsam benutzter Ordner auf einem Dateiserver, ein externes Plattenlaufwerk, eine CD-ROM, ein Memory-Stick, usw. Er könnte auch von einem anderen Benutzer angelegt worden sein und verweist auf ein Objekt, für das der aktuelle Benutzer keine Zugriffsberechtigung hat. In beiden Fällen scheint das originale Objekt aus Sicht des aktuellen Benutzers nicht vorhanden zu sein. Für einen anderen Benutzer oder nach Wiederanschließen des richtigen Dateisystems könnte der Alias aber durchaus noch gültig sein.

Um zu entscheiden, ob ein Alias aufgelöst werden kann, verwendet TinkerTool System die Zugriffsrechte des aktuellen Benutzers und löst keine Wiederverbindungsvorgänge aus.

Um nicht auflösbare Aliase aus einer Ordnerhierarchie zu entfernen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Aliase** auf der Einstellungskarte **Bereinigen**.
2. Ziehen Sie den obersten Ordner, der bearbeitet werden soll, vom Finder in das Feld **Oberster Ordner**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Drücken Sie den Knopf **Löschen** und warten Sie, bis das Programm alle defekten Aliase gesammelt hat.
4. Falls die Einstellung **Vor jeglicher Löschung Analyse zeigen** eingeschaltet ist, erscheint eine Liste der verfügbaren Aliase. Durch Wählen oder Abwählen von Häkchen in der Spalte **Entfernen?** können Sie bestimmen, welche Aliase gelöscht und welche aufbewahrt werden sollen.

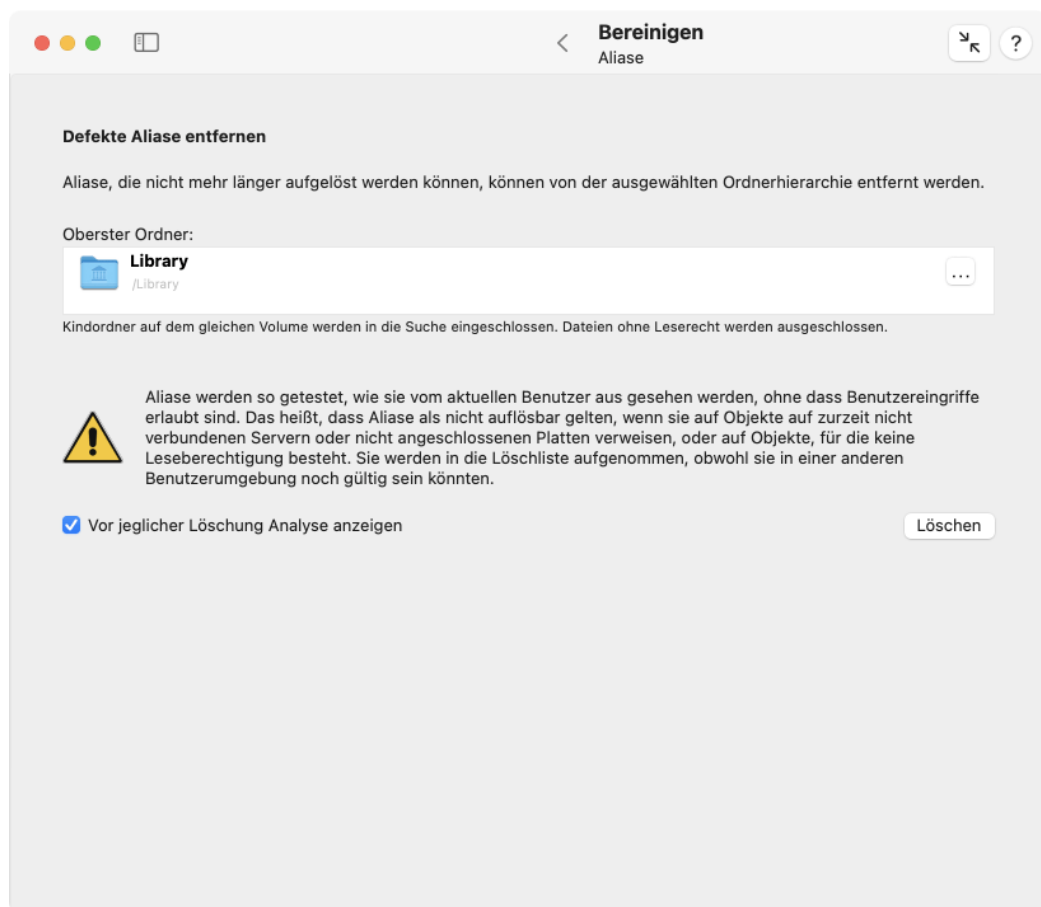


Abbildung 3.17: Aliase

5. Drücken Sie den Knopf **Löschen** im Dialogfenster, um die ausgewählten Aliase zu löschen oder drücken Sie **Abbrechen**, um keinen Vorgang auszulösen.

3.2.7 Entfernbare Platten

Die versteckten Dateien, die zu Eingang dieses Kapitels erläutert wurden, sind nicht die einzigen unsichtbaren Komponenten, die man auf Macintosh-Platten finden kann. Eine Platte enthält üblicherweise weitere versteckte Ordner, um den Papierkorb zu speichern, den Spotlight-Suchindex und einige andere Dateien, die notwendig sind, um die volle Kompatibilität mit dem Finder des klassischen Mac OS aufrecht zu erhalten. Wenn Sie solche Datenträger an Benutzer von Nicht-Mac-Betriebssystemen weitergeben, z.B. Linux oder Microsoft® Windows, und diese Benutzer haben ihre grafischen Datei-Browser so eingestellt, dass auch unsichtbare Dateien angezeigt werden, sind diese möglicherweise etwas verwirrt. Bei einigen Geräten mit eingebauten Betriebssystemen, wie Fernsehern oder Autoradios, können die versteckten Dateien sogar technische Probleme auslösen, beispielsweise wenn Sie MP3-Dateien abspielen möchten, die von macOS auf einen Speicher-Stick kopiert wurden.

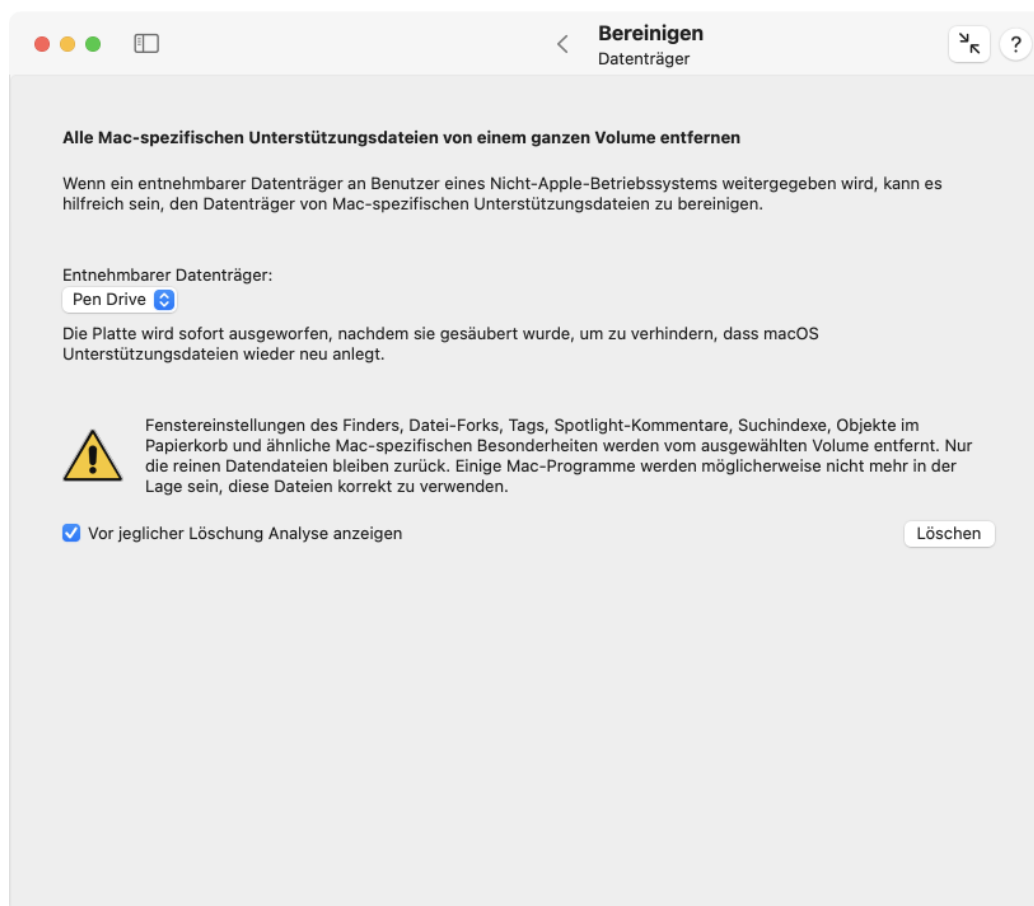


Abbildung 3.18: Entfernbare Platten

TinkerTool System kann den vollständigen Satz von Macintosh-Unterstützungsdateien von einer ganzen Platte entfernen und dann diese Platte auswerfen, um zu verhindern, dass

macOS die Dateien wieder neu anlegt. Sie können diese Prozedur als letzten Schritt durchführen, bevor Sie die Platte an Benutzer eines fremden Betriebssystems weitergeben oder an ein Nicht-Apple-Gerät anschließen. Führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Datenträger** auf der Einstellungskarte **Bereinigen**.
2. Wählen Sie die Platte über das Aufklappmenü **Entnehmbarer Datenträger** aus.
3. Drücken Sie den Knopf **Löschen**.

Die Liste der entnehmbaren Datenträger enthält alle Platten, für die Sie in der aktuellen Situation den Vorgang „Auswerfen“ ausführen können. Dies kann interne Platten miteinschließen, die im physikalischen Sinne nicht direkt entnehmbar sind.



Denken Sie daran, dass Macintosh-spezifische Funktionen von den Dateien auf dem betroffenen Datenträger entfernt werden. Einige Dateien könnten aus der Sicht des Mac unbrauchbar werden. Sie sollten diese Funktion nur auf „Transportplatten“ anwenden, die Sie an Nicht-Mac-Systeme weiterreichen. Der Datenträger sollte nur Kopien der Originaldateien enthalten, die Sie immer noch auf Ihrer Hauptplatte oder einem Dateiserver haben.

3.2.8 Zeitlupen-Bildschirmschoner (nur macOS 14 Sonoma oder höher)

Mit macOS 14 Sonoma hat Apple eine neue Art von Bildschirmschonern in macOS eingeführt, was vom Apple TV übernommen wurde. Diese zeigen Szenarien in Zeitlupe und können mit passenden Hintergrundbildern kombiniert werden. Die Betriebsmitteldateien für diese Bildschirmschoner können eine große Menge an Speicherplatz verbrauchen, typischerweise zwischen 500 MByte und 1 GByte auf der System-Volume-Gruppe für jedes Exemplar. Mit Ausnahme von einem einzelnen bestimmten Standardbildschirmschoner sind alle anderen Zeitlupen-Bildschirmschoner optional. Sie werden nur dann heruntergeladen und gespeichert, sobald ein Benutzer diese ausdrücklich im Abschnitt **Bildschirmschoner** der **Systemeinstellungen** auswählt. Außerdem werden diese Bildschirmschoner von macOS automatisch gelöscht, sobald das System Speichermangel aufweist.

Es kann Situationen geben, wo Sie einen bestimmten Bildschirmschoner sofort entfernen möchten, ohne auf macOS warten zu müssen. TinkerTool System zeigt an, wie viel Speicherplatz von den jeweiligen Bildschirmschonern verbraucht wird und erlaubt es, diese zu löschen, falls Sie möchten.

1. Öffnen Sie den Unterpunkt **Bildschirmschoner** auf der Einstellungskarte **Bereinigen**.
 2. Wählen Sie einen oder mehrere installierte Bildschirmschoner in der Tabelle aus, indem Sie den jeweiligen Eintrag in der Spalte **Entfernen?** ankreuzen.
 3. Drücken Sie den Knopf **Entfernen**.
- Der eingebaute Zeitlupen-Bildschirmschoner, der zum Betriebssystem gehört, kann nicht entfernt werden.
 - Die Bildschirmschoner werden in einer Standardsortierreihenfolge aufgelistet, die von Apple definiert ist. Dies sollte mit der Sortierung der entsprechenden Punkte in Systemeinstellungen übereinstimmen.

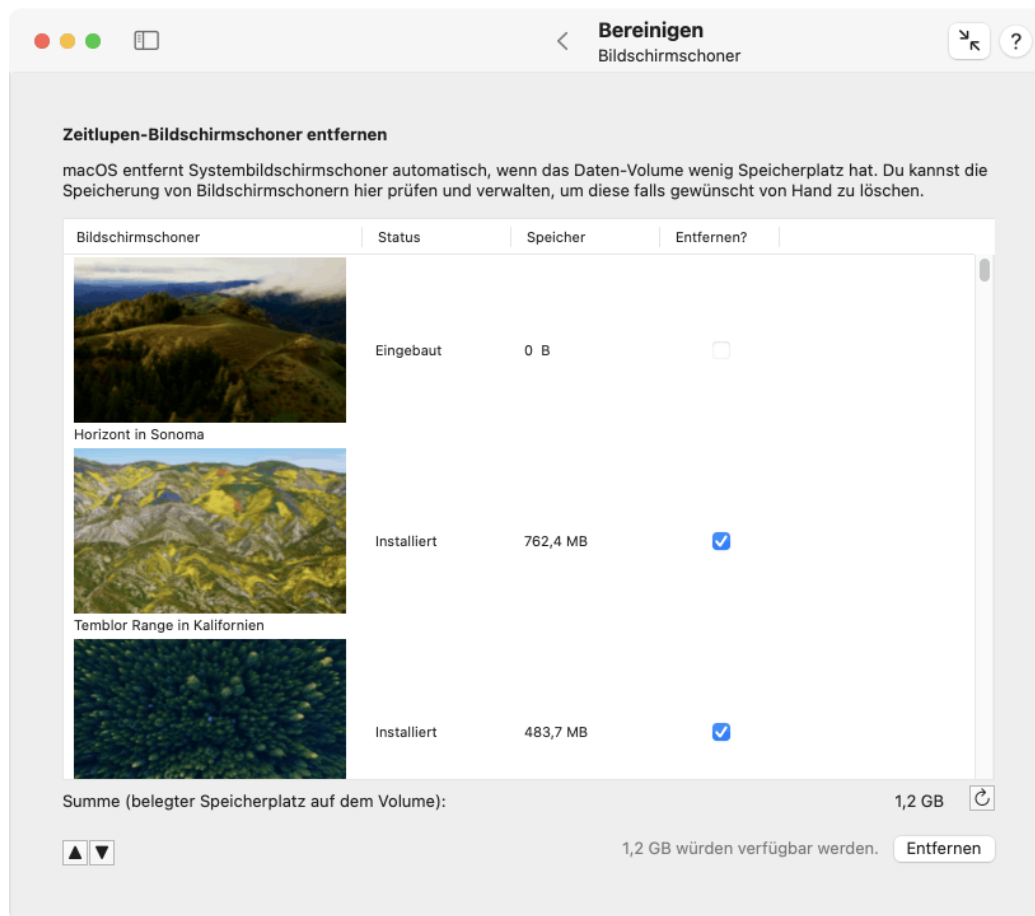


Abbildung 3.19: Zeitlupen-Bildschirmschoner benötigen eine Menge Speicherplatz und können entfernt werden, falls sie installiert sind.

- Um zum nächsten oder vorigen installierten Bildschirmschoner in der Tabelle zu navigieren, können Sie die Pfeilknöpfe in der unteren linken Ecke verwenden.
- TinkerTool System gibt die Summe aller entfernbaren Bildschirmschoner an, als auch den potenziellen Speichergewinn, wenn die ausgewählten Schoner entfernt werden würden.
- Falls Bildschirmschoner in den Systemeinstellungen hinzugefügt wurden, während TinkerTool System läuft, können Sie die Anzeige über die Auffrischungstaste rechts unter der Tabelle aktualisieren.



Es ist nicht möglich, zu prüfen, welche Bildschirmschoner zurzeit für jeden Benutzer-Account auf Ihrem Mac aktiv sind. TinkerTool System wird die ausgewählten löschen, egal ob sie von einigen Benutzern im Moment als bevorzugt eingestellt sind.

Bildschirmschoner sind auf der System-Volume-Gruppe gespeichert, so dass deren Speicherplatz dem üblichen Verhalten von APFS-Dateien entspricht: Der Platz der gelöschten Betriebsmitteldateien wird *verfügbar*, aber nicht unbedingt *frei*. Falls Sie freien Platz brauchen, ist es möglicherweise erforderlich, den jeweiligen APFS-Schnappschuss ebenso freizugeben. Weitere Informationen hierzu finden Sie in den Kapiteln Die Einstellungskarte Systemsicherheit (Abschnitt 3.6 auf Seite 222) und Die Einstellungskarte APFS (Abschnitt 3.7 auf Seite 228).

3.2.9 Speicherabzüge

Werden fortgeschrittene Softwaretestverfahren mit macOS eingesetzt, kann das Betriebssystem so konfiguriert worden sein, sogenannte *Post-Mortem-Speicherabzüge (Core Dumps)* zu erstellen. Nachdem ein getestetes Programm – oder in diesen besonderen Fällen meistens der macOS-Systemkern – abgestürzt sind, schreibt macOS den vollständigen Inhalt des Hauptspeichers des Computers in eine Speicherabzugsdatei auf der Betriebssystemplatte. Der Speicherabzug ist im Prinzip eine Momentaufnahme der Speichersituation, wie sie auf dem Computer vorgelegen hat, als der Absturz aufgetreten ist. Er kann zu einem späteren Zeitpunkt genauer analysiert werden, nachdem das System neu gestartet wurde. Speicherabzugsdateien sind üblicherweise so groß wie die vorhandene Hauptspeichergröße, so dass sie eine große Menge an Speicherplatz auf der Systemplatte belegen können. TinkerTool System kann alle verfügbaren Speicherabzüge automatisch entfernen, falls Sie diese nicht brauchen. Führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Speicherabzüge** auf der Einstellungskarte **Bereinigen**.
2. Drücken Sie den Knopf **Löschen**.

3.3 Die Einstellungskarte Programme

3.3.1 Deinstallationsassistent

Programme, die sich streng an Apples Software-Designrichtlinien für macOS halten und nicht tief in das Betriebssystem integriert werden müssen, werden üblicherweise über

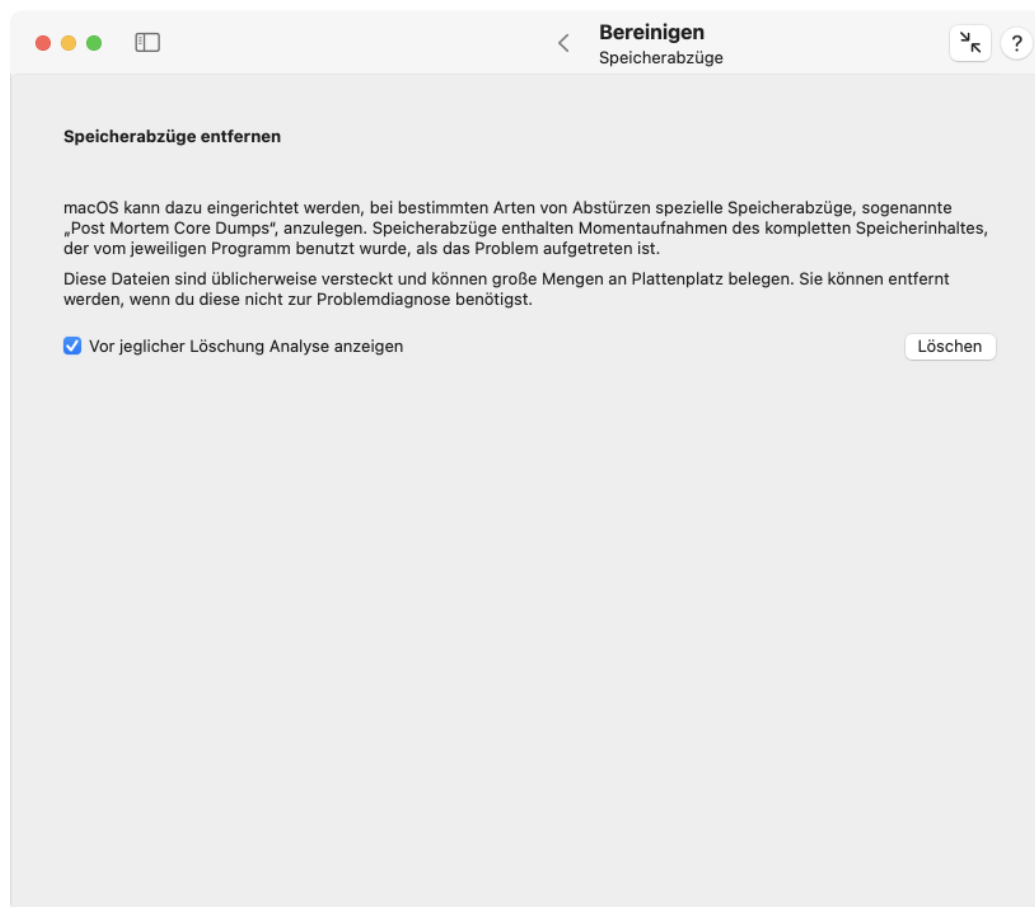


Abbildung 3.20: Speicherabzüge

einen einfachen „Ziehen-und-Ablegen“-Vorgang installiert. Das heißt, es ist gar keine eigentliche Installation notwendig, sondern Sie ziehen lediglich das Programmsymbol in einen Ihrer Programmordner und können das Programm sofort starten.

macOS legt allerdings automatisch zusätzliche Dateien an, wenn Sie mit einem neuen Programm arbeiten, zum Beispiel Dateien, um Ihre persönlichen Einstellungen pro Benutzer zu speichern, oder Cache-Dateien für heruntergeladene Dateien, wenn Programme auf das Internet zugreifen, um nach automatischen Aktualisierungen zu suchen, usw. Sie können ein solches Ziehen-und-Ablegen-Programm einfach deinstallieren, indem Sie sein Symbol in den Papierkorb ziehen. Dies wird allerdings nicht die gerade erwähnten Hilfsdateien mit entfernen. Hierbei kann jedoch der Deinstallationsassistent von TinkerTool System helfen.

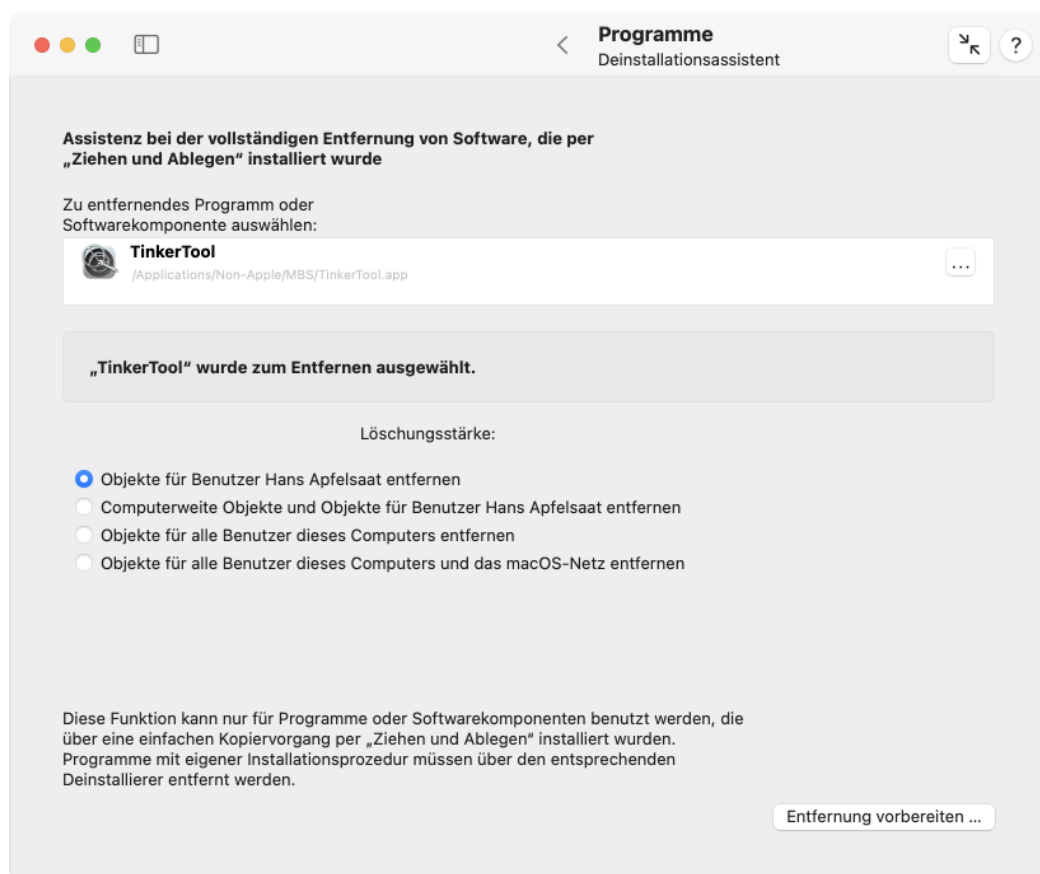


Abbildung 3.21: Deinstallationsassistent

3.3.2 Entfernen von Software-Komponenten und zugehöriger Dateien

Die Aufgabe des Deinstallationsassistenten besteht darin, Ihnen dabei zu helfen, alle zugehörigen Komponenten zu identifizieren, die möglicherweise von der Software-Komponente angelegt wurden, die Sie entfernen möchten. Sie können TinkerTool System diese anderen Dateien und Ordner ebenso entfernen lassen, wodurch der gesamte Computer bereinigt wird. Konkret gibt es vier Lösungsstärken, zwischen denen Sie wählen können:

1. Sie können die Suche auf Komponenten begrenzen, die nur für Ihren eigenen Benutzer-

Account angelegt wurden.

2. Sie können nach Komponenten suchen, die für „computerweite“ Nutzung durch alle Benutzer des lokalen Computers installiert wurden, zusätzlich zu den persönlichen Elementen für Ihren Benutzer-Account.
3. Sie können nach Komponenten suchen, die als persönliche Elemente für alle Benutzer-Accounts auf dem lokalen Computer installiert wurden, inklusive der Komponenten, die für computerweite Nutzung angelegt wurden.
4. Sie können zusätzlich Elemente einschließen, die für „netzweite“ Verwendung installiert wurden. Dies ist nützlich, wenn Sie einen zentralen Softwareverteilungsserver und die Managementfunktionen von macOS einsetzen, die Daten in den Ordnern **Netzwerk > Programme (/Network/Applications)** und **Netzwerk > Library (/Network/Library)** ablegen.



Falls Sie die Lösungsstärken (3) oder (4) verwenden, erlaubt Ihnen TinkerTool System, Dateien und Ordner zu löschen, die anderen Benutzern gehören. Dies ist eine gefährliche Auswahl, die nur von erfahrenen Systemverwaltern benutzt werden sollte. Bitte prüfen Sie jedes Objekt sorgfältig, bevor Sie es tatsächlich löschen.



Es gibt Programme, die vollständig verbergen, wo und wie sie Daten oder Dokumente speichern, die Sie mit solch einem Programm anlegen („*shoebox apps*“). Andere Programme geben Ihnen möglicherweise die Gelegenheit, selbst Dateinamen für Dokumente zu wählen, verwenden aber ebenso ihre eigene private Ablage, um die Dateien zu speichern. Bitte berücksichtigen Sie, dass die Benutzerdokumente solcher Programme möglicherweise mit entfernt werden, wenn Sie eine Deinstallation durchführen.

Bevor irgendein Objekt entfernt wird, wird jedes betroffene Element von TinkerTool System aufgelistet. Sie können dann für jedes einzelne Objekt entscheiden, ob Sie es tatsächlich entfernen möchten oder nicht. Führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Deinstallationsassistent** auf der Einstellungskarte **Programme**.
2. Ziehen Sie das Symbol des Programms, das Sie entfernen möchten, vom Finder in das Feld **Zu entfernendes Programm oder Softwarekomponente auswählen**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Falls ein Programm ausgewählt wurde, müssen Sie zwischen einer der vier oben erwähnten Lösungsstärken auswählen, indem Sie die Knöpfe bei **Lösungsstärke** betätigen.
4. Drücken Sie den Knopf **Entfernung vorbereiten**

Beachten Sie, dass jetzt noch nichts entfernt wird. TinkerTool System analysiert grundsätzlich erst Ihre Auswahl und zeigt die Elemente an, die betroffen sein würden. Das Programm beginnt die Suche nach Objekten, nachdem Sie den Knopf **Entfernung vorbereiten ...** gedrückt haben. Sie können die Suche jederzeit unterbrechen und abbrechen, indem Sie den **Stopp**-Knopf drücken, der während des Suchvorgangs angezeigt wird. Eine Suche kann mehrere Minuten dauern, falls Ihr Computer oder das Netzwerk viele Benutzer-Accounts beherbergen und Sie eine der Lösungsstärken ausgewählt haben, die alle Benutzer betreffen.

Nachdem die Suche zu Ende ist, werden alle Kandidaten für die mögliche Entfernung in einer Tabelle aufgelistet. Die Tabelle enthält die folgenden Spalten:

- **Entfernen:** Setzen oder entfernen Sie das Häkchen, um das betreffende Objekt in den Löschvorgang aufzunehmen, bzw. auszuschließen.
- **Objekt:** Symbol, Name und Pfad des Objekts, das zur Entfernung vorgeschlagen ist.
- **Typ:** die Rolle, die dieses Objekt in Bezug auf die Softwarekomponente einnimmt, die Sie entfernen möchten.
- **Eigentümer:** der Kurzname des Benutzers, dem dieses Objekt gehört. Seien Sie vorsichtig, wenn Sie persönliche Elemente anderer Benutzer löschen.
- **Größe:** die Speichergröße dieses Objekts. Dieser Platz wird freigegeben, nachdem das Objekt gelöscht wurde.
- **Letzte Änderung:** Datum und Uhrzeit, wann das Objekt zuletzt verändert wurde.
- **Zeigen:** drücken Sie auf die Knöpfe in der Zeigen-Spalte, um das jeweilige Objekt im Finder aufzudecken.

Die Gesamtzahl ausgewählter Objekte und der Gesamtspeicherplatz werden rechts unterhalb der Tabelle angegeben. Die beiden Knöpfe in der linken Ecke lassen Sie auswählen,

- ob die zur Entfernung ausgewählten Elemente in den Papierkorb geworfen werden sollen, oder
- ob die markierten Elemente sofort gelöscht werden sollen.

TinkerTool System erlaubt es Ihnen nicht, die Sicherheitsfunktionen von macOS zu umgehen. Obwohl Ihnen dieses Feature gestattet, Objekte zu löschen, die anderen Benutzern gehören, kann dies nicht ausgenutzt werden, um die Inhalte privater Dateien auszuspionieren. Aus diesem Grund ist es *nicht* möglich, Detailinformationen über Dateien abzurufen, die weder Ihnen, noch dem Betriebssystem gehören. Ebenso können Objekte nicht in den Papierkorb geworfen werden, auf die Sie keinen Zugriff haben.

Die ausgewählten Objekte werden entfernt, sobald Sie den Knopf **Entfernen** drücken. Alle Objekte bleiben unberührt, wenn Sie den Knopf **Abbrechen** verwenden.

TinkerTool System erstellt automatisch einen detaillierten Bericht über die Komponenten, die Sie entfernen. Er wird während und nach dem Entfernungsvorgang angezeigt. Nach Abschluss des Vorgangs können Sie den Bericht entweder in eine Textdatei sichern oder ihn durch Drücken der entsprechenden Knöpfe im Berichtsdialogfenster ausdrucken.

Die Liste der zur Löschung vorgeschlagenen Objekte wird nach Apples Richtlinien für macOS-Softwaredesign berechnet. Beachten Sie, dass einige wenige Programme sich möglicherweise nicht voll an diese Richtlinien halten. **In diesem Fall ist die Liste der Löschungskandidaten unvollständig.** Das heißt, es könnte Objekte geben, die von dem im Mittelpunkt stehenden Programm angelegt wurden, die aber in der Liste fehlen. Es könnte auch passieren (dies ist allerdings sehr unwahrscheinlich), dass Objekte in der Liste enthalten sind, die gar nicht vom ausgewählten Programm angelegt worden sind, so dass sie nicht gelöscht werden sollten. Bitte prüfen Sie jedes Objekt sorgfältig, bevor Sie die Entfernungsfunktion nutzen.

Wenn Sie ein Programm entfernen, das in die Liste Ihrer Anmeldeobjekte eingetragen ist, wird es auch von dort entfernt, ohne dass dies in der Liste der Löschungskandidaten erwähnt wird. Aus technischen Gründen ist diese Bereinigung auf den aktuellen Benutzer beschränkt, auch wenn Sie eine Lösungsstärke eingestellt haben, die alle Benutzer umfasst.

TinkerTool System enthält mehrere Sicherheitsfunktionen, die es nicht zulassen, dass wichtige Teile des Systems entfernt werden. Sie können keine Komponenten entfernen, die offizieller Bestandteil von macOS sind. Sie können auch keine Programme entfernen, die gegenwärtig auf dem lokalen Computer laufen.



Sie sollten diese Funktion niemals für Softwarekomponenten nutzen, die nicht über einen Ziehen-und-Ablegen-Vorgang installiert wurden. Programme, die mit einem eigenen Installationsprogramm geliefert wurden oder das Installationsprogramm von macOS verwendet haben, hatten üblicherweise einen technischen Grund dafür. In diesem Fall ist es sehr wahrscheinlich, dass mehr als die üblichen Komponenten auf dem System installiert wurden, so dass diese nicht den Regeln für in sich abgeschlossene Programme folgen. Der Deinstallationsassistent ist für diesen Fall nicht ausgelegt. Sie sollten solche Programme nur nach den Anweisungen ihrer Hersteller entfernen.

3.3.3 Besonderer Start von Programmen

Sie können TinkerTool System dazu benutzen, Programme mit besonderen Wahlmöglichkeiten zu starten, die nicht dem Standard entsprechen, wie er von Finder, Dock oder Launchpad üblicherweise angenommen wird. Die folgenden Sondereinstellungen sind möglich:

- Das System soll nicht sicherstellen, dass Fenster des Programms in den Vordergrund geholt werden und dessen Hauptfenster den Eingabefokus erhält. Das heißt es wird nicht zum aktiven Programm, das auf Tastatur und Maus hört. Stattdessen bleibt TinkerTool System aktiv.
- macOS soll die Anwendung nicht in der Rubrik Programme des Menüs **Benutzte Objekte** hinzufügen.
- Auch wenn das Programm bereits läuft, soll ein weiteres Exemplar gestartet werden.
- Das Programm soll sich nach dem Start ausblenden, also so öffnen, dass die Fenster nicht sichtbar sind.

- Alle anderen Programme sollen sich ausblenden. Nur das gestartete Programm soll sichtbar sein.

Die letzten beiden Auswahlmöglichkeiten dürfen gleichzeitig eingeschaltet werden. macOS wird allerdings versuchen, diesen Konflikt aufzulösen, so dass mindestens ein Programm sichtbar bleibt. Das Detailverhalten kann von der Betriebssystemversion abhängen, die Sie nutzen.

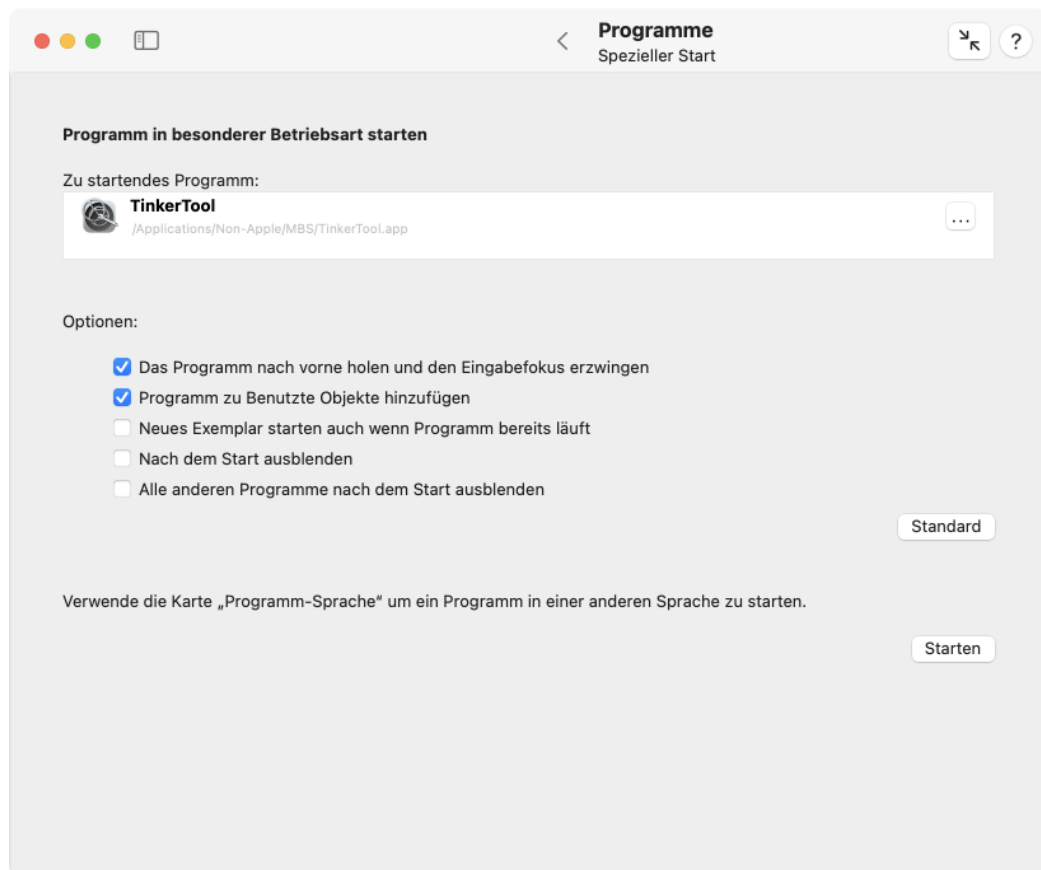


Abbildung 3.22: Programme können mit besonderen Wahlmöglichkeiten gestartet werden

1. Öffnen Sie den Unterpunkt **Spezieller Start** auf der Einstellungskarte **Programme**.
2. Ziehen Sie das Symbol der Anwendung, die Sie starten möchten, vom Finder in das Feld **Zu startendes Programm**. Sie können auch den Knopf [...] drücken, um zum Programm zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Stellen Sie die Optionen ein, die Sie nutzen möchten.
4. Klicken Sie auf den Knopf **Starten**.

3.3.4 Datenschutz

Zusätzlich zu Benutzerrechten unterstützt macOS weitere Funktionen, um die Privatsphäre von Benutzern zu bewahren und Daten zu schützen. Einer dieser Mechanismen basiert auf Datenschutzeinstellungen, die bezüglich Programmen verhindern, dass auf bestimmte Bereiche persönlicher Daten zugegriffen werden kann. Beispielsweise kann der Zugriff auf die persönlichen Kalender der Benutzer so konfiguriert werden, dass nur das Programm **Kalender** von macOS die Erlaubnis hat, die Kalendereinträge zu verarbeiten, nicht jedoch andere Apps, selbst wenn diese Apps von dem Benutzer gestartet worden sind, dem der Kalender gehört.

Die Entscheidungen, welche Programme Zugriff auf welche Gebiete haben, werden von macOS in einer Datenschutzdatenbank gespeichert. Alle Einträge können in der Tabelle unter **Systemeinstellungen** > **Datenschutz & Sicherheit** eingesehen werden. TinkerTool System bietet eine Bedienerschnittstelle, um Apples offizielles Verfahren zu verwenden, diese Erlaubniseinträge zurückzusetzen. Die Entscheidungen, die in der Vergangenheit bezüglich des Zugriffs auf persönliche Datenbereiche gemacht wurden, werden rückgängig gemacht und die Werkseinstellung wiederhergestellt. Dies bewirkt, dass die betroffenen Apps ihr Zugriffsrecht verlieren und den Benutzer noch einmal nach einer Entscheidung fragen, wenn das nächste Mal ein Zugriffsversuch auf persönliche Daten stattfindet.

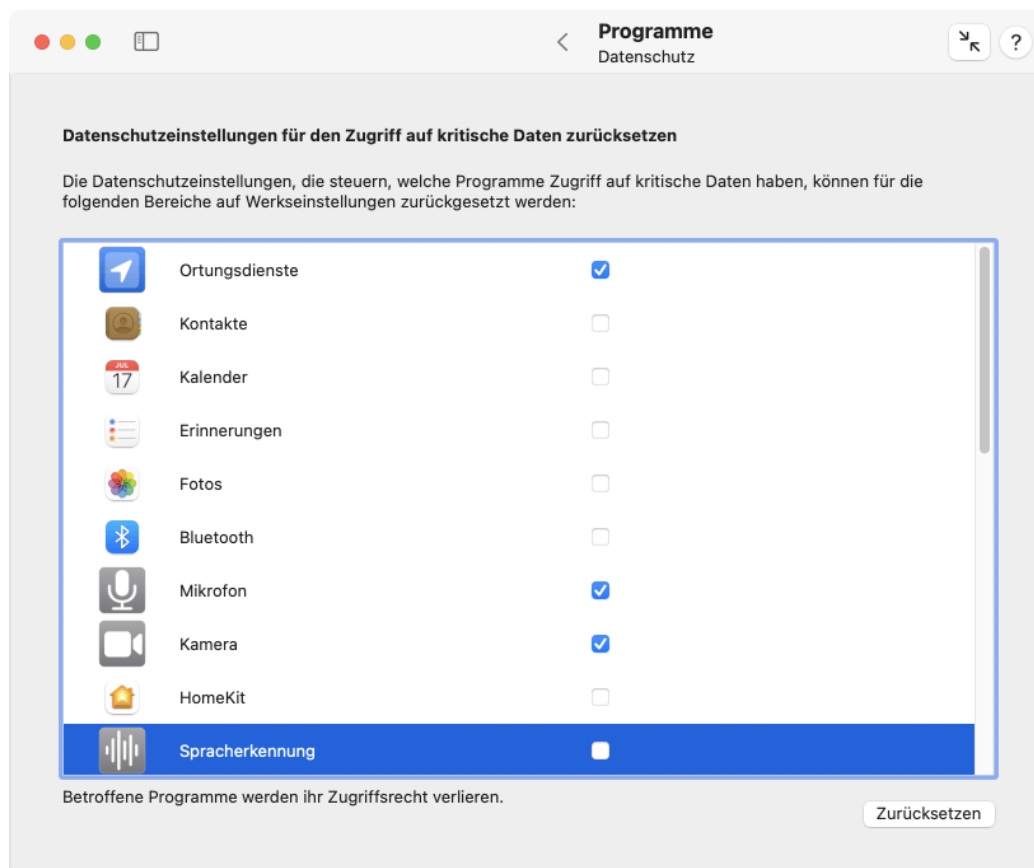


Abbildung 3.23: Datenschutzeinstellungen für Programme zurücksetzen

1. Öffnen Sie den Unterpunkt **Datenschutz** auf der Einstellungskarte **Programme**.

2. Kreuzen Sie alle Zugriffsbereiche an, für die Datenschutzeinstellungen zurückgesetzt werden sollen.
3. Betätigen Sie den Knopf **Zurücksetzen**.

Beachten Sie, dass die Einstellungen systemweit gültig sind und für alle Benutzer wirksam werden.

Die Anzahl der angezeigten Punkte kann sich je nach Betriebssystemversion stark unterscheiden.

3.3.5 Sicherheitsprüfung

Um gegen bösartige Software gewappnet zu sein, verwendet macOS verschiedene Sicherheitstechniken, die sich gegenseitig ergänzen:

- die *Quarantäne*-Funktion, die Downloads aus dem Internet erkennt und ebenso alle Dateien nachverfolgt, die Teil dieses Downloads sind oder indirekt von einem heruntergeladenen Programm angelegt wurden,
- die *Codesigning*-Technik, die es erlaubt, festzustellen, ob eine Software-Komponente aus einer bekannten, vertrauensvollen Quelle stammt und die auch eventuell durchgeführte nachträgliche Änderungen an Dateien oder Speicherseiten über ein digitales Siegel erkennt,
- die *Beglaubigung durch Apple*, manchmal auch *Notarisierung* genannt, die bestätigt, dass dieses Programm vor seiner Veröffentlichung Apple zur Prüfung vorgelegt wurde, um es auf enthaltene bekannte Viren oder ähnliche Malware zu prüfen,
- die *Anwendungs-Sandbox*, die sicherstellt, dass ein geschütztes Programm keinen Zugriff auf bestimmte Systemfunktionen erlangen kann, falls nicht sowohl Apple als auch der ursprüngliche Software-Entwickler einen solchen Zugriff ausdrücklich erlaubt haben. Jeder zugelassene Typ von Zugriff wird *Befugnis* genannt. Programme, die auf solche Art geschützt sind, werden mit einer eingebauten Liste von Befugnissen ausgeliefert, die digital im Programmpaket versiegelt ist. macOS startet ein solches Programm nur, nachdem es dieses vorher in eine Sandbox gesteckt hat, die die Einhaltung von Apples Einschränkungen unter Berücksichtigung der angegebenen Befugnisse erzwingt. Die Befugnisse stellen quasi Ausnahmeregeln dar, die dem Programm, das in der Sandbox läuft, zusätzliche Rechte erteilt, die es standardmäßig nicht hat.
- die *gehärtete Laufzeitumgebung*, die gewissermaßen eine zusätzliche „Light-Version“ der Sandbox darstellt, die Anwendungen nutzen können, um sich selbst von der Benutzung einer oder mehrerer der folgenden Funktionen des Betriebssystems auszuschließen:
 - Nutzung des Just-In-Time-Übersetzers für JavaScript-Code
 - Erzeugen von Code im Speicher zur Laufzeit
 - das Verhalten des dynamischen Code-Binders über Umgebungsvariablen ändern
 - das Binden mit Code-Bibliotheken von Drittanbietern
 - das Ändern von Code im Speicher zur Laufzeit

- das Anbinden an andere Programme in der Rolle eines Fehlersuchewerkzeugs (Debugger)
 - Zugriff auf Mikrofone oder ähnliche Audio-Eingabe
 - Zugriff auf die eingebaute Kamera
 - Zugriff auf die Ortungsdienste
 - Zugriff auf die Kontakte-Datenbank des Benutzers
 - Zugriff auf die Kalendardaten des Benutzers
 - Zugriff auf die Fotos-Mediathek des Benutzers
 - das Senden von Apple-Events an andere Programme
- die *Gatekeeper*-Komponente, technisch auch unter der Bezeichnung *Richtliniensubsystem von macOS zur Einschätzung der Sicherheit* bekannt, die alle Funktionen und Prüfschritte der vorgenannten Features einsetzt, um letztendlich zu bestimmen, ob ein Programm als „sicher genug, um es auszuführen“ beurteilt wird, oder nicht.

TinkerTool System kann eine gegebene Software-Komponente – entweder eine komplette Anwendung, ein Code-Paket wie z.B. ein Plugin, eine ausführbare Datei oder ein signiertes Plattenabbild zur Softwareverteilung – gegen alle erwähnten Sicherheitsüberprüfungen auswerten, wobei alle Details angezeigt werden. Dies erlaubt es Ihnen, die Integrität, die Quelle und die allgemeine Sicherheitsbewertung dieser Software zu prüfen.

Das Prüfen eines Programms ist sehr einfach. Führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Sicherheitsprüfung** auf der Einstellungskarte **Programme**.
2. Ziehen Sie das Symbol des Programms vom Finder in das Feld **Zu prüfendes Objekt**. Dies kann entweder ein Paket (Bundle) einer Standardanwendung für macOS sein, eine einzelne ausführbare Datei oder ein signiertes Plattenabbild (DMG) zur Softwareverteilung. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.

TinkerTool System und die Sicherheitsfunktionen von macOS werden die ausgewählte Software nun analysieren. Dies kann einige Sekunden Zeit benötigen, abhängig von der Größe des Pakets und der Zahl der eingebetteten Unterkomponenten. Die Ergebnisse werden in der unteren Hälfte des Fensters angezeigt:

- **Eindeutige Identifikation:** der interne, eindeutige Name, der von macOS verwendet wird, um dieses Programm zu identifizieren (Einzelne ausführbare Programmdateien tragen üblicherweise keine solche Identifikation.)
- **Als heruntergeladen erkannt:** Ein **Ja**-Wert zeigt an, dass Quarantäne-Markierungen für dieses Programm gesetzt sind, somit also erkannt wurde, dass das ausgewählte Programm aus einer heruntergeladenen Datei (Download) stammt.
- **Heruntergeladen von:** Falls bestätigt wurde, dass es sich um ein heruntergeladenes Programm handelt, gibt dieser Eintrag die Quelle des Downloads an. Sie ist üblicherweise als Internet-Adresse (URL) des Servers ausgewiesen, der das Produkt ausgeliefert hat.
- **Immer noch in aktiver Quarantäne:** Hier gibt ein **Ja**-Wert an, dass die Quarantäne immer noch besteht, ein Benutzer, der das Programm öffnet, also erst bestätigen muss, dass er sich bewusst ist, dass die Dateien aus dem potenziell unsicheren Internet stammen.

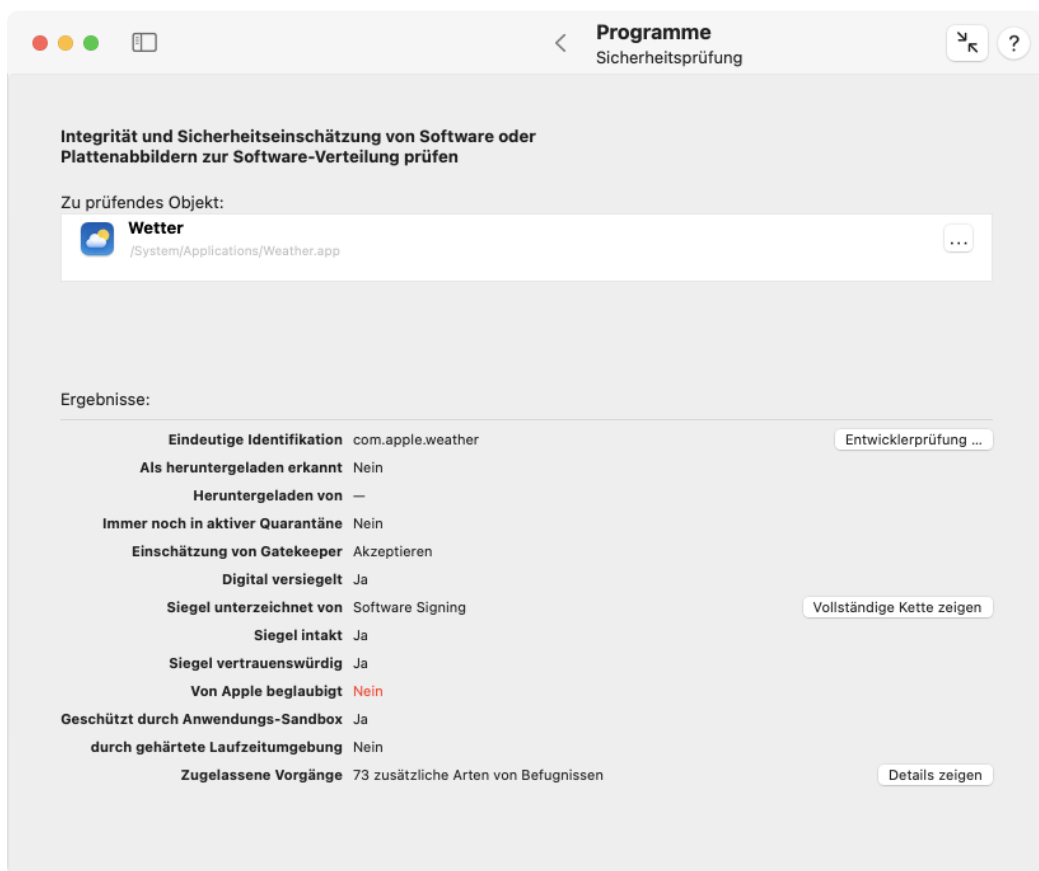


Abbildung 3.24: Sicherheitsprüfung

- **Einschätzung von Gatekeeper:** Diese Zeile zeigt das Ergebnis der offiziellen Auswertung durch die Gatekeeper-Komponente in macOS an, nachdem alle erwähnten Sicherheitsaspekte gemäß Ihrer Richtlinie, die zurzeit unter **Systemeinstellungen > Datenschutz & Sicherheit > Sicherheit > Apps erlauben, die geladen wurden von ...** eingestellt ist, überprüft wurden. Das mögliche Ergebnis ist entweder **Akzeptieren** oder **Ablehnen**.
- **Digital versiegelt:** Der Wert **Ja** zeigt an, dass die Software unterschrieben wurde und durch ein digitales Siegel geschützt wird.
- **Siegel unterzeichnet von:** Diese Zeile gibt den Namen derjenigen Institution an, die das Programm digital unterschrieben hat. Nach Drücken des Knopfes **Vollständige Kette zeigen** listet TinkerTool System die komplette Vertrauenskette auf, welche die Gültigkeit der digitalen Unterschrift bescheinigt. Die Einträge werden von unten nach oben in Rangfolge der Autorität aufgeführt. Der oberste Eintrag wiederholt den Namen der Institution, die die Software unterzeichnet hat. Die darauffolgenden Einträge bestätigen (gemäß der Zertifizierungsrichtlinien der jeweiligen Parteien), dass die Unterschrift der jeweils vorangehenden Zeile echt ist. Der Eintrag am Ende ist üblicherweise eine Zertifizierungsbehörde (CA, *Certificate Authority*) also die oberste Autorität dieser Vertrauenskette.
- **Siegel intakt:** Ein Wert **Ja** bestätigt, dass die ausgewählte Anwendung nicht verändert worden ist (in einer Weise, die vom Unterzeichner der Versiegelung nicht ausdrücklich zugelassen wäre), nachdem diese unterschrieben wurde.
- **Siegel vertrauensvoll:** Diese Angabe spiegelt den wichtigsten Aspekt der digitalen Signatur wider, nämlich ob das Siegel von einer Partei stammt, der Apple vertraut. Da Jeder mit den notwendigen technischen Kenntnissen ein ausführbares Programm versiegeln und unterzeichnen kann, ist dies der Punkt, der die Signatur wirklich aussagekräftig macht in Bezug auf die Frage, ob es sicher ist, das Programm laufen zu lassen. Die Vertrauensanzeige berücksichtigt außerdem, ob einige zusätzliche Sicherheitsprüfungen erfolgreich durchlaufen wurden, z.B. dass sich in einem Programm, das mehrere Code-Teile enthält, keine widersprüchlichen Unterschriften befinden.
- **Von Apple beglaubigt:** Falls die Komponente beglaubigt wurde, bestätigt das, dass die Software bestimmte grundlegende Sicherheitsanforderungen einhält. Apple hat außerdem überprüft, dass die Software zum Zeitpunkt ihrer Veröffentlichung „virusfrei“ war.
- **Geschützt durch Anwendungs-Sandbox:** Ein **Ja**-Wert gibt an, dass das ausgewählte Programm durch die Anwendungs-Sandbox von macOS geschützt wird, sobald das Programm gestartet wird.
- **... durch gehärtete Laufzeitumgebung:** Ein **Ja**-Wert bestätigt, dass das ausgewählte Programm durch die gehärtete Laufzeitumgebung selbstbeschränkt wird.
- **Zugelassene Vorgänge:** Drei mögliche Ergebnisse können hier angezeigt werden: Der Eintrag **Voller Sandbox-Schutz ohne Ausnahmen** gibt an, dass das ausgewählte Programm keinerlei Zugriff auf „ungewöhnliche“ Rechte hat. Apples Sandbox für Anwendungen wird mit den höchstmöglichen Sicherheitseinstellungen angewandt. Der Status **Nur durch Benutzerberechtigungen eingeschränkt** stellt das Gegenteil dar, nämlich dass überhaupt keine Sandbox zum Einsatz kommt. Ein Eintrag nach dem Muster **xx zusätzliche Arten von Befugnissen** bestätigt, dass das Programm

durch die Sandbox geschützt wird, aber Ausnahmen von den Standardregeln benötigt, die über eine Liste zusätzlicher Rechte festgelegt ist, die das Programm haben muss, um ordnungsgemäß laufen zu können. xx wird hierbei durch die tatsächliche Anzahl der Befugnistypen ersetzt. Um die vollständige Liste anzuzeigen, drücken Sie den Knopf **Details zeigen**. Die Tabelle im Detail-Dialogfenster beschreibt dann jede Befugnis, wobei – falls anwendbar – in der Spalte **Objekt** ein variabler Aspekt dieser Befugnis verzeichnet sein kann. Falls einem Programm zum Beispiel das Recht zugestanden werden soll, den Inhalt zweier Ordner A und B aus dem Privatorbinder des Benutzers auszulesen, ohne vorher den Benutzer darüber zu informieren, sind zwei Befugnisse des Typs **Lesezugriff auf angegebene Datei im Privatorbinder ohne Bestätigung** angegeben, wobei einer sich auf das Objekt ~/A und der andere sich auf das Objekt ~/B bezieht.

Viele Programme, die Teil von macOS sind, werden mit der Gatekeeper-Einschätzung **Ablehnen** angezeigt. Dies ist kein Fehler, sondern das korrekte Ergebnis. Die meisten Apples eingebauten Programme halten in der Tat Apples eigene Sicherheitsrichtlinien nicht ein. Dies spielt jedoch keine Rolle, da die betroffenen Programme nicht aus dem Internet heruntergeladen wurden und aus einer Quelle stammen, der Apple traut. Alle ausführbaren Dateien, die nicht die Form eines macOS-Programmpakets aufweisen, werden grundsätzlich von Gatekeeper abgelehnt. Beispiele sind Befehlszeilenprogramme oder Plugins. Dies ist das korrekte und beabsichtigte Verhalten.

Code kann anonym versiegelt werden, d.h. ohne eine gültige Unterschrift anzugeben. Dies wird als **Ad-Hoc-Signatur** bezeichnet und durch eine dementsprechende Markierung in der Zeile **Siegel unterzeichnet von** angegeben.

Ein Plattenabbild zur Softwareverteilung kann mehrere Programme enthalten. Wenn Sie eine solche Abbilddatei (DMG) testen, zeigt TinkerTool System nur die Sicherheitsbewertung für den Container selbst an. Daten, die ausschließlich Programme betreffen (wie Sandbox-Schutz), fehlen in der Übersicht. Eine versiegelte Abbilddatei sollte garantieren, dass deren prüfsummengeschützter Inhalt ebenso authentisch ist. Wenn Sie jedoch die tatsächlichen Prüfergebnisse für die einzelnen Programme sehen möchten, müssen Sie das Abbild öffnen und TinkerTool System auf eine der Dateien darin verweisen.

Nur moderne Plattenabbilder können signiert sein. Diese Sicherheitsfunktion wird hauptsächlich für Softwareprodukte eingesetzt, die sich an macOS 10.12 Sierra oder höher richten.

Apple hat eine Vielzahl von Befugnissen definiert, die undokumentiert bleiben, also der allgemeinen Öffentlichkeit nicht bekannt sind. Nur Apple und in einigen Fällen ein paar ausgewählte Entwickler, die Probleme mit der Sandbox über den Standardsatz von Befugnissen in ihren Programmen sonst nicht lösen konnten, haben die Erlaubnis, diese undokumentierten „Löcher“ in der Sandbox zu nutzen. TinkerTool System listet solche Befugnisse unter dem Stichwort **Inoffizielle Befugnis** auf und gibt den internen Namen an, den Apple für das diesbezügliche Recht verwendet.

Zusätzliche Prüfungen für Software-Entwickler (nur macOS Sonoma oder höher)

Falls Sie macOS 14 oder höher verwenden, bieten macOS und TinkerTool System zwei zusätzliche Prüfungen an, die für Entwickler unabhängiger Software interessant sind. Für Programme, die nicht für den Apple App Store, sondern für den unabhängigen Vertrieb entwickelt wurden, gelten andere Sicherheits- und „Verpackungs“-Regeln. Entwickler können testen, ob die derzeitigen Sicherheitseinstellungen, Signaturen und Paketierung eines Programms so gestaltet sind, dass dieses Programm

- bei Apples Beglaubigungsdienst eingereicht werden kann, oder
- dass es auf jedem beliebigen Computer eines Endkunden gestartet werden kann, d.h. nicht nur auf Entwicklungs-Macs des Anbieters.

Schlägt der Test fehl, wird Apple die Annahme des Programms verweigern, bzw. Gatekeeper wird den Start des Programms verhindern.

Die Ergebnisse der Tests werden teilweise in englischer Sprache angezeigt, was den Gepflogenheiten der Software-Entwicklung entspricht.

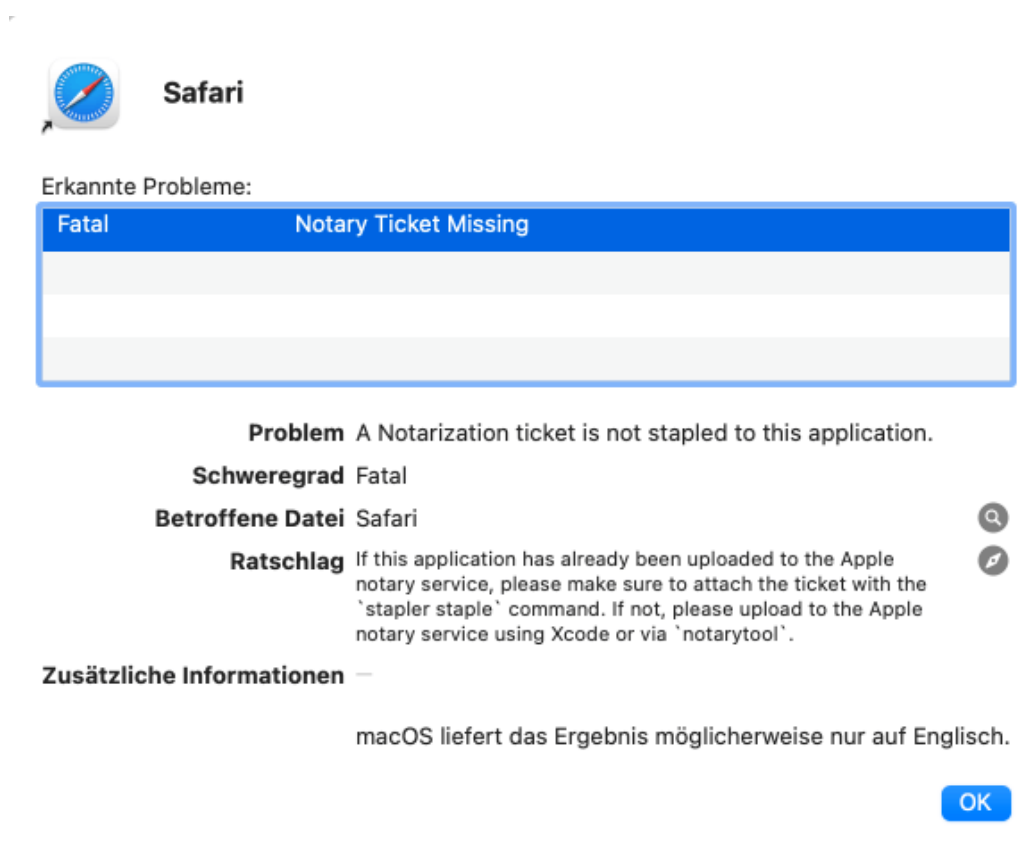


Abbildung 3.25: Beispiel für das Ergebnis einer Prüfung

Wenn Ihr System und das gerade gewählte Programm die Voraussetzungen erfüllen, können Sie die Tests wie folgt durchführen:

1. Betätigen Sie den Knopf **Entwicklerprüfung** ... rechts oben in der Ergebnisanzeige des Sicherheitstests.
2. Wählen Sie im Dialogfenster, welchen der beiden Tests Sie durchführen möchten.
3. Klicken Sie auf **Starten** oder drücken Sie den Zeilenschalter.

Nach etwas Wartezeit werden die Ergebnisse in einem weiteren Dialogfenster angezeigt. Alle erkannten Fehler, Probleme und Hinweise werden in einer Tabelle aufgelistet. Details

werden nach Anklicken einer Tabellenzeile im unteren Bereich des Fensters eingeblendet. Ist eine bestimmte Datei im Programmpaket betroffen, können Sie diese durch Anklicken des Lupensymbols im Finder aufdecken lassen. Stellt Apple Handbücher oder ähnliche Dokumentation mit näheren Informationen über dieses Problem bereit, können Sie diese durch Anklicken des Kompasssymbols über Ihren Standard-Webbrowser im Internet abrufen.

3.4 Die Einstellungskarte ACL-Rechte

3.4.1 Einführung in Berechtigungen

Jede Datei und jeder Ordner, die über Ihren Computer zugänglich sind, sind mit einer bestimmten Menge von Rechten verbunden, die festlegen, welche Benutzer welche Vorgänge mit diesen Objekten vornehmen dürfen, z.B. den Inhalt einer Datei zu lesen, oder eine Datei aus einem Ordner zu entfernen. Diese Menge von Rechten, die mit einem Dateisystemobjekt verbunden sind, werden *Berechtigungen* oder *Zugriffsrechte* genannt. macOS verwendet sowohl die klassischen Berechtigungen, die auf jedem UNIX-System zu finden sind, die sogenannten *POSIX-Berechtigungen*, als auch eine erweiterte Menge von berechtigungähnlichen Markierungen, die sogenannten *Speziellen Rechte* und eine fortgeschrittene Menge von Rechtedefinitionen, die von Microsoft® Windows, den meisten modernen UNIX-Systemen und vielen anderen Betriebssystemen verwendet werden, nämlich *Zugriffssteuerungslisten*, nach dem englischen Fachbegriff *Access Control Lists* auch *ACLs* abgekürzt. ACLs werden auch *POSIX.1e-Berechtigungen* genannt, da sie sich ähnlich zu einem Normentwurf mit dem Namen POSIX.1e verhalten, der ursprünglich dazu geplant war, eines Tages zum industrieweiten Standard für Berechtigungen zu werden. Die 1e-Dokumente sind allerdings aus verschiedenen Gründen offiziell zurückgezogen worden, so dass es eigentlich keine Norm mit diesem Namen gibt. Trotzdem enthält der 1e-Entwurf sehr gute Ideen, so dass Berechtigungen, die den Absichten von 1e sehr ähnlich sind, heute in den meisten Betriebssystemen vorhanden sind. Es sollte allerdings in Erinnerung bleiben, dass sich die genaue Bedeutung von ACL-Berechtigungen zwischen verschiedenen Betriebssystemanbietern leicht unterscheiden kann.

3.4.2 POSIX-Berechtigungen

Die minimale Menge von Berechtigungsdefinitionen, die auf allen UNIX-Systemen und vielen anderen Betriebssystemen zum Einsatz kommt, die sich an die POSIX-Norm (*IEEE 1003*) halten, basiert auf drei vordefinierten „Parteien“, denen Rechte gewährt werden können:

- dem **Eigentümer** des Objekts: Standardmäßig wird derjenige Benutzer, der ein Objekt anlegt, automatisch dessen Eigentümer.
- dem **Gruppeneigentümer** des Objekts: eine benannte Gruppe von Benutzern, die ebenso als spezielle Eigentümer des Objekts betrachtet werden. Auf einem UNIX-System muss jeder Benutzer Mitglied mindestens einer Benutzergruppe sein. Obwohl ein Benutzer Mitglied vieler verschiedener Gruppen sein kann, hat sie oder er immer eine bevorzugte Gruppe, die *Primärgruppe* genannt wird. Standardmäßig wird die Primärgruppe desjenigen Benutzers, der das Objekt anlegt, automatisch dessen Gruppeneigentümer.
- allen **anderen** Benutzern: diese Zugriffspartei ist als der „Rest“ definiert, nämlich alle verbleibenden Benutzer, die weder Eigentümer, noch Mitglied der Gruppeneigentümergruppe sind. Alle nicht identifizierten Benutzer, zum Beispiel Benutzer von ande-

ren Computern im Internet, die noch nicht über ihren Namen und Kennwort identifiziert wurden (oder überhaupt nicht identifiziert werden können), werden automatisch als Benutzer eines besonderen Benutzer-Accounts mit dem Namen **unknown** (unbekannt) angesehen, der zusätzlich Mitglied einer Primärgruppe ist, die ebenso **unknown** heißt. Das heißt, dass alle anderen Benutzer, egal ob das Betriebssystem diese identifizieren konnte oder nicht, in die Kategorie Andere einzuordnen sind. Diese zugreifende Partei bezieht sich in der Tat auf „den Rest der Welt“.

Apple bezeichnet diese dritte Kategorie mit dem Begriff **Jeder** oder **everyone**. Leider ist diese Bezeichnung falsch, da diese Kategorie ausdrücklich nicht den Eigentümer und kein Mitglied der Primärgruppe einschließt. Falls Sie über den Finder „Jedem“ ein Recht gewähren oder verweigern, sind diese Benutzer nicht eingeschlossen, was nicht unbedingt der Bedeutung des Begriffs „Jedem“ entspricht. Aus diesem Grund verwendet TinkerTool System nur die korrekte Bezeichnung „Andere“.

Für jede der drei Kategorien können die folgenden Zugriffsrechte gewährt werden:

- **Lesen:** die Berechtigung ein Objekt zu öffnen und dessen Inhalt zu lesen.
- **Schreiben:** die Berechtigung, dieses Objekt zu schreiben, was einschließt, es anzulegen, den Inhalt zu verändern, Daten hinten anzuhängen, usw.
- **Ausführen:** die Berechtigung, dieses Objekt auszuführen. Bei Programmen heißt das, dass die jeweilige Partei tatsächlich das Programm starten und laufen lassen darf, bei Ordnern heißt das, dass den betreffenden Benutzern erlaubt wird, den Inhalt des Ordners zu durchqueren. Beachten Sie, dass diese Berechtigung auch die Eigenschaft einer Markierung aufweist, die es erlaubt, zwischen ausführbaren und nicht ausführbaren Dateien zu unterscheiden, d.h. zwischen Programmen und anderen Datendateien.

Falls eines dieser Rechte einem Benutzer nicht ausdrücklich erteilt wird, bedeutet das, dass dieser Benutzer keine Erlaubnis für einen Zugriff hat. Das Recht wird verweigert, obwohl in diesem Modell keine ausdrücklichen Verbote vorgesehen sind.

Standardmäßig legen Programme Dateien mit den folgenden Berechtigungseinstellungen an:

- der aktuelle Benutzer wird Eigentümer und hat Lese- und Schreibberechtigung,
- die aktuelle Primärbenutzergruppe wird Gruppeneigentümer und hat Leseberechtigung,
- alle Anderen haben Leseberechtigung.
- Falls das Objekt ein Programm oder einen Ordner darstellt, werden zusätzlich Ausführungs-, bzw. Durchquerungsrechte für Benutzer, Gruppe und Andere gewährt.

Programme können bestimmten Dateien weniger Rechte gewähren, wenn sie dazu programmiert sind, sich so zu verhalten. Beispielsweise ist ein E-Mail-Programm so konstruiert, dass es „weiß“, dass ein neues Mail-Postfach vertraulich behandelt werden sollte, so dass es keine Berechtigungen für eine Gruppe oder Andere erteilt, wenn es einen Postfachordner anlegt. Nur der Eigentümer sollte in diesem Fall Lese- und Schreibrecht haben.

3.4.3 Zusätzliche Berechtigungsmarkierungen

macOS unterstützt des weiteren gewisse spezielle Berechtigungseinstellungen. Sie sind auf den meisten anderen UNIX-Systemen ebenso vorhanden.

- die **SUID**-Einstellung: SUID ist die Abkürzung für „*set user identification*“, also „setze Benutzeridentifikation“. Unter normalen Umständen hat jedes Programm, das von einem gewissen Benutzer gestartet wird, die Rechte dieses Benutzers. (Genau genommen ist ja das Starten und Laufenlassen von Programmen genau das, was ein Benutzer mit einem Computer tut, so dass der Satz „Benutzer A hat das Recht, den Vorgang B durchzuführen“ in Wirklichkeit bedeutet, „alle Programme, die von Benutzer A gestartet werden, haben das Recht, den Vorgang B durchzuführen“.) Die SUID-Einstellung erlaubt, dass bestimmte markierte Programme von dieser Grundregel abweichen. Falls eine SUID-Markierung für ein Programm gesetzt ist, heißt das „beim Lauf soll das Programm die Rechte seines Eigentümers haben, und nicht die Rechte des Benutzers, der das Programm gestartet hat“. Solch eine Ausnahmeregel wird für sehr spezielle Fälle benötigt, in denen kleine, eingeschränkte Programme Zugang zu Systembestandteilen erlangen müssen, die normalerweise geschützt sind. Wenn ein Benutzer beispielsweise sein Kennwort ändern möchte, muss das Programm, das diesen Vorgang durchführt, vorübergehend das Recht haben, die Datei zu ändern, die alle verschlüsselten Kennworte enthält, obwohl – in allen anderen Fällen – kein Benutzer jemals die Erlaubnis hat, diese Datei über „normale“ Programme zu lesen, geschweige denn zu schreiben. Die Verwendung der SUID-Markierung sollte auf sehr spezielle Fälle beschränkt sein. Sehr ernste Sicherheitsprobleme können auftreten, wenn die SUID-Markierung missbraucht wird.
- die **SGID**-Markierung: SGID ist die Abkürzung für „*set group identification*“, also „setze Gruppenidentifikation“. Im Prinzip ist dies das gleiche wie bei der SUID-Markierung, nur dass sie sich hier nicht auf den Benutzer und Dateieigentümer bezieht, sondern auf die Benutzergruppe und den Gruppeneigentümer.
- die **Sticky**-Markierung: Diese Markierung wurde ursprünglich dazu verwendet, um *residente* Programme kennzuzeichnen, d.h. Programme, die immer „im RAM kleben bleiben sollten“ (engl. *sticky* heißt *klebrig*) und nicht aus dem Speicher entfernt werden durften, selbst wenn das Programm beendet wurde. Bei Programmen, die sehr oft benutzt wurden, konnte dies zu Geschwindigkeitsverbesserungen führen, denn das Programm konnte bei späteren Starts direkt aus dem Speicher loslaufen und musste nicht mehr von Platte geladen werden. In heutigen Computern sind solche Mechanismen jedoch üblicherweise kontraproduktiv. Aus diesem Grund ergibt es keinen Sinn mehr, diese Markierung für Programme einzusetzen. Die Sticky-Markierung hat jedoch eine andere Bedeutung, wenn sie auf Ordner angewandt wird und dieser Aspekt wird auch von macOS unterstützt: Ein Ordner, bei dem die Sticky-Markierung eingeschaltet ist, wird zu einem „Nur-Hinzufüge-Ordner“, oder genauer, zu einem Ordner, bei dem die Löschung von Dateien eingeschränkt wird. Eine Datei in einem Sticky-Ordner kann nur dann von einem Benutzer entfernt oder umbenannt werden, wenn der Benutzer Schreibrecht für den Ordner hat und gleichzeitig entweder Eigentümer der Datei oder Eigentümer des Ordners ist. Die Sticky-Einstellung wird üblicherweise für „öffentliche“ Ordner verwendet, wo zwar Jeder Schreibrecht haben sollte, jedoch Benutzer nicht das Recht haben dürfen, sich gegenseitig die Dateien zu löschen.

3.4.4 Zugriffssteuerungslisten

Einführung in Zugriffssteuerungslisten

Zugriffssteuerungslisten, auf Englisch *Access Control Lists* oder kurz *ACLs*, sind eine Ergänzung zu den vorhandenen POSIX-Berechtigungen, d.h. man muss ACLs nicht unbedingt nutzen, wenn man diese nicht braucht. Die althergebrachten Regeln für Zugriffsrechte, die oben skizziert wurden, gelten auch weiterhin, nur einige Zusatzregeln können auf Wunsch hinzugefügt werden.

Technisch gesehen ist eine Zugriffssteuerungsliste eine Liste einzelner Zugriffsrechte, die an ein Dateisystemobjekt angeknüpft werden kann. Die ACL kann entweder leer sein – in diesem Fall gelten nur die herkömmlichen POSIX-Rechte – oder sie kann ein oder mehrere Objekte enthalten, die *Zugriffssteuerungseinträge* (*Access Control Entries* oder *ACEs*) genannt werden. Ein Zugriffssteuerungseintrag gibt Auskunft über die folgenden Aspekte:

- auf *welche Benutzer* bezieht sich dieser Eintrag (dies kann ein einzelner Benutzer oder eine Benutzergruppe sein)?
- *erlaubt* oder *verweigert* dieser Eintrag den Zugriff?
- welche *Rechte* werden im Detail erlaubt, bzw. verweigert?
- wie soll dieser Eintrag von einem Ordner auf den Inhalt dieses Ordners *vererbt* werden?

ACL-Rechte

Zugriffssteuerungslisten erlauben die Definition von 13 einzelnen Zugriffsrechten auf ein Dateisystemobjekt:

- **Daten lesen/Ordnerinhalt auflisten:** das Recht, Daten aus einer Datei zu lesen oder den Inhalt eines Ordners aufzulisten.
- **Datei ausführen/Ordner durchqueren:** das Recht, eine Datei als Programm auszuführen oder – falls es sich um einen Ordner handelt – das Recht, diesen Ordner zu durchqueren, um einen enthaltenen Ordner zu öffnen.
- **Attribute lesen:** das Recht, die Attribute einer Datei oder eines Ordners zu lesen, z.B. das Erstellungsdatum.
- **Erweiterte Attribute lesen:** das Recht, erweiterte Attribute einer Datei oder eines Ordners zu lesen. Erweiterte Attribute sind zum Beispiel Spotlight-Kommentare oder die Quarantänedaten einer Datei.
- **Zugriffsrechte lesen:** das Recht, die Zugriffsberechtigungen einer Datei oder eines Ordners zu lesen.
- **Daten schreiben/Dateien anlegen:** das Recht, Daten in eine Datei zu schreiben oder – falls es sich um einen Ordner handelt – das Recht, eine neue Datei in diesem Ordner anzulegen.
- **Daten anhängen/Ordner anlegen:** das Recht, zusätzliche Daten an eine Datei anzuhängen oder – falls es sich um einen Ordner handelt – das Recht, einen neuen Ordner in diesem Ordner anzulegen.
- **Attribute schreiben:** das Recht, die Attribute einer Datei oder eines Ordners zu schreiben, z.B. das Erstellungsdatum.

- **Erweiterte Attribute schreiben:** das Recht, erweiterte Attribute einer Datei oder eines Ordners zu schreiben. Erweiterte Attribute sind z.B. Spotlight-Kommentare oder die Quarantänedaten einer Datei.
- **Löschen:** das Recht, diese Datei oder diesen Ordner zu löschen.
- **Unterordner und Dateien löschen:** wenn es sich um einen Ordner handelt, das Recht, darin enthaltene Objekte zu löschen.
- **Zugriffsrechte ändern:** das Recht, Zugriffsrechte für diese Datei oder diesen Ordner zu ändern.
- **Eigentümer ändern:** das Recht, den Eigentümer dieser Datei oder dieses Ordners zu ändern.

Diese Rechte können in jeder beliebigen Weise miteinander kombiniert werden.

ACL-Vererbungseinstellungen

Jeder Zugriffssteuerungseintrag kann zusätzliche Informationen darüber enthalten, wie dieser Eintrag an Objekte tiefer in der Dateisystemhierarchie vererbt werden soll, z.B. an eine Datei in einem Ordner, der in einem anderen Ordner liegt. Der Ordner an der Spitze kann mit einer Zugriffssteuerungsliste ausgestattet sein, die automatisch an Objekte in diesem Ordner vererbt wird.

Vererbung findet nur dann statt, wenn Objekte neu angelegt werden. Wenn zum Beispiel eine Datei B in einem Ordner A angelegt wird, dann erbt die Datei B nur in diesem Moment Zugriffssteuerungseinträge von A. Wenn jemand die Berechtigungen für B zu einem späteren Zeitpunkt ändert, wird das System nicht automatisch eine erneute Vererbung von A an B erzwingen. Auch eine Änderung der Zugriffssteuerungseinträge von Ordner A wird nicht an das bereits existierende Objekt B „wiedervererbt“.

Es gibt 4 verschiedene Einstellungen, die steuern, wie die Rechte von Zugriffssteuerungslisten vererbt werden:

- **auf diesen Ordner anwenden:** die ACL-Berechtigungseinstellungen sollen auf den Ordner selbst wirksam werden.
- **auf Unterordner anwenden:** die ACL-Berechtigungseinstellungen sollen auf Ordner vererbt werden, die sich im aktuellen Ordner befinden.
- **auf enthaltene Dateien anwenden:** die ACL-Berechtigungseinstellungen sollen auf Dateien vererbt werden, die sich im aktuellen Ordner befinden.
- **auf alle Unterordnerebenen anwenden:** Die Vererbung von ACL-Einstellungen soll nicht auf der Ebene des aktuellen Ordners stoppen, sondern auch auf allen tieferen Ebenen von verschachtelten Ordnern wirksam werden.

Es gibt 16 mögliche Kombinationen dieser Einstellungen, von denen aber nur 12 in der Praxis wirklich sinnvoll sind.

Geerbte und explizite Einträge

Da Einstellungen in Zugriffssteuerungseinträgen von Ordner auf Objekte, die in ihnen enthalten sind, vererbt werden können, muss das System nachverfolgen, welche Zugriffssteuerungseinträge in einer Zugriffssteuerungsliste vererbt worden sind und welche nicht. Nur Zugriffssteuerungseinträge, die nicht geerbt wurden, können geändert werden. Nicht geerbte Einträge werden *explizite* Einträge genannt. Um einen geerbten Eintrag zu ändern, ist es entweder nötig, den Eintrag auf derjenigen Elternebene zu ändern, von der aus er vererbt worden ist, oder die Zugriffssteuerungsliste für dieses Objekt zu löschen (und damit die Vererbung zu unterbrechen), und danach die vererbten Einträge durch explizite zu ersetzen.

Die Auswertungsregeln für Zugriffssteuerungseinträge

Wie schon erwähnt besteht eine Zugriffssteuerungsliste aus einer Reihe von Zugriffssteuerungseinträgen. Gewisse Regeln legen fest, wie macOS diese Einträge auswertet, wenn ein bestimmter Benutzer auf ein Objekt im Dateisystem zugreifen möchte. Beachten Sie, dass Zugriffssteuerungseinträge sich auch widersprechen können. Wenn Benutzer A beispielsweise auf Datei B zugreifen darf, aber A gleichzeitig Mitglied einer Benutzergruppe ist, der der Zugriff auf die Datei B verweigert wird, liegt ein Widerspruch vor, der aufgelöst werden muss. Es gelten die folgenden Regeln:

- Die Zugriffssteuerungseinträge in einer Zugriffssteuerungsliste werden von oben nach unten abgearbeitet. Der erste Zugriffssteuerungseintrag, der auf den jeweiligen Benutzer passt, „gewinnt“ und gewährt dementsprechend Zugriff oder verweigert ihn.
- Die herkömmlichen POSIX-Berechtigungen werden geprüft, nachdem die ACL verarbeitet wurde. Wenn ein Dateisystemobjekt keine Zugriffssteuerungsliste besitzt, dann gelten nur die POSIX-Berechtigungen.

Wichtige Empfehlungen

Zugriffssteuerungslisten sind ein leistungsfähiges Werkzeug, um bestimmte Berechtigungen fein gegliedert vergeben zu können. Sie sollten allerdings im Auge behalten, dass Zugriffssteuerungslisten sehr komplex sind.

Es gibt 13 unterschiedliche Rechte, die gewährt oder verweigert werden können und 12 verschiedene Arten, die Vererbung zu definieren. Daraus ergibt sich eine Summe von $2^{13} \cdot 12 = 98.304$ unterschiedlichen Begriffen von Zugriffsrechten, die Sie definieren können.

Jedes dieser fast 100.000 Zugriffsrechte kann auf einen Benutzer oder eine Benutzergruppe angewandt werden, um daraus einen Zugriffssteuerungseintrag zu erstellen und eine fast unbegrenzte Anzahl von Zugriffssteuerungseinträgen kann zu einer Zugriffssteuerungsliste zusammengestellt werden. Jeder Datei und jedem Ordner Ihres Systems kann eine unterschiedliche Zugriffssteuerungsliste zugewiesen werden, so dass die Wartung aller dieser Einträge leicht in einem Albtraum enden kann. Aus diesem Grund sollten Sie bei Verwendung von Zugriffssteuerungslisten nur mit größter Sorgfalt arbeiten.

- Verwenden Sie Berechtigungseinstellungen über Zugriffssteuerungslisten nur dann, wenn es notwendig ist, d.h. nur dann, wenn es ein Berechtigungsproblem gibt, das mit konventionellen POSIX-Berechtigungen nicht gelöst werden kann.

- Verwenden Sie so wenig Benutzergruppen wie möglich. Überorganisieren Sie Ihre Benutzer nicht.
- Vermeiden Sie es, Zugriffssteuerungseinträge für Benutzer zu erstellen. Falls möglich, wenden Sie sie auf Benutzergruppen an.
- Falls Sie bestimmte Dateien schützen wollen, verwenden Sie POSIX-Berechtigungen, um sehr eingeschränkte Zugriffsrechte zu definieren, und definieren danach so wenig Zugriffssteuerungseinträge wie möglich, um denjenigen Benutzergruppen Berechtigungen zu gewähren, die Zugriff haben sollen.
- Verwenden Sie Vererbung, wann immer es möglich erscheint. Wenn Sie Berechtigungen vererben, brauchen Sie nur eine kleine Anzahl von Zugriffssteuerungslisten für ein paar übergeordnete Ordner zu warten.
- Vermeiden Sie die Zugriffssteuerungseinträge des Typs „Verweigern“. Verbote können unerwartete Nebenwirkungen haben. Sie könnten unbeabsichtigt selbst das Zugriffsrecht für einige Objekte verlieren, oder noch schlimmer, außerdem das Recht verlieren, diese Einschränkung wieder aufheben zu können.
- Wenden Sie Zugriffssteuerungseinträge niemals auf Teile von macOS an und versuchen Sie nicht, die Zugriffsrechte auf Systemdateien zu verändern. Der Computer könnte unbenutzbar werden.

Dateisysteme, die Zugriffssteuerungslisten unterstützen

Zugriffssteuerungslisten können nur auf Dateisystemen verwendet werden, die sie auch speichern können. macOS erlaubt die Verwendung von ACLs auf den folgenden Dateisystemen, unter der Voraussetzung, dass die Computer, die diese Dateisysteme beherbergen, eine Betriebssystemversion einsetzen, die generell mit ACLs umgehen kann:

- Platten-Volumes, die mit dem System Mac OS Extended (HFS+) oder mit dem Apple File System (APFS) formatiert sind,
- Netz-Volumes, auf die mit dem Apple-Filing-Protokoll (AFP, AppleShare) zugegriffen wird,
- Netz-Volumes, auf die mit dem SMB/CIFS-Protokoll (Microsoft® Windows) zugegriffen wird,
- Netz-Volumes, auf die mit dem NFS-Protokoll Version 4 (moderne UNIX-Systeme; macOS kann NFSv4 nur als Klient, jedoch nicht als Server unterstützen) zugegriffen wird.

Andere Dateisysteme, einschließlich Platten-Volumes, die unter Verwendung von UFS, FAT, VFAT, FAT32, ExFAT, NTFS oder ZFS formatiert wurden, oder Netz-Volumes, auf die mit NFSv2, NFSv3, FTP oder WebDAV zugegriffen wird, können Zugriffssteuerungslisten nicht unterstützen. Über eine Dateiserver-Verbindung hinweg ACLs nicht unterstützen zu können, bedeutet, dass der Client-Computer die auf dem Server gespeicherten ACLs nicht „sehen“ oder ändern kann. Wenn der Server jedoch in der Lage ist, ACLs auf seiner Seite zu verwenden, wird er diese beachten, egal ob der zugreifende Computer dies bemerkt oder nicht.

3.4.5 Zugriffsrechte zeigen oder einstellen

Anzeigen von Berechtigungen

TinkerTool System kann die vollständige Menge von POSIX- und ACL-Zugriffsrechten anzeigen, die zurzeit für eine bestimmte Datei oder einen bestimmten Ordner eingestellt sind. Die Berechtigungen werden in einer übersichtlichen Tabelle angezeigt, in der die Einträge in der Reihenfolge angeordnet sind, wie sie auch zur Bestimmung der Wirksamkeit vom System ausgewertet werden. Die Tabelle wird auch dazu verwendet, die Berechtigungseinstellungen zu ändern.

Der Finder von macOS ist nicht in der Lage, die „wahren“ Berechtigungseinstellungen eines Dateisystemobjekts zu zeigen. Aufgrund mehrerer Konstruktionsfehler wird im Abschnitt **Teilen & Zugriffsrechte** des Dialogfensters **Informationen** des Finders nur eine sehr vereinfachte oder sogar falsche Zusammenfassung der Berechtigungseinstellungen gezeigt. TinkerTool System zeigt dagegen die wahren Einstellungen an, wie sie vom Kernbetriebssystem definiert und gespeichert werden. Aus diesem Grund können einige Berechtigungsdetails sich bei der Anzeige in beiden Programmen voneinander unterscheiden. In solch einem Fall sollten Sie der Anzeige des Finders nicht trauen.

Um die aktuellen Berechtigungseinstellungen eines Dateisystemobjekts anzuzeigen oder zu ändern, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Zugriffsrechte zeigen oder einstellen** auf der Einstellungskarte **ACL-Rechte**.
2. Ziehen Sie eine Datei oder einen Ordner aus dem Finder in das Feld **Datei oder Ordner**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Die aktuellen Einstellungen werden in der Tabelle angezeigt.

Überschriftenzeilen in der Tabelle geben an, welche Rechte ACEs einer ACL darstellen und welche auf konventionellen POSIX-Einstellungen beruhen. Die Spalten enthalten die folgenden Informationen:

- den Benutzer oder die Gruppe, für die ein Eintrag wirksam wird,
- der Typ des Eintrags, und zwar ob er den Zugriff erlaubt oder verweigert,
- die Berechtigungseinstellung in einfachen Worten,
- eine Markierung, ob der Eintrag ererbt oder explizit ist,
- die Vererbungseinstellungen.

Falls eine Berechtigung als **Eigene** angezeigt wird, bedeutet das, dass sich die Rechte nicht mit einfachen Worten wie **Nur Lesen** beschreiben lassen. Erinnern Sie sich daran, dass es 98.304 verschiedene Begriffe von Berechtigungen geben kann, die sich durch Kombination von ACL-Rechten definieren lassen. Um die 13 Detailrechte und 4 Vererbungseinstellungen (für Ordner) genauer zu sehen, doppelklicken Sie auf eine Tabellenzeile. Sie können alternativ auch auf den Knopf mit dem Stiftsymbol unterhalb der Tabelle drücken.

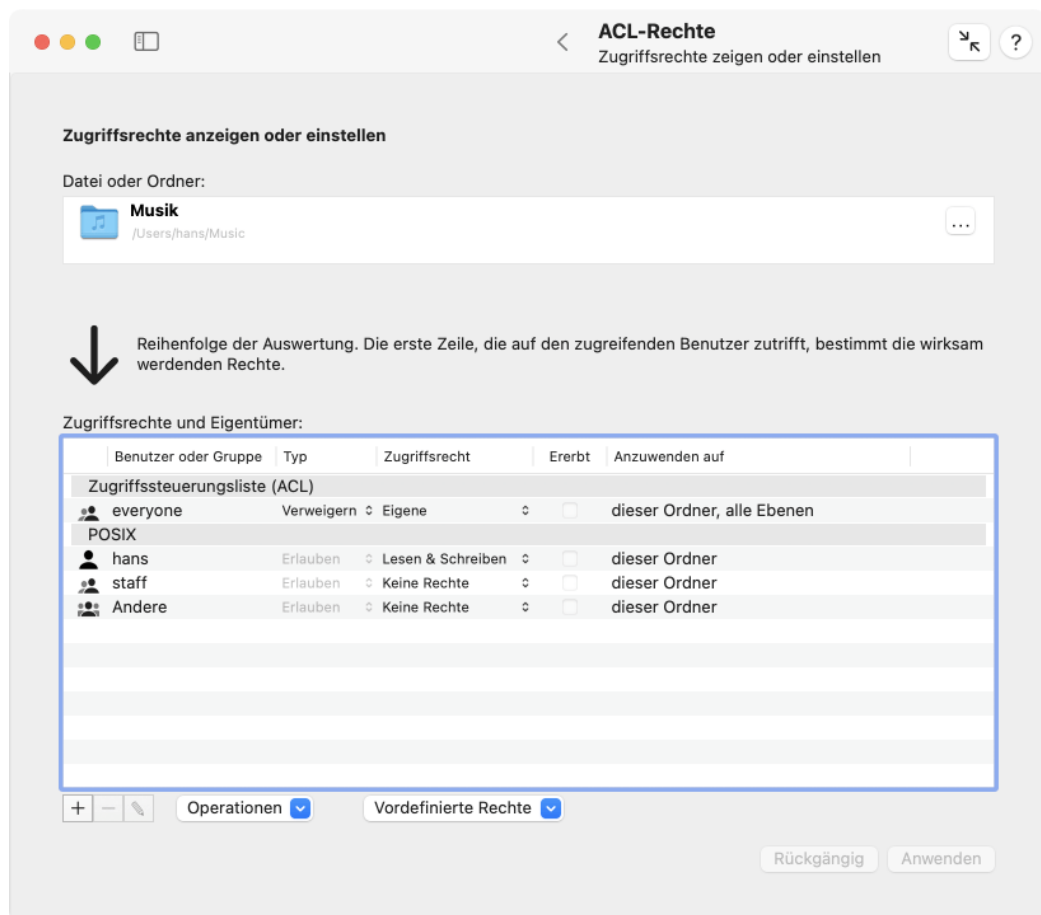


Abbildung 3.26: Zugriffsrechte zeigen oder einstellen

In Fällen, in denen ACL-Rechte oder sogar Berechtigungen im Allgemeinen nicht für das ausgewählte Objekt unterstützt werden, erscheint eine rote Warnung unter der Box **Datei oder Ordner**, zusammen mit einem Fragezeichen-Hilfeknopf. Sie können diesen Knopf drücken, um detaillierte Hinweise darüber zu erhalten, warum es Probleme beim Abrufen oder Ändern von Rechten auf dem betroffenen Volume geben könnte.

Es kann niemals ein Dateisystemobjekt ohne Berechtigungseinstellungen geben, weshalb macOS automatisch die Rechte anderer Systeme in „plausible“ Berechtigungen für das lokale System umwandelt, falls das nötig sein sollte, oder künstliche Rechte vollständig neu erzeugt, ohne dass diese tatsächlich auf dem Volume gespeichert werden. TinkerTool System zeigt in einem solchen Fall die wirksamen Rechte an, die das System für Ihren derzeitigen Benutzer-Account simuliert. Sie sollten aber im Auge behalten, dass Prozesse, die für andere Benutzer laufen, möglicherweise andere Einstellungswerte erhalten. Es ist auch möglich, solche künstlichen Berechtigungen zu ändern und abzuspeichern, aber macOS wird diese für das betreffende Volume beim Anwenden „zurückübersetzen“, so dass das Ergebnis vielleicht nicht mit dem übereinstimmt, was Sie erwarten. Wir empfehlen es nicht, neue Berechtigungseinstellungen in Fällen anzuwenden, in denen TinkerTool System eine Unterstützungswarnung anzeigt.

Ändern von Berechtigungen

Nachdem Sie ein Objekt ausgewählt haben und TinkerTool System dessen Berechtigungseinstellungen in der Tabelle anzeigt, können alle Aspekte der Einstellungen geändert werden. Nachdem Sie alle gewünschten Änderungen vorgenommen haben, können Sie den Knopf **Anwenden** in der rechten unteren Ecke drücken, um die aktuellen Einstellungen abzuspeichern. Der Knopf **Rückgängig** verwirft dagegen alle Änderungen, die Sie gemacht haben und TinkerTool System kehrt wieder zu den ursprünglichen Einstellungen zurück, die für das in Frage kommende Objekt zurzeit gespeichert sind.

Falls Sie den **Typ** eines Eintrags ändern möchten oder das **Zugriffsrecht** auf eines der einfachen Standardkonzepte ändern möchten, können Sie dies über die Aufklappmenüs in den jeweiligen Tabellenspalten erreichen.

Um den Benutzer oder die Gruppe eines Eintrags zu ändern, führen Sie die folgenden Schritte durch:

1. Doppelklicken Sie die entsprechende Zeile in der Tabelle oder wählen Sie die Zeile aus und drücken Sie den Knopf mit dem Stift.
2. Drücken Sie im Detailfenster den Knopf **Einstellen ...** am oberen Rand.
3. Wählen Sie im neuen Dialogfenster entweder **Benutzer** oder **Gruppen** (falls zutreffend).
4. Wählen Sie einen Benutzer oder eine Gruppe aus der Tabelle aus und drücken Sie den Knopf **OK**.
5. Betätigen Sie im Detailfenster den Knopf **Schließen**.

Der Zugriffstyp und die Detailrechte können auf die gleiche Art und Weise geändert werden. Beachten Sie, dass das Detailfenster die Rechte und Vererbungseinstellungen in vier Kategorien gruppiert. Sie können alle Rechte einer Kategorie gleichzeitig ein- oder ausschalten, indem Sie das entsprechende Häkchen in der jeweiligen Gruppenüberschrift ändern. Alle Rechte einer ACE einzuschalten ist außerdem über den Punkt **Vollzugriff** im

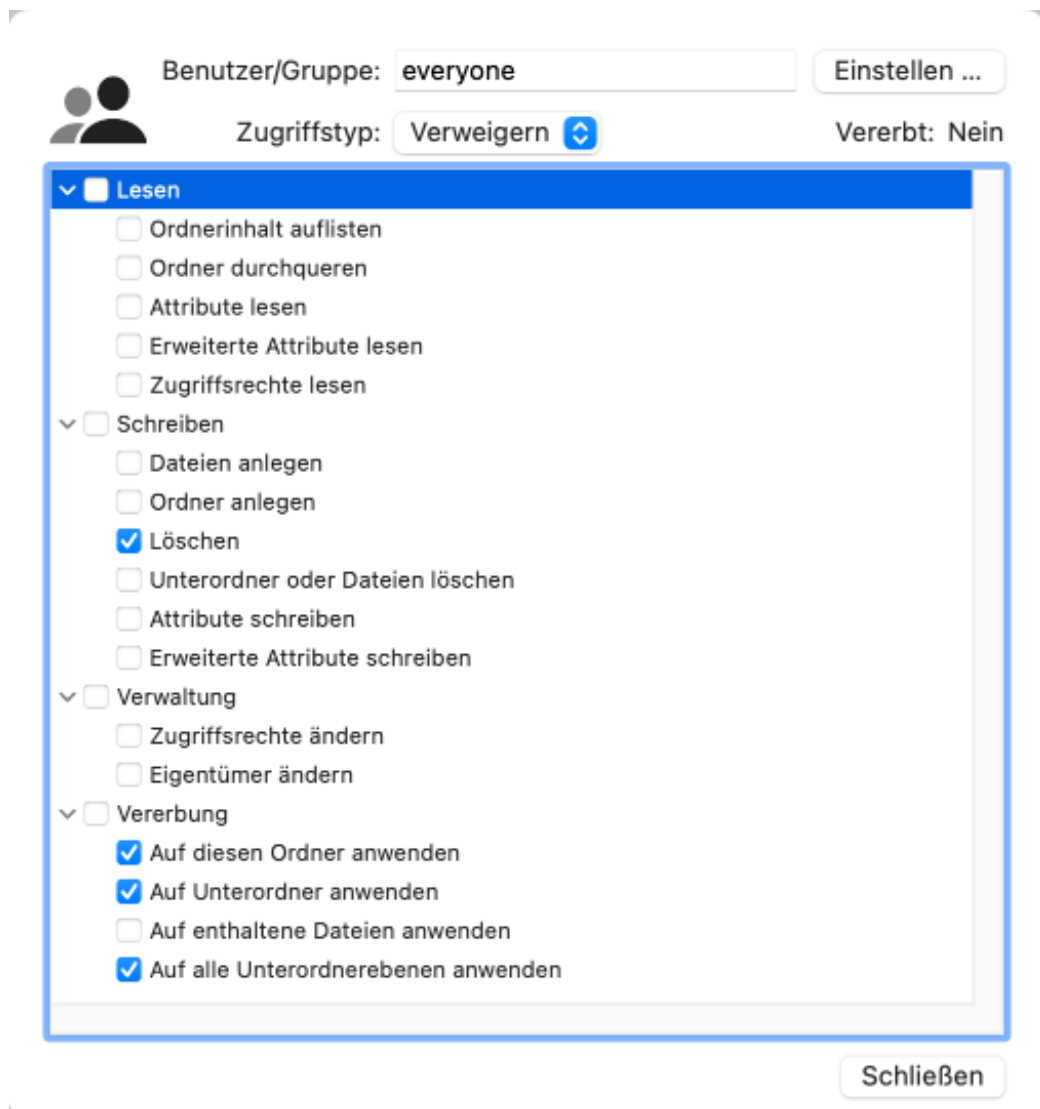


Abbildung 3.27: Berechtigungseinstellungen im Detail

Klappmenü **Zugriffsrecht** möglich. Die Vererbungseinstellungen werden in diesem Fall auf Standardwerte gesetzt.

Um einen Zugriffssteuerungseintrag hinzuzufügen, drücken Sie den Knopf [+] unter der Tabelle. Um einen oder mehrere ACEs zu entfernen, verwenden Sie den Knopf [-]. Um eine ACL umzusortieren, ziehen Sie eine Zeile aus dem ACE-Bereich der Tabelle und legen diese an einer neuen Position ab. Beachten Sie, dass Objekte grundsätzlich wohldefinierte POSIX-Berechtigungen haben und dass POSIX-Berechtigungen immer in der vordefinierten Reihenfolge Benutzer-Gruppe-Andere ausgewertet werden, so dass es nicht möglich ist, Zeilen unterhalb der POSIX-Überschrift zu entfernen oder umzusortieren.

Die Auswahl von Benutzern und Gruppen

Sie müssen möglicherweise einen Benutzer oder eine Gruppe auswählen, wenn Sie Änderungen an Zugriffsrechten vornehmen. TinkerTool System verwendet in diesem Zusammenhang mehrere Arten von Dialogfenstern, in denen Sie leicht einen Eintrag aus einer Liste von Accounts auswählen können, die auf Ihrem Computer verfügbar sind.

In großen Organisationen kann die Liste der Accounts sehr lang sein. In einigen Fällen ist sie vielleicht nicht alleine auf dem lokalen Computer gespeichert, sondern auch auf anderen Computern (*Verzeichnisdienstservern*) in Ihrem Netz, die erst kontaktiert werden müssen. Aus Effizienzgründen zeigt TinkerTool System möglicherweise nicht die vollständige Liste der Accounts, wenn Sie einen Benutzer- oder Gruppendialog das erste Mal öffnen. Die Liste kann auf diejenigen Accounts beschränkt sein, die irgendwo im Betriebssystem benötigt wurden, seitdem der Computer gestartet ist. Um die volle Account-Liste abzurufen, betätigen Sie den Knopf **Alle Einträge holen** in der linken unteren Ecke des Fensters. Dies stellt sicher, dass die Liste der Benutzer oder Gruppen vollständig ist.

Das Abrufen aller Einträge kann eine erhebliche Zeit in Anspruch nehmen, besonders in Umgebungen mit Verzeichnisdienstservern.

Zusätzliche Operationen

Zusätzliche Operationen können durchgeführt werden, indem Sie einen der Punkte im Klappmenü **Operationen** am unteren Rand des Fensters wählen. Die Punkte ändern sich, je nach dem, ob Sie eine Datei oder einen Ordner ausgewählt haben.

Falls Sie einen Ordner gewählt haben, können Sie:

- **Zugriffssteuerungsliste kanonisch sortieren:** Dies bedeutet, dass die ACL in eine empfohlene Reihenfolge gebracht wird, die als „normal“ angesehen wird. Die kanonische Sortierreihenfolge ist: explizite Verweigern-Einträge, explizite Einträge für Erlauben, geerbte Verweigern-Einträge, geerbte Erlauben-Einträge.
- **Geerbte Einträge entfernen:** ACEs, die von Objekten auf höheren Ebenen in der Ordnerhierarchie geerbt wurden, werden entfernt.
- **Vererbte Einträge explizit machen:** alle geerbten ACEs werden durch explizite Einträge mit dem gleichen Inhalt ersetzt.
- **Alle ACLs in diesem Ordner entfernen:** alle Zugriffssteuerungslisten werden von diesem Ordner und allen Dateien und Ordnern, die dieser Ordner enthält, entfernt. Nur die POSIX-Rechte bleiben erhalten.
- **Zugriffsrechte übertragen:** Diese Funktion kann dazu benutzt werden, die Berechtigungseinstellungen des aktuellen Ordners auf alle Objekte zu übertragen, die sich

auf tieferen Ebenen in der Ordnerhierarchie befinden. TinkerTool System fragt danach, welche Kategorien von Berechtigungen Sie im einzelnen übertragen möchten. Sie können jede beliebige Kombination von **Eigentümer**, **Gruppeneigentümer**, **Eigentümerrechte**, **Gruppenrechte**, **Rechte für Andere** und **Zugriffssteuerungsliste (ACL)** übertragen. Dies stellt alle ausgewählten Berechtigungen aller Objekte, die im gewählten Ordner enthalten sind, vollständig zurück. Aus Sicherheitsgründen werden Objekte mit speziellen Berechtigungseinstellungen (SUID und GUID) automatisch von diesem Vorgang ausgeschlossen.

Es gibt eine zusätzliche Wahlmöglichkeit beim Übertragen von Zugriffssteuerungslisten: Es ist entweder möglich, die existierende Zugriffssteuerungsliste des obersten Orders zu *kopieren* so wie sie ist, oder TinkerTool System im Nachhinein *Vererbung simulieren* zu lassen. Im letzteren Fall können die Vererbungsattribute des obersten Ordners dazu führen, dass das Ergebnis unterschiedlich ist. Wenn im obersten Ordner beispielsweise die Option **auf alle Unterordnerebenen anwenden** für eine bestimmte ACE *nicht* eingeschaltet ist, wird die Vererbung dieser ACE nach der obersten Ebene stoppen.

Eine andere Wahlmöglichkeit steuert, wie TinkerTool System mit Objekten umgehen soll, bei denen das Attribut „geschützt“ gesetzt ist. Das Standardverhalten von macOS ist es, das Übertragen zu stoppen und den laufenden Vorgang mit einer Fehlermeldung abzubrechen sobald ein solches Objekt gefunden wird, denn macOS erlaubt es nicht, die Berechtigungseinstellungen eines geschützten Objekts zu ändern. Die Richtlinie, den Vorgang anzuhalten, stellt sicher, dass es keine unerkannten Sicherheitsprobleme geben kann, die auftreten könnten, wenn die Zugriffsrechte für ein geschütztes Objekt unerwartet unverändert bleiben. Möglicherweise möchten Sie aber solche Fälle ignorieren und den Vorgang stillschweigend fortsetzen, was das Verhalten alter Versionen von macOS Server war.

Beim Übertragen von Berechtigungen in Ordnern, die symbolische Links enthalten, bearbeitet das Programm die Links selbst. Die Objekte, auf die die Links verweisen, bleiben unverändert. Ordner, auf die von einem Link verwiesen wird, werden nicht durchschritten. Zugriffssteuerungslisten werden nicht auf symbolische Links übertragen, da macOS dies nicht unterstützt.

Falls Sie sicherstellen möchten, dass kein Objekt beim Übertragen von Berechtigungen ausgelassen wird, ist es empfehlenswert, alle Schutzattribute vor dem Übertragen zu entfernen. Sie können dies mit der Funktion **Schutz** auf der Karte Ablage (Abschnitt 3 auf Seite 145) tun.

Der Übertragungsvorgang wird automatisch auf das Volume beschränkt, auf dem der oberste Ordner liegt.

Falls Sie eine Datei ausgewählt haben, können Sie:

- **Zugriffssteuerungsliste kanonisch sortieren:** siehe oben.
- **Zugriffssteuerungsliste entfernen:** hierdurch wird die gesamte ACL entfernt.
- **Geerbte Zugriffssteuerungsliste holen:** TinkerTool System lädt hierbei eine neue ACL, basierend auf der Zugriffssteuerungsliste, die macOS für neue Dateien in diesem Ordner anlegt und basierend auf den aktuellen Vererbungseinstellungen, die in diesem Ordner wirksam sind.

Mit Ausnahme der Funktion zum Übertragen von Rechten, ändern alle Operationen zunächst nur den Inhalt der Berechtigungstabelle, nicht die eigentlichen Einstellungen auf der Platte. Die Änderungen werden wirksam, nachdem Sie den Knopf **Anwenden** gedrückt haben.

Speichern und Wiederverwenden von Rechten

In der Praxis kann es vorkommen, dass Sie eine ganz bestimmte Vergabe von Rechten mehrfach auf verschiedene Objekte anwenden möchten, z.B. Zugriffsrechte für mehrere Netzwerkfreigaben, die sich auf unterschiedlichen Volumes befinden. Um zu vermeiden, dass Sie alle Einstellungen für Benutzer, Gruppen, Zugriffssteuerungseinträge und deren Optionen immer wieder neu angeben müssen, können Sie sich eine einmal gemachte Definition von Rechten auf Wunsch im Programm speichern und auf dem gleichen Computer später noch einmal aufrufen und für ein anderen Eintrag im Dateisystem wiederverwenden. TinkerTool System bezeichnet dies als *Vordefinieren von Rechten*. Die zugehörigen Funktionen werden über den Menüknopf **Vordefinierte Rechte** aufgerufen.

Nachdem Sie alle Zugriffsrechte für ein Objekt eingestellt und angewandt haben, können Sie den zugehörigen Satz von Einstellungen wie folgt noch einmal unabhängig von diesem Objekt im Programm speichern:

1. Stellen Sie sicher, dass TinkerTool System den gewünschten Satz von Rechteeinstellungen auf dem Unterpunkt **Zugriffsrechte zeigen oder einstellen** in der Tabelle anzeigt und diese Einstellungen bereits angewandt sind (der Knopf **Anwenden** ist grau). Sie können die Rechte eines bestehenden Objekts jederzeit in das Programm laden, indem Sie es bei **Datei oder Ordner** auswählen.
2. Wählen Sie über den Knopf **Vordefinierte Rechte** den Menüpunkt **Als vordefinierte Rechte sichern ...** aus.
3. Vergeben Sie im erscheinenden Dialogfenster für diesen Satz von Rechten einen Namen, unter dem Sie die Rechte später wieder abrufen möchten. Klicken Sie auf **Sichern**.

TinkerTool System speichert diese vordefinierten Rechte in Ihren persönlichen Einstellungen für diesen Computer ab.

Möchten Sie einen so abgespeicherten Satz von Rechten später auf ein anderes Objekt anwenden, gehen Sie wie folgt vor:

1. Öffnen Sie den Unterpunkt **Zugriffsrechte zeigen oder einstellen** auf der Einstellungskarte **ACL-Rechte**.
2. Ziehen Sie eine Datei oder einen Ordner aus dem Finder in das Feld **Datei oder Ordner**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Aktivieren Sie die gewünschten vordefinierten Rechte, indem Sie über den Knopf **Vordefinierte Rechte** den entsprechenden Menüpunkt **Lade xxx** aufrufen. Hierbei ist xxx der Name, den Sie vorher vergeben hatten. Die aktuelle Einstellung von Rechten wird nun mit den vordefinierten Rechten überschrieben.
4. Speichern Sie die Rechte mit dem Knopf **Anwenden** bei dem gewählten Objekt ab.

Rechte für Ordner und Rechte für Dateien (bzw. andere Objekte mit Nicht-Ordner-Charakter) haben leicht unterschiedliche Bedeutungen. Für Zugriffssteuerungseinträge stehen außerdem andere Optionen zur Verfügung. Aus diesem Grund können Sie die Berechtigungseinstellungen für eine Datei nicht auf einen Ordner anwenden und umgekehrt.

Einstellungen für Rechte beziehen sich in der Regel auf Accounts. Da Accounts einmalig sind, können Sie vordefinierte Rechte nicht von einem Computer auf einen anderen übertragen.

Über den Knopf **Vordefinierte Rechte** können Sie einen Satz von Einstellungen jederzeit umbenennen oder löschen.

3.4.6 Wirksame Zugriffsrechte

Die Kombination zahlreicher Zugriffssteuerungseinträge und der POSIX-Berechtigungen kann es schwierig machen, abzuschätzen, wie die endgültigen Rechte eines bestimmten Benutzers sein werden. TinkerTool System kann die wirksam werdenden Rechte für einen Benutzer berechnen und anzeigen. Diese Funktion ist insbesondere dann nützlich, wenn Sie noch nicht viel Erfahrung mit Berechtigungseinstellungen haben. Um die wirksam werdenden Zugriffsrechte anzeigen zu lassen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Wirksame Zugriffsrechte** auf der Einstellungskarte **ACL-Rechte**.
2. Ziehen Sie eine Datei oder einen Ordner aus dem Finder in das Feld **Datei oder Ordner**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Drücken Sie den Knopf **Auswählen ...**, um einen der bekannten Benutzer-Accounts des aktuellen Computers auszuwählen.
4. TinkerTool System zeigt die Ergebnisse in der Tabelle unten an. Rechte, die diesem Benutzer gewährt werden, sind durch grüne Markierungen dargestellt, Rechte, die verweigert werden, über eine rote Markierung.

3.4.7 Spezielle Rechte

Die Menge der POSIX-Berechtigungen schließt die drei speziellen Einstellungen SUID, GUID und Sticky mit ein. Für deren Bedeutung ziehen Sie bitte die einführenden Abschnitte zu Beginn dieses Kapitels zu Rate. TinkerTool System kann jede der drei Einstellungen anzeigen und ändern. Führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Spezielle Rechte** auf der Einstellungskarte **ACL-Rechte**.
2. Ziehen Sie eine Datei oder einen Ordner aus dem Finder in das Feld **Datei oder Ordner**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Die aktuellen Einstellungen werden angezeigt. Sie können die Felder **Eigentümer**, **Gruppeneigentümer**, **SUID**, **GUID** und **Sticky** wie gewünscht verändern.
4. Betätigen Sie den Knopf **Anwenden**, um die neuen Einstellungen zu speichern.



Warnung: Wie in der Einführung erläutert, kann das Setzen der SUID- oder GUID-Markierungen sehr ernste Sicherheitsprobleme auslösen, die das gesamte Betriebssystem betreffen. Es sollte niemals notwendig sein, die SUID/GUID-Markierungen für Programme zu setzen, wenn dies deren Installationsprogramme nicht bereits getan haben. Das Entfernen der Marken kann zu Fehlfunktionen in den betreffenden Programmen führen. Sie sollten diese Funktion nur benutzen, wenn Sie genau wissen, was Sie tun.

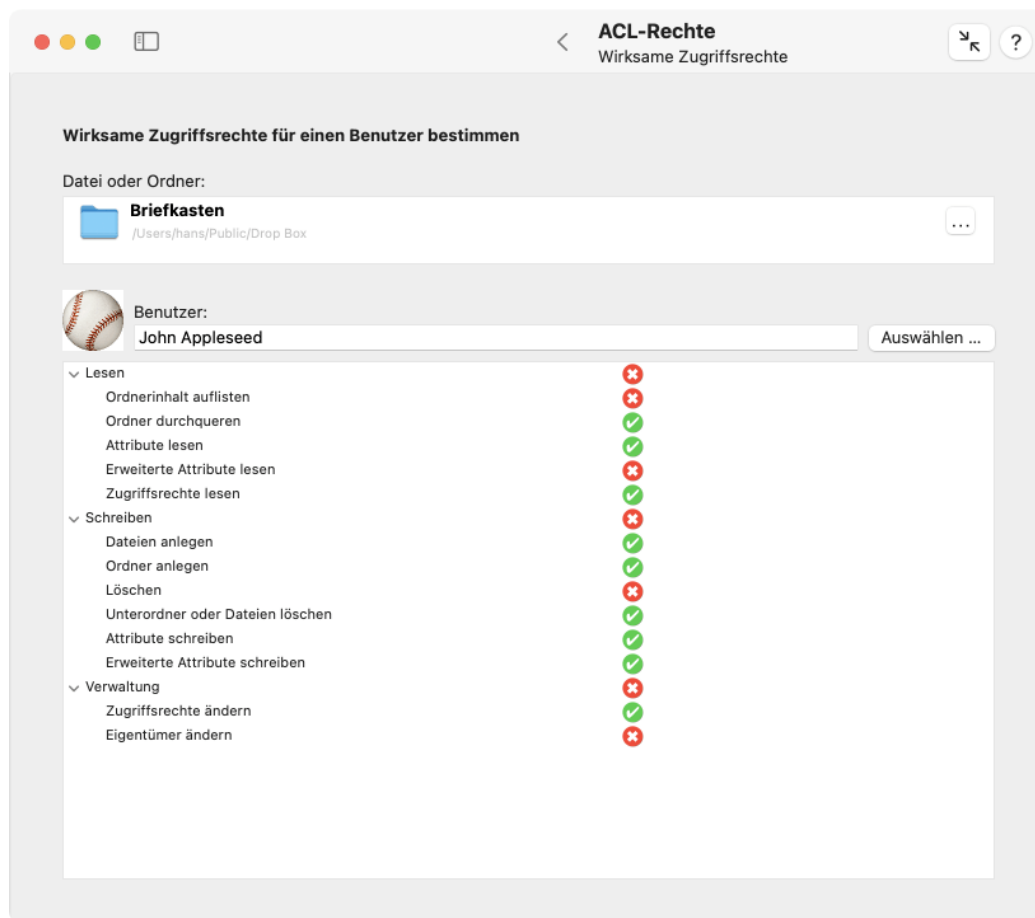


Abbildung 3.28: Wirksame Zugriffsrechte

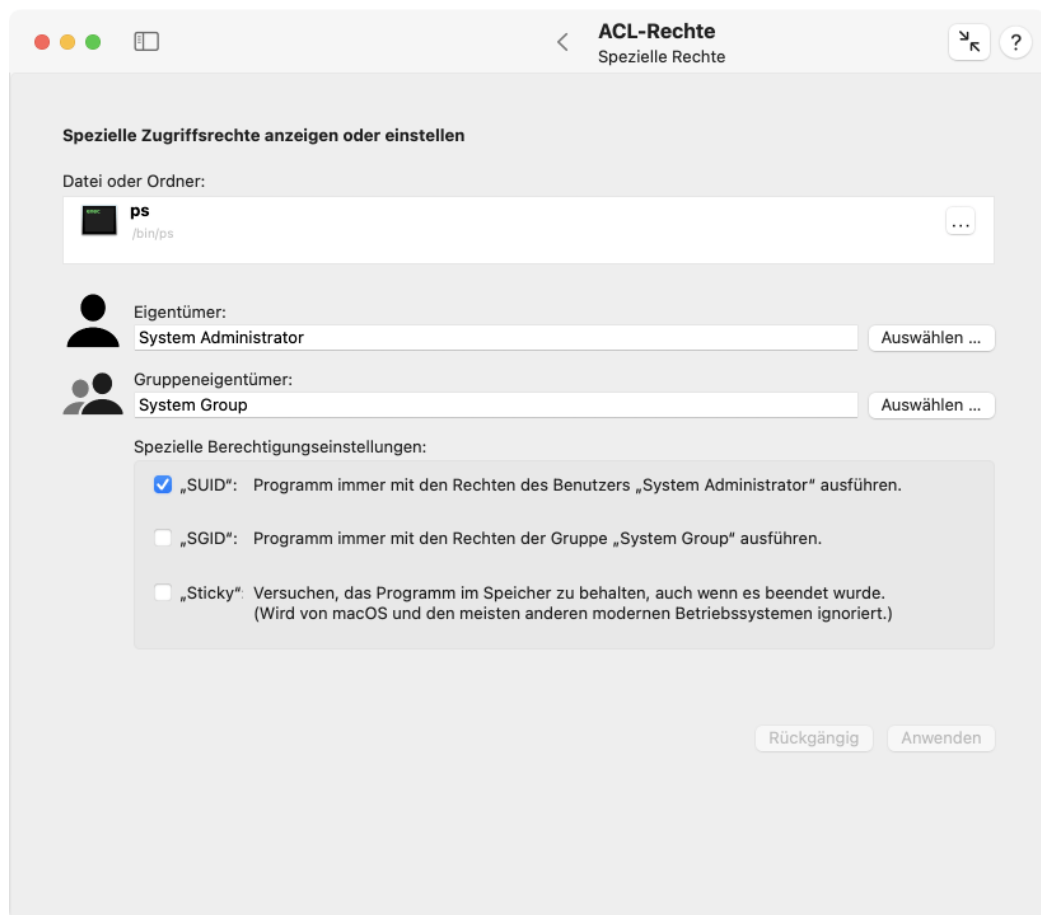


Abbildung 3.29: Spezielle Rechte

3.4.8 Verwaiste Zugriffssteuerungslisten entfernen

Einträge in Zugriffssteuerungslisten enthalten Verweise auf die jeweilige Zugriffspartei, denen eine bestimmte Kombinationen von Rechten erteilt oder verweigert werden soll. Wird diese Partei, also entweder ein Benutzer- oder ein Gruppen-Account, gelöscht, haben alle Einträge, die sich auf diese Partei bezogen haben, keine Funktion mehr. Sie bleiben jedoch weiterhin im Dateisystem eines Volumes gespeichert, obwohl sie überflüssig sind. Wir bezeichnen solche Einträge als *verwaist*. Der Finder zeigt für solche Einträge nur noch den Text **Laden ...** an. TinkerTool System verwendet bei der Anzeige den Hinweis **ID x**, wobei x eine alphanumerische Identifikation ist (siehe oben).

TinkerTool System kann auf Wunsch bestimmen, ob ein Volume verwaiste ACEs enthält. Diese können dann vollautomatisch entfernt werden.

Beachten Sie, dass es bei ACLs immer nur um „zusätzliche Rechte“ geht, die über die Rechte des Dateieigentümers hinausgehen. Falls sogar der Account eines *Dateieigentümers* gelöscht wird, ist die gesamte Datei als verwaist zu betrachten, was andere Auswirkungen hat. Sie können auch solche Fälle von TinkerTool System behandeln lassen. Weitere Informationen finden Sie im Kapitel Die Einstellungskarte Bereinigen (Abschnitt 3.2 auf Seite 164) unter **Verwaiste Dateien**.



Warnung: Falls der Computer Teil eines verwalteten Netzes ist, so werden in der Regel Accounts nicht nur von diesem Computer selbst, sondern auch von einem oder mehreren anderen Computern im Netz gespeichert. Diese netzweiten Accounts sind dazu in *Verzeichnisdiensten* abgelegt. Bevor Sie mit dieser Funktion arbeiten, sollten Sie sicherstellen, dass der Computer gerade mit allen für Ihr Netzwerk relevanten Verzeichnisdiensten verbunden ist und dass diese Verzeichnisse ordnungsgemäß arbeiten. Ansonsten ist es nicht zuverlässig möglich, zu entscheiden, welche Accounts vorhanden und welche nicht vorhanden sind. Einträge, die zu Netzbenutzern gehören, könnten so fälschlicherweise als verwaist eingestuft werden.



Warnung: Sie dürfen diese Funktion nicht auf einem Volume verwenden, das von einem anderen als Ihrem aktuellen Betriebssystem verwaltet wird. Das andere System verwendet höchstwahrscheinlich eine andere Account-Datenbank, so dass die Information, welche Benutzer noch vorhanden und welche nicht mehr verfügbar sind, sehr unterschiedlich sein könnte.

Führen Sie die folgenden Schritte durch, um nach Zugriffssteuerungslisten mit verwaisten Einträgen zu suchen:

1. Öffnen Sie den Unterpunkt **Verwaiste ACLs** auf der Einstellungskarte **ACL-Rechte**.
2. Bestimmen Sie über das Klappmenü **Wähle ein Volume aus**, wo nach verwaisten Rechten gesucht werden soll.
3. Betätigen Sie den Knopf **Suche beginnen**

Ist die Suche abgeschlossen, erhalten Sie eine Liste mit allen betroffenen Dateipfaden und allen nicht mehr vorhandenen Einträgen für Zugriffsparteien. Die Namen dieser Einträge

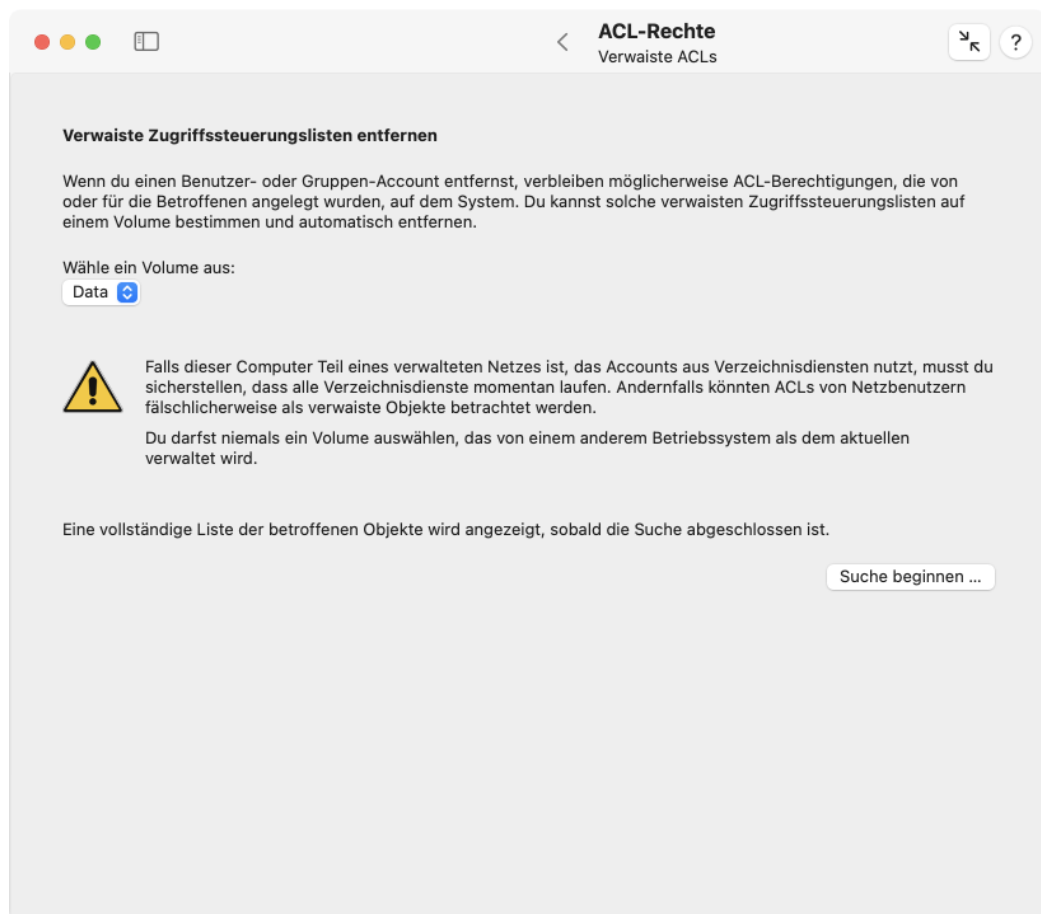


Abbildung 3.30: Falls durch Löschung von Accounts ACL-Einträge zurückbleiben, die nicht mehr gültig sind, können diese automatisch von einem Volume entfernt werden

können nicht mehr bestimmt werden, da die zugehörigen Accounts ja nicht mehr vorhanden sind. Stattdessen werden die Identifikationen (UUIDs) angegeben. Durch Klick auf **Löschen** können Sie alle angezeigten Einträge entfernen lassen. Dies löscht nur ungültige Zugriffssteuerungslisteneinträge. Die Dateisystemobjekte selbst und deren immer noch gültige ACEs bleiben unberührt.

3.4.9 Berechtigungen in einem Benutzerordner auf Standardwerte stellen

Falls Sie mit dem Finder oder auf andere Weise Rechte für Dateien in Ihrem Benutzerordner auf eine Weise verstellt haben, so dass Programme nicht mehr richtig laufen, keine Einstellungen mehr speichern können, oder Sie selbst den Zugriff auf Ihre eigenen Daten verloren haben, können Sie die Berechtigungseinstellungen von TinkerTool System wieder auf vorgeschlagene Standardwerte zurückstellen. Dies bezieht sich auf sämtliche Dateien und Ordner im Privatordner irgendeines lokalen Benutzers.

Für älteren Versionen von macOS hatte Apple vorübergehend ein Unix-Befehlszeilenprogramm bereitgestellt, mit dem ein ähnlicher Vorgang vom macOS-Wiederherstellungssystem aus möglich war. Dies war außerdem an das Zurücksetzen des Kennworts des betroffenen Benutzers gebunden. In aktuellen Versionen von macOS besteht diese Möglichkeit nicht mehr.

Fälschlicherweise wird dieser Vorgang manchmal als „Reparieren von Rechten“ bezeichnet. Dieser Begriff ist irreführend, denn Berechtigungseinstellungen können immer nur von einem Programm oder Benutzer verstellt, aber niemals beschädigt werden.



Warnung: Sie sollten diese Funktion niemals „auf Verdacht“ oder gar regelmäßig verwenden. Die zurückgestellten Rechte sind eine Art sauberer Vorschlag, der garantiert, dass der betroffene Benutzer mit den eigenen Dateien problemlos arbeiten kann. Diese Standardwerte könnten jedoch auch Dateien für fremde Benutzer lesbar machen, obwohl das Programm, das die Daten angelegt hat, sie vielleicht ursprünglich mit der Einstellung „nur für diesen einen Benutzer lesbar“ gespeichert hatte. Weder macOS noch TinkerTool System können für jede einzelne Datei und jeden Ordner „wissen“, welche Bedeutung diese haben und ob sie aus Sicht des Eigentümers eher als vertraulich oder als öffentlich einzustufen sind. Es handelt sich ja um frei verwaltete Benutzerdaten. Mit anderen Worten: Für vertrauliche Daten könnten die Standardeinstellungen im Einzelfall zu unsicher sein. Der betroffene Benutzer muss selbst durch nachträgliche Kontrolle und eventuelles Nachschärfen der Rechte dafür sorgen, dass keine Unbefugten die Daten lesen oder löschen können. Viele (nicht alle) Anwenderprogramme korrigieren aber auch automatisch unsichere Rechte, das nächste Mal wenn automatisch gespeicherte Daten für den Benutzer gesichert werden.

Für diese Funktion gelten folgende Grundregeln:

- Der betroffene Benutzer muss einen lokalen Privatordner haben, der sich auf diesem Computer befindet.
- Falls im Benutzerordner Daten gespeichert sind, die *Spezielle Rechte* (siehe voriger Abschnitt) aufweisen, bleiben diese aus Sicherheitsgründen immer unberührt.

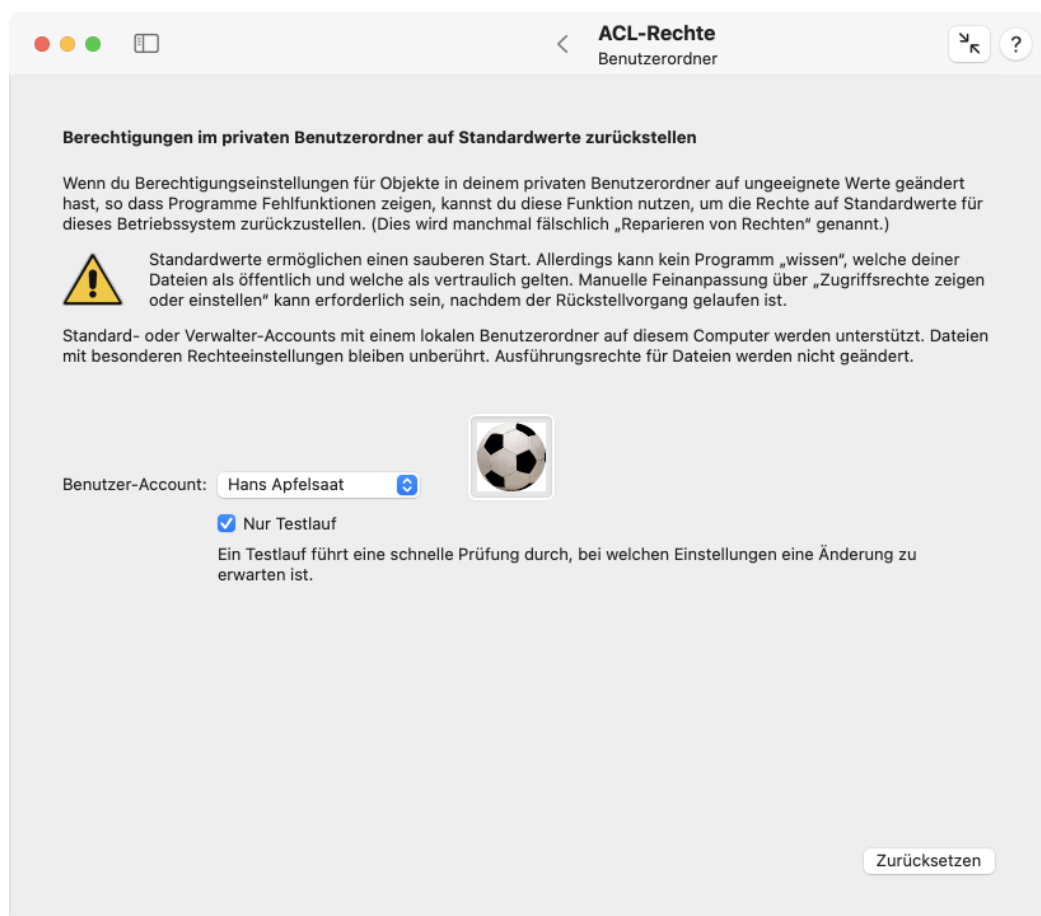


Abbildung 3.31: Verstellte Berechtigungen in einem Benutzerordner können auf Standardvorschläge zurückgestellt werden

- Die gleiche Vorgehensweise gilt auch für Objekte, die als *datenlose Dateien* markiert sind und automatisch von iCloud oder Cloud-Lösungen anderer Anbieter synchronisiert werden. Das Ändern der Berechtigungseinstellungen einer solchen Datei würde ansonsten ein automatisches Herunterladen des Dateiinhalts in macOS auslösen.
- Rechte, die sich auf die Ausführbarkeit oder Nichtausführbarkeit von Programmen beziehen, werden niemals geändert.
- Als Standardwerte für Berechtigungen werden Einstellungen vorgesehen, die Apple üblicherweise für die gerade laufende Betriebssystemversion verwendet, wenn ein neuer Benutzerordner angelegt wird. Die Ergebnisse können also in jeder Systemversion unterschiedlich sein. Wurde der Benutzerordner ursprünglich mit einer älteren Betriebssystemversion angelegt und dann ein Upgrade auf eine höhere Version von macOS durchgeführt, ändern sich oft viele Rechte.

Auf Wunsch können Sie einen Testlauf durchführen, der alle Dateien und Ordner eines Benutzerordners überprüft, aber nicht wirklich Rechte verändert. Sie erhalten dann einen Bericht, wie viele Einstellungen geändert und nicht geändert würden, und welche Dateien betroffen wären.



Aufgrund der besonderen Natur der Vererbung von Zugriffssteuerungslisten gibt es allerdings Fälle, in denen das Ergebnis eines Testlaufs nicht hundertprozentig mit dem Ergebnis eines echten Laufs übereinstimmt. Die Änderung einer Zugriffssteuerungsliste kann indirekt zukünftige Änderungen auf andere Ordner auslösen, die nicht immer vorhergesagt werden.

Um die Rechte im Privatordner eines lokalen Benutzers auf einen funktionsfähigen Vorschlag zurückzustellen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Benutzerordner** auf der Einstellungskarte **ACL-Rechte**.
2. Wählen Sie bei **Benutzer-Account** den Benutzer aus, dessen Ordner verarbeitet werden soll.
3. Wählen Sie bei **Testlauf**, ob wirklich eine Änderung durchgeführt werden soll oder Sie nur eine vorläufige Vorschau erhalten möchten.
4. Drücken Sie auf den Knopf **Zurücksetzen**.

Der ausgewählte Vorgang wird durchgeführt und Sie erhalten zum Abschluss einen ausführlichen Bericht, der auf Wunsch auch in eine Textdatei gespeichert werden kann. Während der Vorgang läuft, wird bereits eine Vorschau des Berichts als durchlaufender Text gezeigt.

Der Bericht kann im Einzelfall mehrere Millionen Zeilen enthalten. Um macOS bei der Anzeige nicht mit dieser Datenmenge zu überlasten, wird der Text ausnahmsweise nicht in einer rollbaren Textbox dargestellt.

3.4.10 Interne Identifikationen von Benutzer- und Gruppen-Accounts finden

Jeder Benutzer- und Gruppen-Account ist ein Datensatz, der von macOS verwaltet wird, und der die Daten von Personen enthält, die bestimmte Rechte für den Zugriff auf gewisse Informationen haben. Je nach den Umständen kann das Betriebssystem verschiedene Darstellungen verwenden, um Bezug auf einen Account zu nehmen:

- den **Account-Namen**, manchmal auch *Kurzname* genannt, üblicherweise nur in Kleinbuchstaben und ohne Leerzeichen geschrieben.
- den **vollen Namen**, wie man ihn normal schreiben würde, üblicherweise länger als der Account-Name, mit Leerzeichen und Großbuchstaben. Dieser Punkt wird manchmal auch *GECOS-Name* genannt, ein traditioneller Hinweis auf die Zeit der sehr frühen Unix-Betriebssysteme in den 1960er-Jahren, als Unix noch ausschließlich die kurzen Namen für Benutzer gespeichert hatte, andere Betriebssysteme aus dieser Ära, wie *GECOS* von *General Electric* (*GE Comprehensive Operating Supervisor*) jedoch schon mehr Daten in einem Benutzer-Account ablegten, wie die vollen Namen der Benutzer, Raumnummern, Telefonnummer, usw.
- einen *numerischen Bezeichner* in Form einer ganzen Zahl. Dies hält sich an den *POSIX*-Industriestandard für Betriebssysteme.
- einen alphanumerischen Bezeichner, der dem Industriestandard für **Universal Unique Identifier** (UUIDs, universelle eindeutige Bezeichner) entspricht. UUIDs verwenden mathematische Verfahren um zu garantieren, dass sie nur ein einziges Mal in der Welt vorkommen. Sie werden nicht nur zur Identifikation von Benutzer- und Gruppen-Accounts verwendet, sondern können sich auf alles beziehen, was ein eindeutiges Etikett benötigt.

Falls Sie eine dieser vier Bezeichnungen angeben, kann Ihnen TinkerTool System dabei helfen, die anderen drei Punkte herauszufinden. Dies kann zum Beispiel dann hilfreich sein, wenn das Betriebssystem in einer internen Protokollmeldung auf ein „Problem mit Benutzer 502“ hinweist und Sie herausfinden müssen, um welchen Benutzer es sich dabei handelt.

Eine übereinstimmende Identifikation kann manchmal sowohl für einen Benutzer als auch für eine Gruppe verwendet werden, auch wenn es sich dabei um völlig verschiedene Objekte handelt. Deshalb müssen Sie angeben, nach welcher Art von Account Sie suchen. Für UUIDs ist dies allerdings nicht nötig, da diese ja grundsätzlich einzigartig sind. Accounts sind möglicherweise nicht nur auf Ihrem Mac gespeichert, sondern Ihr Netzwerk könnte eine oder mehrere Datenbanken für Accounts bereitstellen, die für alle Computer im Netz gelten. Ein Server, der solch eine zentrale Account-Datenbank beherbergt, stellt einen sogenannten *Verzeichnisdienst* zur Verfügung.

1. Öffnen Sie den Unterpunkt **ID-Finder** auf der Einstellungskarte **ACL-Rechte**.
2. Geben Sie Daten in das Feld **Entweder Account-Namen, vollen Namen, POSIX-Bezeichner oder UUID angeben** ein.
3. Wählen Sie entweder **Benutzer** oder **Gruppe**, falls Sie keine UUID angegeben haben.
4. Wenn Ihr Mac dazu eingerichtet ist, auf einen Verzeichnisdienst im Netz zuzugreifen, könnte die Suche einige Tausend Accounts betreffen und dabei sehr viel Netzwerkdatenverkehr verursachen. Sie können wählen, ob Sie eine **Erschöpfende Suche** über alle Einträge auf allen Verzeichnisdienstservern zulassen möchten, oder ob die

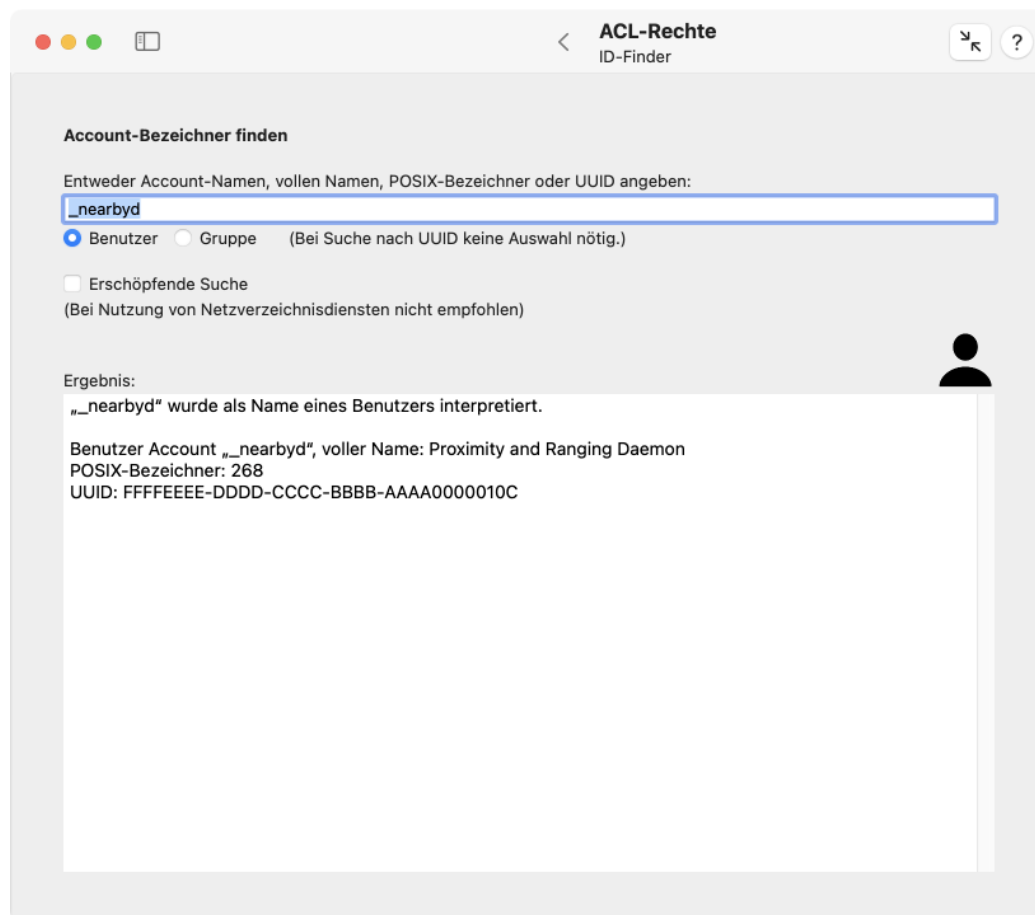


Abbildung 3.32: ID-Finder

Suche sich auf Accounts beschränken soll, die aktiv auf dem lokalen Mac genutzt wurden. (Eine nicht erschöpfende Suche berücksichtigt in der Regel immer noch Accounts von fernen Verzeichnisdiensten, falls das System vor kurzem mit diesen Accounts gearbeitet hat.)

5. Betätigen Sie die Eingabetaste.

Das Ergebnis der Suche wird in der Box **Ergebnis** angezeigt.

3.5 Die Einstellungskarte Installationsmedien

3.5.1 Betriebssysteminstallation

Seit Sommer 2011 liefert Apple seine Betriebssysteme nur noch als Download von Installations-Apps aus dem App Store aus, oder zusammen mit neuen Macs. Das heißt, es gibt kein materielles Medium mit einer Kopie des Betriebssystems mehr, das im Notfall verwendet werden könnte, falls die laufende Kopie des Betriebssystems auf Ihrem Computer beschädigt oder gelöscht wird. Es gibt nur ein kleines Mini-Betriebssystem für Notfälle, das in einem *Wiederherstellungs-Volume* gespeichert ist, das parallel für jede macOS-Installation auf Ihrem Mac und für jede Time Machine-Zielplatte angelegt wurde. Neue Macs mit Apple-Chips enthalten darüberhinaus noch ein weiteres Notfall-Wiederherstellungssystem, das in einem normalerweise nicht erreichbaren Teil des Flash-Speichers abgelegt ist und sich ähnlich wie Firmware verhält. Jedes Wiederherstellungssystem erlaubt es, ein Exemplar des vollständigen Betriebssystems erneut aus dem Internet herunterzuladen wenn Sie es verloren haben. Abhängig von der Geschwindigkeit Ihrer Internet-Leitung kann ein voller Download allerdings mehr als 4 Stunden Zeit benötigen. In Fällen, in denen alle Laufwerke Ihres Mac gelöscht wurden oder anderweitig unbrauchbar sind, können Sie das Wiederherstellungssystem auch über eine NetBoot-Funktion laden, so dass auch das Notsystem selbst direkt von einem Internet-Server von Apple geladen wird.

Alle diese Notfall-Verfahren helfen nicht, wenn Sie ein neues Betriebssystem auf einem Mac installieren müssen, der keine Internet-Verbindung hat, bzw. aus Sicherheitsgründen keine haben darf. Für solche Fälle bieten alle Mac-Betriebssysteme seit OS X 10.9 oder höher eine Funktion an, um ein selbständiges Installationsmedium zu erstellen. Solche ein Medium verhält sich wie eine klassische Betriebssystem-DVD: Der Computer kann damit gestartet werden und Sie können ein vollständiges Exemplar des Betriebssystems installieren, ohne dass eine Internet-Verbindung erforderlich ist. Das Medium kann auch das Wiederherstellungssystem komplett ersetzen: Alle Komponenten des Wiederherstellungssystems sind enthalten, so dass Sie zum Beispiel das Festplattendienstprogramm, Terminal, oder Time Machine zu Wartungszwecken nutzen können, wenn das Hauptsystem nicht mehr ordnungsgemäß arbeitet.

TinkerTool System führt Sie durch den Prozess der Erstellung eines macOS-Installationsmediums. Ein startbarer Installer kann mit wenigen Mausklicks erstellt werden.

3.5.2 Notwendige Voraussetzungen

Sie benötigen zusätzliche Software und Hardware um ein macOS-Installationsmedium anzulegen. Die folgenden Dinge sind erforderlich:

- ein Installationsprogramm für das Betriebssystem, das Sie verwenden möchten, heruntergeladen aus dem Mac App Store. Jeder Betriebssystem-Installer für OS X oder macOS, Version 10.9 oder höher kann verwendet werden. Falls Sie eine Installations-App zwischen Version 10.9 und 10.11 aus dem App Store in der Vergangenheit heruntergeladen haben, können Sie diese so oft Sie möchten über die Seite **Gekauft** erneut

herunterladen, wenn Sie die Daten Ihres Benutzer-Accounts (Apple-ID) im Programm **App Store** anzeigen lassen. Ab macOS 10.12.4 sind die Installationsprogramme frei erhältlich geworden und werden nicht mehr als vorheriger Kauf angezeigt, aber es ist nicht möglich, nach etwas anderem als der aktuellen Version im App Store zu suchen. Falls Sie an einem Installer zwischen Version 10.12.4 und der neuesten Version interessiert sind, öffnen Sie *Apples Webseite für Support* und suchen Sie dort nach dem Namen des Betriebssystems, z.B. „Upgrade auf macOS High Sierra“. Sie sollten eine Webseite finden, die einen Link auf einen versteckten Eintrag im App Store, bzw. auf dem Apple Software-Update-Server enthält, der das entsprechende Installationsprogramm anbietet. Bei bestimmten Macintosh-Modellen kann Apple jedoch eine Anforderung zum Herunterladen ablehnen, wenn erkannt wird, dass auf Ihrem Mac ein Betriebssystem mit höherer Versionsnummer zum Einsatz kommen könnte. Außerdem können Sie versuchen, Installationsprogramme direkt in TinkerTool System herunterzuladen (siehe unten).

- ein plattenartiges Massenspeichergerät, das von macOS unterstützt wird, das eine Kapazität von 8 GiBiByte oder mehr hat. (Neuere Versionen von macOS benötigen mehr als 8 GiBiByte Speicher. TinkerTool System weist Sie darauf hin, falls erforderlich.) Ein USB-Flash-Laufwerk („USB stick“) kommt üblicherweise zum Einsatz. Sie können zum Beispiel aber auch ein externes Plattenlaufwerk oder eine SSD einsetzen. Beachten Sie, dass das Laufwerk vollständig gelöscht werden kann, wenn das Installationssystem angelegt wird.

Auch wenn das Ziel-Volume während der Erstellung des Mediums gelöscht und als HFS+ neu formatiert wird, lehnen die neuesten Versionen von Apples Installationsprogrammen Speichergeräte generell auch im Vorhinein ab, wenn Partitionen oder Dateisysteme nicht bestimmte Regeln einhalten. TinkerTool System wurde entsprechend angepasst und schlägt nur noch Volumes mit HFS+ als mögliche Zielplatten vor.

Falls macOS oder TinkerTool System Probleme haben, ein externes Speichergerät zu erkennen, das als Installationsmedium verwendet werden soll, löschen Sie das Gerät zuerst und legen Sie ein leeres HFS+-Dateisystem an:

1. Starten Sie das **Festplattendienstprogramm**.
2. Stellen Sie sicher, dass der Punkt **Darstellung** > **Alle Geräte einblenden** eingeschaltet ist.
3. Wählen Sie das Gerät in der Seitenleiste des Festplattendienstprogramms aus.
4. Drücken Sie den Knopf **Löschen** in der Symbolleiste.
5. Wählen Sie **Format: Mac OS Extended (Journaled)** und **Schema: GUID-Partitionstabelle** aus und geben Sie einen **Namen** Ihrer Wahl an.
6. Drücken Sie den Knopf **Löschen**.

Nachdem das Gerät gelöscht wurde, werden macOS und TinkerTool System es als Zielmedium akzeptieren.

Einige wenige Betriebssystem-Installationsprogramme, die vom App Store heruntergeladen wurden, können unvollständig sein. In solch einem Fall ist die Installations-App nur eine Hülle, die nicht das vollständige Betriebssystem enthält, sondern nur Informationen, wie die fehlenden Teile bei Bedarf intern von Apple heruntergeladen werden können, wenn diese gebraucht werden. Leider ist es mit solch einem unvollständigen Installationsprogramm nicht möglich, ein Installationsmedium zu erstellen. TinkerTool System erkennt dies korrekt und zeigt in diesem Fall eine entsprechende Warnung an. Der App Store kann pro Kunde und pro macOS-Version entscheiden, ob er ein vollständiges oder unvollständiges Installationspaket für das Betriebssystem ausliefert.

3.5.3 Herunterladen von Installationsprogrammen ohne den App Store

Falls Sie Probleme haben, den richtigen Installer aus dem App Store zu beziehen, können Sie macOS den Befehl geben, automatisch ein bestimmtes Installationsprogramm zu finden und es herunterzuladen:

1. Öffnen Sie die Einstellungskarte **Installations-Medien**.
2. Betätigen Sie den Knopf **Installer-App von Apple laden**
3. Wählen Sie im Dialogfenster einen Installer aus der Tabelle der verfügbaren Apps aus und klicken Sie auf den Knopf **Download starten**.
4. TinkerTool System sendet nun eine Anforderung an Apple, das Installationsprogramm zu finden und herunterzuladen. Sie werden entsprechende Statusmeldungen im Fenster zum Herunterladen sehen. Aus technischen Gründen können einige dieser Meldungen in englischer Sprache erscheinen. Der Vorgang kann jederzeit durch Drücken des **Stopp**-Knopfes abgebrochen werden.

In der Regel werden Ihnen keine Systemversionen angeboten, die auf Ihrem Mac nicht laufen würden. Sie können also mit einem neuen Mac kein zu altes Betriebssystem herunterladen, das mit diesem nicht kompatibel wäre. Je nach Baureihe des gerade genutzten Macintosh erhalten Sie also unterschiedliche Ergebnisse in der Liste. Wir können nicht vorhersagen, welche Installer-Versionen Apple in Ihrer Region und für Ihren jeweiligen Mac anbietet. Die verfügbaren Versionen können sich ohne vorherige Ankündigung jede Minute ändern.

Abhängig von der Geschwindigkeit Ihrer Internet-Leitung, kann das Herunterladen mehrere Stunden benötigen. Nachdem das Herunterladen erfolgreich abgeschlossen wurde, werden Sie das Installationsprogramm im Hauptordner **Programme** finden, der von TinkerTool System automatisch geöffnet wird. Falls Sie den Download-Vorgang stoppen, kann sich macOS dazu entscheiden, das Herunterladen im Hintergrund fortzusetzen. TinkerTool System hat darauf keinen Einfluss.

3.5.4 Herunterladen von IPSW-Dateien

Neben den Installationsprogrammen stellt Apple für Macintosh mit Apple-Chips noch eine weitere Art von Dateien bereit, mit denen es möglich ist, den Computer neu zu installieren. Aus historischen Gründen wird diese Technik *IPSW-Datei (iPhone Software)* genannt. In einer einzelnen Datei ist dabei sowohl das Betriebssystem als auch die Firmware des Mac enthalten. Solche eine Datei kann für zwei verschiedene Anwendungen genutzt werden:

- Sie können damit einen Macintosh mit Apple-Chip komplett löschen und auf einen wohldefinierten, „leeren Werkszustand“ bringen. Die Benutzerdaten werden entfernt, Firmware und Betriebssystem werden ersetzt. Ein Mac mit beschädigter Firmware oder ein Gerät, bei dem sämtliche Recovery-Systeme zerstört wurden, kann auf diese Weise wieder repariert werden. Zum Einspielen der IPSW-Datei muss der Mac in den sogenannten *DFU-Modus (Device Firmware Update)* gebracht werden. Sie benötigen hierzu einen zweiten Mac, ein passendes Verbindungskabel, sowie die Software *Apple Configurator* Version 2 oder höher, die von Apple kostenlos erhältlich ist.
- Sie können eine komplett leere Virtuelle Maschine während ihrer Ersteinrichtung mit der notwendigen Firmware und Betriebssystem-Software bestücken. Die Hypervisor-Software zum Betrieb der Virtuellen Maschine muss dabei die Funktion anbieten, eine Installation per IPSW zu ermöglichen.

Klicken Sie auf den Knopf **IPSW-Datei von Apple herunterladen ...** um über das Internet die Liste von IPSW-Dateien abzurufen, die Apple im Moment anbietet. Diese Liste kann sich jederzeit ohne Ankündigung ändern. Sie finden in der Tabelle

- die Macintosh-Baureihe, für die eine IPSW-Datei angeboten wird,
- die Versionsnummer des Betriebssystems,
- die Build-Nummer des Betriebssystems.

Nach Auswählen einer Tabellenzeile und Anklicken von **Ausgewählte Datei herunterladen** wird der Download gestartet. Der Vorgang kann einige Zeit in Anspruch nehmen, da etwa 12 GByte Daten übertragen werden müssen. Nach dem Herunterladen wird die Datei automatisch in Ihren persönlichen Downloads-Ordner abgelegt.

Auch wenn mehrere Einträge für die verschiedenen Macintosh-Baureihen in der Liste der IPSW-Dateien enthalten sind, muss das nicht bedeuten, dass Sie für jedes Modell tatsächlich eine andere Datei brauchen. In vielen Fällen kann eine einzelne Datei auch für weitere oder sogar alle Baureihen verwendet werden. Das Verwenden von Apple Configurator oder eines Hypervisors geht über die Funktion von TinkerTool System hinaus. Der Umgang mit der IPSW-Datei wird deshalb nicht in diesem Handbuch beschrieben.

3.5.5 Anlegen des Installationsmediums

Um die selbständige Installationsplatte zu erzeugen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie die Einstellungskarte **Installations-Medien**.
2. Ziehen Sie das Symbol der Installations-App für OS X oder macOS, vom Finder in das Feld **Installer-App**. Sie können auch den Knopf [...] drücken, um zur App zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Verwenden Sie das Klappmenü **Speichermedium**, um das Zielgerät auszuwählen.
4. Drücken Sie den Knopf **Starten**



Warnung: Das Volume, das als Installationsmedium ausgewählt wurde, wird vollständig gelöscht. Sie sollten nicht davon ausgehen, dass andere Volumes oder Partitionen auf dem gleichen Gerät unberührt bleiben. Im schlimmsten Fall könnten diese auch entfernt werden, falls Apples Installationsprogramm Änderungen am Partitionsschema vornehmen muss. Um Missverständnisse zu vermeiden, ist es empfehlenswert, ein Installationsmedium zu verwenden, das nur ein einzelnes Volume enthält.

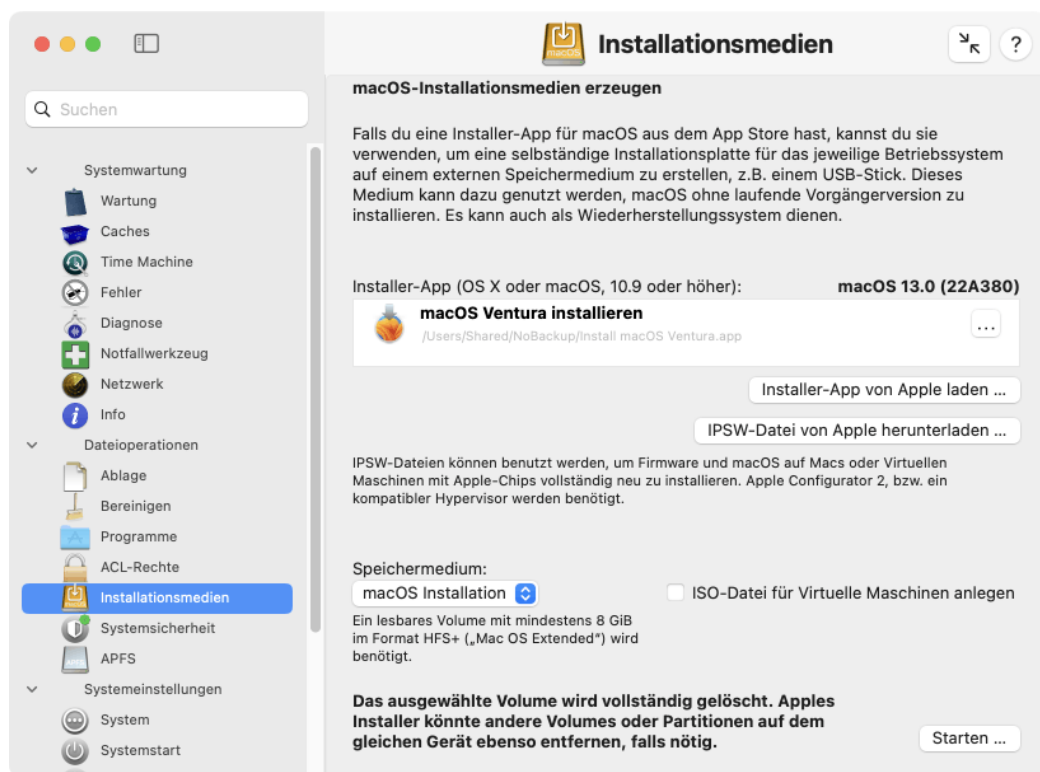


Abbildung 3.33: Ein selbständiges Installationsmedium für das Betriebssystem kann mit wenigen Mausklicks angelegt werden

Falls TinkerTool System nicht das Gerät auflistet, das Sie verwenden möchten, lesen Sie bitte die Anleitung im vorigen Abschnitt.

Das Anlegen der Installationsplatte wird nicht direkt von TinkerTool System gesteuert, sondern von der Installations-App, die Sie aus dem App Store geladen haben. Aus diesem Grund kann diese Prozedur leicht unterschiedlich sein, je nach dem, welche Betriebssystemversion Sie einsetzen.

Wenn Sie einen Prozess zum Anlegen von Medien das erste Mal basierend auf einer frisch heruntergeladenen Installations-App starten, kann macOS manchmal seine interne Antivirus-Software *XProtect* automatisch aktivieren, um den Inhalt des Programms zu überprüfen. Dies kann eine Verzögerung von mehreren Minuten zu Beginn

des Anlageprozesses auslösen, wobei weder macOS noch TinkerTool System Meldungen anzeigen.

Nicht alle Versionen von macOS erlauben das Anlegen von Installationsmedien über unterschiedliche Prozessorarchitekturen hinweg. Zum Beispiel funktioniert es eventuell nicht immer, eine Installations-Disk für ein Nur-Intel-Betriebssystem auf einem Mac mit Apple-Chip zu erzeugen. TinkerTool System informiert Sie automatisch, falls Sie eine solche „Überkreuzerstellung“ mit einer macOS-Version versuchen, bei der Apple das nicht zulässt.

Als Teil des Erzeugungsvorgangs öffnet macOS möglicherweise Teile des angelegten Systems in einem neuen Finder-Fenster, das am Ende der Prozedur erscheint. Das Fenster kann dazu genutzt werden, das erfolgreiche Anlegen der Platte zu überprüfen. Sie können dieses Fenster ohne Bedenken schließen und die Platte auswerfen.

3.5.6 Ein Installationsmedium als ISO-Datei anlegen

Falls Sie das Installationsmedium dazu benötigen, macOS in einer Virtuellen Maschine zu installieren, kann der Ablauf dadurch vereinfacht werden, dass Sie nicht eine separate Speicherplatte, sondern ein Plattenabbild (Disk Image) anlegen. Alle Hypervisor für Virtuelle Maschinen akzeptieren üblicherweise eine ISO-Datei, ein Disk Image, das den Industrienormen für das Mastering von CD-ROMs oder DVDs folgt.

Um solch ein Plattenabbild anzulegen, kreuzen Sie den Punkt **ISO-Datei für Virtuelle Maschinen anlegen** an, zusätzlich zu den üblichen Schritten zum Anlegen von Installationsmedien, die wir bereits erwähnt haben, und geben Sie außerdem ein Ziel für die Ausgabe-datei an, sobald das Programm danach fragt.

TinkerTool System benötigt vorübergehend den zweifachen empfohlenen Speicherplatz für das Anlegen der ISO-Datei. Das bedeutet 16 GiB für ältere Versionen von macOS und 32 GiB für die neuesten Versionen. Die endgültige Ausgabedatei wird automatisch daraufhin optimiert, so wenig Speicherplatz zu verwenden wie möglich.

3.5.7 Reparieren der Oktober-2019-Ausgabe des Sierra-Installers

Apple hat ein aktualisiertes Exemplar der Installations-App für macOS 10.12.6 am 23. Oktober 2019 veröffentlicht. Diese spezielle Version des Programms hat allerdings interne Fehler, die das automatische Anlegen von Installationsmedien üblicherweise verhindern. Apple gibt offiziell an, dass diese App hierzu nicht in der Lage ist.

TinkerTool System kann diese App erkennen und reparieren, so dass sie dennoch dazu verwendet werden kann, Installationsmedien anzulegen. In diesem Fall wird ein Knopf **Reparieren ...** auf der Einstellungskarte erscheinen. Sie können diesen Knopf betätigen und den Anweisungen folgen um eine Reparatur durchzuführen. Danach ist es möglich, das reparierte Exemplar auf normale Weise zum Anlegen von Installationsmedien zu verwenden, wie es oben beschrieben wurde.

3.5.8 Mängel und Einschränkungen im laufenden Betriebssystem

Ab macOS 13.3 hat Apple dem Betriebssystem neue Sicherheitsfunktionen hinzugefügt. Ein Teil dieser Funktionen ist nicht besonders gut durchdacht und entsprechend unausgereift. Apples eigene Installationsprogramme können von macOS fälschlicherweise als

unsicher oder beschädigt eingestuft werden. TinkerTool System kennt diesen Konstruktionsfehler und enthält mehrere Zusatzfunktionen, die die damit zusammenhängenden Probleme umgehen können. Das Programm analysiert die Situation genau und zeigt, wenn nötig, entsprechende Zusatzschritte beim Erstellen von Installationsmedien an. Beachten Sie in diesem Zusammenhang Folgendes:

- Wenn die Installations-App, die Sie verwenden, *nicht* auf dem System-Volume abgelegt ist, kann es sein, dass TinkerTool System vorübergehend zusätzlichen Speicher auf dem System-Volume benötigt. Der zusätzliche Speicherbedarf entspricht der Größe des jeweiligen Installers.
- Beim Erstellen eines Installationsmediums kann es bis zu zweimal dazu kommen, dass der Antiviren-Scanner von macOS TinkerTool System anhält, um Apples Installationsprogramm auf mögliche Malware zu untersuchen. Dies stellt sich jeweils nach außen hin als längere Pause dar, in der das Programm scheinbar nicht arbeitet. Wenn Sie während dieser Pause Funktionen zur Anzeige laufender Prozesse aufrufen, kann es passieren, dass TinkerTool System mit dem Status **reagiert nicht** gezeigt wird. *Dies ist normal und kein Fehler.* Nachdem macOS das Installationsprogramm auf Viren getestet hat, wird die Arbeit ganz normal fortgesetzt.
- Bei bestimmten Versionen des Installationsprogramms kann macOS anzeigen, dass das Programm angeblich beschädigt ist und in den Papierkorb geworfen werden sollte. Wenn Sie wissen, dass Sie den Installer direkt von Apple heruntergeladen haben, sollten Sie dies ignorieren.
- Wenn Sie auf einem Mac mit Apple-Chip ein Installationsmedium für eine Version von macOS 10 erstellen möchten, wird Apples Zusatzprogramm **Rosetta** benötigt, um den Intel-Code des Installers verarbeiten zu können. macOS erkennt dies automatisch und führt Sie durch eine eventuell nötige Installation.

3.6 Die Einstellungskarte Systemsicherheit

3.6.1 Speicherplatz

In neueren Versionen von macOS kommt es regelmäßig zu Verwirrung bei Anwendern, wie viel Speicherplatz auf einem bestimmten Volume tatsächlich frei und belegt ist. Diese Verwirrung hat mehrere Ursachen:

1. Programme können verschiedene Definitionen von Maßeinheiten bei der Angabe von Speicherplatz verwenden, ohne dies korrekt zu markieren. So kann 1 Kilobyte je nach Definition entweder 1.024 Byte oder 1.000 Byte darstellen. Apple hat die Richtlinien für die Angaben von Speicher in den letzten Jahren mehrfach geändert. Ausführliche Hinweise hierzu finden Sie im Kapitel Grundlegende Bedienungshinweise (Abschnitt 1.3 auf Seite 8), Abschnitt *Anzeigen von Speichergrößen*.
2. Programme können den Speicherplatz aus Sicht des Benutzers (Finder) oder aus technischer Sicht (Festplattendienstprogramm) anzeigen. Der Finder sieht beispielsweise Speicherplatz, der für die Ablage von Lokalen Time Machine-Schnappschüssen belegt wird, als frei an. Dies soll dem Benutzer signalisieren, dass der hierfür genutzte Speicher bei Bedarf vollautomatisch vom Betriebssystem freigegeben werden könnte, wenn er für etwas anderes benötigt wird. Manche Programme unterscheiden ausdrücklich zwischen „freien“ und „verfügbarem“ Speicher, wobei „verfügbar“ dann als „frei plus löschtbar“ definiert ist. Ausführliche Informationen zu lokalen

Time Machine-Schnappschüssen finden Sie im Kapitel Die Einstellungskarte Time Machine (Abschnitt 2.5 auf Seite 55).

3. Moderne Dateisysteme können spezielle Abbuchungstechniken für die Verwaltung von Speicher verwenden, bei denen Kapazitäten mehrfach gezählt werden, obwohl sie in Wirklichkeit nur einmal vorhanden sind.

Apples Dateisystem *APFS* gehört zu diesen modernen Dateisystemen. Es unterstützt unter anderem die folgenden, heute üblichen Techniken, die zu Verwirrung bei Speicherplatzangaben führen können:

- *APFS* benötigt keine Partitionierung mehr. Innerhalb eines *APFS*-Speicherbereichs können mehrere Volumes angelegt werden, ohne dass der Bereich in Partitionen unterteilt werden muss. (Ein von *APFS* verwalteter Bereich liegt jedoch selbst in einer Partition, einem sogenannten *APFS-Container*, damit er gegenüber den nicht von *APFS* verwalteten Bereichen abgegrenzt werden kann.) Die Volumes im Container können sich den Speicherplatz teilen, d.h. freie Blöcke müssen nicht fest einem Volume zugeordnet werden, sondern stehen potenziell jedem der Volumes zur Verfügung. Daraus ergibt sich, dass der freie Speicher nun mehrfach gezählt wird, von jedem Volume, der ihn nutzt. Betrachten Sie einen *APFS-Container* mit 250 GB, der 4 Volumes enthält: Wir haben nun 4 Volumes à 250 GB, also scheinbar 1.000 GB, obwohl real nur 250 GB vorhanden sind. Die Kapazität wird *überbucht*, was erst dann einen Konflikt auslöst, wenn jedes Volume tatsächlich sein zugewiesenes Maximum nutzen würde.
- *APFS* unterstützt eine Schnappschussfunktion. Auf Wunsch kann sich das Dateisystem seinen Zustand zu einem bestimmten Zeitpunkt über das ganze Volume hinweg „merken“. Auf Knopfdruck kann dieser Zustand innerhalb von Sekunden wiederhergestellt werden. Es können beliebig viele dieser „eingefrorenen“ Zustände angelegt werden, so lange noch freie Kapazität vorhanden ist, um die jeweils alte und aktuelle Version aller Daten zu speichern. Technisch funktioniert die Schnappschussfunktion so, dass gelöschte oder überschriebene Versionen von Datenblöcken nicht mehr wirklich verworfen werden, sondern in ihrer früheren Fassung gespeichert bleiben. Beachten Sie, dass der hierfür verbrauchte Speicher nicht auf der Dateiebene sichtbar wird. Ein Volume verbraucht auf diese Weise mehr Platz als die Summe aller seiner momentan gespeicherten Dateien. Moderne Datensicherungsprogramme verwenden üblicherweise Schnappschüsse.

Wenn ein Volume *APFS* nutzt, kann daher die Frage nach freiem Speicherplatz möglicherweise gar nicht mehr so einfach beantwortet werden.

TinkerTool System kann die verschiedenen Sichten auf Speicherplatz, die von macOS unterstützt werden, für jedes Volume anzeigen:

1. Öffnen Sie den Unterpunkt **Speicherplatz** auf der Einstellungskarte **Systemicherheit**.
2. Wählen Sie das gewünschte Volume mit dem Aufklappmenü **Volume** aus.

Das System-Volume ist intern in einen Nur-Lese-Teil, einen Schreib-/Lese-Teil und einen gerade laufenden, versiegelten Volume-Schnappschuss aufgespalten. Dies wird in der Regel von macOS verborgen und alle drei Volumes teilen sich den gleichen Speicherplatz, so dass sie nur als einzelnes Volume im Aufklappmenü präsentiert werden.

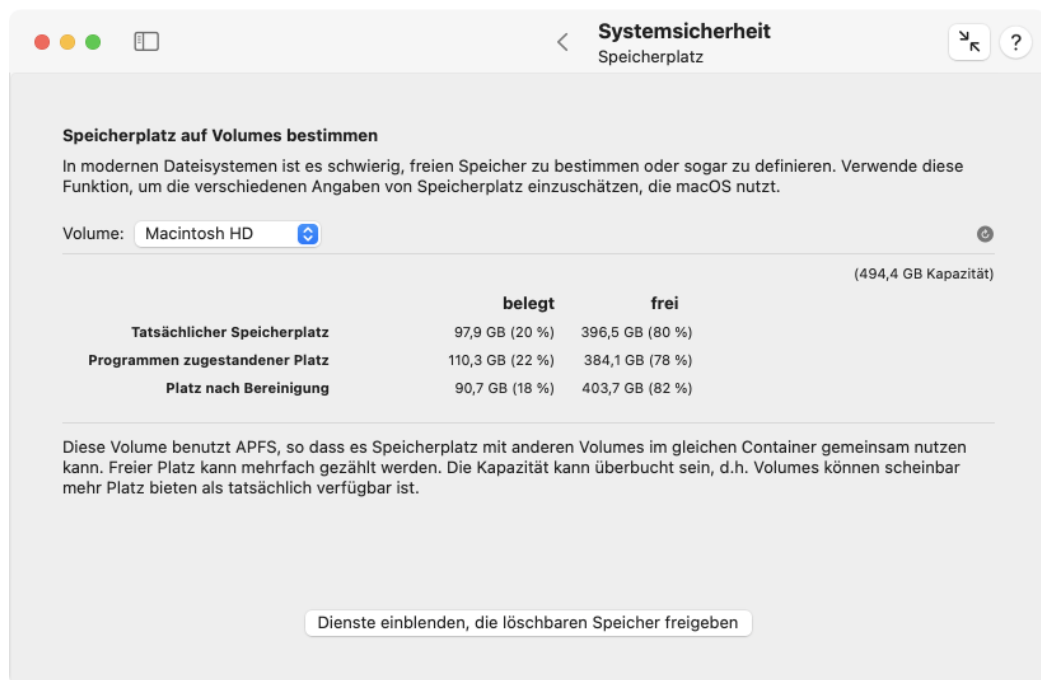


Abbildung 3.34: Freier Speicherplatz kann bei modernen Dateisystemen unterschiedlich definiert sein

Die verschiedenen Definitionen von belegten und freiem Speicher werden nun in einer Tabelle dargestellt, ebenso wird die physische Gesamtkapazität genannt. Unterhalb der Tabelle finden Sie bei Verwendung von APFS einen entsprechenden Warnhinweis. Beachten Sie beim Vergleich mit anderen Programmen, dass die korrekte Maßeinheit für die Anzeige von Speicher wie gewünscht in TinkerTool System eingestellt ist, siehe auch Grundlegende Bedienungshinweise (Abschnitt 1.3 auf Seite 8), Abschnitt *Anzeigen von Speichergrößen*.

- **Tatsächlicher Speicherplatz** ist der physische Speicher, der auf dem Volume zur Nutzung abgebucht ist.
- **Programmen zugestander Platz** ist der Speicher, der für normale Anwenderprogramme uneingeschränkt zur Verfügung steht. Aus Sicherheitsgründen wird für das Betriebssystem selbst eine gewisse Reserve einkalkuliert.
- **Platz nach Bereinigung** ist Speicher, der zur Verfügung stehen würde, wenn das Betriebssystem gezwungen wird, „unwichtige“ Daten automatisch zu löschen, um auf diese Weise mehr tatsächlichen Speicherplatz zurückzugewinnen. Die Differenz zwischen physisch freiem und unbereinigt freiem Speicher wird von Apple *löschrer Speicher* genannt. Was darunter konkret zu verstehen ist, kann je nach Systemversion verschieden sein. Es kann sich zum Beispiel um Mediendateien für bereits abgespielte Leihfilme handeln, die jederzeit aus der Cloud wieder heruntergeladen werden könnten, oder um Lokale APFS-Schnappschüsse, die von Time Machine angelegt wurden.

Was Apple unter „Bereinigung“ versteht, um den löschbaren Speicher wiederzugewinnen, ist nicht genau definiert.

Sie können sich allerdings über den Knopf **Dienste einblenden, die löschbaren Speicher freigeben** die Liste derjenigen Systemdienste anzeigen lassen, die sich im Moment bei macOS angemeldet haben, um bei Bedarf löschbaren Plattenplatz freigeben zu können.

3.6.2 Programmintegrität

Auf der Einstellungskarte Programme (Abschnitt 3.3 auf Seite 178) haben Sie bereits den Punkt **Sicherheitsprüfung** kennengelernt, mit dem verschiedene Aspekte eines Programms unter Sicherheitsgesichtspunkten untersucht werden konnten.

Auf der Einstellungskarte **Systemsicherheit** können Sie einen bestimmten Teil dieser Prüfung, nämlich denjenigen, der auf der digitalen Versiegelung von Programmcode (*Codesigning*) beruht, für eine große Zahl von Programmen gleichzeitig durchführen, z.B. für das gesamte System-Volumen. Hiermit ist es möglich, die gesamte Sicherheitssituation eines Computers schnell einzuschätzen.

Die Prüfung berücksichtigt die folgenden Punkte:

- Ist jedes Programm digital versiegelt und erfüllt die Versiegelung die Sicherheitsanforderungen des gerade laufenden Betriebssystems?
- Ist irgendein Programm nach seiner Versiegelung verändert worden?
- Ist jedes Siegel vertrauenswürdig?

Diese Massenprüfung ist auf Programme für die grafische Oberfläche beschränkt. Sie können im Rahmen einer solchen Prüflaufs keinen ausführbaren Code für die Befehlszeile, oder andere versiegelte Komponenten, wie z.B. Disk Images, prüfen.

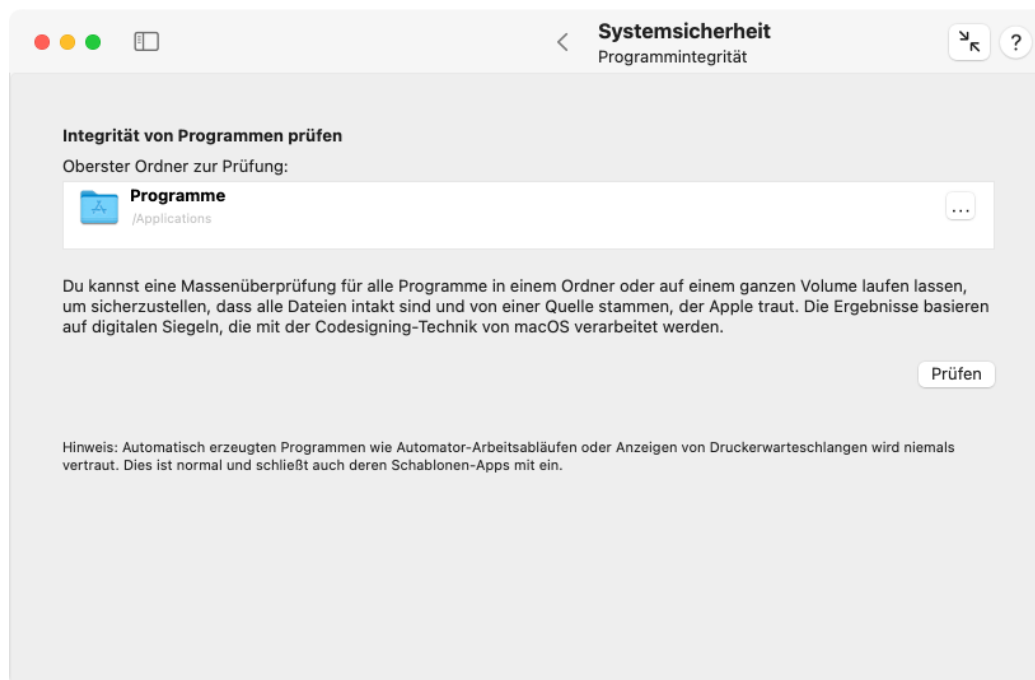


Abbildung 3.35: Alle Programme des Systems können auf Wunsch überprüft werden

1. Öffnen Sie den Unterpunkt **Programmintegrität** auf der Einstellungskarte **System-sicherheit**.
2. Ziehen Sie den Ordner mit den Programmen, die Sie prüfen möchten, aus dem Finder in das Feld **Oberster Ordner zur Prüfung**. Sie können auch den Knopf [...] drücken, um zum Ordner zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.
3. Drücken Sie den Knopf **Prüfen**.

Sie können nicht nur einen Ordner, sondern auch ein ganzes Volume zur Prüfung auswählen. Die Massenprüfung wird automatisch auf ein einzelnes Volume begrenzt, auch wenn es Verweise auf andere Volumes enthält.

Die Prüfung kann sehr lange Zeit benötigen, je nach dem, wie viele Programme enthalten und wie groß diese sind. Besonders große Programme, wie z.B. Xcode oder aufwändige Computerspiele können die Prüfung stark verzögern. Während die Massenprüfung läuft, können Sie den Knopf **Stopp** im Wartefenster betätigen, um die Prüfung abubrechen.

Aus technischen Gründen können angefangene Prüfvorgänge nicht in allen Fällen sofort beendet werden, wenn Sie den **Stopp**-Knopf drücken. TinkerTool System führt angefangene Prüfungen möglicherweise noch im Hintergrund zu Ende, was den Mac noch für einige Zeit belasten kann, verwirft aber dann die Ergebnisse. Um laufende Prüfungen wirklich sofort abubrechen, müssen Sie das Programm nach Drücken von **Stopp** beenden.

Nach dem Ende aller Prüfungsschritte wird das Endergebnis in einer Tabelle angezeigt. Es werden alle Programme mit Namen aufgelistet und die oben genannten Aspekte der Prüfung in den hinteren drei Spalten mit Symbolen gekennzeichnet:

- **Versiegelt:** das Programm ist mit Apples Codesigning-Technik versiegelt
- **Intakt:** das Siegel ist nicht gebrochen, d.h. alle Komponenten des Programms sind unverändert. Es wurde auch nichts hinzugefügt oder entfernt. Die Anforderungen des laufenden Betriebssystems an das Siegel werden eingehalten.
- **Vertrauenswürdig:** Das Siegel wurde von einer Partei unterzeichnet, der Apple im Moment vertraut.

Als Symbole werden verwendet:

- **grüner Punkt:** die Prüfung wurde bestanden
- **rotes Kreuz:** die Prüfung wurde nicht bestanden
- **leeres Feld:** die Prüfung konnte nicht durchgeführt werden

Wenn Sie eine Zeile der Ergebnistabelle auswählen, werden Details über das Programm und die Prüfung angezeigt. Über das Lupensymbol können Sie das jeweilige Programm im Finder anzeigen lassen. Die Zeile **Entdecktes Problem** gibt bei einem Fehlschlag der Prüfung an, welche Ursache dazu geführt hat, dass die Prüfung nicht bestanden wurde. Sie können für das ausgewählte Programm auch den Knopf **Schließen und volle Sicherheitsprüfung für gewähltes Programm durchführen** drücken, um das Programm automatisch auf der Karte Programme (Abschnitt 3.3 auf Seite 178) zu öffnen und dort ausführlich prüfen zu lassen.

Durch Anklicken des Knopfes **Textbericht** können Sie eine Kopie der Ergebnistabelle in Textform erhalten. Der Bericht kann ausgedruckt werden oder Sie können ihn im *Rich Text Format* in eine Textdatei exportieren.

Programme, die automatisch vom Betriebssystem erzeugt wurden und nicht von einem Software-Entwickler werden grundsätzlich *nicht* als vertrauenswürdig eingestuft. Dazu gehören unter anderem Arbeitsabläufe, die mit Automator erstellt wurden, Programme zur Anzeige von Druckerwarteschlangen, aber auch deren jeweils zugehörige Schablonenprogramme, aus denen macOS bei Bedarf die konkreten Programme erstellt. Dieses Verhalten ist normal und kein Grund zur Besorgnis.

3.6.3 Systemprotokoll auf verdächtige Benutzeraktivität prüfen

Um die Sicherheit eines Mac zu gewährleisten, der öffentlich zugreifbar ist, kann es hilfreich sein, das Systemprotokoll automatisch auf Einträge durchsuchen zu lassen, die sich auf das Identifizieren von Benutzern oder das Freischalten privilegierter Vorgänge beziehen. Tritt hier eine Häufung ungewöhnlich vieler Fehlschläge (beispielsweise die Eingabe von falschen Kennworten) auf, ist zu vermuten, dass Einbruchsversuche auf dem Computer stattgefunden haben. Öffentlich zugreifbar kann hierbei heißen, dass sich Tastatur und Bildschirm (in der klassischen Datentechnik *Konsole* genannt) nicht an einem überwachten Ort befinden, z.B. in einem Arbeitsraum einer Schule. Es kann aber genauso heißen, dass geschützte Dienste, für die eine Anmeldung eines Benutzers erforderlich ist, aus dem lokalen Netzwerk oder aus dem Internet erreichbar sind.

TinkerTool System kann das vorhandene Systemprotokoll bezüglich der folgenden Vorgänge auswerten:

- erfolgreiche und fehlgeschlagene Anmeldung am Anmeldeschirm von macOS,
- erfolgreiche und fehlgeschlagene Anmeldung im Sperrbildschirm, d.h. nach dem Beenden des Bildschirmschoners oder nach dem Ruhezustand,
- alle erfolglosen Versuche, einen privilegierten Vorgang genehmigen zu lassen, sowohl lokal, als auch bei Zugriff über einen Netzwerkdienst.

Diese Liste erhebt keinen Anspruch auf Vollständigkeit. Wie lange Einträge im Systemprotokoll gespeichert bleiben, ist nicht vorhersagbar. Dies hängt von der jeweiligen Betriebssystemversion, individuellen Einstellungen, der Verwendung von Wartungsfunktionen und dem vorhandenen Speicherplatz ab. Anmeldungen bei FileVault finden außerhalb von macOS statt und sind deshalb in der Regel nicht im Protokoll enthalten.

Um die Auswertung zu starten, wählen Sie bei **Suche nach** den gewünschten Punkt aus und drücken Sie dann auf den Knopf **Prüfen**. Die Suche kann einige Zeit in Anspruch nehmen, je nach dem wie groß das vorhandene Protokoll ist. Das Ergebnis wird in einem herausgleitenden Fenster dargestellt.

- Bei der Auswertung der Daten zu Konsole und Sperrbildschirm werden erfolgreiche Anmeldevorgänge mit einer grünen Markierung hinterlegt, fehlgeschlagene mit einer roten Markierung.
- Bei der Auswertung zur Genehmigung privilegierter Vorgänge beziehen sich *alle* aufgelisteten Einträge auf Fehlschläge.

Die Übersichten werden durch Originalauszüge aus dem Systemprotokoll gebildet. Sie enthalten deshalb in der Regel Einträge in englischer Sprache, die von der jeweiligen macOS-Version abhängen.

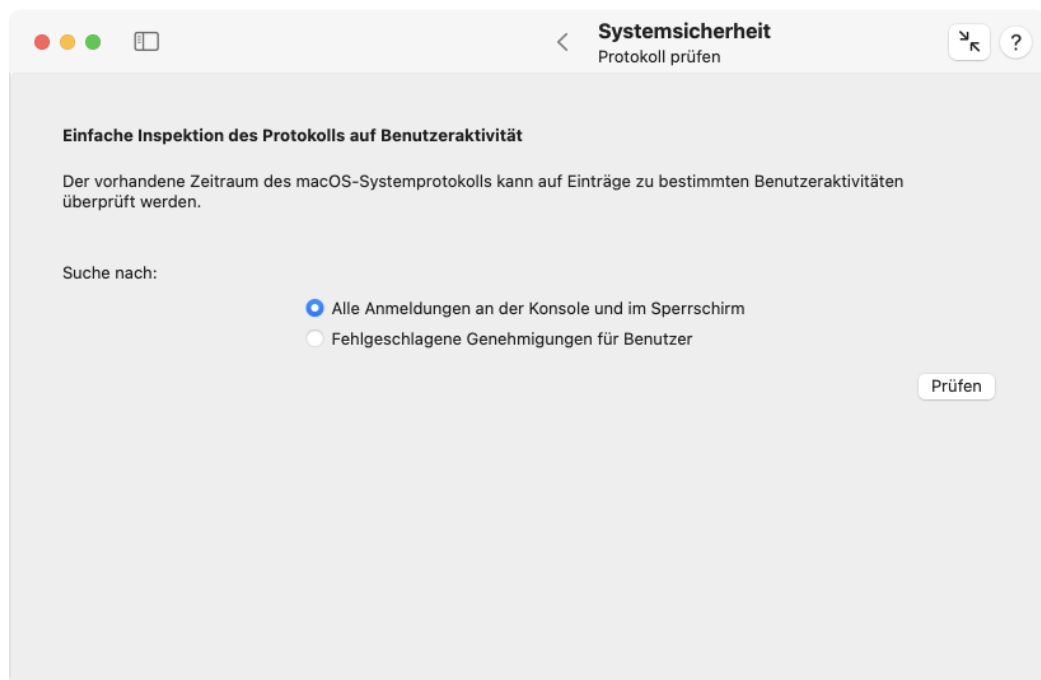


Abbildung 3.36: Das Systemprotokoll lässt sich auswerten, um mögliche Einbruchversuche zu erkennen

3.7 Die Einstellungskarte APFS

3.7.1 Überblick über APFS-Volumes

Wie bereits im vorigen Kapitel (Abschnitt 3.6 auf Seite 222) erläutert, verwendet Apples Dateisystem *APFS* (*Apple File System*) moderne Techniken zur Organisation von Speicherplatz, die auf den ersten Blick verwirrend sein können.

Der Unterpunkt **Überblick** auf der Einstellungskarte **APFS** versucht, die einzelnen Objekte, die im Rahmen der verschiedenen APFS-Techniken auf den Festplatten angelegt wurden, aus Sicht ihrer hierarchischen Beziehungen untereinander darzustellen und zeigt eine vollständige Liste aller APFS-Datenstrukturen auf allen Datenträgern, die im Moment an den Mac angeschlossen sind. Mithilfe der Aufdeckungsdreiecke in der Spalte **Objekt** können Sie die einzelnen Elemente aufklappen und deren Bestandteile einsehen. Es werden die folgenden Begriffe verwendet:

- **APFS-Container** sind die physischen Abschnitte auf Festplatten oder SSDs, welche die „Zonen“ des Speichermediums markieren, in denen APFS aktiv ist.
- **Physische Datenträger** befinden sich eine Ebene unterhalb in der Hierarchie, denn ein APFS-Container kann sich über mehrere physische Speichereinheiten erstrecken. Im Standardfall befindet sich ein APFS-Container auf einer einzelnen Platte. Er könnte aber auch mehrere Platten eines Software-RAIDs verwenden, oder er könnte auf einem Fusion Drive abgelegt sein, einem Verbund aus einer SSD und einer mechanischen Festplatte.
- **APFS-Volume-Gruppen** stellen eine Möglichkeit dar, um mehrere Volumes aus dem gleichen Container zu einer einzelnen Einheit zusammenzufassen. APFS-Volume-

Gruppen sind in der Lage, eine Funktion namens *Firmlink* bereitzustellen, was bedeutet, dass ein und dieselbe Datei mehrfach auf verschiedenen Volumes dieser Gruppe auftauchen kann, obwohl sie tatsächlich nur ein einziges Mal gespeichert ist.

- **APFS-Volumes** erscheinen als getrennte Einheiten, die klassische Plattenlaufwerke simulieren. Partitionen werden von APFS-Volumes nicht benötigt. Sie können zur Laufzeit hinzugefügt oder entfernt werden, ohne dass das Betriebssystem angehalten werden muss. Volumes innerhalb desselben Containers teilen sich den gleichen physischen Speicherplatz, so dass jedem Volume aus seiner Sicht der gesamte Container zur Verfügung steht. Dies heißt allerdings, dass der gleiche belegte oder freie Speicherplatz mehrfach gezählt werden kann. Beispielsweise stellt ein Container mit 1 TB, der 4 Volumes enthält, virtuell 4 TB an Speicher bereit, obwohl nur 1 TB tatsächlich verfügbar ist. Um Konkurrenzsituationen zwischen Volumes des gleichen Containers zu vermeiden, ist es möglich, für ein Volume *reservierten Speicher* zu definieren, d.h. ein Minimum an physischem Speicherplatz, der garantiert immer für dieses Volume verfügbar bleibt, oder *kontingentierte Speicher*, ein Maximum an physischem Platz, der genutzt werden darf, selbst wenn mehr im Container zur Verfügung steht.

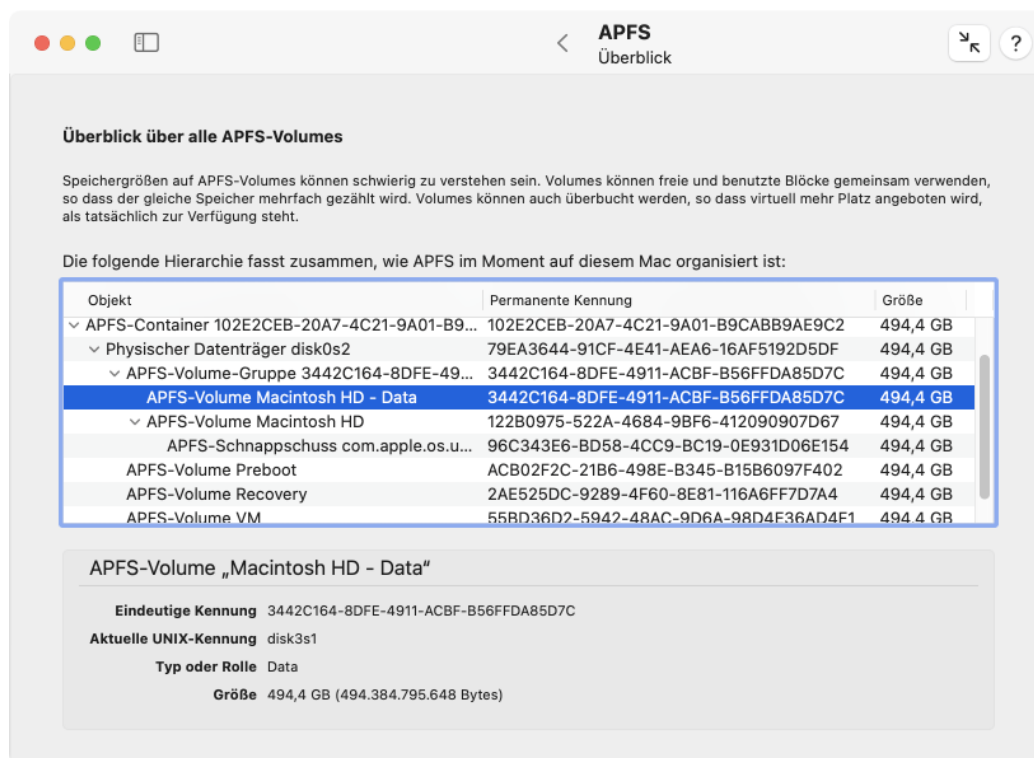


Abbildung 3.37: Der Zusammenhang der einzelnen APFS-Objekte lässt sich als Hierarchie darstellen

Wenn Sie eine Zeile der Tabelle anklicken, werden die ausführlichen Kennungs- und Größendaten in der Detailbox im unteren Bereich des Fensters eingeblendet. Die Tabelle wird automatisch aktualisiert, wenn Sie APFS-Datenträger anschließen oder trennen. Dies gilt auch, wenn Sie z.B. mit dem Festplattendienstprogramm Änderungen an der APFS-Organisation vornehmen. APFS-Volumes erscheinen auch dann in der Tabelle, wenn sie gerade nicht aktiviert sind.

Beachten Sie, dass sich ein APFS-Container über mehrere physische Datenträger erstrecken kann. Das gilt beispielsweise dann, wenn ein Container auf einem *Apple Fusion Drive* gespeichert ist, einem per Software realisierten Verbund aus einer SSD und einem mechanischen Festplattenlaufwerk. Bei einem Fusion Drive ist das von macOS als „schneller“ eingestufte Laufwerk mit der Typangabe **Main** und das als langsamer, aber größer eingestufte Laufwerk mit dem Typ **Secondary** markiert.

APFS-Volumes können mit einer besonderen Kennzeichnung versehen sein, die diesem Volume eine spezielle Aufgabenstellung zuweist. Diese Angabe wird als *APFS-Rolle* bezeichnet. Im Moment hat Apple die folgenden Typen von Rollen vorgesehen:

- **System:** Volume zur Speicherung des Betriebssystems
- **Data:** alle veränderlichen Daten von Benutzer und Betriebssystem
- **Recovery:** Minibetriebssystem zur Wiederherstellung
- **VM:** Auslagerungsspeicher als Teil des Virtuellen Speichermanagements
- **Preboot:** der Boot-Loader zum Laden und Starten des Betriebssystems
- **Installer:** Vorübergehende Nutzung für Daten, die während der Installation des Betriebssystems benötigt werden
- **Baseband:** Firmware zum Betrieb der Funk-Hardware eines Mobilgeräts, wird nur von iOS oder iPadOS genutzt.
- **Update:** ein Hilfs-Volume, das während der Verarbeitung von Betriebssystem-Updates verwendet wird
- **XART:** ein Hilfs-Volume, das dazu benötigt wird, Informationen in die oder aus der sicheren Enklave zu transportieren, z.B. Fingerabdruckdaten
- **Hardware:** ein Hilfs-Volume, das Firmware für Hardware-Komponenten speichert
- **Backups:** ein Volume, das als Ziel für Time Machine-Sicherungen verwendet wird
- **Enterprise:** ein Volume, das Gerätedaten speichert, falls dieser Computer in das Fernmanagementsystem einer Organisation eingebunden ist
- **Sidecar:** reserviert für zukünftige Funktionen von Time Machine

3.7.2 APFS-Schlüssel und Volume-Eigentum

APFS-Volumes können verschlüsselt werden. Bei modernen Macintosh-Baureihen wird der eingebaute Flash-Speicher grundsätzlich per Hardware verschlüsselt, auch wenn die Benutzer sich dessen nicht bewusst sind und den eigentlichen Schlüssel gar nicht kennen. In diesem Fall muss die Hardware die zugehörigen Schlüssel oder Schlüsselteile verwalten und den Zugriff auf diese Daten auf sichere Weise regeln. Hierzu wird die *Sichere Enklave* verwendet, ein kryptografisch abgesicherter Hochsicherheitsbereich im Prozessor, der für jeden Mac einzigartig ist und für den auch Apple bestimmte Schlüsselteile nicht kennt. Für jedes verschlüsselte APFS-Volume gibt es eine Liste von Benutzern, die in der Lage sind, auf die zur Entschlüsselung des Volumes nötigen Daten zugreifen zu können. Dies hat nichts mit Dateirechten zu tun. In der Liste der Accounts können neben echten Personen auch institutionelle Rollen eingetragen sein. Kommt beispielsweise FileVault auf dem macOS-Start-Volume zum Einsatz, können nicht nur lokale Benutzer das Volume entschlüsseln. Die Entschlüsselung ist alternativ auch über einen *Wiederherstellungsschlüssel*

möglich, der bei der Einrichtung wahlweise einem Administrator als Textcode mitgeteilt wurde, oder auf Wunsch bei Apple in der iCloud hinterlegt wird. In diesem Fall wird die Rolle der FileVault-Wiederherstellung auch als scheinbarer Benutzer in die Schlüsselverwaltungsliste eines APFS-Volumes eingetragen.

TinkerTool System kann für jedes APFS-Volume die Liste der zur Entschlüsselung fähigen Benutzer, bzw. Schlüsselzugriffsrollen abrufen. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie den Unterpunkt **Schlüssel & Eigentum** auf der Einstellungskarte **APFS**.
2. Klicken Sie auf **Volume-Schlüssel Zugriffsparteien abfragen**
3. Wählen Sie das gewünschte APFS-Volume aus.

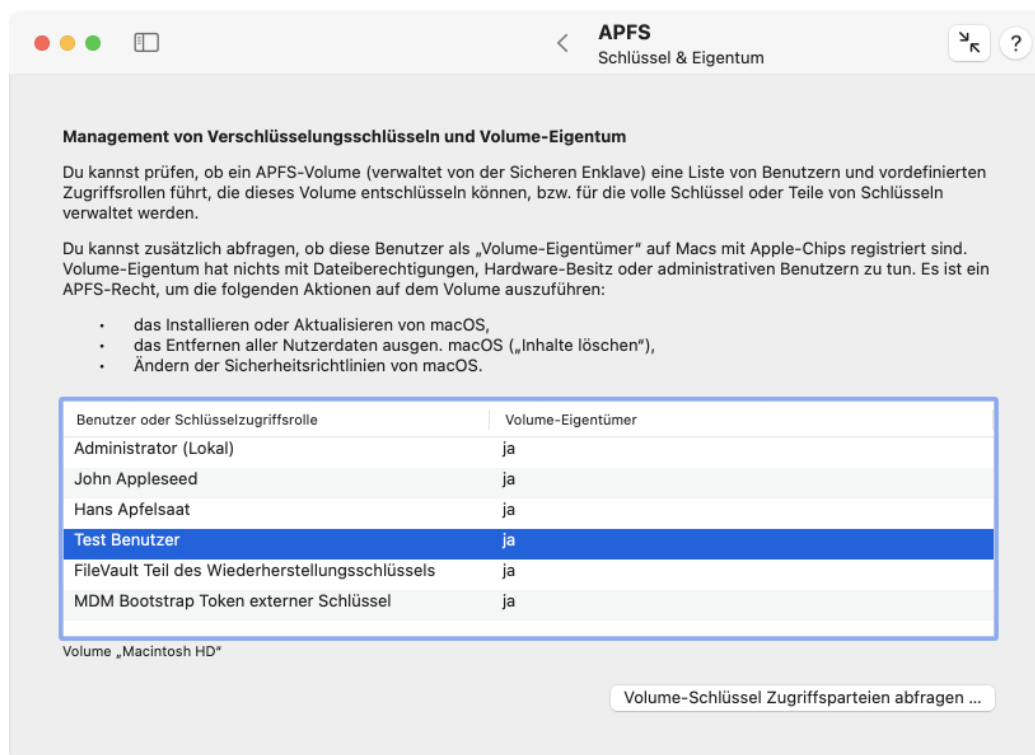


Abbildung 3.38: Ist ein APFS-Volume verschlüsselt, wird eine Liste der Benutzer mit Schlüsselzugriff verwaltet. Bei Macs mit Apple-Chips kann zusätzlich eine Eigentümereigenschaft hinterlegt sein.

Der Flash-Speicher moderner Macs ist wie erwähnt immer verschlüsselt. Handelt es sich um einen Mac mit Apple-Chips wird diese Tatsache darüberhinaus für weitergehende Sicherheitsmaßnahmen verwendet. Für diese Macs wird der Begriff des **Volume-Eigentums** eingeführt. Dieser Begriff hat nichts mit Dateirechten oder legalem Besitz des Mac zu tun. Unter anderem werden die folgenden Operationen für alle Benutzer gesperrt, die nicht als Volume-Eigentümer des Volumes gelten, auf denen das betroffene macOS-System gespeichert ist:

- das Installieren oder Aktualisieren von macOS,
- das Entfernen aller Benutzerdaten bei Beibehaltung des Betriebssystems, d.h. das Nutzen der Funktion **Einstellungen und Inhalte löschen**,

- das Ändern der Startsicherheitsrichtlinien.

Diese Eigenschaft wird in der Spalte **Volume-Eigentümer** für jeden Benutzer angezeigt, der das Volume entschlüsseln kann. Bei Macs mit Intel-Prozessoren gibt es diese Sicherheitsmaßnahme nicht.

3.7.3 Automatische Defragmentierung

macOS ist in der Lage, Datenträger automatisch zu defragmentieren. *Defragmentieren* bedeutet, dass die Speicherblöcke, aus denen jeweils eine einzelne Datei besteht, möglichst nahe auf dem Speichermedium beieinander liegen und nicht in weit auseinanderliegenden Teilen (*Fragmenten*). Auf diese Weise muss der Schreib-/Lesekopf einer magnetischen Festplatte sich möglichst wenig bewegen, wenn eine Datei gelesen wird. Dadurch steigt die gefühlte Geschwindigkeit von Festplattenzugriffen. Der Computer arbeitet schneller. Die Fragmente entstehen, wenn Dateien vergrößert werden müssen und direkt „hinter“ den belegten Blöcken der Speicher bereits durch andere Dateien belegt ist. Die Defragmentierung verschiebt alle Blöcke an eine andere Stelle der Festplatte, wo im Moment gerade ein genügend großer freier Bereich bereitsteht, alle Blöcke direkt hintereinander abzulegen, wenn möglich.

Bei modernen SSD-Speichermedien, bzw. Flash-Speicher gibt es keinen Schreib-/Lesekopf. Jeder Block kann direkt adressiert und gleich schnell gelesen werden, egal wie weit auseinander die Teile einer Datei auf dem Speichermedium verstreut sind. Deshalb ist es nicht sinnvoll, Defragmentierung auf solchen Speichermedien einzusetzen. Im Gegenteil: Da bei der Defragmentierung viele oder alle Blöcke einer Datei an eine andere Stelle kopiert werden müssen und jeder Speicherblock eines Flash-Speichers nur eine begrenzte Anzahl von Schreiboperationen verträgt, erhöht sich die Abnutzung. Die Lebensdauer des Speichermediums sinkt.

Defragmentierung darf deshalb nur auf konventionellen magnetischen Festplatten mit Schreib-/Lesekopf eingesetzt werden, nicht auf SSDs.

Da Apple seit einigen Jahren keine magnetischen Platten in Macs mehr verwendet, ist die automatische Defragmentierung für das APFS-Format standardmäßig in macOS abgeschaltet. Es kann aber sinnvoll sein, für externe magnetische Platten die automatische Defragmentierung einzuschalten. Dabei werden die Dateien nicht zu bestimmten Terminen defragmentiert, sondern nur bei Bedarf, nämlich wenn eine Datei genügend groß ist, so dass sich der Aufwand für eine Defragmentierung lohnt, und nur wenn diese Datei sowieso bereits während eines laufenden Schreibvorgangs geändert werden muss.

Mit TinkerTool System können Sie abfragen, auf welchen APFS-Volumes automatische Defragmentierung aktiv ist. Auf Wunsch können Sie diese Funktion ein- oder ausschalten. Führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Defragmentierung** auf der Einstellungskarte **APFS**.
2. Klicken Sie den Knopf **Aktualisieren** unterhalb der Tabelle.

In der Tabelle werden Volumes, die sich auf SSDs, bzw. Flash-Speicher befinden, automatisch weggelassen, wenn diese Eigenschaft zuverlässig erkannt wurde. Es kann jedoch Speichermedien geben, bei denen aus technischen Gründen nicht ermittelt werden kann, ob die Speicherung magnetisch oder per Solid-State-Technik erfolgt. Sie sollten selbst anhand der jeweiligen Volume-Namen erkennen, auf welchem Medium ein Volume liegt und Defragmentierung nur für magnetische Platten einschalten.

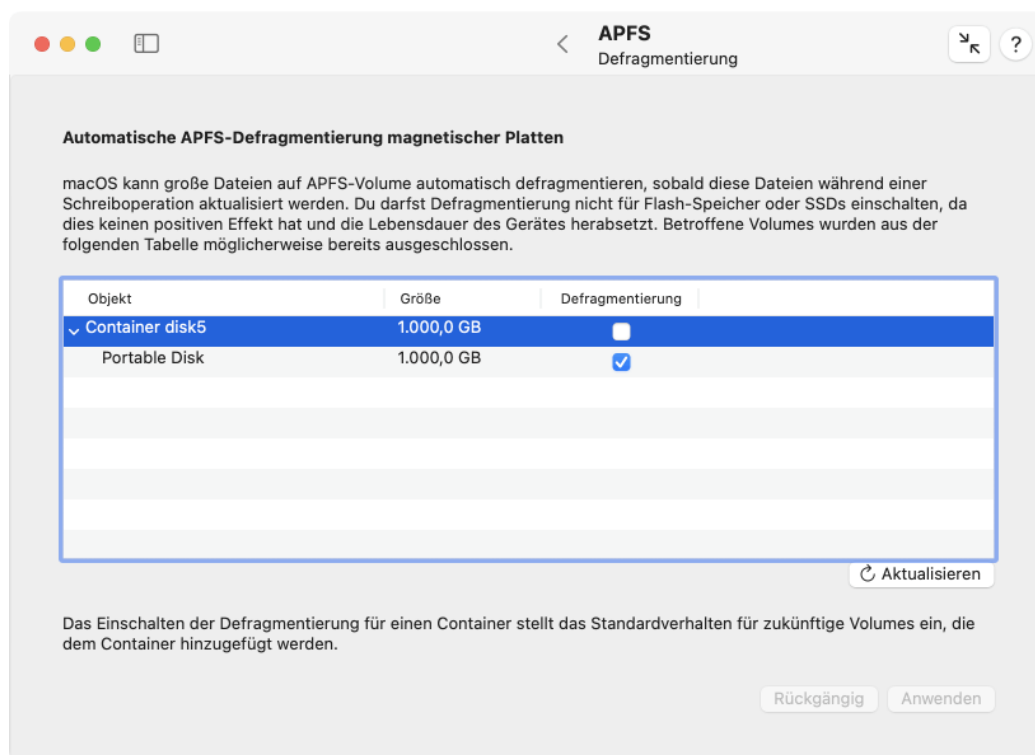


Abbildung 3.39: Automatische Defragmentierung kann für APFS-Volumes und Container aktiviert werden, die sich auf magnetischen Platten befinden

Durch Ankreuzen der jeweiligen Tabellenzeile können Sie für jedes Volume und jeden Container die automatische Defragmentierung aktivieren. Die Änderungen treten in Kraft, sobald Sie auf **Anwenden** klicken. Falls Sie Defragmentierung für einen APFS-Container einschalten, wirkt sich dies nur auf *zukünftige* Volumes aus, die auf diesem Container später angelegt werden, nicht auf bereits bestehende Volumes.

3.7.4 Arbeiten mit APFS-Schnappschüssen

Sinn und Zweck von Schnappschüssen wurde bereits im Kapitel zur Karte Time Machine (Abschnitt 2.5 auf Seite 55) ausführlich behandelt. Jeder *Lokale Schnappschuss* von Time Machine ist technisch mithilfe eines *APFS-Schnappschusses* realisiert. Dem Betriebssystem steht es jedoch frei, Schnappschüsse auch für andere Zwecke als Time Machine einzusetzen. Mit dem Unterpunkt **Schnappschüsse** auf der Einstellungskarte **APFS** haben Sie die Gelegenheit, mit *allen* APFS-Schnappschüssen zu arbeiten, also nicht nur mit denen, die im Moment von Time Machine genutzt werden.

Apple gesteht dem Benutzer allerdings nicht das Recht zu, nach eigenem Ermessen neue APFS-Schnappschüsse auf einem Volume anzulegen. Es gibt keine offizielle Möglichkeit, diesen Vorgang für ein Volume einzuleiten, wenn dies nicht von einem Datensicherungsprogramm aus durchgeführt wird, das von Apple eine offizielle Genehmigung hierzu erhalten hat. *Der Benutzer kann nur indirekt neue APFS-Schnappschüsse erstellen, indem an Time Machine ein Wartungsbefehl geschickt wird, Lokale Schnappschüsse anzulegen.* Das ist naturgemäß mit der Einschränkung verbunden, dass *nur* auf denjenigen APFS-Volumes Schnappschüsse angelegt werden, die von Time Machine zur Datensicherung vorgesehen sind, und dass auf *allen* diesen Volumes gleichzeitig ein Schnappschuss erzeugt wird.

Wenn Sie auf diese indirekte Art APFS-Schnappschüsse anlegen möchten, betätigen Sie den Knopf **Neue Schnappschüsse per Time Machine anlegen ...** in der linken unteren Ecke des Fensters.

Möchten Sie die aktuellen Schnappschüsse einsehen, die sich auf einem bestimmten APFS-Volume befinden, gehen Sie wie folgt vor:

1. Öffnen Sie den Unterpunkt **Schnappschüsse** auf der Einstellungskarte **APFS**.
2. Wählen Sie das gewünschte Volume mit dem Aufklappmenü **APFS-Volume auswählen:**.

Die vollständige Liste der Schnappschüsse wird daraufhin in der Tabelle eingeblendet. Wenn Sie eine Zeile der Tabelle auswählen, werden Detailangaben auch noch einmal ausführlich in der Box in der unteren Hälfte des Fensters angezeigt. Sie sehen den von macOS vergebenen Namen des Schnappschusses, eine kurze, numerische Kennung, die auch als *XID* bezeichnet wird und eine weltweit einmalige Kennung in Form einer UUID. Das Feld **private Größe** gibt an, wie viel Speicherplatz der jeweilige Schnappschuss tatsächlich für sich selbst verbraucht. Virtuell enthält ein Schnappschuss eine Kopie des gesamten Volumes, wie dieses zu einem bestimmten Zeitpunkt in der Vergangenheit war, also sehr viel mehr Speicher. Dabei teilt der Schnappschuss sich diesen Speicherplatz jedoch mit dem aktuellen Volume-Inhalt oder anderen Schnappschüssen. Solcher mehrfach gezählter Speicher wird jedoch nicht wirklich zusätzlich verbraucht und geht in die private Größe eines Schnappschusses nicht ein.

Der Hinweis **Begrenzer** gibt an, ob macOS diesen Schnappschuss auch dazu verwendet, die minimale Größe des jeweiligen APFS-Containers festzulegen. In macOS ist es möglich,

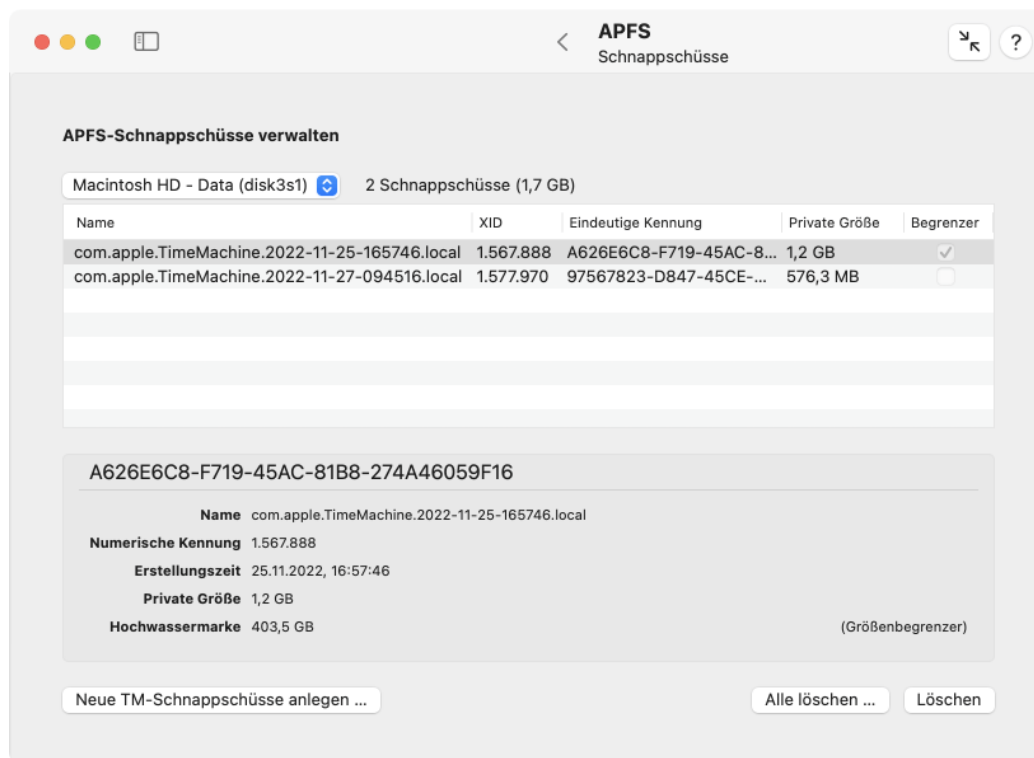


Abbildung 3.40: APFS-Schnappschüsse können eingesehen und gelöscht werden

die Größe einer Festplattenpartition nachträglich zu verändern, ohne die gesamte Platte löschen und neu partitionieren zu müssen. Bei Nutzung von APFS entspricht das Verkleinern einer Partition dem Schrumpfen des in der Partition enthaltenen APFS-Containers. Da sich jedoch mehrere Volumes und mehrere Schnappschüsse den Speicherplatz eines Containers teilen, kann das Schrumpfen ein komplizierter Vorgang sein. Der „hinterste“ APFS-Schnappschuss im Container bestimmt dabei, auf welche Minimalgröße der Container geschrumpft werden könnte. In der Detailansicht wird diese hintere Grenze eines Schnappschusses als **Hochwassermarkte** angegeben.

Wenn Sie ein oder mehrere Schnappschüsse in der Tabelle ausgewählt haben, können Sie den Knopf **Löschen** betätigen, um die jeweiligen Schnappschüsse sofort zu löschen. Dabei verändern sich die sichtbaren Nutzdaten des APFS-Volumes nicht. Nur die Möglichkeit, per Knopfdruck auf den jeweiligen früheren Zustand des Volumes zurückgehen zu können, fällt weg. Mit dem Knopf **Alle löschen ...** werden nach einer ausdrücklichen Bestätigung alle APFS-Schnappschüsse des Volumes entfernt.

3.7.5 Kopieren von APFS-Daten

macOS stellt Systemfunktionen zur Verfügung, mit denen es möglich ist, die einzelnen Teile der APFS-Hierarchie, also Container, Volume-Gruppen oder Volumes, besonders schnell zu kopieren. In diesem Zusammenhang wird die Schnellkopierfunktion auch als *Replizieren* bezeichnet. Die Kopie weist eine besonders hohe Wiedergabetreue auf. Sie ist ein identischer Klon des Originals und übernimmt auch dessen Volume-Namen. Die weltweit eindeutigen UUIDs werden natürlich trotzdem neu vergeben.

Im einzelnen können Sie folgende APFS-Objekte klonen:

- einen APFS-Container in einen anderen APFS-Container: Hierbei wird der Ziel-Container komplett gelöscht. Der Kopiervorgang ist allerdings nur dann möglich, wenn alle Volumes im Quell-Container eindeutige APFS-Rollen haben (siehe auch einleitender Abschnitt).
- eine Volume-Gruppe oder ein Volume in einen anderen APFS-Container: die betroffenen Volumes werden dem Ziel-Container hinzugefügt. Es gehen also keinerlei Daten verloren.
- eine Volume-Gruppe in ein bestehendes Volume: Das Ziel-Volume wird hierbei gelöscht. Es darf außerdem nicht bereits Teil einer anderen Volume-Gruppe sein.
- ein Schnappschuss eines Volumes in ein anderes Volume: Auch hier wird das Ziel-Volume gelöscht. Der Kopiervorgang erfordert es, dass das Quell-Volume gerade aktiviert ist.

Es ist möglich, eine vollständige Installation von macOS zu klonen. Das Betriebssystem und Ihre Benutzerdaten sind in einer Volume-Gruppe gespeichert, die aus einem Volume mit der Rolle *System* und einem Volume mit der Rolle *Daten* besteht. Falls das System gerade läuft, gibt es dort außerdem ein versiegeltes Schnappschuss-Volume für das System-Volume. Mindestens zwei zusätzliche Volumes mit den Rollen *Preboot* und *Recovery* müssen ebenso kopiert werden. TinkerTool System und macOS erkennen automatisch, ob Sie vorhaben, eine macOS-Installation zu replizieren und fügen automatisch den Minimalsatz benötigter Volumes hinzu. Dies funktioniert nur dann richtig, wenn folgende Bedingungen eingehalten werden:

- Falls Sie das laufende System kopieren möchten, wählen Sie das *Schnappschuss-Volume des System-Volumes* als Quelle aus und ein leeres APFS-Volume als Ziel.
- Falls Sie ein anderes System kopieren möchten, wählen Sie *dessen Volume-Gruppe* als Quelle und ein leeres APFS-Volume als Ziel.



Leider bedeutet eine erfolgreiche Replikation aller benötigten macOS-Volumes nicht immer, dass die Kopie korrekt starten kann oder auf jedem Computer starten könnte. Insbesondere Macs mit Sicherheits-Chips können den Start verweigern, bevor nicht die angefertigte Kopie von Apple per Internet erneut für diesen Mac freigeschaltet wurde.

- Falls die Hardware durch einen Apple-Sicherheits-Chip oder einen Apple-Prozessor geschützt wird, kann eine zusätzliche Autorisierung durch einen Benutzer-Account des kopierten Systems erforderlich sein, um starten zu dürfen.
- Falls die Hardware durch einen Apple-Prozessor geschützt wird, kann es notwendig sein, das Betriebssystem mit einer übereinstimmenden Version „überzuinstallieren“, um OS und Hardware wieder aneinander zu binden. Ihre Benutzerdaten bleiben unberührt.
- Falls eine solche Neuinstallation von macOS nötig ist, unterstützt dies Apple möglicherweise nicht für alle Typen von Plattenlaufwerken, Firmware-Versionen und Macintosh-Modellen.

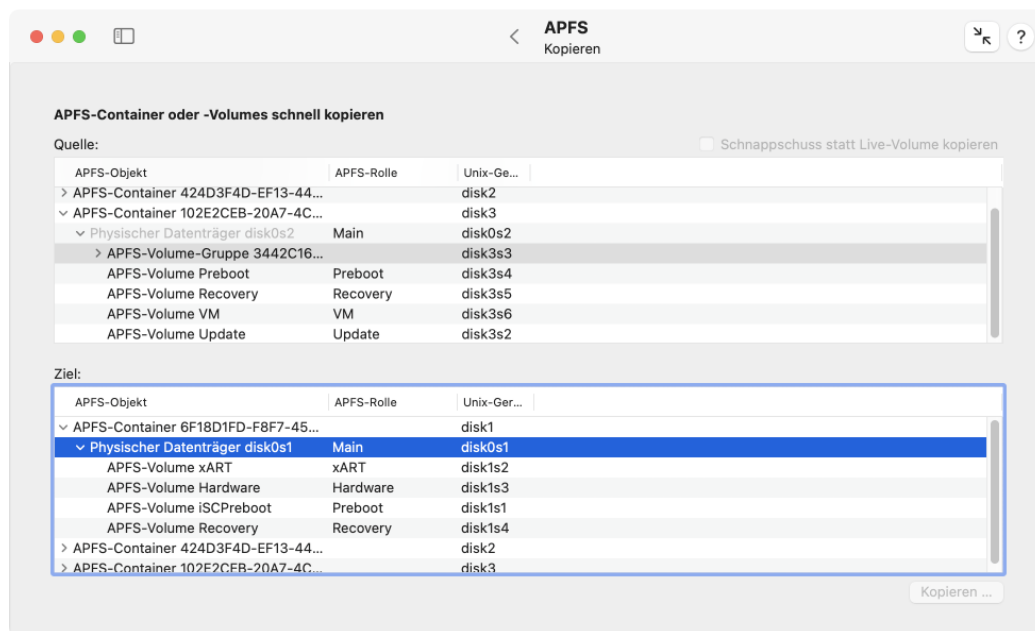


Abbildung 3.41: APFS-Objekte lassen sich besonders schnell kopieren

Quelle und Ziel müssen sich grundsätzlich in zwei verschiedenen APFS-Containern befinden. Es ist also nicht möglich, ein Volume im gleichen Container zu duplizieren. Führen Sie die folgenden Schritte durch, um ein APFS-Objekt zu kopieren:

1. Öffnen Sie den Unterpunkt **Kopieren** auf der Einstellungskarte **APFS**.
2. Wählen Sie das Objekt, das kopiert werden soll, in der Tabelle **Quelle** aus. Falls gewünscht, kreuzen Sie die Option **Schnappschuss statt Live-Volume kopieren** an.
3. Wählen Sie das Ziel, wohin kopiert werden soll, in der Tabelle **Ziel** aus.
4. Betätigen Sie den Knopf **Kopieren**

Während Sie Quelle und Ziel auswählen, blendet TinkerTool System am unteren Rand des Fensters bereits eine Vorschau ein, welche Operation ausgeführt wird, wenn Sie das Kopieren starten würden. Falls im Ziel-Container Daten verloren gehen (weil ein oder mehrere Volumes bereits bestehende Volumes ersetzen), werden Sie in einem gesonderten Dialog noch einmal extra darauf hingewiesen und müssen dies bestätigen. Wenn Sie einen Schnappschuss kopieren, wird außerdem der Name des Schnappschusses abgefragt. Ist das Klonen gestartet, erscheint ein herausgleitendes Dialogfenster, in dem ein Bericht des laufenden Kopiervorgangs erstellt wird. Der Kern des Berichts wird von macOS selbst erstellt und ist aus technischen Gründen nur in englischer Sprache verfügbar. Nach Beendigung des Vorgangs kann der Bericht gesichert oder gedruckt werden.

Durch Betätigen des Knopfes **Stopp** kann TinkerTool System dazu veranlasst werden, einen laufenden Kopiervorgang abubrechen. Dies wird jedoch nicht empfohlen und sollte nur im Notfall verwendet werden. macOS ist im Moment noch nicht ausgereift genug, mit einem „halb“ kopierten APFS-Volume korrekt umzugehen. Das Volume wird im Ziel-Container als beschädigtes Volume unter einem vorübergehend vergebenen Namen erscheinen. In solch einem Fall wird empfohlen, den Computer neu

zu starten und dann das betroffene Volume mit dem Festplattendienstprogramm aus dem Ziel-Container zu entfernen.

Kapitel 4

Systemeinstellungen

4.1 Die Einstellungskarte System

4.1.1 Laufwerk

Ruhezustandszeitgeber für Festplatten

Fast alle Festplatten enthalten einen eingebauten Zeitgeber für den Ruhezustand, der dazu gedacht ist, den Spindelmotor abzuschalten und damit Energie zu sparen, wenn das Laufwerk eine bestimmte Zeit lang nicht genutzt wurde. macOS unterstützt eine simple ja/nein-Einstellung, um diese Ruhezustandsfunktion von Festplatten steuern zu können. Sie kann über die Wahlmöglichkeit **Wenn möglich, Ruhezustand für Festplatten aktivieren** auf der Karte **Energie sparen** (bzw. **Batterie**) der **Systemeinstellungen** kontrolliert werden. Das Einschalten dieser Funktion bewirkt, dass der Ruhezustandswecker jedes Festplattenlaufwerks auf 10 Minuten Inaktivität gestellt wird.

Mit TinkerTool System können Sie die eingebauten Zeitgeber der Festplatten genauer steuern, indem Sie den exakten Wert für die Zeit vorgeben. Zeitintervalle zwischen 1 Minute und 2 Stunden 59 Minuten können ausgewählt werden. Um die Ruhezustandszeit für alle Plattenlaufwerke zu ändern, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Laufwerke** auf der Einstellungskarte **System**.
2. Ziehen Sie den Schieberegler **Ruhezustand der Festplatten aktivieren wenn unbe-
nutzt für** auf den gewünschten Wert.

Drosseln von Operationen mit niedriger Priorität

Der Kern des Betriebssystems verwendet Prioritäten, um seine Ein-/Ausgabe-Jobs zu organisieren, hauptsächlich Platten- und Netzwerkoperationen, die als Dienst für Anwendungen ausgeführt werden, die gerade laufen. Die Arbeit, die für unsichtbare Hintergrundprogramme erledigt wird (wie beispielsweise Time Machine), hat niedrigere Priorität als Vorgänge, die für interaktive Anwendungen (wie ein Textverarbeitungsprogramm) ausgeführt werden. Operationen mit niedriger Priorität werden durch *Throttling* gedrosselt, d.h. sie werden künstlich verlangsamt, indem sie in gewissen kurzen Zeitintervallen pausieren. In einigen Situationen kann diese Leistungsbenachteiligung lästig sein, z.B. wenn Sie darauf warten, dass ein ausgedehnter Time Machine-Sicherungslauf abgeschlossen wird. Time Machine-Jobs bestehen hauptsächlich aus Ein-/Ausgabe-Vorgängen auf Platten oder dem Netz, so dass sie entscheidend von dieser Verlangsamung betroffen sind.

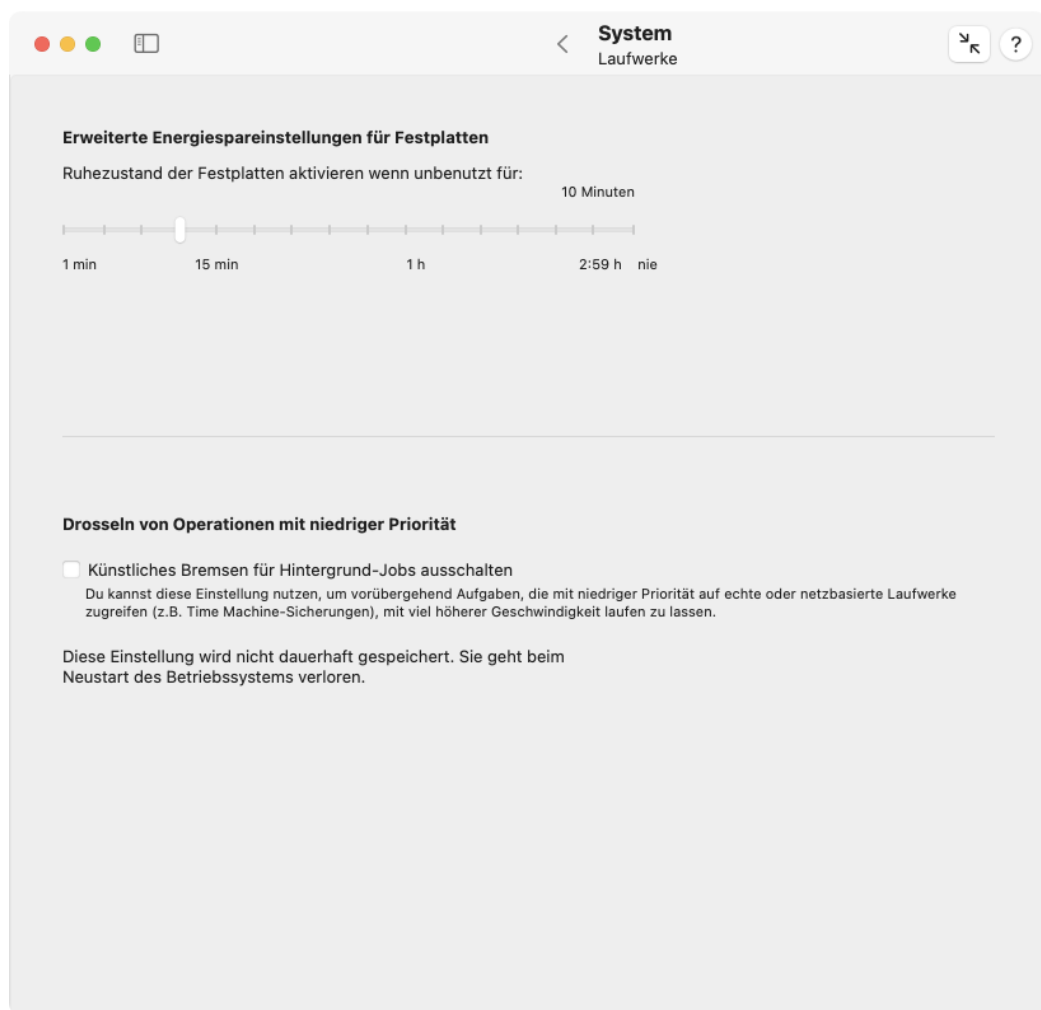


Abbildung 4.1: Laufwerke

Sie können die Drosselung von Ein-/Ausgabe-Operationen für Hintergrundprogramme vorübergehend abschalten, so dass sie die gleiche Priorität erhalten wie andere Aufgaben. Die Änderung tritt sofort in Kraft, aber wird nicht dauerhaft als Vorgabe gespeichert. Die Einstellung wird nur so lange beibehalten, bis Sie entweder das Betriebssystem herunterfahren oder die Einstellung wieder ändern.

Um das Drosseln von Ein-/Ausgabevorgängen niedriger Priorität im Systemkern abzuschalten, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Laufwerke** auf der Einstellungskarte **System**.
2. Setzen Sie ein Häkchen bei **Künstliches Bremsen für Hintergrund-Jobs ausschalten**.

Unter sehr seltenen Umständen können laufende Jobs sich gegenseitig blockieren während die Drosselung abgeschaltet ist, was dazu führt, dass das System hängt. Da alle Ein-/Ausgabe-Vorgänge in diesem Fall mit gleicher Priorität laufen, kann das System wichtige Jobs nicht mehr so verplanen, dass sie vor denen mit niedriger Priorität abgearbeitet werden. Vorgänge mit hoher Priorität müssen möglicherweise auf eine große Zahl von Vorgängen niedriger Priorität warten, was die Wahrscheinlichkeit erhöht, dass Jobs, die voneinander abhängig sind, reihum aufeinander warten, was eine gegenseitige Blockade auslöst.

4.1.2 Volumes

macOS verfolgt die Strategie, automatisch alle Plattenlaufwerke und deren Volumes zu erkennen, die gegenwärtig am Computer angeschlossen sind, wobei diese aktiv gemacht und auf der Bedieneroberfläche angezeigt werden. Dies ist in gewissen Situationen nicht nützlich, z.B. wenn sich eine Windows-Partition auf Ihrem Computer befindet, die bei der Arbeit mit macOS nicht angezeigt werden soll, oder wenn Sie eine Sicherungskopie Ihrer Systempartition auf einem zweiten Laufwerk als Reserve vorhalten. Mithilfe von TinkerTool System können Sie macOS veranlassen, bestimmte Volumes nicht mehr automatisch zu aktivieren.

Diese Einstellung bezieht sich nur auf rein automatische Aktivierungsvorgänge. Falls Sie eine verschlüsselte Platte verwenden, wird macOS grundsätzlich versuchen zu ermitteln, ob diese Platte Volumes enthält, wobei diese Platte keine lesbaren Identifizierungsmerkmale enthält (weil sie verschlüsselt ist). Sobald Sie das Kennwort zur Entsperrung eingeben, werden die zugehörigen Volumes aktiviert, denn dies ist ein manueller Vorgang auf dieser Platte.

Eine zweite, davon unabhängige Auswahl erlaubt es Ihnen, zu bestimmen, ob das System die Ausführung von Programmen zulassen soll, die auf bestimmten Volumes gespeichert sind. Diese Funktion kann hilfreich sein, wenn Sie „fremde“ Laufwerke an Ihren Computer anschließen, die Programme enthalten, die für andere Betriebssysteme geschrieben wurden und mit macOS nicht kompatibel sind. Sie können dann nicht mehr irrtümlich versuchen, die Programme auf solchen Laufwerken zu starten.

In beiden Fällen muss macOS eine Technik verwenden, sich zuverlässig auf jedes Laufwerk, bzw. jedes Volume beziehen zu können. Dies wird über sogenannte universelle, einzigartige Bezeichner (*Universal Unique Identifiers, UUIDs*) realisiert. UUIDs sind z.B. eine Zeichenfolge wie 7F176A72-72B2-3D69-19FC-27ABBEFA662D, für die garantiert ist, dass sie auf jedem Volume jeder Platte der Welt nur ein einziges Mal vorkommt. Sie brauchen UUIDs nicht von Hand einzugeben. TinkerTool System findet die UUIDs automatisch heraus und

hilft Ihnen dabei, die Laufwerke durch Angabe von deren aktuellen Volume-Namen und Dateisystemen zu identifizieren.

Neben den oben erwähnten Einschränkungen für verschlüsselte Volumes bestehen weitere Einschränkungen für Volumes, die durch Benutzerprogramme, *also nicht durch macOS selbst*, aktiviert werden. Solche Volumes werden entweder direkt von TinkerTool System ausgeschlossen, weil sie bereits als nicht kompatibel mit den Volume-Tabellen erkannt werden, oder ein Eintragen in die beiden Tabellen hat keinerlei Wirkung, da macOS am Aktivierungsvorgang gar nicht beteiligt ist. Beispiel für solche Aktivierung durch Benutzerprogramme ist Apples Technik *LIFS (Live File Provider File System)* oder die Drittanbieter-Software *macFUSE (Macintosh File System in User Space)*. In manchen Versionen von macOS wird LIFS standardmäßig dazu verwendet, Daten von fremden Dateisystemen wie ExFAT oder NTFS zu verarbeiten. Apples Nutzung von LIFS kann sich in jeder Version von macOS ändern.

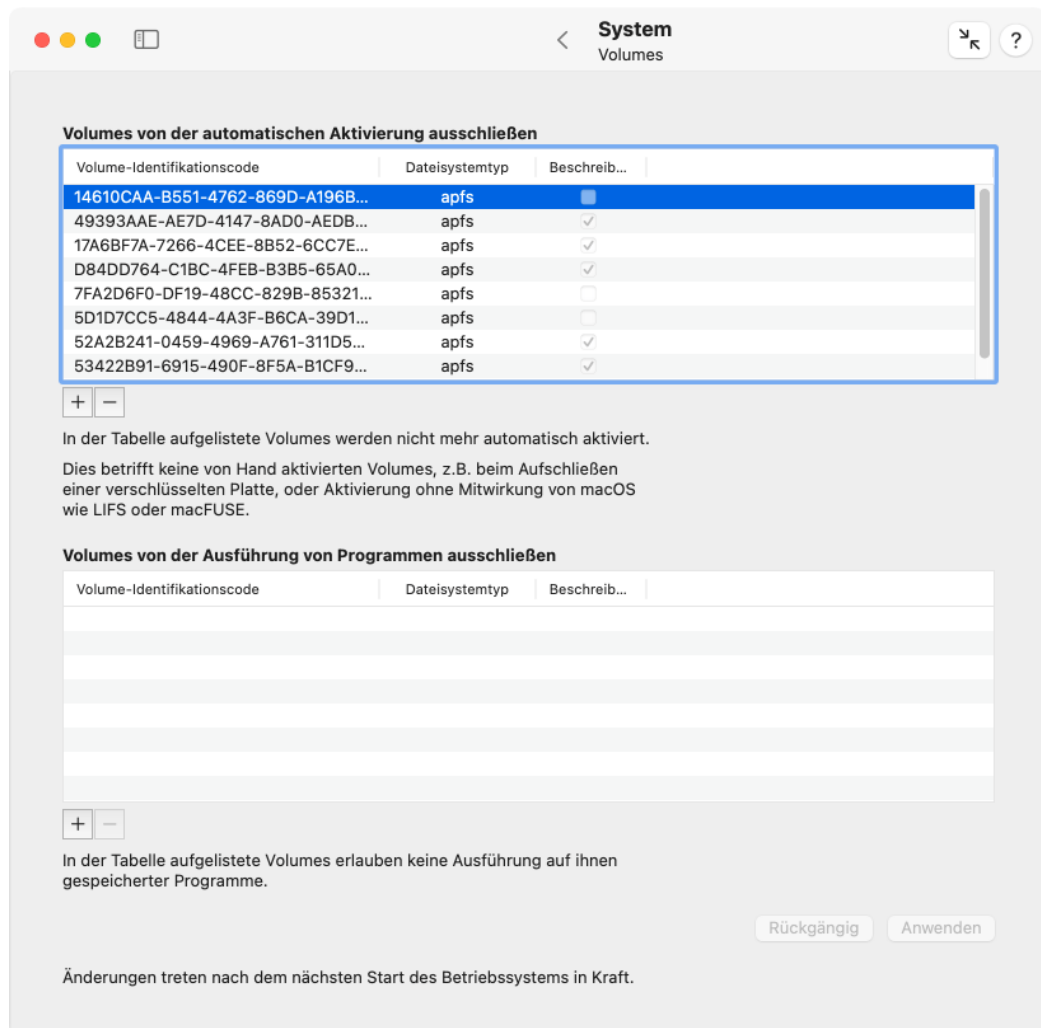


Abbildung 4.2: Volumes

Führen Sie die folgenden Schritte durch, wenn Sie bestimmte Platten-Volumes von der

automatischen Aktivierung oder der Ausführung von Programmen ausnehmen möchten:

1. Öffnen Sie den Unterpunkt **Volumes** auf der Einstellungskarte **System**.
2. Betätigen Sie den Knopf [+] unterhalb der Tabelle, deren Funktion Sie nutzen möchten.
3. Wählen Sie im Dialogfenster ein oder mehrere Platten-Volumes und drücken Sie **OK**.
4. Nachdem alle Volumes so wie gewünscht eingerichtet wurden, drücken Sie den Knopf **Anwenden** in der unteren rechten Ecke des Fensters.

Es ist auch möglich, Volumes direkt vom Schreibtisch oder dem Computerordner des Finders in die Tabelle zu ziehen. Sie können ein oder mehrere Volumes durch Drücken des Knopfs [-] aus der jeweiligen Tabelle entfernen und Ihre Änderungen abspeichern. Um Ihre Änderungen zu verwerfen und die Tabellen in den Zustand zurückzubringen, der gegenwärtig in macOS eingerichtet ist, drücken Sie den Knopf **Rückgängig**.

Nachdem Sie neue Volumes der Tabelle **Volumes von der automatischen Aktivierung ausschließen** hinzugefügt haben, fragt Sie TinkerTool System, ob Sie die betroffenen Volumes sofort auswerfen möchten, sobald Sie die Änderungen anwenden.

Falls Sie zusätzliche Exemplare von macOS auf Ihrem Mac installiert haben und Sie ein oder mehrere System-Volumes, die macOS 11 oder höher enthalten, zu einer Ausschlusstabelle des Systems hinzugefügt haben, das Sie gerade verwenden, stellen Sie möglicherweise fest, dass Tabelleneinträge für diese Volumes nicht mehr wirksam sind, sobald Sie ein Update oder Upgrade auf den betreffenden System-Volumes eingespielt haben. Dies ist das korrekte und zu erwartende Verhalten, denn ein modernes macOS-Update *löscht* das vorherige System-Volume und *fügt ein neues* mit dem gleichen Namen hinzu.

TinkerTool System kann hier helfend eingreifen: Sobald das Programm genau die beschriebene Situation vorfindet, erscheint automatisch der Knopf **System-Volumes aktualisieren** ... unter den Tabellen. Klicken Sie den Knopf an, um die betroffenen Einträge zu prüfen. Nach Betätigung von **Tabellen aktualisieren** werden die Identifikationscodes der betroffenen System-Volumes automatisch aktualisiert, um die neue Konfiguration widerzuspiegeln. Der Knopf für die Aktualisierungsfunktion ist nicht verfügbar, wenn Sie beginnen, Tabelleneinträge von Hand zu ändern.

4.1.3 Spotlight

Spotlight-Betrieb

Spotlight ist die eingebaute Suchtechnik von macOS, die dazu gedacht ist, Dateien sehr schnell aufzufinden, nachdem der Benutzer Schlüsselworte oder andere Suchkriterien angegeben hat. Die technische Realisierung baut auf verschiedenen Systemdiensten auf, die still im Hintergrund arbeiten. Spotlight kann allerdings manchmal von technischen Problemen betroffen sein, so dass Systemverwalter in bestimmten Situationen den Spotlight-Betrieb feinanzupassen müssen.



Spotlight ist dazu konstruiert, eine der grundlegenden Kernkomponenten von macOS darzustellen. Aus diesem Grund hängen andere Systemdienste und

Programme, die für macOS entwickelt wurden, vom korrekten Betrieb von Spotlight ab und zeigen möglicherweise Fehlfunktionen, nachdem Spotlight abgeschaltet wurde. Dies schließt den Sicherungsdienst Time Machine und das App Store-Programm ein. Aus diesem Grund unterstützt TinkerTool System keine Möglichkeit, Spotlight vollständig abzuschalten. Sie können lediglich den Aufbau der Spotlight-Indexdatenbanken (Indexierung) auf ausgewählten Platten-Volumes ausschalten.

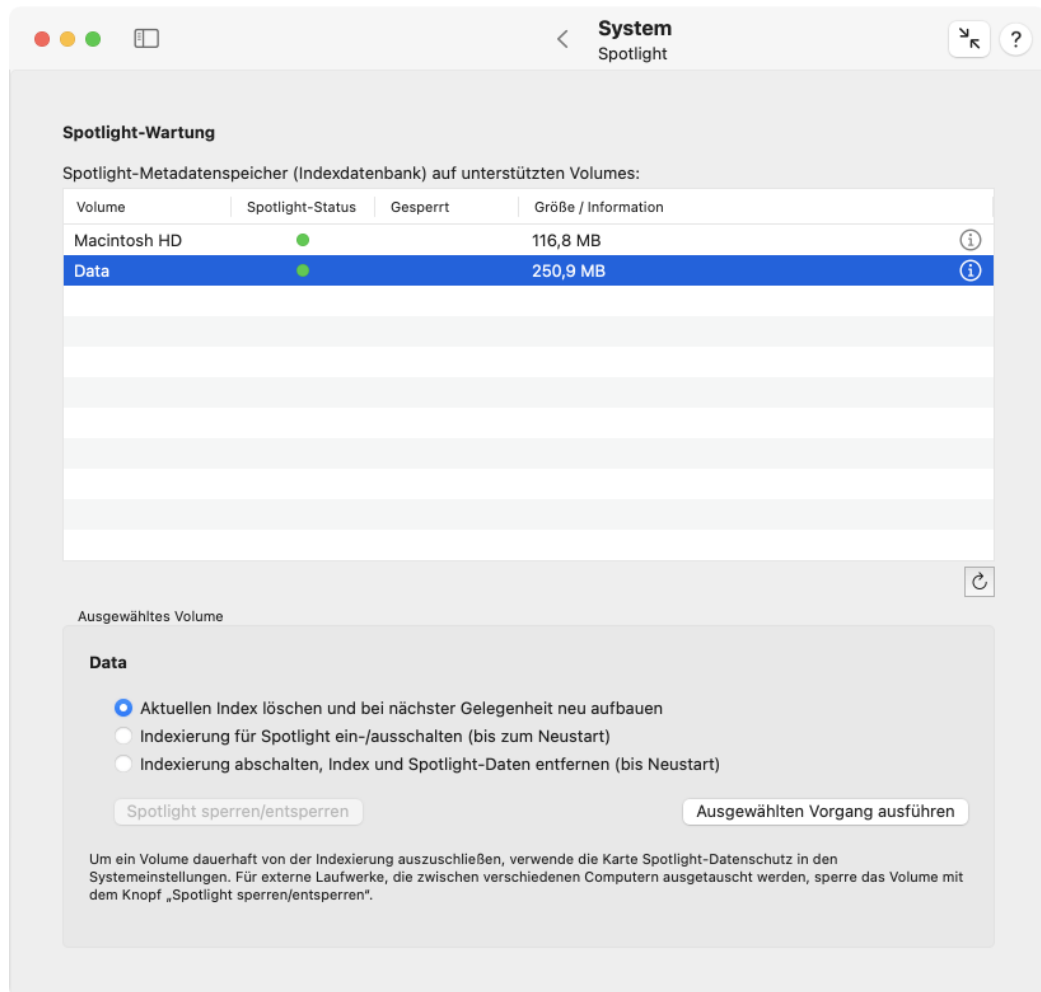


Abbildung 4.3: Spotlight

4.1.4 Spotlight-Indexdatenbanken

Wenn Spotlight aktiv ist, erzeugt es automatisch eine versteckte Indexdatenbank und einige Einstellungsdaten auf jedem Volume, das aktuell mit Ihrem Computer verbunden ist. Die Datenbank und die Einstellungswerte werden gebraucht, um schnell die Inhalte zu finden, nach denen Sie suchen. Diese versteckten Komponenten werden auch *Metadaten Speicher* genannt.

Für jedes Volume erlaubt Ihnen TinkerTool System anzuzeigen, ob Spotlight auf diesem

Volume aktiviert ist (Spalte **Spotlight-Status** mit Anzeige in grün oder rot), ob die Verwendung von Spotlight generell blockiert ist (Spalte **Gesperrt**) und wie viel Plattenspeicherplatz im Moment für den Metadatenpeicher verbraucht wird. Diese Daten werden in der Tabelle **Spotlight-Metadatenpeicher** dargestellt. Nur Volumes, die technisch in der Lage sind, Spotlight zu unterstützen, werden in der Tabelle aufgeführt. Ein Aktualisierungsknopf rechts unter der Tabelle, frischt den Inhalt der Tabelle auf. Dieser Schritt ist außerdem notwendig, damit macOS dem Programm TinkerTool System (nach Anmeldung) die Erlaubnis gewährt, die Größe der Indexdatenbanken berechnen zu dürfen. Der Zugriff auf diese Datenbanken ist abgesichert, da diese möglicherweise vertrauliche Daten beinhalten, nämlich alle Worte aller Dokumente aller Benutzer, die auf dem aktuellen Computer gespeichert sind.

Nachdem Sie eine Zeile in der Tabelle ausgewählt haben, können Sie zwischen mehreren Operationen wählen, die durchgeführt werden können:

- Sie können den Metadatenpeicher auf dem gewählten Volume **löschen**. Hierbei werden die Privatsphären-Einstellungen dieses Volumes zurückgesetzt und eine vollständige Neu-Indexierung aller Dokumente des Volumes erzwungen. Diese Funktion ist hilfreich, wenn die Metadaten beschädigt zu sein scheinen. Sie würden diese Funktion üblicherweise dann verwenden, wenn Sie erkennen, dass Spotlight weniger Dokumente findet, als eigentlich vorhanden sind.
- Sie können die **Indexierung für Spotlight ein-/ausschalten**, was bedeutet, dass alle Indexvorgänge auf dem ausgewählten Volume in der aktuellen Sitzung von macOS entweder gestoppt oder wieder aktiviert werden. Wenn Sie die Indexierung wieder einschalten, wird macOS im Hintergrund die Indexoperationen nach eigenem Ermessen zu einem späteren Zeitpunkt fortsetzen.
- Sie können die Metadatenpeicher auf dem gewählten Volume **entfernen** und die **Indexierung** gleichzeitig **abschalten**. Die Suchdatenbank wird entfernt und Spotlight greift auf die betreffenden Volumes in der gerade laufenden macOS-Sitzung nicht mehr zu.

Um eine dieser Funktionen zu aktivieren, betätigen Sie den Knopf **Ausgewählten Vorgang ausführen**.

Beachten Sie, dass das Abschalten von Indexoperationen nur wirksam ist, bis Sie macOS neu starten. Falls Sie Spotlight nicht über die Einstellung **Siri & Spotlight > Spotlight-Datenschutz ...** in den **Systemeinstellungen** auf den betreffenden Volumes gesperrt haben, wird macOS seine Indexdienste beim nächsten Systemstart wieder aufnehmen.

Wenn Sie das Info-Symbol am Ende einer Tabellenzeile anklicken, können Sie weitere Informationen über Spotlight auf dem betreffenden Volume erhalten. Das Programm blendet eine zusätzliche Anzeige mit folgenden Daten ein:

- die aktuelle Position im UNIX-Dateisystem, an dem sich das Volume tatsächlich befindet
- eine ausführliche Darstellung von Status, Speichergröße und Sperrzustand
- die Information, ob eine Sperre grundsätzlich technisch möglich wäre und TinkerTool System auch nicht davon abrät
- die Betriebssystemversion, die verwendet wurde, um Spotlight ursprünglich auf diesem Volume einzurichten, zusammen mit der Zeitangabe

- die Betriebssystemversion, mit der zum letzten Mal etwas an der Konfiguration von Spotlight auf diesem Volume geändert wurde, zusammen mit der Zeitangabe
- eine Liste von UNIX-Dateipfaden, die vom einem oder mehreren Benutzern dieses Volumes ausdrücklich für die Durchsuchung gesperrt wurden.

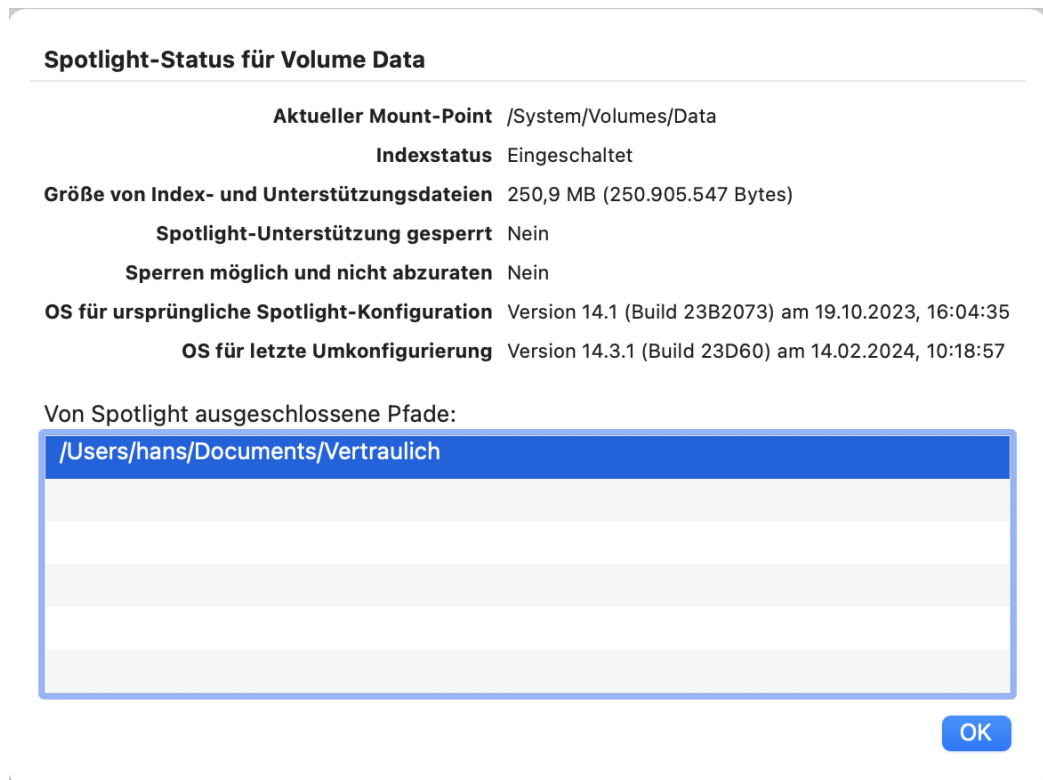


Abbildung 4.4: Weitere Details zu einem indexierten Volume lassen sich abrufen

Unter bestimmten Umständen kann es hilfreich sein, Spotlight-Vorgänge auf einem Platten-Volume dauerhaft zu blockieren, z.B. auf einem langsamen Speicher-Stick, der nur benutzt wird, um Daten an andere Computer weiterzugeben. Dies kann über eine spezielle Markierung geschehen, die unabhängig von der Privatsphäreneinstellung von Spotlight ist. Das Setzen einer solchen Markierung ist insbesondere auf externen Laufwerken, die mit mehreren macOS-Computern genutzt werden, hilfreich, da alle Systeme diese Einstellung automatisch berücksichtigen werden, nachdem sie eingerichtet wurde. Um diese Markierung zu setzen oder zu entfernen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Spotlight** auf der Einstellungskarte **System**.
2. Klicken Sie den Aktualisierungspfeil rechts unterhalb der Tabelle, um sicherzustellen, dass das Programm alle Volumes vollständig analysieren konnte.
3. Wählen Sie das gewünschte Volume in der Tabelle aus.
4. Klicken Sie den Knopf **Spotlight sperren/entsperren ändern ...** in der linken unteren Ecke.

Vorgänge, die schwere Schäden an der Funktionsweise von macOS auslösen könnten, z.B. das Löschen des Spotlight-Index von Time Machine, werden automatisch gesperrt.



Sie sollten es vermeiden, innerhalb kurzer Zeitabstände widersprüchliche Befehle an Spotlight zu senden, z.B. den Index aus-, ein-, dann wieder auszuschalten. Spotlight arbeitet asynchron im Hintergrund und kann mehrere Minuten brauchen, um einen Befehl erfolgreich abzuschließen. Wenn im Hintergrund ein noch nicht abgeschlossener Vorgang läuft, kann die Statusanzeige vorübergehend unstimmig sein oder ein Volume kann komplett aus der Tabelle verschwinden.

Wenn Sie Befehle ausgelöst haben, einen Suchindex neu erstellen zu lassen, können Sie folgt kontrollieren, ob der Indexierungsvorgang im Hintergrund bereits abgeschlossen ist:

1. Öffnen Sie eine Spotlight-Suchabfrage über das Lupensymbol rechts oben in der Menüleiste und geben Sie einen Dateinamen ein, von dem Sie wissen, dass er auf dem betroffenen Volume vorhanden ist.
2. Lassen Sie den Dialog ein paar Sekunden offen.

Wenn der Spotlight-Index noch *nicht* verfügbar ist, blendet macOS nach kurzer Zeit eine Fortschrittsanzeige ein, um darzustellen, wie viel Zeit noch für den Neuaufbau des Index benötigt wird. Wenn der Spotlight-Index bereit ist, wird das Suchergebnis ohne zusätzliche Fortschrittsanzeige dargestellt.

4.1.5 Netz

Einstellungen für das Verbinden mit Dateiservern

Wenn Sie versuchen, eine Verbindung zu einem Dateiserver manuell aufzunehmen, erscheint ein Fenster zur Kennworteingabe. TinkerTool System kann die Systemeinstellung ändern, die steuert, welcher Name von macOS in diesem Fenster vorgeschlagen wird. Sie können zwischen dem **Kurznamen** des aktuellen Benutzers, einem **anderen vorbestimmten Namen** oder der Möglichkeit wählen, überhaupt keinen Namen vorzuschlagen (**Kein Name**). Führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Netz** auf der Einstellungskarte **System**.
2. Wählen Sie die gewünschte Möglichkeit bei **Vorgeschlagener Anmeldename**.

Veraltete Anmeldemethoden

Apple missbilligt den Einsatz veralteter Anmeldemethoden für AFP-Server, die nach heutigen Maßstäben als unsicher gelten. Das Betriebssystem bietet die betroffenen Anmeldeverfahren bei der Kontaktaufnahme zu einem Server nicht mehr an. Dies kann allerdings dazu führen, dass Sie sich mit alten Servern nicht mehr verbinden können. Mit TinkerTool System können Sie ausgewählte Verfahren wieder zur Verwendung freischalten. Führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Netz** auf der Einstellungskarte **System**.

2. Kreuzen Sie alle gewünschten Verfahren bei **Veraltete Anmeldemethoden zulassen** an.

Die folgenden Methoden können aktiviert werden:

- Zwei-Wege-Zufallsschlüsselaustausch
- Diffie-Hellman-Schlüsselaustausch, implementiert nach dem CBC128-Verfahren (Carlisle Adams -/Stafford Tavares -Verschlüsselung mit 128 Bit im Cipher Block Chaining-Betrieb)
- Kennwortübertragung im Klartext
- Verschlüsselungsverfahren Version 2 der „Microsoft® Services für Macintosh“

Da alle Verfahren unsicher und veraltet sind und die Nutzung von AFP-Technik ebenso missbilligt ist, sollten Sie nur so wenige einschalten wie möglich, um die Sicherheit Ihres Netzwerks nicht zu gefährden.

Richtlinien für die Verbindung mit drahtlosen Netzwerken

Jede WLAN-Schnittstelle, die an Ihrem Mac vorhanden ist, unterstützt zwei Einstellungen, die auf der grafischen Oberfläche von macOS normalerweise nicht sichtbar sind: Diese Einstellungen steuern, nach welcher Strategie sich macOS mit vorhandenen WLAN-Netzen verbinden soll. Die Einstellung **Falls mehrere Netze verfügbar** legt fest, welches Netzwerk ausgewählt werden soll, falls gerade mehrere in der Nachbarschaft zugreifbar sind. Zugreifbar bedeutet konkret, dass die Empfangsstärke hoch genug ist und die Zugangsdaten für die eventuelle Verschlüsselung des Netzes bekannt sind. Die folgenden Einstellungen sind möglich:

- **Automatisch:** macOS soll von sich aus das „beste“ Netzwerk auswählen.
- **Bevorzugtes Netz wählen:** Das Netz, mit dem der Mac in der Vergangenheit am häufigsten verbunden war, soll gewählt werden.
- **Nach Rang wählen:** Anhand der Konfiguration im Programm **Systemeinstellungen** und den beobachteten Verbindungen in der Vergangenheit soll eine Rangfolge gebildet und daraus das erste Netz gewählt werden.
- **Letztes Netz wählen:** Das Netz, mit dem der Mac zuletzt verbunden war, soll gewählt werden.
- **Stärkstes Netz wählen:** Das Netz, das im Moment gerade am besten empfangbar ist, soll gewählt werden.

Die besondere Anzeige **Nicht eingestellt** gibt an, dass macOS seit der Installation des Betriebssystems noch keine feste Richtlinie festgelegt hat. Diese Einstellung kann nicht ausgewählt werden.

Falls die Verbindung mit dem nach dieser Richtlinie ausgewählten Netz gerade nicht möglich oder fehlgeschlagen ist, wird die zweite Einstellung **Wenn Verbindung nicht möglich** verwendet. Hier gibt es folgende Werte, die einstellbar sind:

- **Benutzer fragen:** Beim Benutzer wird über einen Dialog angefragt, wie weiter vorgehen werden soll.

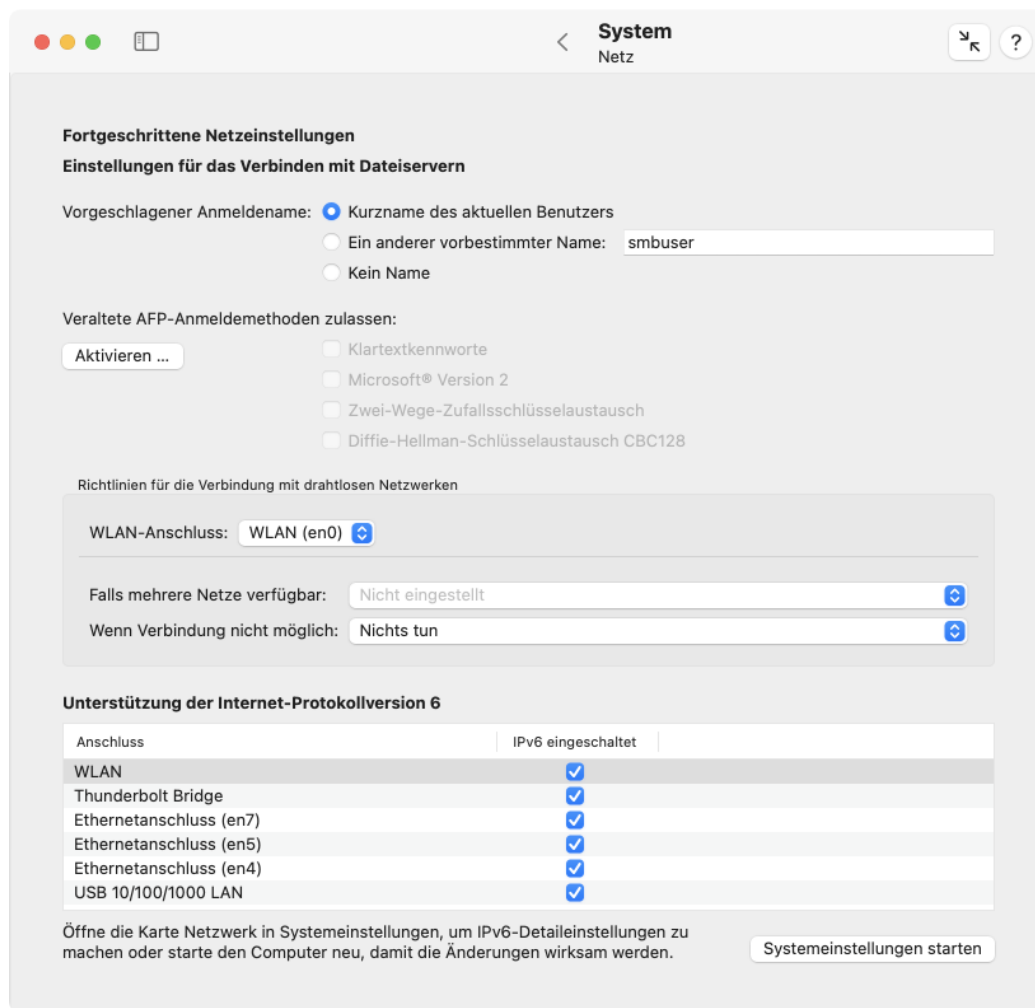


Abbildung 4.5: Netz

- **Mit offenem Netz verbinden:** Es wird das erstbeste Netz ohne Verschlüsselung verwendet, auch wenn es aus der Vergangenheit nicht bekannt ist.
- **Weitersuchen:** Die Suche soll so lange fortgeführt werden, bis eine Verbindung gelingt.
- **Nichts tun:** Die Suche soll nach einem Fehlschlag abgebrochen werden. Es wird dann keine drahtlose Verbindung aufgebaut.

Unterstützung der Internet-Protokollversion 6

macOS zeigt auf der Karte **Netzwerk** des Programms **Systemeinstellungen** standardmäßig keinen Menüpunkt an, um die Unterstützung von IPv6 für bestimmte Netzanschlüsse abschalten zu können. Die Funktion, um **IPv6 auf Aus** zu stellen, ist im Betriebssystem jedoch vorhanden. Sie können TinkerTool System verwenden, um diese Wahlmöglichkeit zu steuern.

1. Öffnen Sie den Unterpunkt **Netz** auf der Einstellungskarte **System** in TinkerTool System.
2. Suchen Sie den Netzwerkanschluss, den Sie ändern möchten, in der Tabelle **Unterstützung der Internet-Protokollversion 6**.
3. Entfernen Sie das Häkchen in der Spalte **IPv6 eingeschaltet**, um IPv6 für den Anschluss in der jeweiligen Zeile abzuschalten.

Sobald Sie die Unterstützung von IPv6 für einen aktiven Netzdienst abgeschaltet haben, gibt Systemeinstellungen dies korrekt wieder, indem ein Menüpunkt **Aus** bei **IPv6 konfigurieren** hinzugefügt wird. Sie können entweder Systemeinstellungen oder TinkerTool System verwenden, um diese Funktion später wieder einzuschalten. Falls Sie hierzu TinkerTool System nutzen, wird Ihre Konfigurationseinstellung automatisch wieder auf diejenige Betriebsart zurückgestellt, die vorher in den Systemeinstellungen definiert war.

Falls Sie Ihre Netzumgebung oder die IPv6-Betriebsart mit **Systemeinstellungen** ändern während TinkerTool System läuft, ist es empfehlenswert, TinkerTool System neu zu starten, um sicher zu stellen, dass das Programm den aktualisierten Status anzeigt.

4.1.6 Zugriffsrechtsfilter für neue Dateisystemobjekte

Im Berechtigungssystem von macOS, das detailliert im Kapitel Die Einstellungskarte ACL-Berechtigung (Abschnitt 3.4 auf Seite 192) beschrieben wird, entscheidet jedes Programm für sich selbst, welche Zugriffsrechte es für eine neue Datei oder einen Ordner gewährt, wenn das Dateisystemobjekt angelegt wird. Dies schließt auch den Finder mit ein, der typischerweise das Programm ist, mit dem neue Ordner angelegt werden.

Sicherheitsprobleme könnten auftreten, wenn Sie schlecht geschriebene oder sehr alte Programme einsetzen, die sich nicht um Berechtigungseinstellungen kümmern. Solche Programme könnten Schreibberechtigung für die Kategorie „Andere Benutzer“ vergeben, was bedeutet, dass fast Jeder – egal ob der Benutzer im aktuellen Computer überhaupt „bekannt“ ist – jedes Dokument, was von diesem Programm angelegt wird, verwenden, überschreiben oder löschen könnte. In Umgebungen, in denen nicht unbedingt angenommen werden kann, dass sich alle Benutzer kooperativ verhalten, wie Schulen oder großen Firmen, könnte eine solche laxen Richtlinie zur Rechtevergabe das System unbenutzbar

machen. Aus diesem Grund verwenden macOS und jedes andere UNIX-System einen *Zugriffsrechtsfilter*. Immer wenn ein Programm eine neue Datei oder einen Ordner anlegt und dabei die anfänglichen Berechtigungseinstellungen vornehmen muss, werden die Berechtigungen zunächst durch einen Filter geschickt, der entscheidet, ob das Programm ein bestimmtes Recht vergeben darf oder nicht. Der Filter korrespondiert direkt mit den drei POSIX-Rechten **Lesen**, **Schreiben** und **Ausführen**, sowie den drei Zugriffsparteien **Eigentümer**, **Gruppeneigentümer** und **Andere**. Für weitere Erläuterungen siehe das Kapitel Die Einstellungskarte ACL-Berechtigung (Abschnitt 3.4 auf Seite 192).

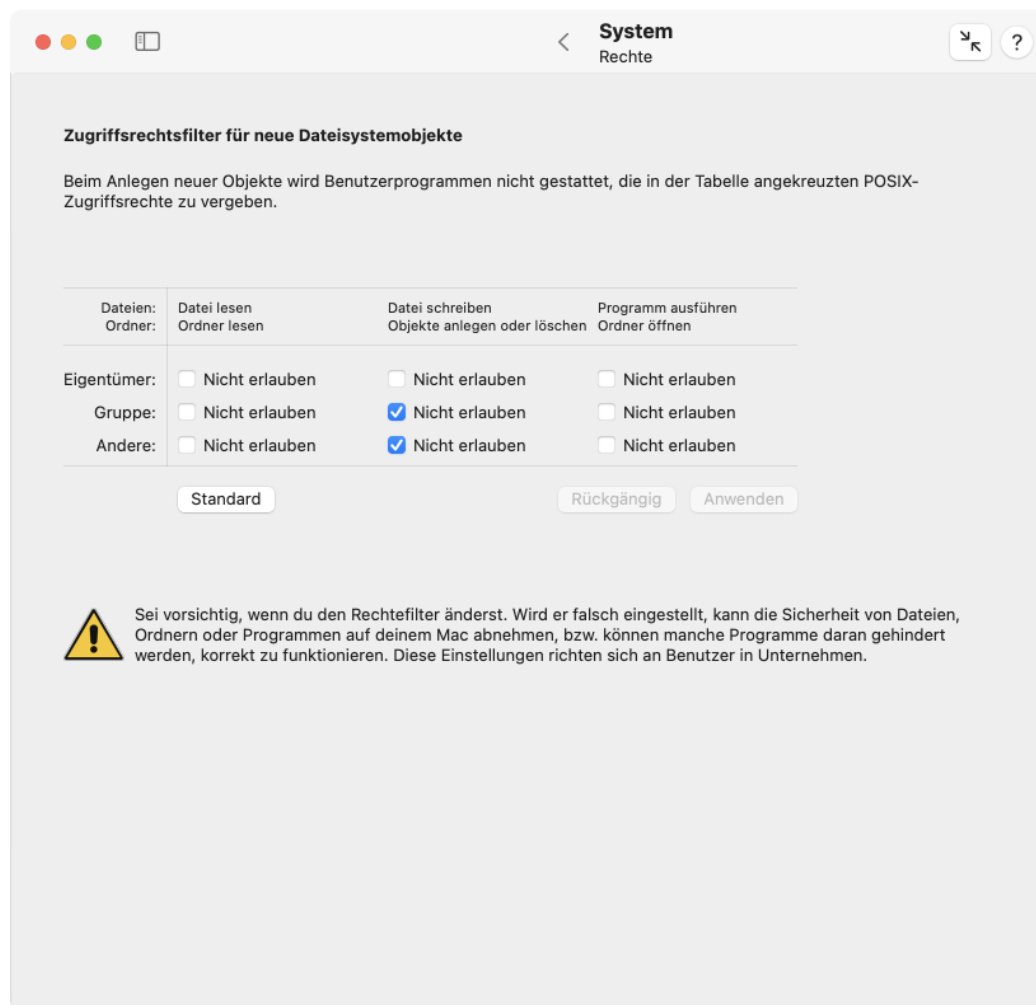


Abbildung 4.6: Zugriffsrechtsfilter

Standardmäßig verwendet macOS einen Berechtigungsfilter, der gemäß folgender Richtlinie voreingestellt ist:

- Programmen wird nicht erlaubt, ursprünglich Schreibrecht für den Gruppeneigentümer eines neuen Objekts zu gewähren.
- Programmen wird nicht erlaubt, ursprünglich Schreibrecht für andere Benutzer zu gewähren, die weder Eigentümer, noch Gruppeneigentümer des neuen Objekts sind.

Systemverwalter können diese Richtlinie für den Berechtigungsfilter ändern, so dass die

anfänglichen Zugriffsrechte entweder lockerer oder strenger werden. Um den Berechtigungsfilter von macOS zu verändern, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Rechte** auf der Einstellungskarte **System**.
2. Setzen oder entfernen Sie Häkchen in der Tabelle **Zugriffsrechtsfilter für neue Dateisystemobjekte**. Die Zeilen der Tabelle stellen die drei Zugriffsparteien **Eigentümer**, **Gruppe** und **Andere** dar, die Spalten beziehen sich auf die Rechte, die beim Anlegen neuer Objekte blockiert werden sollen, nämlich Lesen, Schreiben und Ausführen. Erinnern Sie sich daran, dass Schreiberlaubnis für einen Ordner dem Recht entspricht, Objekte im Ordner anlegen, umbenennen und löschen zu dürfen, und dass Ausführungserlaubnis für einen Ordner bedeutet, den Inhalt des Ordners durchqueren zu dürfen.
3. Drücken Sie den Knopf **Anwenden** unterhalb der Tabelle.

Die Änderung wird beim nächsten Start des Computers wirksam. Der Knopf **Standard** kann gedrückt werden, um zur empfohlenen Normaleinstellung zurückzukehren. Drücken des Knopfes **Rückgängig** bewirkt, dass TinkerTool System Ihre Änderungen verwirft und die Einstellungen anzeigt, die zurzeit im System aktiv sind.



Warnung: Es ist sehr gefährlich, Häkchen in der Zeile **Eigentümer** zu setzen. Das Einschalten eines Filterpunkts in diesem Bereich bedeutet, dass Programme nicht mehr das Recht haben, auf Dateien zuzugreifen, die sie gerade selbst angelegt haben.

Die Einstellung betrifft nur Programme, die in Benutzersitzungen gestartet werden. Hintergrundprogramme des Betriebssystems sind nicht betroffen (es sei denn, diese werden als Teil der Benutzersitzung gestartet).

Es gibt besondere Umstände, in denen TinkerTool System erkennt, dass es nicht möglich sein wird, den Berechtigungsfilter zu ändern. In diesem Fall ist die Tabelle nicht änderbar und eine Fehlermeldung erscheint unterhalb der Tabelle. Ein solches Problem kann in den folgenden Situationen auftreten:

- Ein Vorgang, den Filter zu ändern, ist gerade im Gang. Neue Werte wurden zur Aktivierung eingerichtet, aber der Computer ist noch nicht neu gestartet worden.
- Ein Programm eines Drittanbieters manipuliert den Berechtigungsfilter. Dies könnte von einem anderen Programm beabsichtigt sein, könnte aber auch auf einen Fehler hinweisen. Es ist nicht möglich, die Filtereinstellungen zu ändern, bevor dieses Problem nicht behoben wurde.

4.1.7 Verschiedenes

Sicherheitsvorgabe für Ferne Apple-Events steuern

Seit macOS 10.15 gelten strengere Sicherheitsrichtlinien als früher bezüglich der Nutzung von AppleScript, bzw. damit zusammenhängenden Apple-Events über eine ferne Netzverbindung hinweg. Ein Apple-Event, der ein Programm auf einem fernen System anspricht, muss sich als gleicher Benutzer auf dem fernen System identifizieren. Falls er dies nicht

tut, wird das sendende Programm den Fehler *procNotFound* erhalten. Wenn Sie diese Regel aufweichen, also die laxere Sicherheitsvorgabe älterer Betriebssysteme nutzen möchten, führen Sie die folgenden Schritte auf demjenigen Computer durch, der die fernen Apple-Events empfängt:

1. Öffnen Sie den Unterpunkt **Verschiedenes** auf der Einstellungskarte **System**.
2. Entfernen Sie das Häkchen bei **Gleichen Benutzer-Account auf Clients für Zugriff auf aktuelle Sitzung fordern**.

Die neue Einstellung tritt nicht sofort in Kraft. Um eine Aktualisierung zu erzwingen, können Sie entweder den Computer neu starten oder die Einstellung für **Entfernte Apple-Events** auf der Karte **Allgemein** > **Teilen** der **Systemeinstellungen** zweimal umschalten.

Bildschirmfreigabe

Wenn ein ferner Systemverwalter die Bildschirmfreigabefunktion von macOS nutzt, um den aktuellen Inhalt des Computerbildschirms auf seinem eigenen Computer über eine Netzwerkverbindung hinweg zu empfangen, versucht macOS automatisch, die Privatsphäre des Benutzers zu schützen, der zurzeit mit dem lokalen Bildschirm arbeitet: Falls der ferne Administrator sich mit einem Benutzer-Account anmeldet, der *unterschiedlich* zu dem des lokalen Benutzers ist, beginnt die Bildschirmsitzung nicht sofort. Stattdessen wird der zugreifende Benutzer gefragt, ob er auf einem eigenen, getrennten Schirm arbeiten möchte, oder ob der lokale Benutzer gefragt werden soll, dem fernen Nutzer die Genehmigung zu erteilen, dass er den aktuellen Bildschirm übernehmen darf. Der lokale Benutzer könnte private oder vertrauliche Informationen auf dem Schirm haben, so dass dieses Vorgehen die angezeigten Daten schützt.

In einigen Fällen ist dieses Verhalten nicht sinnvoll. Sie können diese Datenschutzfunktion wie folgt abschalten:

1. Öffnen Sie den Unterpunkt **Verschiedenes** auf der Einstellungskarte **System**.
2. Klicken Sie auf den Punkt **Klient erlauben, die vorderste Bildschirmsitzung sofort zu übernehmen**.

Sie sollten überprüfen, ob diese Vorgehensweise mit den örtlichen Gesetzen und, falls anwendbar, mit den Richtlinien Ihrer Organisation übereinstimmt.

FileVault-Optionen

Falls Sie FileVault auf Ihrem Computer eingeschaltet haben, wird das komplette System-Volumen mit einem sicheren Schlüssel verschlüsselt und es wird nötig, die Platte mit einem Kennwort aufzuschließen und zu entschlüsseln. Wenn der Computer eingeschaltet wird, kann das Betriebssystem nicht sofort starten, da der Mac die verschlüsselte Platte nicht lesen kann. Stattdessen präsentieren die Firmware des Computers und ein Minibetriebssystem auf dem PreBoot-Volumen einen besonderen Anmeldeschirm (der dem Anmeldeschirm von macOS ähnelt). Benutzer müssen sich zuerst hier anmelden, wodurch für berechtigte Benutzer der geheime Entschlüsselungsschlüssel aufgeschossen wird, mit dem danach das Betriebssystem-Volumen entschlüsselt und macOS gestartet wird.

Zu diesem Zeitpunkt ist bekannt, dass derjenige Benutzer der die Platte entschlüsselt hat, gleichzeitig ein gültiger Benutzer von macOS sein muss, so dass die Firmware Name und

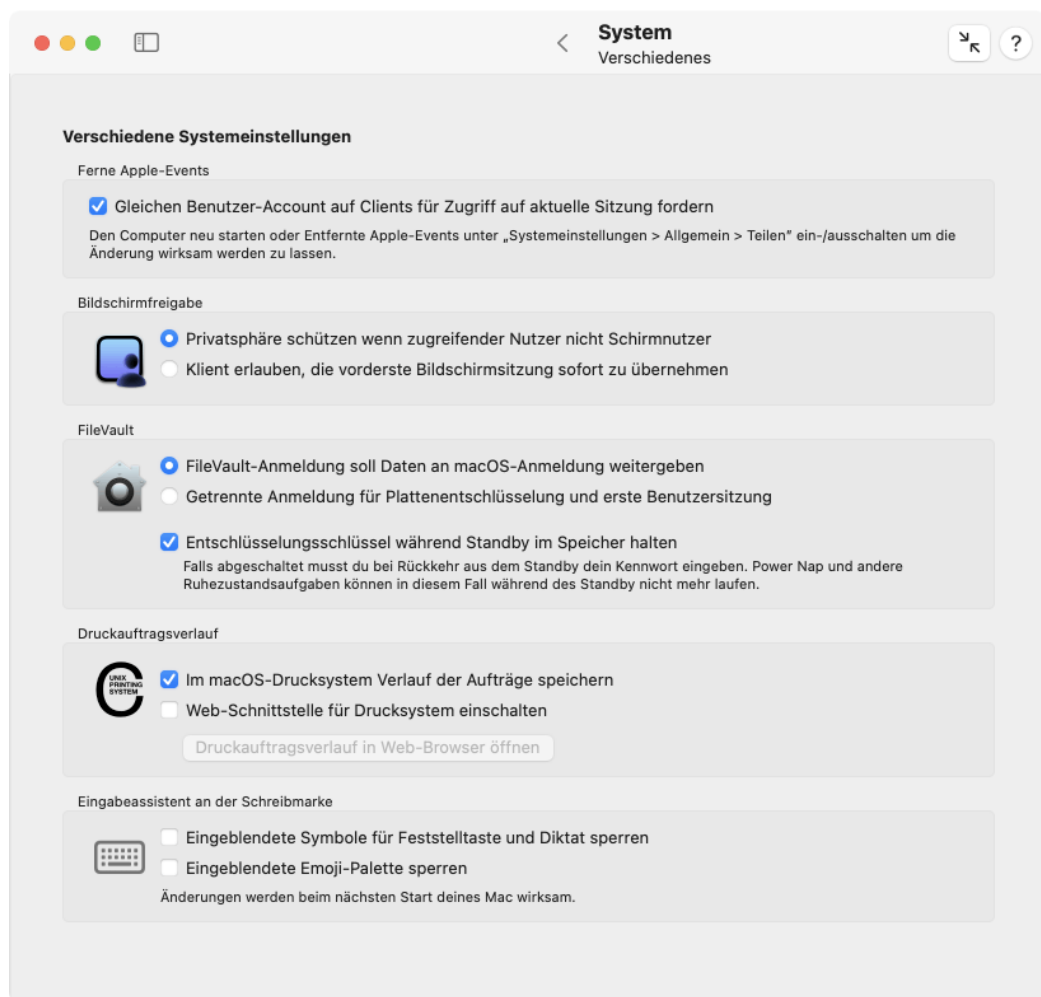


Abbildung 4.7: Verschiedenes

Kennwort dieses Benutzers an das Betriebssystem *weiterreicht* und eine automatische Anmeldung durchführt, so dass vermieden wird, die Anmeldedaten noch ein zweites Mal eingeben zu müssen. Aus diesem Grund bewirkt das Einschalten von FileVault automatisch auch das Einschalten der automatischen Anmeldefunktion von macOS.

In einigen Fällen ist dieses Verhalten nicht gewünscht. macOS unterstützt eine spezielle Funktion, um das Entschlüsseln der FileVault-Platte von der initialen Anmeldung beim Betriebssystem zu entkoppeln:

1. Öffnen Sie den Unterpunkt **Verschiedenes** auf der Einstellungskarte **System**.
2. Klicken Sie auf den Punkt **Getrennte Anmeldung für Plattenentschlüsselung und erste Benutzersitzung**.

Sie können in Fällen, in denen das benötigt wird, auch eine fortgeschrittene Sicherheitsfunktion von FileVault aktivieren. Um fortlaufenden Zugriff auf das Speichermedium zu gewährleisten, muss Ihr Mac den Schlüssel für die Plattenverschlüsselung immer im Speicher halten damit er jeden Block der Platte verarbeiten kann, den das Betriebssystem lesen oder schreiben muss. Das schließt die Zeiten ein, in denen der Mac in den Ruhezustands- oder Standby-Modus geht. Dies ist notwendig, um sicher zu stellen, dass der Mac immer noch regelmäßige Wartungsaufgaben erledigen kann, auch wenn er nicht voll eingeschaltet ist, und um Power Nap-Funktionen auszuführen.

Diese Vorgehensweise stellt einen gewissen Komfort sicher, kann aber zum Problem werden, falls Ihr Mac gestohlen wird und ein Angreifer versucht, direkten Speicherzugriff zu bekommen, indem er spezielle Hardware-Geräte an den schlafenden Mac anschließt. Theoretisch könnte der Schlüssel zur Plattenverschlüsselung auf diese Weise offengelegt werden.

Durch Entfernen des Häkchens bei **Entschlüsselungsschlüssel während Standby im Speicher halten** können Sie diesen möglichen Angriffsweg vermeiden. Falls dieser Punkt nicht angekreuzt ist, zerstört der Mac den FileVault-Schlüssel im RAM sobald das System in den Standby-Betrieb wechselt. In dieser Konfiguration hat Ihr Mac während des Standby keinen Plattenzugriff mehr, so dass Power Nap und ähnliche Wartungsfunktionen nicht mehr länger aktiv sind, egal wie Sie diese eingerichtet haben.

Druckauftragsverlauf

Die Druckfunktionen von macOS werden von *CUPS*, dem *Common Unix Printing System* realisiert. Standardmäßig verwaltet macOS ein Protokoll aller Druckaufträge, die vom aktuellen Computer verarbeitet wurden, den Druckauftragsverlauf. TinkerTool System kann das Protokoll auf Wunsch abschalten und die Einträge, die sich gerade im Protokoll befinden, anzeigen. Um die Systemeinstellung zum Führen des Druckauftragsverlaufs zu ändern, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Verschiedenes** auf der Einstellungskarte **System**.
2. Setzen oder entfernen Sie das Häkchen **Im macOS-Drucksystem Verlauf der Aufträge speichern**.

Das Protokoll kann eingesehen werden, indem Sie den Knopf **Druckauftragsverlauf im Web-Browser öffnen** betätigen. TinkerTool System gibt diese Aufgabe an Ihren bevorzugten Web-Browser ab. In einigen Versionen von macOS ist der Web-Zugriff auf das Drucksubsystem standardmäßig abgeschaltet. Sie können über die Option **Web-Schnittstelle für Drucksystem einschalten** steuern, ob der Web-Zugang möglich sein soll, oder nicht.

Eingabeassistent an der Schreibmarke (nur macOS Sonoma oder höher)

Mit macOS 14 hat Apple neue Einblendungen beim Tippen von Text eingeführt, die direkt neben der Schreibmarke, an der Einfügeposition des Textes, dargestellt werden. Viele Anwender empfinden diese Einblendungen als lästig. Sie können diese mit TinkerTool System abschalten, wobei dies systemweit (für alle Benutzer des Computers) erfolgt. Zwei Systemeinstellungen stehen zur Verfügung:

- die Einblendung für die Feststelltaste zur Großschreibung sowie für das Diktieren von Text
- die Einblendung einer Palette mit Vorschlägen für Emojis, wenn Sie passenden Text eingegeben haben und den Menüpunkt **Bearbeiten** > **Emoji & Symbole**, bzw. die entsprechende Tastenkombination aufrufen.

Führen Sie die folgenden Schritte durch, um diese Systemeinstellungen zu ändern:

1. Öffnen Sie den Unterpunkt **Verschiedenes** auf der Einstellungskarte **System**.
2. Setzen oder entfernen Sie Häkchen **Eingabeassistent an der Schreibmarke**.
3. Starten Sie den Mac neu, falls die Änderung sofort wirksam werden soll.

4.2 Die Einstellungskarte „Immer an“-Mobilcomputer

Die Einstellungskarte **„Immer an“-Mobilcomputer** ist nur dann sichtbar, wenn Sie TinkerTool System auf einem mobilen Mac mit „Immer an“-Verhalten und einem Intel-Prozessor nutzen. Die Einstellungen, die von dieser Karte aus gesteuert werden, sind für andere Computertypen nicht verfügbar.

4.2.1 Automatisches Einschalten

Einige der portablen Computer, die von Apple Ende 2016 eingeführt wurden, haben keine eigene Einschalttaste mehr. Diese Baureihen simulieren ein „Immer an“-Verhalten und besitzen keine Kontrolllampen, weder am Gehäuse, noch auf dem Stecker des Stromanschlusses. Das System startet, sobald Sie den Bildschirmdeckel öffnen. Einige Benutzer ziehen jedoch das herkömmliche Verhalten vor. TinkerTool System gibt Ihnen den Zugriff auf eine Hardware-Einstellung, die dies kontrolliert. Statt ein Einschaltsignal zu senden, wenn der Deckel geöffnet oder ein Netzteil angeschlossen wird, wird alternativ die Funktion ausgelöst, kurz eine Batteriestandsanzeige auf dem Bildschirm einzublenden.

Führen Sie die folgenden Schritte durch:

1. Öffnen Sie die Einstellungskarte **„Immer an“-Mobilcomputer**.
2. Wählen Sie einen der Punkte bei **Automatisches Einschalten**.

Die Anzeige des Akkustandes wird von der Firmware vorgenommen. Wenn das automatische Einschalten deaktiviert ist, arbeitet der Knopf für Touch ID als Einschalttaste. Drücken Sie diese kurz, um das System einzuschalten.

4.3 Die Einstellungskarte Systemstart

Die Einstellungskarte **Systemstart** ist dazu gedacht, spezielle Einstellungen des Betriebssystems oder der Firmware des Computers zu verwalten, die sich nicht auf den normalen Betrieb, sondern nur auf die Startphase von macOS auswirken.

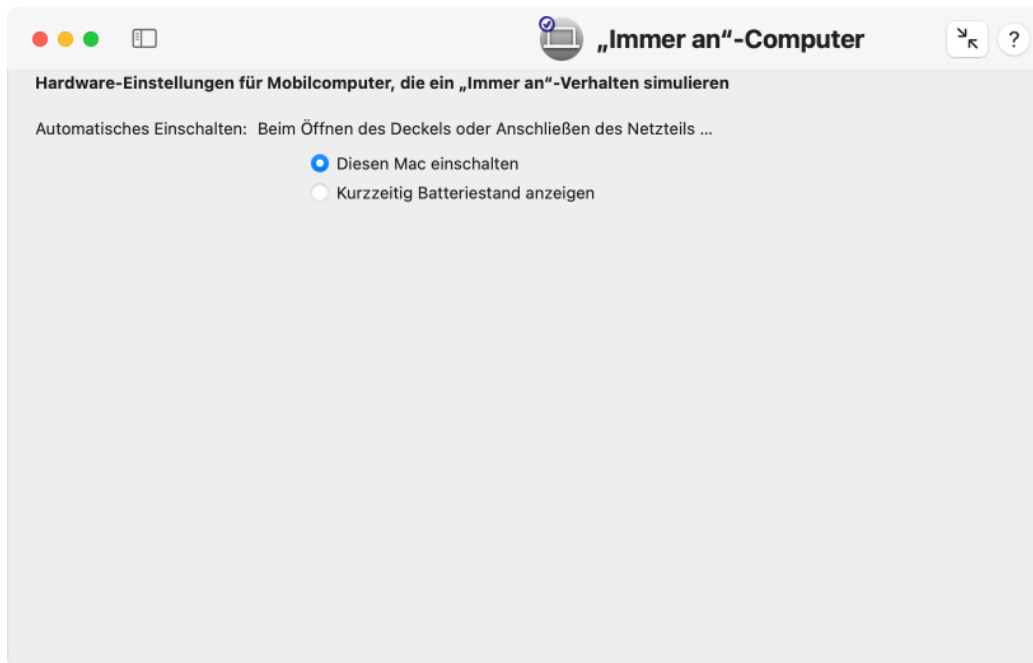


Abbildung 4.8: Einstellungen für die automatische Einschaltfunktion

4.3.1 Hinweise zu Macs mit Apple-Prozessoren

Macs mit Apple-Prozessoren verwenden eine andere Startabfolge und eine andere technische Architektur als Macs mit Intel-Prozessoren. Die folgenden Auswahlmöglichkeiten sind nicht verfügbar, wenn Sie einen Mac mit *Apple-Chip* einsetzen:

- Startbetriebsart
- Sondersystem einmal starten
- System für Serverbetrieb optimieren
- Diagnoseoptionen

4.3.2 Optionen

macOS unterstützt verschiedene Betriebsarten für den Start, die mit TinkerTool System voreingestellt werden können:

- **Normaler Start:** die Standardeinstellung. Das Betriebssystem startet im grafischen Modus und alle Funktionen sind eingeschaltet.
- **Wortreicher Modus:** macOS zeigt im ersten Teil der Startphase, dem Startvorgang des inneren Systemkerns, Textmeldungen an. Nach dieser Phase schaltet das System auf den Grafikmodus zurück und setzt den normalen Betrieb fort. Auch das Herunterfahren des Systems wird von Diagnosemeldungen im Textmodus begleitet.

macOS kann auch im *Sicheren Modus* starten, was heißt, dass es normal startet, dabei jedoch nur einen minimalen Satz von Funktionen einschaltet. Alle Startkomponenten von Drittanbietern, wie Treiber, Kernel-Erweiterungen oder Hintergrunddienste bleiben inaktiv. Diese Betriebsart ist nützlich, wenn Sie schlechte Systemsoftware oder Treiber installiert haben, die macOS daran hindern, erfolgreich hochzufahren. Zusätzlich werden fast alle System- und Benutzer-Caches bereinigt. Der Sichere Modus wird vorübergehend aktiviert, indem Sie beim Start die Umschalttaste () gedrückt halten. Es ist nicht sinnvoll, den Sicheren Modus dauerhaft einzuschalten.

Neben diesen besonderen Betriebsarten, die für den Start des Hauptsystems gelten, können Sie den Mac anweisen, beim nächsten Neustart nicht das normale Betriebssystem, sondern ein Sondersystem für Wartungszwecke zu starten. Diese Auswahl gilt nur einmalig, für den nächsten Start. Zur Verfügung stehen die Auswahlmöglichkeiten:

- **Nicht aktiviert:** Das normale Betriebssystem wird gestartet.
- **Wiederherstellungssystem:** Das Mini-Betriebssystem zur Wiederherstellung des Hauptbetriebssystems wird vom Datenträger des lokalen Computers gestartet. Falls mehrere Betriebssysteme vorhanden sind, wird der Mac dasjenige Wiederherstellungssystem auswählen, das mit dem gerade eingestellten Start-Volume verknüpft ist.
- **Wiederherstellungssystem per Internet:** wie vor, jedoch wird der Mac von Apples Servern im Internet gestartet. Eine Internet-Verbindung ist Voraussetzung. Mit diesem System können auch Wartungsaufgaben durchgeführt werden, falls der eingebaute Systemdatenträger des Mac defekt ist oder er komplett gelöscht werden soll.
- **Apple Diagnose:** Das Programm für die Hardware-Diagnose des jeweiligen Macintosh-Modells wird vom Datenträger des lokalen Computers gestartet. Mithilfe dieses Programms ist eine schnelle Einschätzung möglich, ob alle Komponenten des Mac korrekt arbeiten.
- **Apple Diagnose per Internet:** wie vor, jedoch wird der Mac von Apples Servern im Internet gestartet. Auf diese Weise ist eine Diagnose auch dann möglich, wenn das Testprogramm auf der System-Disk beschädigt wurde.

Energieversorgungsoptionen

Moderne Versionen von macOS sind daraufhin optimiert, zu erkennen, ob ein echter Benutzer oder ein anderes externes Ereignis einen Mac aus dem Ruhezustand geweckt hat. Wenn nicht tatsächlich ein vor dem Bildschirm sitzender Anwender für das Wecken verantwortlich ist, kann der Bildschirm ausgeschaltet bleiben. Dies spart Energie ein und vermeidet ungewollte Lichteffekte. Ein solches „dunkles Aufwecken“ (*Dark Wake*) findet beispielsweise dann statt, wenn ein Gerät im Netzwerk auf einen Server-Dienst des schlafenden Mac zugreifen möchte, oder wenn ein Mobilgerät zum Laden an einen USB-Anschluss des Mac angeschlossen wird.

Bei einigen Einsatzgebieten kann es aber trotzdem gewünscht sein, dass der Mac „voll“, also inklusive Bildschirm aufwachen soll und dann für längere Zeit einsatzbereit bleibt. Ein Beispiel wäre ein Mac, der als Multimedia-Abspieler zusammen mit einem Fernseher an einer schlecht erreichbaren Stelle montiert ist und per Netzwerk-Fernbedienung geweckt wird. Es soll möglich sein, den Mac zum Abspielen eines Films ohne Tastatur aufzuwecken und ihn dann für längere Zeit aktiv zu lassen. Ist ein solches Verhalten gewünscht, kreuzen Sie die Wahlmöglichkeit **Bildschirm bei Wecken durch Netzwerk oder Mobilgerät nicht dunkel lassen** an.

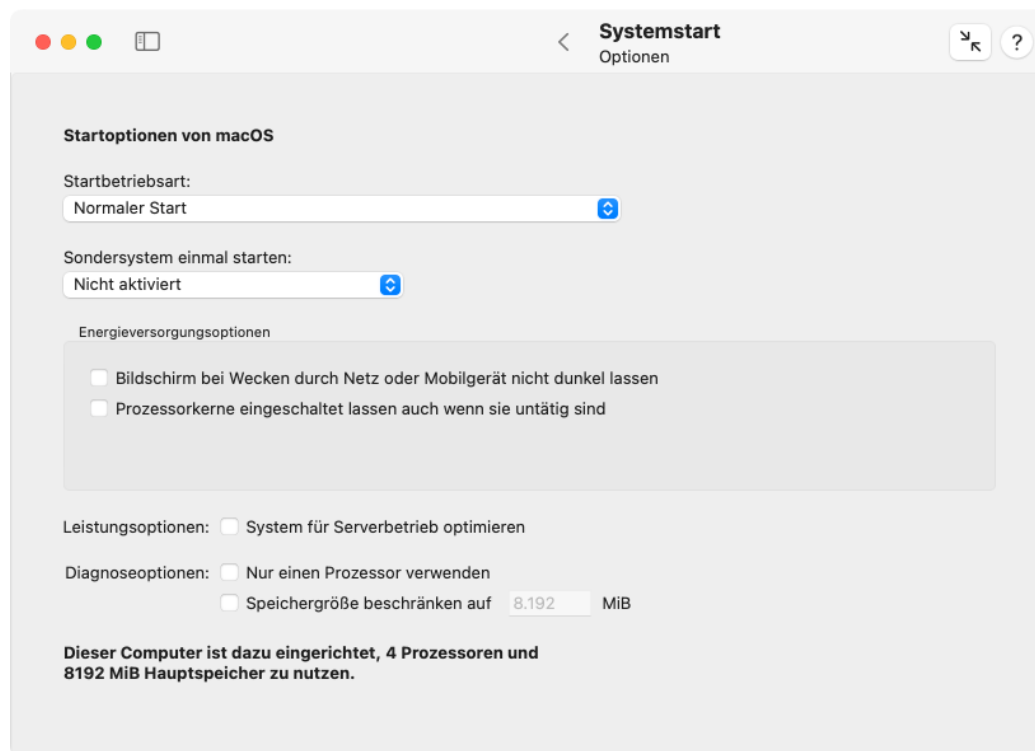


Abbildung 4.9: Optionen für den Systemstart

Prozessorkerne eingeschaltet lassen auch wenn sie untätig sind: Normalerweise schalten moderne Computer alle Prozessorkerne ab, die gerade nicht gebraucht werden. „Nicht gebraucht“ heißt hierbei, dass der Prozessverplaner nicht genügend Jobs hat, um alle Kerne für eine komplette Vergabezeitscheibe beschäftigt zu halten, die üblicherweise 10 Millisekunden dauert. Für den Zeitraum, in dem nichts zu tun ist (Prozessorlast pro Kern liegt unter 100%), werden die betreffenden Kerne in einen Ruhezustand geschaltet. Die Kerne immer eingeschaltet zu lassen, ist hauptsächlich für Diagnosezwecke interessant. Es hat keine positiven Auswirkungen auf die Systemleistung. Das System verbraucht möglicherweise spürbar mehr Energie und erzeugt mehr Hitze, wenn diese Funktion aktiv ist.

Leistungsoptionen

macOS kann seinen Systemkern neu konfigurieren, um sich selbst für die Arbeit als Server zu optimieren. Das heißt, dass bestimmte Systemparameter, wie die Strategie zur Reservierung von Netz- und Datei-Caches oder die Multi-Threading-Charakteristik so verändert werden, dass typische Serverprogramme eine höhere Leistung erzielen. Solche Serverprogramme laufen üblicherweise ohne sichtbare Bedieneroberfläche im Hintergrund und verwenden viele Threads, die hauptsächlich Netz- und Dateioperationen erledigen. Auf der anderen Seite ist eine Standardinstallation von macOS üblicherweise daraufhin optimiert, dem vordersten Programm, das auf der grafischen Bedieneroberfläche läuft, das beste Geschwindigkeitsverhalten zu bieten.

Wenn Sie diesen Standard ändern möchten, um bessere Leistung für typische Serveraufgaben zu erzielen, setzen Sie ein Häkchen bei **System für Serverbetrieb optimieren**. Nach einem Neustart des Computers wird der Systemkern die neue Einstellung beachten.

Apple kann die genaue Bedeutung dieser Einstellung jederzeit ohne vorherige Ankündigung ändern.

Diagnoseoptionen

Für Diagnosezwecke sind zusätzliche Wahlmöglichkeiten verfügbar:

- **Nur einen Prozessor verwenden:** bewirkt, dass das Betriebssystem nur eine CPU verwendet, falls mehrere Prozessoren (oder Kerne) im System vorhanden sind.
- **Speichergröße beschränken auf:** macOS kann dazu gezwungen werden, weniger RAM-Speicher zu verwenden, als im System eingebaut ist. Diese Funktion kann für Programmentwickler nützlich sein, um die Auswirkungen von Situationen bei Speicherplatzmangel zu simulieren. Sie kann auch dabei helfen, Probleme mit defekten Speichermodulen zu diagnostizieren.

Ändern der Optionen

Um eine der aufgeführten Wahlmöglichkeiten zu verwenden, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Optionen** auf der Einstellungskarte **Systemstart**.
2. Schalten Sie die Wahlmöglichkeiten wie gewünscht ein oder aus.

4.3.3 Job-Übersicht

Wenn das Betriebssystem startet und der Benutzer sich anmeldet, wird eine hohe Zahl von Systemdiensten und Benutzerprogrammen automatisch gestartet. TinkerTool System kann Ihnen dabei helfen, eine Übersicht über alle automatisch startenden Komponenten zu bekommen, die für Ihren persönlichen Benutzer-Account wirksam sind. Es analysiert außerdem alle selbststartenden Jobs und vergleicht deren Konfigurationseinträge mit deren aktuellem Status. Wenn eine Abweichung gefunden wird, werden Sie vom Programm gewarnt. Auf diese Weise können Sie ungültige oder veraltete Konfigurationseinträge leicht erkennen.

Um TinkerTool System einen Bericht über alle automatisch startenden Jobs erstellen zu lassen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Optionen** auf der Einstellungskarte **Systemstart**.
2. Betätigen Sie den Knopf **Bericht erstellen**.

Nach wenigen Sekunden wird der Bericht in der Textanzeige erscheinen. Über die Funktion Kopieren und Einsetzen können Sie ihn falls nötig in andere Programme übertragen. Um alle „normalen“ Jobs herauszufiltern, die von Apple vorkonfiguriert und Bestandteil des Betriebssystems sind, setzen Sie ein Häkchen bei **Jobs ausblenden, und zusammenfassen, die zum Lieferumfang von macOS gehören**. Sie können den gerade angezeigten Bericht durch Anklicken des Knopfes **Bericht sichern ...** abspeichern.

Die Konfiguration selbststartender Jobs ist Teil verschiedener Verhaltensweisen beim Hochfahren und verschiedener Zuständigkeitsbereiche: Sogenannte *Daemons* sind Dienste, die im Hintergrund laufen und gestartet werden können, sobald das Betriebssystem läuft, auch wenn noch kein Benutzer angemeldet ist. Sogenannte *Agents* sind Hintergrunddienste, die für jede Benutzersitzung laufen. Diese können hochgefahren werden, sobald sich

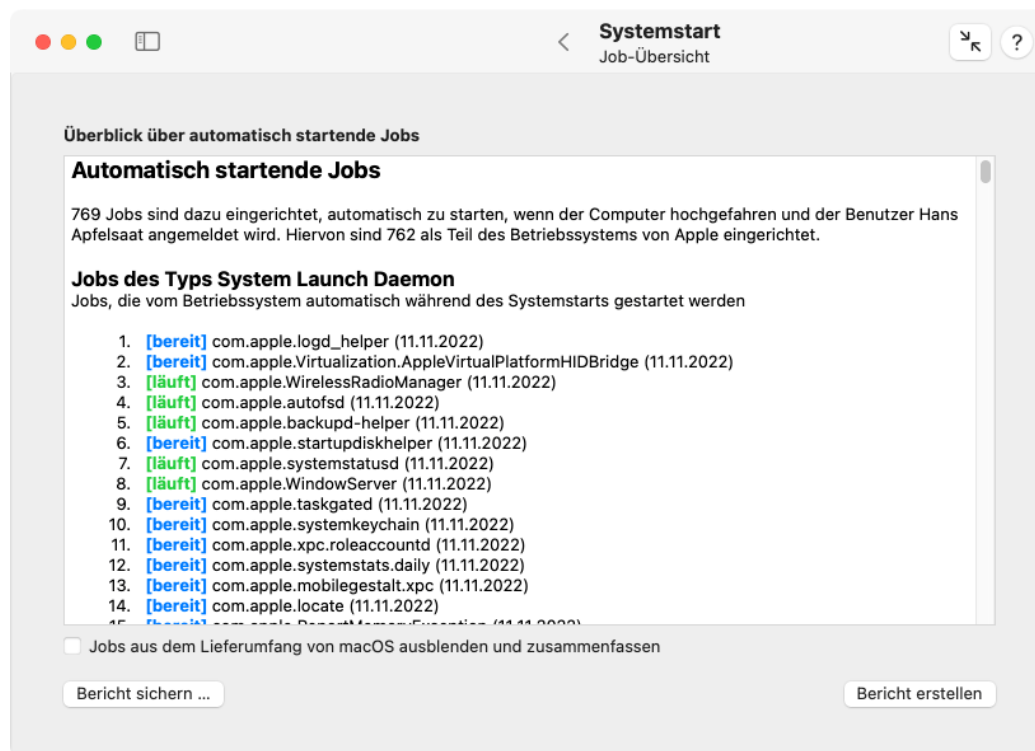


Abbildung 4.10: Übersicht über alle automatisch startenden Jobs

der Benutzer angemeldet hat, und sie werden automatisch beendet, wenn sich der Benutzer abmeldet. Wenn mehrere Benutzer angemeldet sind, laufen mehrere Sätze von Agents für jede Sitzung gleichzeitig. Daemons und Agents können entweder vom Betriebssystem selbst definiert sein (*System*), oder es sind Einträge von Drittanbietern für alle Benutzer eines Computers (*Computer*), oder für einen ganz bestimmten Benutzer (*Benutzer*), ein Fall, der dann natürlich auf Agents beschränkt ist.

Ein Benutzer kann automatisch startende Programme außerdem selbst hinzufügen, indem er die Einstellung **Anmeldeobjekte** auf der Karte **Allgemein** der **Systemeinstellungen**, oder das Kontextmenü des Dock verwendet.

Apps, die im Mac App Store verkauft werden, haben keine Erlaubnis, irgendeine der Einstellungen für Daemons, Agents oder Anmeldeobjekte zu berühren. Dies wird von Apple überwacht und zusätzlich durch technische Maßnahmen innerhalb von macOS sichergestellt. Wenn eine solche App allerdings steuern muss, dass sie oder Teile von ihr automatisch starten sollen, nachdem der Benutzer sich angemeldet hat, muss sie den Benutzer zunächst ausdrücklich um Erlaubnis fragen (z.B. indem eine Einstellung innerhalb der App geändert wird), und muss dann einen speziellen Antrag an macOS stellen, die selbststartende Komponente zu registrieren. Wenn dieser Antrag in Ordnung ist, speichert macOS den Anmeldewunsch in einer internen Datenbank, was vor dem Benutzer verborgen bleibt und nur für die betreffende App sichtbar ist, die den Antrag gestellt hat. TinkerTool System verwendet die Bezeichnung *Benutzerdienst-Anmeldeobjekt*, um sich auf solche speziellen Konfigurationseinträge für Apps zu beziehen.

Falls macOS oder das verwaltende Programm die Konfiguration eines Benutzerdienst-Anmeldeobjekts für einen Benutzer-Account ändert, wird diese Änderung erst dann

in TinkerTool System sichtbar, nachdem sich dieser Benutzer abgemeldet hat.

Für jeden Job, der dazu eingerichtet ist, automatisch gestartet zu werden, zeigt TinkerTool System die folgenden Einträge an:

- eine laufende Nummer, was es einfach macht, die Einträge abzuzählen und sich auf diese zu beziehen,
- den aktuellen Status des Jobs als der Bericht erstellt wurde,
- die Identifikationsbezeichnung, die macOS intern verwendet, um den Konfigurationseintrag zu verwalten,
- das Datum, an dem das automatisch startende Programm zuletzt geändert wurde.

Die unterschiedlichen Statuseinträge, die mit Farbmarkierungen und in zwischen eckigen Klammern angezeigt werden, haben die folgende Bedeutung:

- **benutzergesteuert:** dieser Eintrag wurde vom Benutzer angelegt. Der Benutzer steuert außerdem, wann die selbststartende Komponente beendet wird.
- **abgebrochen:** das Betriebssystem hat den Job automatisch gestartet, aber den Prozess später gestoppt, da auf dem Computer sehr hoher Speicherdruck aufgrund Mangel von RAM aufgetreten ist, und der betroffene Job für den Betrieb des Computers nicht absolut notwendig ist. Wenn dies passiert, kann das System langsamer als normal arbeiten und einige Funktionen können eingeschränkt sein. Es ist zu empfehlen, die Funktion **Diagnose > RAM-Größe auswerten** von TinkerTool System zu verwenden, um herauszufinden, ob Sie mehr RAM kaufen sollten, damit der Computer mit Ihrer typischen Arbeitsbelastung besser zurechtkommt.
- **fehlgeschlagen:** das Betriebssystem hat den Job automatisch gestartet, aber das zugehörige Programm wurde mit einem Fehlercode beendet. Es scheint ein technisches Problem aufgetreten zu sein, wodurch der Job fehlgeschlagen ist.
- **läuft:** der Job wurde automatisch gestartet und läuft im Moment.
- **bereit:** der Job ist korrekt dazu eingerichtet, automatisch zu starten, aber er läuft im Moment nicht. Dies ist normal für Jobs, die nur in gewissen Situationen laufen, zu bestimmten Zeiten, beim Eintreten bestimmter Ereignisse, beim Anschließen bestimmter Hardware-Geräte, usw.
- **abgeschaltet:** der Job ist allgemein dazu voreingerichtet, automatisch gestartet zu werden, aber eine Einstellung im Betriebssystem hat diesen Job ausdrücklich deaktiviert. Das ist normal für Dienste, die nur in bestimmten Fällen laufen sollen, z.B. nachdem bestimmte Funktionen eingeschaltet wurden.
- **inaktiv:** der Job hat einen Konfigurationseintrag für automatischen Start, aber das Betriebssystem hat es aus irgendeinem Grund abgelehnt, den Eintrag zu registrieren. Dies ist üblicherweise nicht kritisch und der exakte Grund wurde von TinkerTool System nicht ermittelt.
- **beendet (einzelner Lauf):** der Job ist für automatischen Start eingerichtet, aber erfüllt eine gewisse Aufgabe, die nur einmal während des Systemstarts erledigt werden muss, so dass der Prozess beendet werden kann, sobald die Arbeit abgeschlossen ist. Alles wurde korrekt ausgeführt und der Job läuft im Moment nicht mehr.

- **ungültig (Programm fehlt):** der Job ist für automatischen Start konfiguriert, aber konnte nicht laufen, da das zugehörige ausführbare Programm fehlt. TinkerTool System hat ermittelt, dass dieser Eintrag ungültig ist. In den meisten Fällen wird ein Problem dieser Art dadurch ausgelöst, dass ein Programm gelöscht wird, ohne es korrekt zu deinstallieren.

Leider ist es zur Gewohnheit geworden, dass Apple das Betriebssystem mit einigen ungültigen Konfigurationseinträgen ausliefert. Wenn TinkerTool System einen Job mit einem unnormalen Status entdeckt, der auf einem dieser bekannten Fehler beruht (die üblicherweise unkritisch sind), gibt es dies mit der zusätzlichen Meldungszeile **Hinweis: Dies ist ein bekannter Defekt des Betriebssystems und daher „normal“ an.**

Ungültige Autostart-Einträge entfernen

TinkerTool System kann ungültige Einträge für automatisch startende Jobs automatisch in denjenigen Fällen entfernen, in denen seine Analyse bestätigt hat, dass es absolut sicher ist, dies zu tun. Falls ein oder mehrere solcher Einträge gefunden wurden, wird der zusätzliche Knopf **Probleme beheben ...** im unteren Bereich des Fensters sichtbar. Es handelt sich hierbei üblicherweise um Fälle, in denen ein veralteter Eintrag auf dem System verblieben ist, weil das zugehörige Programm gelöscht wurde, ohne es korrekt zu deinstallieren.

Nach dem Drücken des Knopfes **Probleme beheben ...** zeigt TinkerTool System eine Tabelle mit allen Einträgen, die sicher entfernt werden können. Durch Anklicken von Zeilen in der Tabelle können Detailinformationen aufgerufen werden. Drücken Sie entweder den Knopf **Ausgewählten Eintrag bereinigen** um ein Problem mit dem Job zu beheben, der gerade ausgewählt ist, oder den Knopf **Alle Einträge bereinigen** für alle Einträge, die gerade in der Tabelle gezeigt werden.

Beim Bereinigen von Einträgen des Typs *Benutzerdienst-Anmeldeobjekt* müssen besondere Bedingungen berücksichtigt werden: Apple hat diese Einträge ausdrücklich unter der Maßgabe entworfen, sicher zu stellen, dass nur die Apps, die diese auch angelegt haben, darauf zugreifen können. TinkerTool System kann diesen Schutz umgehen, aber dies wird nicht empfohlen und sollte nur als letzter Ausweg verwendet werden. Um einen fehlerhaften Eintrag für ein Benutzerdienst-Anmeldeobjekt zu entfernen, wird empfohlen, diejenige App, die als „verwaltet durch ...“ beim Eintrag im Bericht der Job-Übersicht angezeigt wird, noch einmal zu installieren und dann die Einstellungsdialoge innerhalb dieser App zu verwenden, um deren selbststartende Funktionen abzuschalten.

Falls ungültige Einträge des Typs *Benutzerdienst-Anmeldeobjekt* in der Liste enthalten sind, fragt TinkerTool System sie danach, ob diese bei der Bereinigung berücksichtigt werden sollen oder nicht.

Um ungültige Anmeldeobjekte zu entfernen, verwenden Sie die diesbezügliche Funktion auf der Karte Benutzer (Abschnitt 5 auf Seite 283).

4.3.4 NVRAM

Diese Funktion ist nur auf Macs mit Apple-Prozessoren vorhanden. Sie wird auf Intel-basierten Macs nicht benötigt.

Das *NVRAM* (*Non-Volatile Random Access Memory*) ist der nicht-flüchtige Schreib-/Lesespeicher, den ein Mac verwendet, um Einstellungen dauerhaft zu speichern, die für den gesamten Computer und alle installierten Betriebssysteme gelten sollen. Der für den Benutzer sichtbare Bereich dieses Speichers wird manchmal auch als *Parameter-RAM* (*PRAM*) bezeichnet. Zu den Einstellungen, die im NVRAM abgelegt werden können, gehören die Lautstärke der Audioausgabe, die Bildschirmauflösung, die Auswahl des Start-Volumes, die Zeitzone und ggf. Informationen zu Systemabstürzen, die vor kurzem aufgetreten sind. Welche Einstellungen im NVRAM gespeichert werden, hängt vom Mac und von den mit ihm verwendeten Geräten ab. Wenn Probleme im Zusammenhang mit diesen oder anderen Einstellungen auftreten, kann ein Löschen des NVRAM für Abhilfe sorgen.

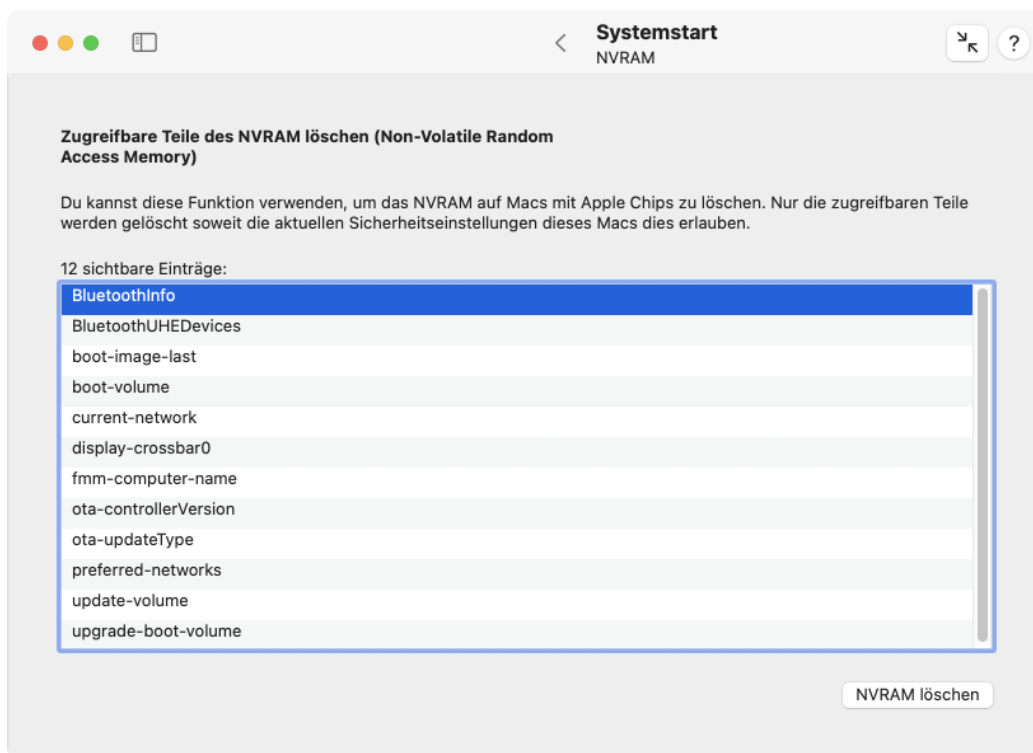


Abbildung 4.11: Löschen des NVRAM

Bei klassischen Macs kann das NVRAM direkt beim Einschalten durch eine bestimmte Tastenkombination zurückgesetzt werden. Bei modernen Macs mit Apple-Chip ist diese Funktion nicht mehr vorhanden. TinkerTool System kann hier helfen, indem es so viele Einstellungen wie möglich aus dem NVRAM löscht. Wie viele das im konkreten Fall sind, hängt von den aktuellen Sicherheitseinstellungen des Mac, insbesondere dem Systemintegritätsschutz ab. Führen Sie die folgenden Schritte durch, um den Löschvorgang durchzuführen:

1. Öffnen Sie den Unterpunkt **NVRAM** auf der Einstellungskarte **Systemstart**.
2. Betätigen Sie den Knopf **NVRAM löschen**.

Sie können die sichtbaren Parameter-Einträge des NVRAM in einer Tabelle vor und nach dem Löschen begutachten.

4.3.5 FileVault

FileVault, genauer gesagt *FileVault 2*, ist die Bezeichnung für Apples Technik, auch das Start-Volume eines Macintosh verschlüsseln zu können, obwohl sich dort neben den Benutzerdaten auch das Betriebssystem befindet. Beim Start steht macOS noch nicht zur Verfügung, da es ja zu diesem Zeitpunkt auf dem verschlüsselten Volume liegt, also muss eine zweite Anmeldung mit einer zweiten Verwaltung von Benutzern aufgebaut werden, die mit der Benutzerverwaltung von macOS erst nach der Entschlüsselung und nach dem Start verbunden werden kann.

Bei modernen Macintosh-Baureihen ist der eingebaute Flash-Speicher immer verschlüsselt, auch wenn FileVault ausgeschaltet ist (siehe auch das Kapitel Die Einstellungskarte APFS (Abschnitt 3.7 auf Seite 228), Abschnitt APFS-Schlüssel). Um den Vorgang der Verschlüsselung muss sich FileVault deshalb nur auf älteren Macs kümmern. Die eigentliche Leistung von FileVault besteht darin, noch vor dem Start von macOS eine Benutzeranmeldung zu verwalten und damit den Zugriff auf die zur Entschlüsselung nötigen Schlüssel freizugeben. FileVault kann deshalb als vorgeschaltetes Minibetriebssystem angesehen werden, das steuert, welche Benutzer das eigentliche Betriebssystem entschlüsseln und starten können.

TinkerTool System zeigt diese beiden Aspekte voneinander getrennt in der oberen Fensterhälfte der Funktion **FileVault** an:

- **Verschlüsseltes Start-Volume:** gibt an, ob die Volume-Gruppe, die das laufende macOS und die Benutzerdaten enthält, verschlüsselt ist
- **Benutzerverwaltung für Entschlüsselung beim Start:** gibt an, ob die Anmeldung bei FileVault dem Start von macOS vorgeschaltet wird

Der Zugriff auf die FileVault-Daten in der unteren Hälfte des Fensters wird von macOS geschützt und wird erst dann aktiv, wenn ein Administrator dies durch Anklicken von **Benutzerliste holen** freigeschaltet hat. Voraussetzung ist außerdem, dass FileVault eingeschaltet ist.

Die Tabelle **FileVault-Benutzer-Accounts** listet alle macOS-Benutzer auf, die auch in der Benutzeranmeldung von FileVault aufgeführt werden sollen. Der Punkt **Persönlicher Wiederherstellungsschlüssel** gibt an, ob beim Einschalten von FileVault ein spezieller Schlüssel hinterlegt wurde, der es ermöglicht, in einem Notfall durch Eingabe eines Textcodes das Start-Volume zu entschlüsseln, auch wenn alle aufgelisteten Benutzer-Accounts ausgefallen sein sollten.

Ein persönlicher Wiederherstellungsschlüssel ist ein lesbarer Code nach dem Muster

ABCD-EFGH-IJKL-MNOP-QRST-UVWX

der in einer Textdatei oder klassisch auf Papier dauerhaft für Notfälle aufbewahrt werden kann. Alternativ kann der Wiederherstellungsschlüssel auch bei Apple in der iCloud hinterlegt werden. In diesem Fall wird er allerdings an eine Apple-ID gebunden.

Für große Organisationen ist die weitere Alternative gedacht, für FileVault einen Generalschlüssel anzulegen, der auf alle Macs passt, statt für jedes einzelne Gerät einen eigenen Schlüssel zu archivieren.

Solche institutionellen Schlüssel oder iCloud-Schlüssel werden von TinkerTool System nicht angezeigt.

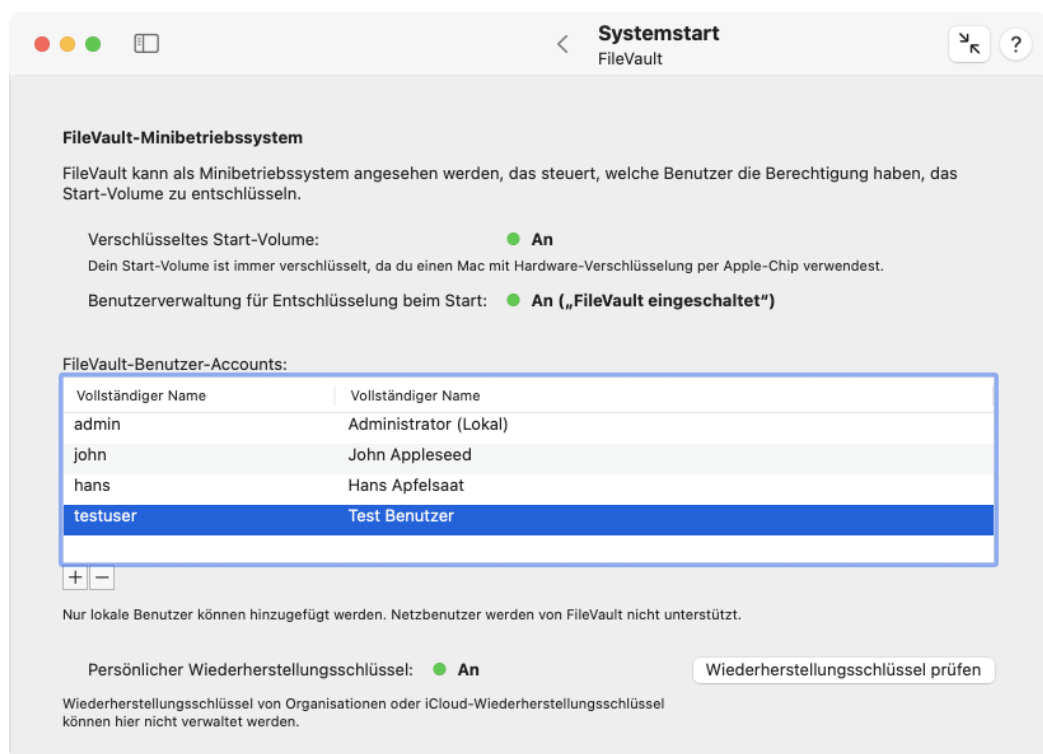


Abbildung 4.12: TinkerTool System zeigt den Status und die Benutzerverwaltung von FileVault an. Falls vorhanden kann auch ein persönlicher Wiederherstellungsschlüssel geprüft werden.

FileVault-Benutzer verwalten

Wie erwähnt muss die Benutzerverwaltung von FileVault von der Benutzerverwaltung von macOS technisch getrennt sein. Sie können mit den beiden Knöpfen + und – unterhalb der Benutzertabelle Accounts zu FileVault hinzufügen oder löschen.

Um Benutzer aus FileVault zu löschen, wählen Sie eine oder mehrere der betreffenden Zeilen aus der Tabelle und klicken auf –.

Um Benutzer zu FileVault hinzuzufügen, müssen mehrere Voraussetzungen erfüllt sein:

- Sie müssen wissen, welcher Benutzer-Account gerade als primärer FileVault-Account gilt. Das ist üblicherweise der Account, der FileVault ursprünglich eingerichtet hat und der in der Tabelle an der obersten Position gezeigt wird. Dies könnte sich aber nachträglich durch Löschvorgänge verändert haben.
- Sie müssen für den primären FileVault-Account das macOS-Kennwort wissen.
- Sie müssen für jeden Benutzer-Account, den Sie nachträglich zu FileVault hinzufügen, ebenso das macOS-Kennwort wissen.

Falls die Voraussetzungen erfüllt sind, führen Sie die folgenden Schritte durch:

1. Drücken Sie auf den Knopf + unterhalb der Benutzertabelle.
2. Wählen Sie aus der Liste der lokalen macOS-Benutzer diejenigen aus, die zu FileVault hinzugefügt werden sollen und klicken Sie **Weiter**.
3. Geben Sie Name und Kennwort des primären FileVault-Accounts ein und klicken Sie **Weiter**.
4. Geben Sie für jeden Benutzer, der hinzugefügt wird, das passende Kennwort ein und klicken Sie **Weiter**.

Ist das Hinzufügen erfolgreich, wird dies in der Tabelle angezeigt.

Das Minibetriebssystem von FileVault ist nicht in der Lage, mit Verzeichnisdienst-Servern zu arbeiten. Deshalb lassen sich nur lokale Benutzer dieses Mac hinzufügen, keine Netzwerk-Accounts.

Persönlichen Wiederherstellungsschlüssel prüfen

Wenn Sie mehrere Macs einsetzen oder mehrere Macs über die Jahre hinweg verwaltet haben, kann es sein, dass Sie viele Notizen zu persönlichen FileVault-Wiederherstellungsschlüsseln angelegt haben. Hier können in der Praxis leicht Unsicherheiten auftreten, ob ein notierter Schlüssel tatsächlich zu einem bestimmten Mac passt. Mit TinkerTool System lässt sich das schnell überprüfen:

1. Klicken Sie auf **Wiederherstellungsschlüssel prüfen**.
2. Geben Sie den Textcode des Schlüssels ein, wenn das Programm danach fragt.

Danach erhalten Sie die Auskunft, ob der Schlüssel zu diesem Mac passt oder nicht. Wie erwähnt lassen sich institutionelle Generalschlüssel oder iCloud-Schlüssel nicht auf diese Weise prüfen.

4.3.6 Sprache (nur macOS Ventura)

In den neuesten Versionen von macOS wurde der Startvorgang stark überarbeitet und optisch dem Start von iPhones angeglichen. Die FileVault-Anmeldung und die macOS-Anmeldung sind noch enger zusammengeführt und kaum voneinander zu unterscheiden. Probleme mit der Startsprache treten in der Praxis so gut wie nicht mehr auf, so dass eine manuelle Änderung in der Regel unnötig ist. Die in diesem Abschnitt vorgestellte Funktion wird deshalb für macOS Sonoma und höher nicht mehr angeboten.

Benutzer können die Sprache, die sie bei der Arbeit mit Programmen bevorzugen, individuell einstellen. Diese persönliche Vorgabe wird durch die Prioritätsliste gesteuert, die im Programm **Systemeinstellungen** unter **Allgemein > Sprache & Region > Bevorzugte Sprachen** angezeigt wird. Diese Einstellung bezieht sich jedoch nur auf Programme, die vom jeweiligen Benutzer gestartet werden, nicht auf die Startphase des Betriebssystems und dessen Anmeldebildschirm, also Situationen, bei denen noch kein Benutzer angemeldet ist. Unter normalen Umständen kann diese zusätzliche Spracheinstellung nur eingestellt werden, während das Betriebssystem installiert wird.

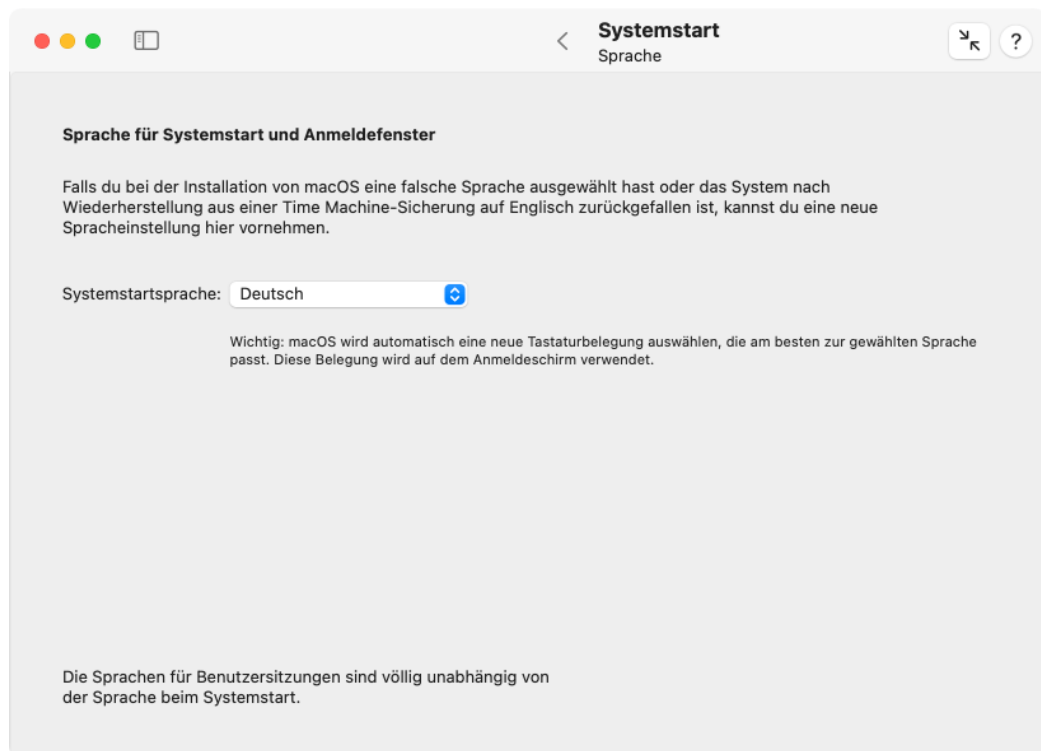


Abbildung 4.13: Startsprache

TinkerTool System erlaubt es Ihnen, diese Spracheinstellung zu ändern, ohne dass Sie das System neu installieren müssen. Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Sprache** auf der Einstellungskarte **Systemstart**.
2. Wählen Sie die bevorzugte Sprache mit dem Aufklappmenü **Systemstartsprache**.

Dies ändert ebenso die Tastaturbelegung, die beim Betrieb des Anmeldefensters verwendet wird. Falls Sie nicht den Tastatortyp besitzen, der für die ausgewählte Startsprache üblicherweise benutzt wird, könnte es schwierig sein, Name und Kennwort korrekt einzugeben.

Unter bestimmten Umständen kann die Einstellung für die Startsprache von macOS beschädigt worden sein, z.B. wenn Sie Ihr System aus einer Time Machine-Datensicherung wiederhergestellt haben. TinkerTool System zeigt in diesem Fall einen zusätzlichen Knopf an, der es Ihnen erlaubt, die Einstellung zu reparieren.

4.4 Die Einstellungskarte Anmeldung

Die Einstellungskarte **Anmeldung** steuert Vorgaben für den Anmeldeschirm, den Eingabedialog für Name und Kennwort, der angezeigt wird, bevor eine eigentliche Benutzersitzung beginnen kann. macOS verwendet nur dann eine Anmeldung, falls Sie Ihr System nicht dazu eingerichtet haben, eine automatische Anmeldung mit einem vordefinierten Benutzer-Account durchzuführen. Sie können die Anmeldung in den **Systemeinstellungen** einschalten, indem Sie die Abfolge **Benutzer:innen & Gruppen > Automatisch anmelden als ... > Deaktiviert** verwenden.

macOS verwendet außerdem die automatische Anmeldung, falls Sie die Verschlüsselungsfunktion **FileVault** zur Absicherung der Systemplatte eingeschaltet haben. In diesem Fall verwendet die Firmware ihren eigenen, eingebauten Anmeldeschirm und fragt nach einem Kennwort, das danach genutzt wird, um das Betriebssystem zu entschlüsseln und zu starten. Das Kennwort wird hierbei von der Firmware an das System weitergegeben, um zu vermeiden, dass es doppelt eingegeben werden muss. Sie können die automatische Anmeldung in diesem Fall nicht abschalten, und der eigentliche Anmeldeschirm wird überhaupt nicht benutzt. Der alternative Anmeldeschirm liegt außerhalb von macOS und kann von TinkerTool System nicht angepasst werden.

Wahlmöglichkeiten, die Sie auf der Einstellungskarte **Anmeldung** von TinkerTool System verändern, treten sofort in Kraft. Um den Anmeldeschirm wieder auf die Werkseinstellungen von Apple zurückzustellen, betätigen Sie den Knopf **Alles auf Standard zurücksetzen** in der unteren rechten Ecke des Fensters. Beachten Sie, dass das Drücken des Knopfes sämtliche Einstellungen auf allen Karteireitern der Karte **Anmeldung** zurücksetzt, nicht nur die Wahlmöglichkeiten, die auf der vordersten Ansicht zu sehen sind. Einzige Ausnahme von dieser Regel sind die Einstellungen zum Ausblenden lokaler Benutzer, da deren Rücksetzen eine ganz spezielle Art von Anmeldung erfordert. Mehr Details hierüber sind in den nachfolgenden Abschnitten zu finden.

4.4.1 Einstellungen

Der erste Karteireiter steuert den grundlegenden Stil und fortgeschrittene Funktionen des Anmeldebildschirms. Sie können umschalten zwischen

- **Textfelder für Name und Kennwort** und
- **Benutzerliste für diesen Computer.**

Falls die letztere Option gewählt wurde, können Sie noch genauer beeinflussen, welche Benutzer in die Liste aufgenommen werden sollen:

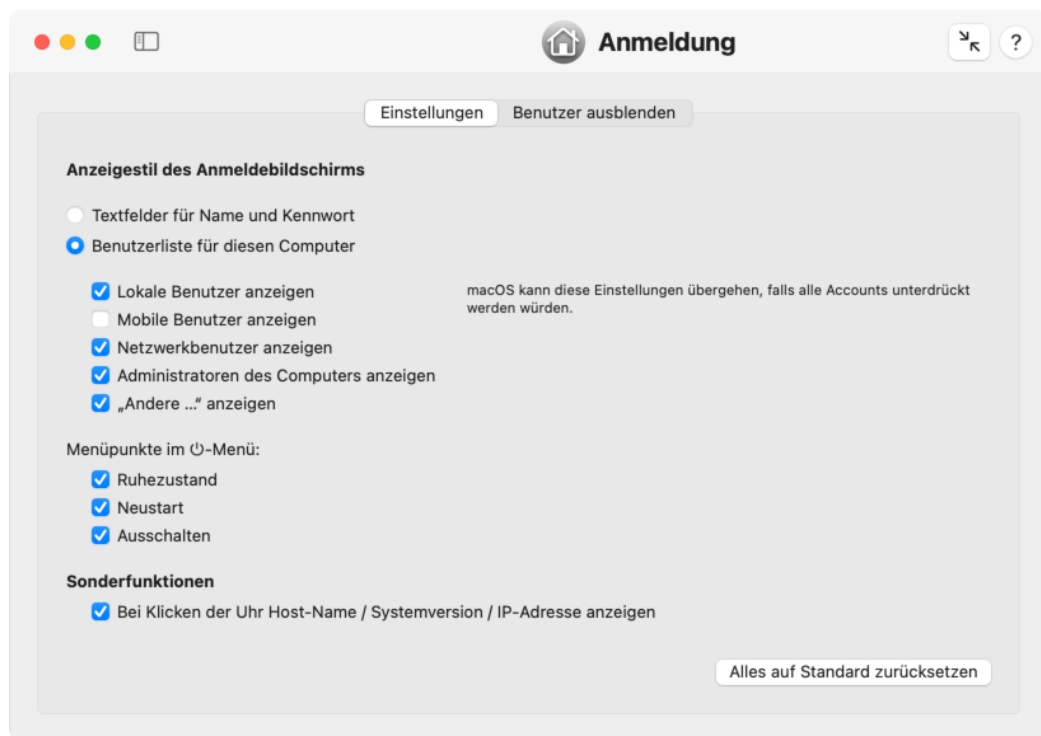


Abbildung 4.14: Einstellungen für den Anmeldeschirm

- **Lokale Benutzer anzeigen:** die „normalen“ Benutzer-Accounts, die auf dem aktuellen Computer eingerichtet sind.
- **Mobile Benutzer anzeigen:** hierbei handelt es sich um spezielle Benutzer, die von einem Verzeichnisdienst verwaltet werden und die sowohl einen Privatordner auf einem zentralen File-Server, als auch einen automatisch synchronisierten Privatordner auf einem mobilen Notebook-Computer verwenden.
- **Netzwerkbenutzer anzeigen:** die Benutzer-Accounts, die in Ihrem Netzwerk bekannt sind. Ihr Computer muss dazu eingerichtet sein, einen Netzwerkverzeichnisdienst mit einem Suchpfad für Benutzer-Accounts zu verwenden, damit diese Funktion genutzt werden kann.
- **Administratoren des Computers anzeigen:** die Benutzer-Accounts, die auf dem aktuellen Computer eingerichtet sind und Verwalterberechtigung haben.
- **„Andere ...“ anzeigen:** ein besonderer Knopf mit der Beschriftung „Andere“, der verwendet werden kann, um manuell auf Name- und Kennwortfelder umzuschalten.

Abhängig von der Liste der Benutzer-Accounts, die auf dem lokalen System und in den Netzwerkverzeichnisdiensten vorgefunden wird, kann sich der Anmeldeschirm dazu entschließen, einige oder alle der zuvor genannten Einstellungen nicht zu beachten. Dies ist notwendig, um zu garantieren, dass mindestens ein Benutzer sich erfolgreich anmelden kann. Ansonsten könnte es passieren, dass die Liste leer wäre, und das System würde unbenutzbar werden.



Sie sollten sich allerdings auf diese Sicherheitsfunktion nicht verlassen. Abhängig von der Betriebssystemversion und den Benutzer-Accounts, die auf Ihrem Computer verfügbar sind, kann das Abschalten zu vieler Benutzerkategorien dazu führen, dass das System keine „sinnvollen“ Anmeldungen mehr anbietet. Im Notfall können Sie das Notfallwerkzeug TinkerTool System für Wiederherstellung (Abschnitt 2.8 auf Seite 108) einsetzen, um den Anmeldeschirm auf Werkseinstellungen zurückzusetzen.

Ein-/Ausschalteinstellungen in macOS Ventura

Falls Sie macOS Sonoma oder höher verwenden, springen Sie bitte zum nächsten Abschnitt.

Zusätzliche Wahlmöglichkeiten erlauben die Kontrolle, welche Knöpfe am unteren Rand des Bildschirms angezeigt werden sollen:

- **Taste „Ruhezustand“ anzeigen:** der Knopf, der verwendet wird, um von Hand in den Ruhezustand zu schalten
- **Taste „Neustart“ anzeigen:** der Knopf, der verwendet wird, um das Betriebssystem neu zu starten
- **Taste „Ausschalten“ anzeigen:** der Knopf, der benutzt wird, um den Computer abzuschalten

Während der Benutzer angemeldet ist, stehen die Punkte für Neustart und Ausschalten auch über das Apfelmenü zur Verfügung. Sie können auch diese Menüpunkte ein- und ausschalten, indem Sie die Häkchen bei **Menüpunkte in Apple-Menü** verwenden. Alle Einstellungen sind unabhängig voneinander.

Ein-/Ausschalteinstellungen in macOS Sonoma

Falls Sie macOS Ventura verwenden, lesen Sie bitte den vorigen Abschnitt.

Zusätzliche Wahlmöglichkeiten erlauben die Kontrolle, welche Menüpunkte im Schaltmenü in der rechten oberen Ecke des Anmeldebildschirms eingeblendet werden sollen:

- **Ruhezustand:** der Menüpunkt, der verwendet wird, um von Hand in den Ruhezustand zu schalten
- **Neustart:** der Menüpunkt, der verwendet wird, um das Betriebssystem neu zu starten
- **Taste Ausschalten:** der Menüpunkt, der benutzt wird, um den Computer abzuschalten

Sonderfunktionen

Standardmäßig zeigt der Anmeldeschirm neben den Eingabefeldern nur die aktuelle Zeit und die gewählte Tastaturbelegung (sowie bei mobilen Systemen den Ladezustand des Akkus) an. Zu Diagnosezwecken kann es besonders in großen Netzwerken nützlich sein, noch weitere Informationen einzublenden. Der Anmeldeschirm ist in der Lage, den TCP/IP-Hostnamen des Computers, die Versionsnummer von macOS und die primäre IP-Adresse anzuzeigen. Die Punkte werden in der genannten Reihenfolge dargestellt, wenn Sie die Uhr in der oberen rechten Ecke des Anmeldeschirms anklicken. Um diese Funktion einzuschalten, kreuzen Sie die Wahlmöglichkeit **Bei Klicken der Uhr Host-Name/Systemversion/IP-Adresse anzeigen** an.

4.4.2 Benutzer ausblenden

macOS unterstützt eine Funktion zum Ausblenden gewählter Benutzer-Accounts für den Fall, dass Sie den Anzeigestil **Benutzerliste für diesen Computer** für den Anmeldeschirm eingerichtet haben. Dies kann sinnvoll sein, um die Liste sauber zu halten und nur „richtige“ Benutzer in der Liste anzubieten, keine Sonder-Accounts, die zur Verwaltung, für Techniker oder ähnliche Zwecke angelegt wurden. Solche Rollen-Accounts können sich immer noch über die Schaltfläche **Andere** in der Liste anmelden.

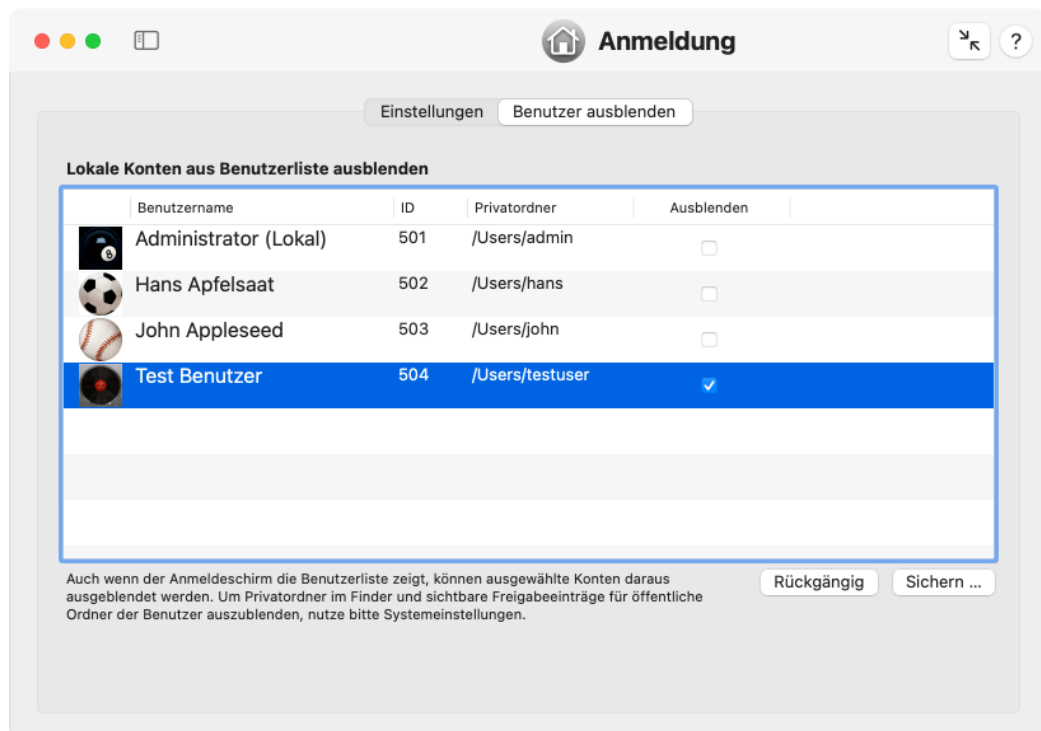


Abbildung 4.15: Accounts in der Benutzerliste der Anmeldung ausblenden

TinkerTool System zeigt alle lokalen Benutzerkonten, die zu Standardbenutzern gehören, denen die Anmeldung gestattet ist, auf dem Karteireiter **Benutzer ausblenden** an. Die Accounts sind nach ihren numerischen Identifikationen sortiert, was üblicherweise der Reihenfolge entspricht, in der diese angelegt wurden. Um einen Benutzer auszublenden, setzen Sie ein Häkchen in der Spalte **Ausblenden** und betätigen Sie den Knopf **Sichern ...**, um Ihre Änderungen abzuspeichern.

Nach Betätigen des Sicherungsknopfes fragt TinkerTool System nach Name und Kennwort, um eine Anmeldung bei der Open Directory-Kontendatenbank auf dem lokalen Computer zu erreichen. Obwohl Sie hier die gleichen Namen und Kennworte von Systemverwaltern wie in einer normalen Anmeldesituation nutzen können, unterscheidet sich diese Art der Anmeldung technisch.

In diesem besonderen Fall ist es tatsächlich TinkerTool System, **nicht macOS**, das nach dem Kennwort fragt. Die Anmeldedaten werden vom lokalen Open Directory-Subsystem geprüft, das je nach Ergebnis eine Erlaubnis erteilt oder verweigert.

Um Änderungen, die noch nicht gespeichert wurden, rückgängig zu machen, können Sie den Knopf **Rückgängig** betätigen. TinkerTool System bietet nur lokale Benutzer in der Liste an, keine Netzwerkbenutzer, die auf anderen Verzeichnisdiensten gespeichert sein können.

Die ausgeblendeten Benutzer-Accounts können immer noch indirekt sichtbar sein, z.B. über deren Privatordner im Ordner **Benutzer:innen (/Users)** und über deren jeweiligen Einträge zur Dateifreigabe. Um diese Punkte ebenso auszublenden, können erfahrene Administratoren zusätzlich Folgendes tun:

1. Verschieben Sie den betroffenen Privatordner eines ausgeblendeten Benutzers in einen unsichtbaren Unix-Ordner, zum Beispiel innerhalb von **/var**. Öffnen Sie dann **Systemeinstellungen > Benutzer:innen & Gruppen**, führen Sie einen Rechtsklick auf das betroffene Konto aus und wählen Sie **Erweiterte Optionen** im Kontextmenü. Setzen Sie **Benutzerordner** auf den neuen Ablageort des Privatordners dieses Benutzers.
2. Öffnen Sie **Systemeinstellungen > Allgemein > Teilen > Dateifreigabe > i** und entfernen Sie alle Einträge in der Liste **Geteilte Ordner**, die nicht mehr länger aktiv sein sollen.

4.5 Die Einstellungskarte Programmsprache

Alle Teile von macOS und viele Programme von Drittanbietern sind mehrsprachig. Das bedeutet, dass die Bedienungsoberfläche eines Programms zwischen verschiedenen Sprachen umgeschaltet werden kann, ohne dass eine spezielle sprachangepasste Version des Programms installiert werden muss. Unter normalen Umständen wird die Sprache, die ein Programm verwenden soll, während dessen Start bestimmt. macOS überprüft die vorhandenen Sprachunterstützungspakete, die in das Programm eingebettet sind, und vergleicht diese mit der Prioritätsliste der bevorzugten Sprachen des Benutzers. Die erste Sprache in dieser Liste, die mit einer im Programm verfügbaren Sprache übereinstimmt, wird „gewinnen“ und dazu ausgewählt, die aktive Sprache zu werden, in der das Programm läuft. Jeder Benutzer kann seine persönliche Prioritätsliste unter **Systemeinstellungen > Allgemein > Sprache & Region > Bevorzugte Sprachen** verändern. Alle Sprachen, die Sie verwenden möchten, können mit dem **[+]**-Knopf unterhalb der Tabelle hinzugefügt werden. Danach ziehen Sie die einzelnen Einträge mit der Maus in Ihre bevorzugte Prioritätsreihenfolge. Die oberste Sprache in der Tabelle wird zu Ihrer primären Sprache.

TinkerTool System erlaubt es, die persönliche Sprachprioritätsliste vorübergehend nicht zu beachten und ein Programm dazu zu zwingen, in einer bestimmten Sprache zu starten, die sich von Ihrer üblichen bevorzugten Sprache unterscheidet. Weder Ihre Spracheinstellungen, noch die Sprachpakete innerhalb des Programms müssen hierzu berührt werden. Dies kann sehr hilfreich sein, wenn Sie in einem mehrsprachigen Land oder einer

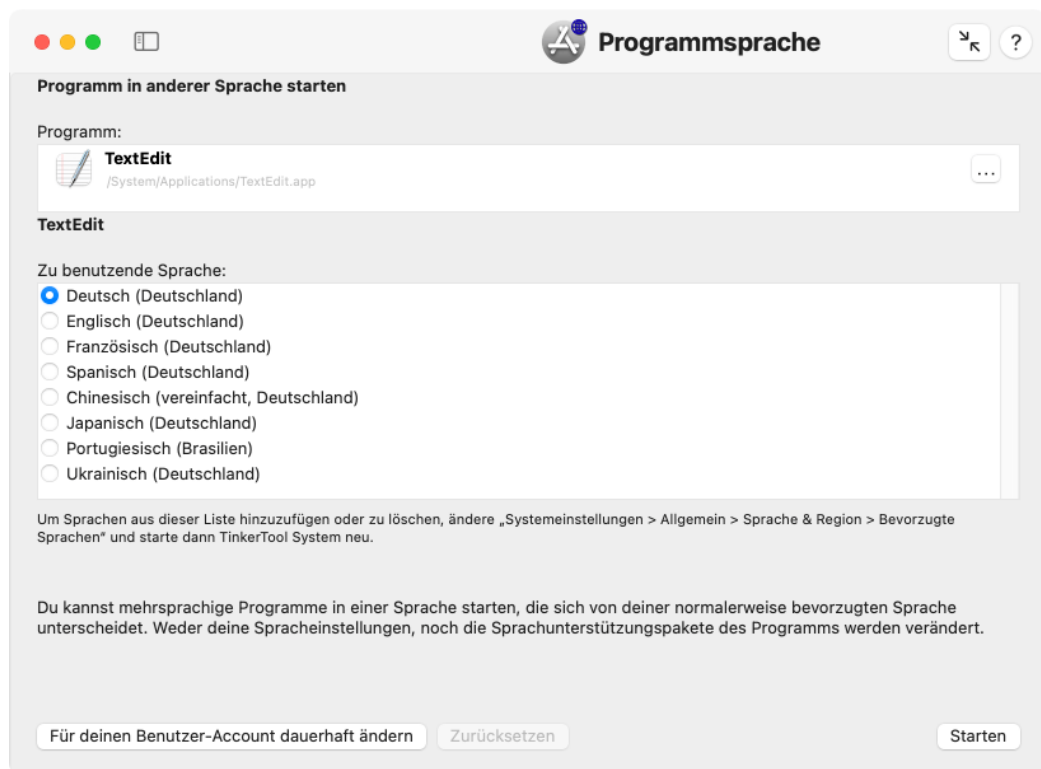


Abbildung 4.16: Programmsprache

mehrsprachigen Organisation arbeiten. Es ist ebenso nützlich, wenn Sie einem Benutzer Fernunterstützung geben möchten, der seine macOS-Umgebung auf eine andere Sprache eingestellt hat als Ihre eigene. Sie können sogar das gleiche Programm mehrfach laufen lassen, wobei Sie für jedes Exemplar eine andere Sprache auswählen können.

Einige Programme sind möglicherweise nicht darauf vorbereitet, mehrfach parallel in der gleichen Benutzersitzung zu laufen. Konflikte können entstehen, wenn die mehrfachen Exemplare dieselben Konfigurationsdateien ändern, so dass Sie vorsichtig sein sollten, wenn Sie Daten ändern. Bitte überprüfen Sie die Dokumentation der jeweiligen Programme auf mögliche Hinweise.

Führen Sie die folgenden Schritte durch, um ein Programm in einer bestimmten Sprache zu starten:

1. Stellen Sie sicher, dass alle Sprachen, mit denen Sie arbeiten möchten, in der Tabelle **Bevorzugte Sprachen** in den **Systemeinstellungen** angezeigt werden, so wie oben beschrieben. Falls nicht, nehmen Sie Änderungen an dieser Tabelle vor und starten Sie TinkerTool System erneut.
2. Öffnen Sie die Einstellungskarte **Programmsprache**.
3. Ziehen Sie das Programm aus dem Finder in das Feld **Programm**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.

4. Wählen Sie die Sprache durch Anklicken einer der Knöpfe in der Liste **Zu benutzende Sprache**.
5. Drücken Sie den Knopf **Starten**.

Falls das Programm, das Sie starten, keine Unterstützung für die Sprache anbietet, die Sie gewählt haben, wird die Standardsprache des Programms ausgewählt. Das ist üblicherweise die Sprache, für die das Programm ursprünglich entwickelt wurde.

Besondere Überlegungen beim Einsatz von macOS Sonoma oder höher

Ab macOS 14 hat Apple eine neue Sicherheitsfunktion eingeführt, die sich *Startumgebungsbeschränkung* (*Launch Environment Constraints*) nennt. Dieses Funktionsmerkmal macht es möglich, dass Programme einschränken können, von welchen anderen Programmen sie gestartet werden dürfen. Abhängig von Apples derzeitigen Sicherheitsrichtlinien können die Umgebungsbeschränkungen des Betriebssystems selbst extrem streng voreingestellt sein: In einigen Fällen erteilt macOS möglicherweise keine Erlaubnis für TinkerTool System, Programme zu starten, die von Apple hergestellt und als Teil des Betriebssystems mitgeliefert wurden. Hierzu zählt zum Beispiel TextEdit. In solch einem Fall löst macOS sofort einen absichtlichen Absturz des Apple-Programms aus, sobald es über TinkerTool System gestartet wurde.

Falls Sie hiervon betroffen sind, können Sie das jeweilige Apple-Programm nicht mit einer vorübergehenden Spracheinstellung nutzen. Alternativ können Sie mit **Systemeinstellungen** die Sprache kurzzeitig für alle Programme umstellen, oder die Spracheinstellung für dieses eine Programm dauerhaft überschreiben.

4.5.1 Startsprache für ein Programm dauerhaft überschreiben

Die Funktion, die im vorhergehenden Abschnitt skizziert wurde, erfordert es, dass Sie TinkerTool System verwenden, um ein Programm zu starten. In manchen Fällen möchten Sie jedoch vielleicht ein bestimmtes Programm *immer* in einer anderen Sprache starten, zum Beispiel wenn die Übersetzung des Programms in Ihrer Standardsprache schlecht ist, so dass Sie eine alternative Sprache nutzen möchten, jedes Mal wenn Sie das Programm laufen lassen.

TinkerTool System kann bevorzugte Spracheinstellungen für bestimmte Programme in Ihrem Benutzer-Account speichern. Nachdem eine solche Vorgabe eingestellt wurde, startet macOS das ausgewählte Programm in Ihrer persönlich bevorzugten Sprache, unabhängig von Ihren normalen Prioritätseinstellungen für Sprachen. Sie müssen nicht TinkerTool System verwenden, um das Programm zu starten. Führen Sie die folgenden Schritte durch, um solch eine Einstellung vorzunehmen:

1. Stellen Sie sicher, dass alle Sprachen, mit denen Sie arbeiten möchten, in der Tabelle **Bevorzugte Sprachen** in den **Systemeinstellungen** angezeigt werden, so wie oben beschrieben. Falls nicht, nehmen Sie Änderungen an dieser Tabelle vor und starten Sie TinkerTool System erneut.
2. Öffnen Sie die Einstellungskarte **Programmsprache**.
3. Ziehen Sie das Programm aus dem Finder in das Feld **Programm**. Sie können auch den Knopf [...] drücken, um zum Objekt zu navigieren oder auf die weiße Fläche klicken und den UNIX-Pfad des Objektes eingeben.

4. Wählen Sie die Sprache durch Anklicken einer der Knöpfe in der Liste **Zu benutzende Sprache**.
5. Drücken Sie den Knopf **Für deinen Benutzer-Account dauerhaft ändern**.

Sie können ein solches Überschreiben der Sprache jederzeit wieder entfernen. Ziehen Sie das Programm einfach nochmal in die Karte und betätigen Sie den Knopf **Zurücksetzen**.

Obwohl der Knopf zum Überschreiben der Sprache sich auf einer Karte der Kategorie **Systemeinstellungen** befindet, ist es in Wirklichkeit eine Benutzereinstellung. Das Überschreiben wird nur für Ihren Benutzer-Account wirksam, nicht für das gesamte System.

4.6 Die Einstellungskarte Cloud-Schutz

Apple bietet unter dem Namen *iCloud* eine Reihe von Dienstleistungen an, mit denen es unter anderem möglich ist, Daten, die auf einem Apple-Gerät gespeichert sind, vollautomatisch über das Internet mit anderen Apple-Geräten des gleichen Benutzers zu synchronisieren. Wird eine Datei auf einem der beteiligten Geräte „in die Cloud“ gespeichert, erscheint sie danach als Kopie auf allen anderen Geräten.

Wenn Sie Daten über andere Personen auf Ihrem Computer zu mehr als nur rein privaten Zwecken speichern, z.B. Geburtsdaten der Mitglieder eines Sportvereins, müssen Sie, je nach Land, in dem Sie sich befinden, besondere gesetzliche Regeln und Sorgfaltspflichten beim Umgang mit diesen Daten beachten. Personenbezogene Daten dürfen im Allgemeinen nicht an Dritte weitergegeben werden, es sei denn, Ihnen liegt eine ausdrückliche Genehmigung jeder betroffenen Person vor. Die Verarbeitung dieser Daten durch einen fremden Dienstleister kann auch dann erlaubt sein, wenn Sie

- mit dem entsprechenden Dienstleister einen Einzelvertrag, einen sogenannten *Auftragsverarbeitungsvertrag* abgeschlossen haben, der sicherstellt, dass dieser Dienstleister auf seinen Computern die erforderlichen Schutz- und Sorgfaltspflichten einhält, und Sie
- die Gelegenheit haben, diese Schutzmaßnahmen selbst, z.B. in Form eines Audits vor Ort, überprüfen zu können.

Apple bietet für iCloud keinen dieser beiden Punkte an, so dass die Nutzung von iCloud je nach Art der gespeicherten Daten und Gesetzeslage unzulässig sein kann. Sie können sich bei einem Rechtsbeistand über die für Ihr Land gültigen Regeln informieren. In vielen Regionen gibt Apple die Daten außerdem an andere Cloud-Dienstleister weiter und speichert sie nicht selbst. Hierzu gehören AIPO Cloud (Guizhou) Technology Co. Ltd in Festlandchina, IXcellerate in Russland, sowie Amazon Web Services, Google Cloud Storage oder Microsoft Azure in anderen Ländern.

TinkerTool System kann für bestimmte Teildienste von iCloud sicherstellen, dass diese nicht versehentlich auf Ihrem Computer aktiviert werden. Sie können so Ihren Computer dagegen absichern, Daten nicht unabsichtlich an Apple weiterzugeben. Hierdurch bleibt der Datenschutz gewährleistet.

Für die

- allgemeine Synchronisierung von Dateien (z.B. iCloud Drive oder die Nutzung der Funktion „Mac-Speicher optimieren“, je nach Betriebssystemversion) und das

- Synchronisieren der Benutzerordner **Dokumente** und **Schreibtisch**

kann TinkerTool System die Dienste ausschalten und danach gegen Wiedereinschalten sperren.

Ausgewählte andere Funktionen von iCloud kann TinkerTool System ebenso sperren. *Dabei wird aus technischen Gründen allerdings zunächst der aktuelle Zustand (an/aus) der jeweiligen Funktion beibehalten und kann über die Systemeinstellungen vom Benutzer nicht mehr geändert werden.* Aus Sicherheitsgründen kann TinkerTool System weder prüfen, was der aktuelle Zustand ist, noch die jeweilige Funktion von sich aus abschalten. Trotzdem nimmt macOS an, dass die Standardeinstellung für eine gesperrte iCloud-Funktion „aus“ ist. Wenn macOS aus internen Gründen die Einstellungen überprüft, kann es die gesperrten iCloud-Funktionen zu einem nicht vorhersagbaren, späteren Zeitpunkt abschalten.

Sind also iCloud-Funktionen (außer der Dateisynchronisation) versehentlich eingeschaltet, wenn Sie diese mit TinkerTool System sperren, ist ungewiss, ob und wann macOS diese Funktionen tatsächlich abschaltet.

Aus diesem Grund sollten Sie diesen unsicheren Übergangszustand vermeiden und immer wie folgt vorgehen:

1. Klicken Sie auf den Knopf **Zustand in Systemeinstellungen zeigen**. Die derzeitigen iCloud-Einstellungen werden geöffnet.
2. Klicken Sie in den Systemeinstellungen bei **Apps, die iCloud verwenden** auf **Alle anzeigen**, um die derzeitigen Zustände aller iCloud-Funktionen einzusehen.
3. Stellen Sie sicher, dass alle Teilfunktionen, die Sie mit TinkerTool System sperren möchten, auf **Aus** geschaltet sind.
4. Kreuzen Sie nun in TinkerTool System in der Tabelle **Die folgenden iCloud-Funktionen im aktuellen Zustand sperren** an, welche iCloud-Funktion dauerhaft ausgeschaltet bleiben sollen.

Beachten Sie, dass nicht jedes Apple-Betriebssystem jeden iCloud-Dienst anbietet. Ebenso kann nicht jede Version von macOS jeden iCloud-Dienst sperren. TinkerTool System zeigt auf der Karte **Cloud-Schutz** nur diejenigen Dienste an, die sich in der jeweiligen Situation sperren lassen.

Sie können eine Sperre jederzeit durch Entfernen des jeweiligen Häkchens wieder aufheben. Die Einstellung wird sofort an macOS weitergeleitet. Je nach aktuellem Zustand und den Hintergrundaufgaben, die iCloud gerade ausführt, kann die Einstellung jedoch verzögert wirksam werden.

Um sicher zu stellen, dass die Einstellung tatsächlich wirksam geworden ist, ist es empfehlenswert, etwas zu warten und dann den Computer neu zu starten. Sperren werden für alle Benutzer des jeweiligen Computers gültig. Ist die Dateisynchronisierung deaktiviert und gesperrt worden, verschiebt macOS möglicherweise iCloud-Daten automatisch in einen Archivordner im Privatordner des jeweiligen Benutzers. Je nach Version von macOS kann es sein, dass das Programm **Systemeinstellungen** fälschlicherweise anzeigt, die iCloud-Einstellungen wären durch ein Konfigurationsprofil gesperrt worden, auch wenn TinkerTool System keine Profile verwendet.

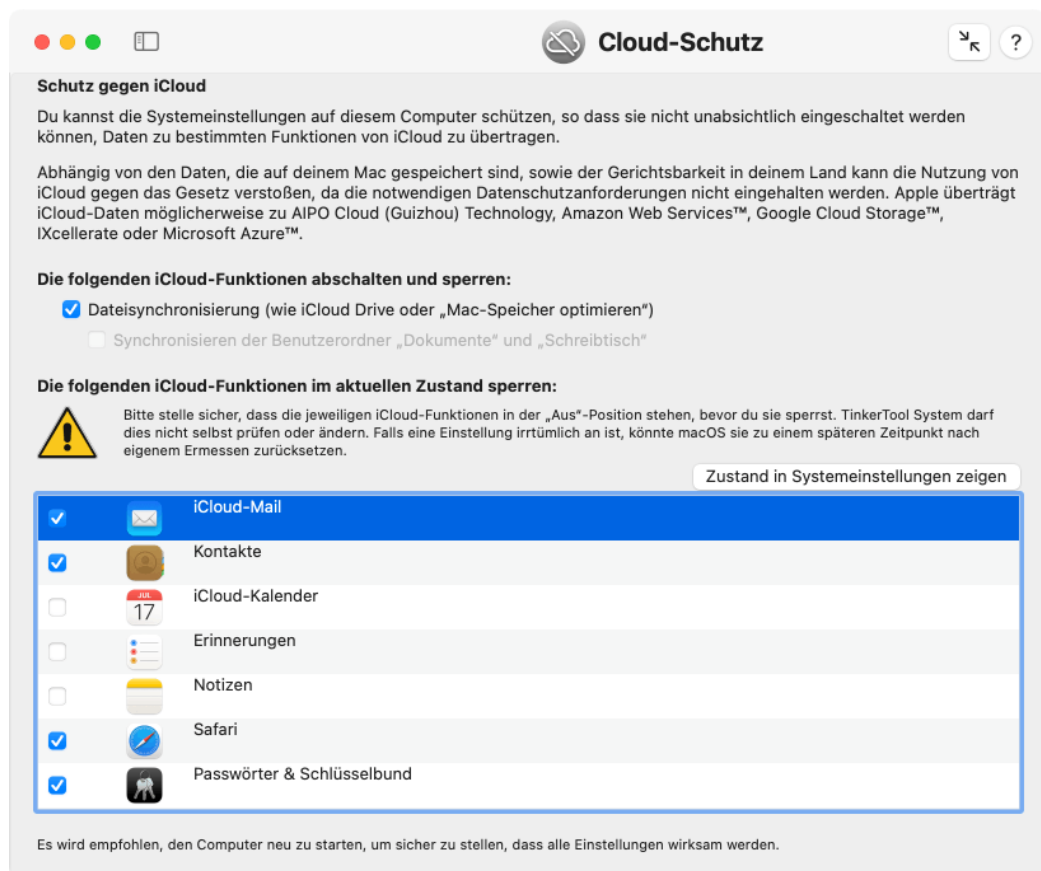


Abbildung 4.17: Cloud-Schutz

4.7 Die Einstellungskarte Energiezeitplan

Die Einstellungskarte **Energiezeitplan** kann dazu genutzt werden, die weggefallenen Funktionen aus der früheren Karte **Energie sparen**, bzw. **Batterie** zu ersetzen, die in älteren Versionen von macOS Bestandteil des Programms Systemeinstellungen war. TinkerTool System stellt den weitestgehend identischen Funktionsumfang zur Verfügung und ermöglicht darüber hinaus auch den Zugriff auf zusätzliche Einstellungen für den Zeitplan einmaliger Energieereignisse.

4.7.1 Termine für wiederkehrende Ereignisse

Durch eine ständig laufende Uhr mit Weckfunktion ist ein Mac in der Lage, sich im ausgeschalteten Zustand selbst einschalten zu können. Ist der Mac zu dieser Zeit bereits eingeschaltet, aber im Ruhezustand oder Standby-Modus, wird stattdessen ein Aufwachvorgang ausgelöst, so dass macOS in jedem Fall zum gewählten Zeitpunkt betriebsbereit ist. Auch die umgekehrte Funktion, nämlich wahlweise

- das Aktivieren des Ruhezustands,
- ein geplanter Neustart oder
- ein Herunterfahren des Computers

lässt sich termingesteuert programmieren. Es lässt sich zu einer gewählten Uhrzeit entweder ein einzelnes Ereignis oder ein Paar aus einem aktivierenden und einem deaktivierenden Ereignis einrichten, das sich täglich wiederholt. Zusätzlich kann vereinbart werden, dass die Ereignisse nicht wirklich jeden Tag, sondern nur an bestimmten Tagen der Woche stattfinden. TinkerTool System erlaubt die Einrichtung wiederkehrender Termine

- täglich,
- an Wochenenden,
- an allen Tagen außer am Wochenende,
- an einem bestimmten Wochentag,
- an beliebigen Kombinationen von Wochentagen (über den Menüpunkt **Angepasst ...**)

Sie können solche, sich regelmäßig wiederholende Termine für die Energiesteuerung des Computers wie folgt einrichten:

1. Öffnen Sie die Einstellungskarte **Energiezeitplan**.
2. Kreuzen Sie eine oder beide Zeilen in der Box **Wiederkehrende Ereignisse** an. Wählen Sie mit den Aufklappmenüs die entsprechenden Wochentage und die gewünschte Uhrzeit aus. Mit der oberen Zeile können Sie einen aktivierenden Termin vereinbaren, mit der unteren Zeile einen deaktivierenden Termin, wobei Sie die Art des Abschaltvorgangs wählen können.
3. Betätigen Sie den Knopf **Sichern** rechts unten.

Sofern Sie keine Fehlermeldung erhalten, ist der Zeitplan aktiv und wirksam. Sie können alle wiederkehrenden Ereignisse löschen, indem Sie auf den Knopf **Alle löschen** drücken. Die Änderung findet in diesem Fall sofort statt, ohne dass Sie die Einstellung sichern müssen.

Über die UNIX-Befehlszeile von macOS lassen sich auch Zeitpläne mit relativen Zeitpunkten einrichten. Apple rät hiervon ab, da dies aus technischen Gründen nicht exakt umgesetzt werden kann. Ein solcher Zeitplan kann von TinkerTool System aus nicht bearbeitet werden. In der Box erscheint dann eine Fehlermeldung in rot. Sie können in diesem Fall den Knopf **Alle löschen** drücken, um den Zeitplan zu löschen und durch einen einfacheren zu ersetzen.

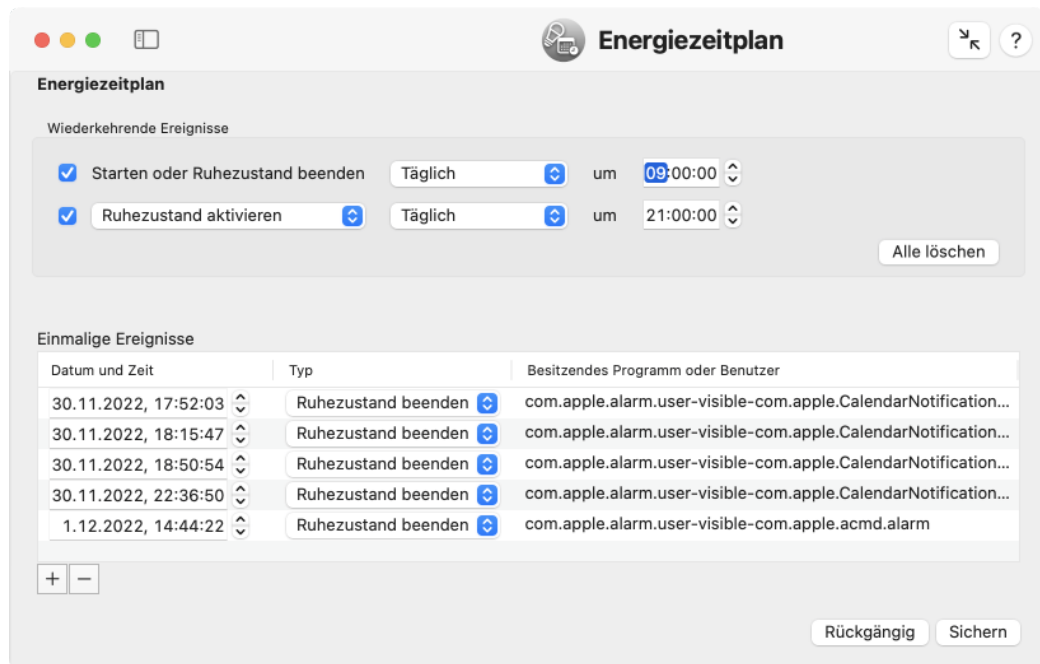


Abbildung 4.18: Regelmäßig wiederkehrende Zeitplanereignisse und einmalige Termine können eingesehen und verändert werden.

4.7.2 Termine für einmalige Ereignisse

Neben den sich wöchentlich, bzw. täglich wiederholenden Ereignissen lassen sich auch einmalige Ereignisse einrichten, die durch ein festes Datum und Uhrzeit vorgegeben sind. Hierfür stehen alle bisher genannten Ereignistypen mit einschaltendem oder ausschaltendem Charakter zur Verfügung. Apple empfiehlt, solche Ereignisse zusätzlich mit einer Bemerkung zu versehen, aus der hervorgeht, welches Programm oder welcher Benutzer diesen Termin „besitzt“.

macOS verwendet den Zeitplan einmaliger Ereignisse auch für sich selbst, um zu bestimmten Zeitpunkten das Beenden des Ruhezustands zu erzwingen. Hierdurch können Wartungsarbeiten oder Erinnerungen an den Benutzer ausgelöst werden. Sie erkennen solche Einträge in der Regel an einer Eigentümerbemerkung, die mit **com.apple** ... beginnt. Die von macOS selbst eingerichteten Termine werden automatisch bereinigt.

Sie können einmalige Ereignisse wie folgt einrichten:

1. Öffnen Sie die Einstellungskarte **Energiezeitplan**.
2. Fügen Sie mit dem Knopf **+** eine neue Zeile am Ende der Tabelle ein.

3. Wählen Sie in der neuen Zeile den Termin und den Typ des Energieereignisses. Geben Sie auf Wunsch auch einen kurzen Bemerkungstext an.
4. Betätigen Sie den Knopf **Sichern** rechts unten.

Wenn Sie keinen Bemerkungstext für einen Termin eingeben, wird automatisch die interne Kennung von TinkerTool System als „Besitzer“ dieses Eintrags angegeben.

Beim Sichern kann sich macOS dazu entschließen, die Tabelle nach eigenem Ermessen anders zu sortieren. Dies lässt sich nicht beeinflussen.

Sie können auch ein oder mehrere Zeilen in der Tabelle markieren und die zugehörigen Termine durch Betätigen des Knopfes – löschen.

4.7.3 Allgemeine Hinweise zum Energiezeitplan

Haben Sie Änderungen eingegeben, aber noch nicht gesichert, können Sie über den Knopf **Rückgängig** alle Einstellungen wieder auf den vorigen Stand zurücksetzen. Dies schließt sowohl wiederkehrende als auch einmalige Ereignisse ein.

Für das Umsetzen der eingestellten Termine ist weder TinkerTool System noch macOS verantwortlich. Die Umsetzung wird *durch die Hardware des Macintosh* gesteuert. Falls Sie macOS in einer Virtuellen Maschine verwenden oder keine Original-Hardware von Apple nutzen, wird der Zeitplan möglicherweise nicht wirksam.

Beachten Sie außerdem, dass der Zeitplan unerwarteten Einschränkungen unterliegt: Das automatische Herunterfahren des Computers ist nur dann möglich, wenn sich der Mac zur jeweiligen Uhrzeit *nicht* im Ruhezustand befindet und mindestens ein Benutzer lokal angemeldet ist. Wenn gerade ältere Software mit nicht gesicherten Dokumenten läuft, kann der Ruhezustand, der Neustart oder das Abschalten verhindert werden. Ist der Computer durch FileVault gesichert, kann er zwar automatisch eingeschaltet werden, aber er kann nicht das Betriebssystem starten, da ein Benutzer erst ein Kennwort zur Entschlüsselung des System-Volumes eingeben muss.

Wenn Sie als Benutzer mit Verwaltungsrechten angemeldet sind, dürfen Sie die Einstellungen für den Energiezeitplan ohne zusätzliche Eingabe eines Kennworts ändern. Dies entspricht der vereinfachten Sicherheitsrichtlinie, die Apple auch früher im Programm Systemeinstellungen verwendet hat.

Kapitel 5

Benutzereinstellungen

5.1 Die Einstellungskarte Benutzer

Alle Vorgänge, die auf der Einstellungskarte **Benutzer** auswählbar sind, beziehen sich nur auf einen einzelnen Benutzer-Account, nämlich den Benutzer, der das Programm gerade gestartet hat. Detaildaten über den ausgewählten Benutzer-Account können über den Unterpunkt **Info** dieser Karte abgerufen werden.

5.1.1 Einstellungen („Präferenzen“)

Motivation

Macintosh-Software-Produkte werden normalerweise gemäß sehr hoher Standards für Benutzereinfreundlichkeit entwickelt. Technische Probleme werden in der Regel von den Programmen selbst behandelt, in den meisten Fällen „still“, ohne dass eine Interaktion mit dem Benutzer erforderlich wäre. Es gibt jedoch eine bestimmte Art von technischen Problemen, die oft nicht von den betroffenen Programmen abgefangen werden, nämlich Fälle, in denen die Einstellungsdaten (*Preferences*, „Präferenzen“) des jeweiligen Programms beschädigt wurden. TinkerTool System bietet Funktionen an, um automatisch schadhafte Einstellungsdateien zu finden und zu beseitigen.

Das Einstellungssystem von macOS

Programme senden Nachrichten an das Betriebssystem um Benutzereinstellungen zu speichern und wieder abzurufen, z.B. Farbwünsche, die letzte Position von Fenstern auf dem Bildschirm, das letzte gesicherte Dokument, usw. macOS verwendet eine Kerntechnologie des Systems, die *Eigenschaftslisten* (*Property Lists*), um alle Einstellungswerte in einer Art Datenbank abzulegen. Die Datenbank ist auf eine große Zahl von Dateien verteilt, die die Namensendung **plist** tragen. Jede dieser Eigenschaftslisten enthält Einstellungswerte, die sich nur auf ein ganz bestimmtes Gebiet des Systems beziehen, d.h. eine Untermenge der vollständigen Sammlung der Einstellungen. Solche eine Untermenge wird *Einstellungsdomäne* genannt. Eine Einstellungsdomäne hängt normalerweise eng mit einem Programm zusammen, das verwendet wurde. So werden z.B. die Einstellungen des Programms **Mail** in einer Einstellungsdomäne mit dem Namen **com.apple.mail** gespeichert. Es gibt jedoch nicht immer solch eine Eins-zu-Eins-Beziehung. Apples Mail-Programm macht zum Beispiel auch von weiteren Einstellungsdomänen Gebrauch, wie **com.apple.mail-shared**.

Gemäß Apples Richtlinien für Software-Design müssen die Bezeichnungen von Einstellungsdomänen aus einer hierarchisch aufgebauten Liste beschreibender Namen bestehen, die von links nach rechts von der höchsten zur niedrigsten Hierarchiestufe angeordnet und durch Punkte getrennt werden. Der erste Teil der Hierarchie muss dem Internet-Domännennamen (DNS-Namen) des Programmanbieters entsprechen, so dass gewährleistet ist, dass zwei unterschiedliche Software-Firmen niemals die gleiche Bezeichnung für eine Domäne wählen, sogar wenn ihre Produkte zufällig den gleichen Namen haben sollten.

Beispiel: Die eindeutige Bezeichnung für Apples Web-Browser Safari ist **com.apple.Safari**, denn er wird von einer Firma herausgegeben, die den Internet-Domännennamen **apple.com** trägt und **Safari** ist der beschreibende Name, der dieses Programm innerhalb von Apples Software-Angebot identifiziert. Beachten Sie, wie **com.apple.Safari** in der Reihenfolge von der höchsten zur niedrigsten Hierarchiestufe notiert wird, mit der wichtigsten Angabe am Anfang, während Internet-Domännennamen wie **www.apple.com** in umgekehrter Reihenfolge geschrieben werden, mit dem maßgeblichsten Teil zum Schluss.

Software-Firmen ist es freigestellt, mehr als einen beschreibenden Namen zu verwenden, um ein bestimmtes Programm oder einen Aspekt eines Programms kennzuzeichnen. Beispiele hierfür sind **com.apple.airport.airportutility** und **com.apple.airport.clientmonitor**, die zwei verschiedene Programme bezeichnen, die beide Teil des Gebietes „Airport“ sind. Das Namensschema garantiert, dass jedes Programm einer eindeutigen, einzigartigen Einstellungsdomäne angehört.

Die Integrität von Einstellungsdateien prüfen

Falls die Eigenschaftslistendatei einer Einstellungsdomäne aus irgendeinem Grund beschädigt wurde, füttert macOS das Programm, das zu dieser Datei gehört, mit ungültigen Einstellungswerten, eine Situation, die von vielen Programmen nicht korrekt abgefangen wird, da sie nicht erwarten, dass so etwas passieren könnte. Das Programm könnte abstürzen oder sich fehlerhaft verhalten.

Um dies zu vermeiden, können Sie die Integrität aller Einstellungsdateien überprüfen lassen, die für den aktuellen Benutzer wirksam werden. Dies schließt alle Programme ein, die jemals von diesem Benutzer gestartet wurden. Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Einstellungen** auf der Einstellungskarte **Benutzer**.
2. Betätigen Sie den Knopf **Dateien prüfen**.

Klassische Mac OS-Programme und Altlastenprogramme, die nicht korrekt auf die macOS-Plattform portiert wurden, verwenden Einstellungsdateien, die diese selbst angelegt haben. Solche Dateien können nicht überprüft werden, da sie keiner Norm folgen.

Während der Prüfvorgang läuft, können Sie ihn jederzeit durch Drücken des **Stopp**-Knopfes abbrechen. Nachdem alle Tests abgeschlossen sind, zeigt TinkerTool System einen tabellenförmigen Bericht an, in dem alle vorgefundenen Probleme aufgeführt sind. Die Probleme sind nach Schwere gewichtet, was über verschiedene Farben dargestellt wird:

- **Gelb:** eine Warnung, die vernachlässigt werden kann. Die Einstellungsdatei hält sich nicht ganz an die Richtlinien von macOS, scheint aber keine Probleme zu verursachen.

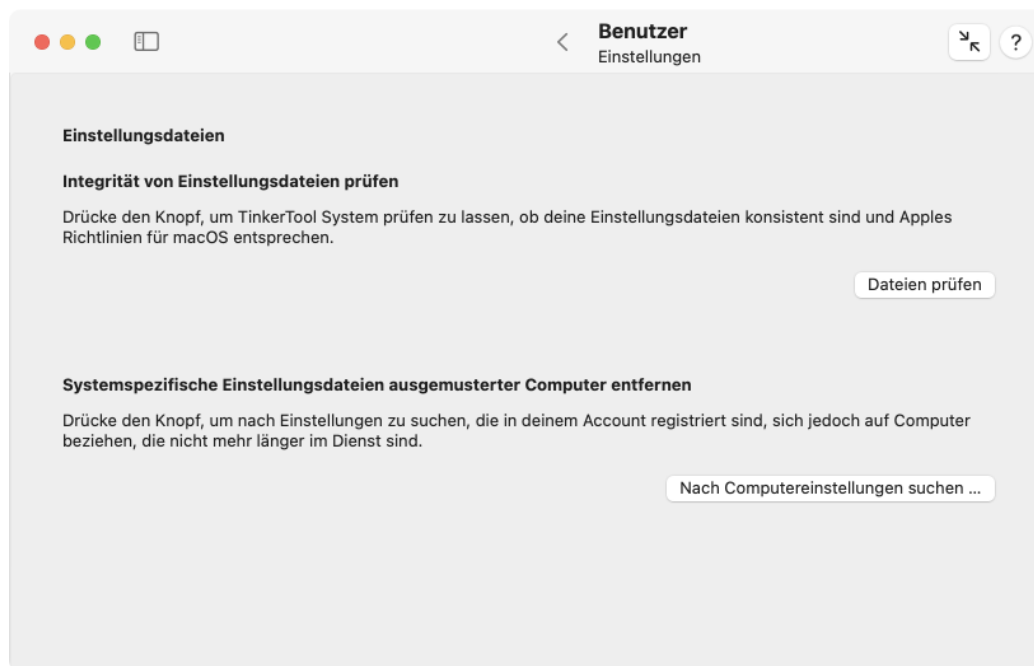


Abbildung 5.1: Einstellungen

- **Orange:** eine Warnung. Ein Problem mit der Einstellungsdatei wurde erkannt und es wird empfohlen die Datei und das Programm, zu dem sie gehört, weiter zu überprüfen. In einigen Fällen kann nur der Software-Entwickler des jeweiligen Programms das Problem vollständig beheben, da das Programm eventuell Operationen auf den Einstellungen ausführt, die sich nicht an die Richtlinien für Software-Design von macOS halten.
- **Rot:** die Datei verursacht definitiv Probleme. Ihre Struktur ist beschädigt, so dass das Programm, zu dem die Datei gehört, entweder mit gar keinen oder ungültigen Benutzereinstellungen gefüttert wird.

Die Berichtstabelle enthält für jedes vorgefundene Problem eine Zeile. Einstellungsdaten, die fehlerfrei sind, werden nicht aufgeführt. Jeder Eintrag enthält eine kurze Problembeschreibung und den Namen der jeweiligen Einstellungsdomäne.

Um Detailinformationen über ein gefundenes Problem abzurufen, wählen Sie einen Eintrag der Tabelle aus. Der volle Pfad zur betroffenen Eigenschaftslistendatei und eine ausführliche Fehlerbeschreibung werden unter der Tabelle angezeigt. Sie können den Finder zur betreffenden Datei navigieren lassen, indem Sie auf das Symbol mit dem Vergrößerungsglas klicken. In den Fällen, in denen es sinnvoll ist, können Sie die problematische Einstellungsdatei entweder deaktivieren oder löschen, indem Sie die entsprechenden Knöpfe betätigen.

- **Deaktivieren:** Benennt die Datei so um, dass sie von macOS nicht mehr weiter verwendet wird. Das betroffene Programme wird beim nächsten Start bereinigte Einstellungen verwenden. Das Deaktivieren einer Einstellungsdatei gibt Ihnen die Möglichkeit, alle Programmeinstellungen später wiederherzustellen, falls Sie feststellen sollten, dass die Einstellungsdatei, das eigentliche Problem gar nicht ausgelöst hatte, sondern etwas anderes. In diesem Fall sollten Sie das jeweilige Programm beenden, die neue Einstellungsdatei, die angelegt wurde, löschen und die deaktivierte

Einstellungsdatei wieder auf den früheren Namen umbenennen. Wenn Sie dann das betroffene Programm wieder neu starten, wird es wieder die früheren Einstellungswerte verwenden. TinkerTool System deaktiviert Einstellungsdateien, indem es die Dateinamenserweiterung auf **INACTIVE-plist** umbenennt. Wenn Sie die Erweiterung wieder zurück auf **plist** ändern, wird die Datei wieder aktiv.

- **Löschen:** löscht die Einstellungsdatei. Hierbei verlieren Sie alle Einstellungsdaten des zugehörigen Programms. Beim nächsten Start des Programms legt macOS wieder eine neue, bereinigte Einstellungsdatei an.

Sie sollte keine Einstellungen von Programmen löschen oder deaktivieren, die im Moment laufen, da dies keine Wirkung haben wird. Beenden Sie die betroffenen Programme und lassen Sie den Test erneut ablaufen, bevor Sie sich dazu entschließen, eine beschädigte Einstellungsdatei zu entfernen.

Entfernen von systemspezifischen Einstellungsdateien ausgemusterter Computer

In professionellen Netzwerken werden die Privatordner der Benutzer nicht auf den lokalen Festplatten der Computer gespeichert, sondern auf einem zentralen File-Server. In diesem Fall spielt es keine Rolle mehr, mit welchem konkreten Computer ein bestimmter Benutzer arbeitet. Die persönlichen Dokumente des Benutzers und alle persönlichen Einstellungen werden automatisch „mitgenommen“, wenn ein anderer Computer verwendet wird. Der Account benutzt immer die gleichen Daten, ohne dass irgendeine Art von Dateisynchronisation nötig wäre. macOS verfolgt automatisch nach, welche Einstellungswerte eines Benutzers für alle Computer in einem Netzwerk gelten, und welche computerspezifisch sind. Beispielsweise sollten die Trackpad- und Maus-Einstellungen für jeden Computer individuell gespeichert werden, da jedes Computermodell möglicherweise unterschiedliche Arten von Mäusen, bzw. Trackpads einsetzt. Ähnliche Regeln gelten für Bluetooth, Airport, Drucker, Bildschirmschoner und viele andere Einstellungen, die individuell pro Benutzer sind, gleichzeitig jedoch auch individuell für jeden Computer, denn sie hängen von der jeweiligen Hardware-Ausstattung ab.

Eine ähnliche Situation kann auch bei Computern von Privatpersonen auftreten: Falls Sie Ihren persönlichen Home-Ordner von einem alten Computer auf einen neuen migriert haben – möglicherweise sogar über mehrere Generationen von Computern hinweg – liegt genau das gleiche Szenario vor. Nachdem ein Computer ein gewisses Alter erreicht hat, wird er üblicherweise aus dem Netzwerk, bzw. aus Ihrem persönlichen Zugriff entfernt, so dass die Speicherung von computerbezogenen Benutzereinstellungen für diesen Computer nicht mehr länger sinnvoll ist.

Um diese Funktion nutzen zu können, müssen Sie den Computer identifizieren, der nicht mehr länger in Betrieb ist. Dies muss von Hand geschehen, da kein Programm Informationen von einem Computer bekommen kann, der nicht mehr länger zugreifbar ist. Um einen Computer zu identifizieren, verwendet macOS entweder die MAC-Adresse des ersten eingebauten Netzwerkanschlusses oder einen UUID-Code (*Universal Unique Identifier*).

Bei modernen Versionen von macOS, die UUID-Codes verwenden, zeigt TinkerTool System die Identifikation unter **Info > Mac > Computer > Eindeutige Hardware-Identifikation** an. Falls TinkerTool System auf dem in Frage kommenden Computer nicht zur Verfügung steht, können Sie auch das Programm **Systeminformationen** nutzen, die Kategorie **Hardware** öffnen und dort die Zeile **Hardware-UUID** suchen.

Nachdem Sie den in Frage kommenden Computer identifiziert haben, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Einstellungen** auf der Einstellungskarte **Benutzer**.
2. Drücken Sie den Knopf **Nach Computereinstellungen suchen**

Während die Suche läuft, können Sie diese jederzeit durch Druck auf den **Stopp**-Knopf abbrechen. Ist das Durchsuchen der Einstellungen abgeschlossen, zeigt TinkerTool System einen Bericht an, der alle Dateien auflistet, die computerspezifische Einstellungen für den aktuellen Benutzer-Account enthalten. Neben dem Identifikationscode des Computers finden Sie das Datum der letzten Nutzung und die Anzahl der Einstellungsdateien, die sich auf den jeweiligen Computer beziehen. Durch Abwählen der Knöpfe in der Spalte **Entfernen?** können Sie Einstellungsdateien aus dem Löschvorgang ausschließen. Das Betätigen der Knöpfe **Alle auswählen** oder **Alle abwählen** bewirkt, dass alle Häkchen gesetzt, bzw. entfernt werden. Durch Druck auf den Knopf **OK** werden alle Dateien, bei denen das Häkchen **Entfernen?** gesetzt war, gelöscht. Falls Sie den Knopf **Abbrechen** betätigen, wird keine Datei berührt.

Die Umschaltknöpfe in der unteren linken Ecke des Berichtsfensters steuern, wie das Entfernen durchgeführt werden soll. Sie können entweder **Dateien sofort löschen**, **Dateien in den Papierkorb werfen**, oder die **Dateien in einen Archivordner bewegen**, den Sie zusätzlich angeben müssen.

5.1.2 Benutzte Objekte

Neben vielen anderen Einstellungen führt jedes Programm Buch darüber, welche Dokumente bei der letzten Benutzung des Programms geöffnet worden sind. Diese Einträge werden im Untermenü **Ablage > Benutzte Dokumente** jedes Programms angezeigt. Zusätzlich gibt es eine zentrale Liste benutzter Dokumente und Programme im Apfelmenü und der Finder unterhält eine Liste von Servern, zu denen manuelle Netzverbindungen aufgebaut wurden.

Um Ihre Privatsphäre zu schützen, möchten Sie diese Einträge möglicherweise entfernen, da sie es erlauben, nachzuverfolgen, wie Sie den Computer in der Vergangenheit genutzt haben. Die Serverliste kann außerdem Kennworte im Klartext enthalten, die ebenso geschützt werden sollten. TinkerTool System kann für Sie die folgenden Einträge automatisch löschen:

- alle benutzten Dokumente im Apfelmenü
- alle benutzten Programme im Apfelmenü
- alle benutzten Server im Apfelmenü
- alle benutzten Server im Finder

Um die Einträge für benutzte Objekte zu entfernen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Benutzte Objekte** auf der Einstellungskarte **Benutzer**.
2. Wählen Sie jede Kategorie, für die die Einträge benutzter Objekte entfernt werden sollen.
3. Drücken Sie den Knopf **Ausgewählte Einträge entfernen**.

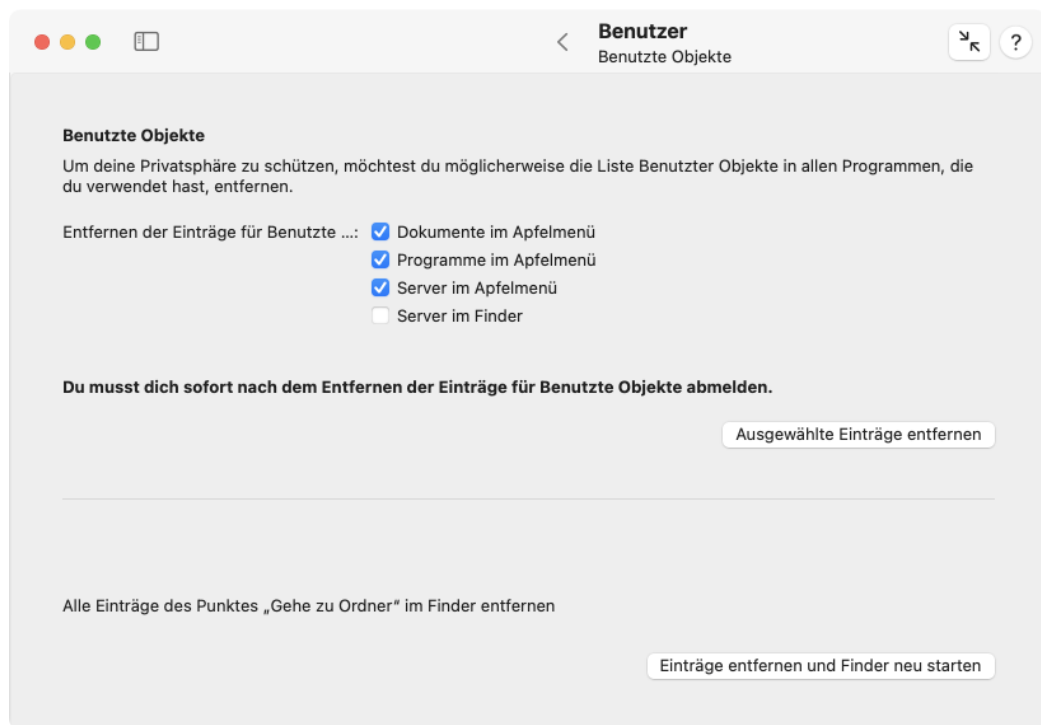


Abbildung 5.2: Benutzte Objekte

Hierbei werden die Einträge gelöscht, selbstverständlich nicht die Dokumente, auf die sich die Einträge beziehen. Wir empfehlen dringend, sich sofort abzumelden, nachdem Sie Benutzte Objekte bereinigt haben. Andernfalls kann nicht immer garantiert werden, dass macOS die Einträge nicht einfach wieder anlegt.

Auch der Dialog **Gehe zu > Gehe zu Ordner**, der vom Finder angeboten wird, merkt sich eine größere Zahl von Ordnern, die Sie zuletzt mit dieser Funktion genutzt hatten. Auch diese Einträge können entfernt werden, hierfür ist jedoch zusätzlich ein Neustart des Finders erforderlich. Betätigen Sie hierzu die Schaltfläche **Einträge entfernen und Finder neu starten**.

5.1.3 Startdienste

macOS führt eine interne Datenbank, die alle Programme enthält, auf die Ihr Computer zugreifen kann. Diese Daten werden dazu benutzt, die richtigen Symbole für Dokumente anzuzeigen und Buch darüber zu führen, welches Programm gestartet werden soll, wenn Sie ein Dokument doppelklicken. Unter normalen Umständen aktualisiert macOS diese Datenbank ununterbrochen im Hintergrund. In seltenen Fällen kann die Datenbank aber ungültige Informationen enthalten. Typische Symptome sind:

- Wenn Sie den Punkt **Öffnen mit ...** im Kontextmenü des Finders anklicken oder den Abschnitt **Öffnen mit** im Fenster **Informationen** des Finders verwenden, werden ungültige oder doppelte Einträge angezeigt.
- Dokumente werden mit falschen Symbolen dargestellt,
- die Funktion „Markierungen“ (das Hinzufügen von Notizen oder ähnlichen Änderungen in Dokumenten, die Sie von Anderen erhalten haben) arbeitet nicht wie erwartet,

- der Teilen-Knopf oder das Teilen-Menü, das in einigen Programmen angezeigt wird, funktioniert nicht oder bietet nicht alle Dienste an, die normalerweise zum Teilen von Inhalten zur Verfügung stehen.

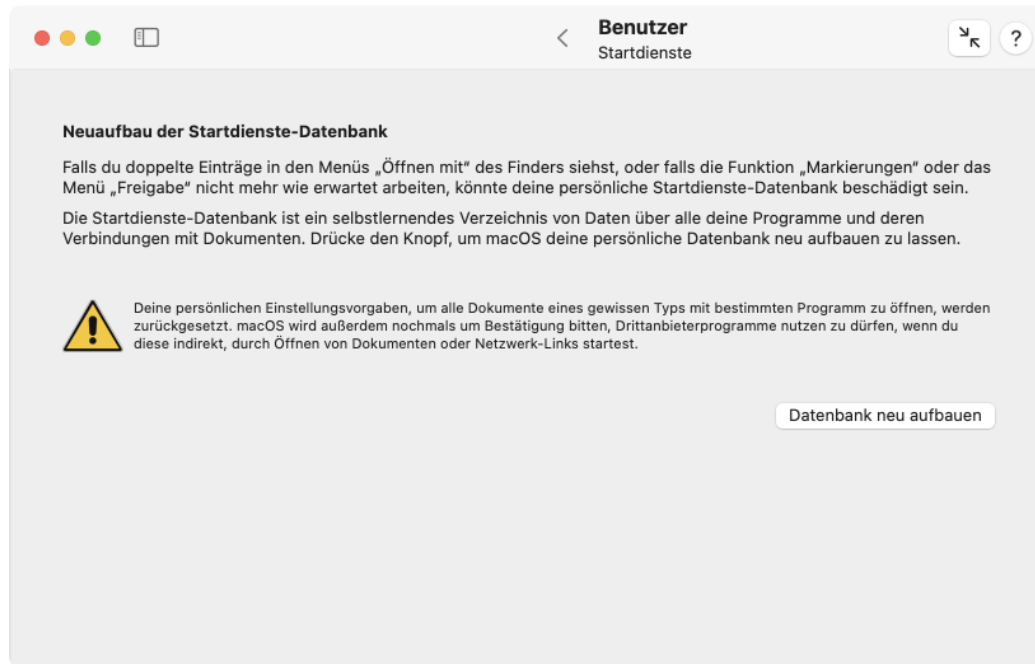


Abbildung 5.3: Startdienste

In diesem Fall können Sie macOS dazu zwingen, die Datenbank für den aktuellen Benutzer neu aufzubauen. Führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Startdienste** auf der Einstellungskarte **Benutzer**.
2. Drücken Sie den Knopf **Datenbank neu aufbauen**.

Hierbei wird auch die Sicherheitsfunktion zurückgesetzt, die verhindert, dass Dokumente mit unbekannten (möglicherweise gefährlichen) Programmen geöffnet werden. Falls Sie ein Dokument öffnen, das mit einem Programm verbunden ist, das noch nie zuvor verwendet wurde, wird macOS wieder um Genehmigung fragen, das Programm starten zu dürfen.

Falls Programme außerhalb eines **Programme**-Ordners abgelegt wurden (was im Allgemeinen nicht zu empfehlen ist), kann macOS möglicherweise vergessen, dass es diese Programme gibt, so dass sie aus den Menüs **Dienste** und **Öffnen mit** verschwinden. Sie müssen den Finder verwenden, um den Ordner zu öffnen, der die Programme enthält, damit das System sich dieser Programme wieder bewusst wird.

Nach dem Wiederaufbau der Datenbank fragt TinkerTool System, ob es den Finder neu starten soll. Sie können somit sofort überprüfen, ob die Reparatur der Datenbank einen positiven Effekt auf die Funktion des Finders hat.

5.1.4 Wörterbücher

macOS enthält eine systemweite Rechtschreibprüfung, die alle Sprachen unterstützt, die als Hauptsprachen im Vermarktungsgebiet des Systems angesehen werden. Die Rechtschreibprüfung kann über den Menüpunkt **Bearbeiten > Rechtschreibung und Grammatik** in allen Programmen genutzt werden, die von diesem Dienst Gebrauch machen. Wenn die Rechtschreibprüfung den Text eines Dokuments überprüft, kann der Benutzer unbekannte, aber richtig geschriebene Wörter in sein persönliches Rechtschreibwörterbuch aufnehmen. Pro Sprache kann jeweils ein Wörterbuch vorliegen und alle hinzugefügten Wörter werden von allen Programmen gemeinsam benutzt, die die Rechtschreibprüfung von macOS verwenden.

Einige Programme werden mit eigener Rechtschreibprüfung geliefert. Sie nehmen an dem hier beschriebenen Mechanismus nicht teil.

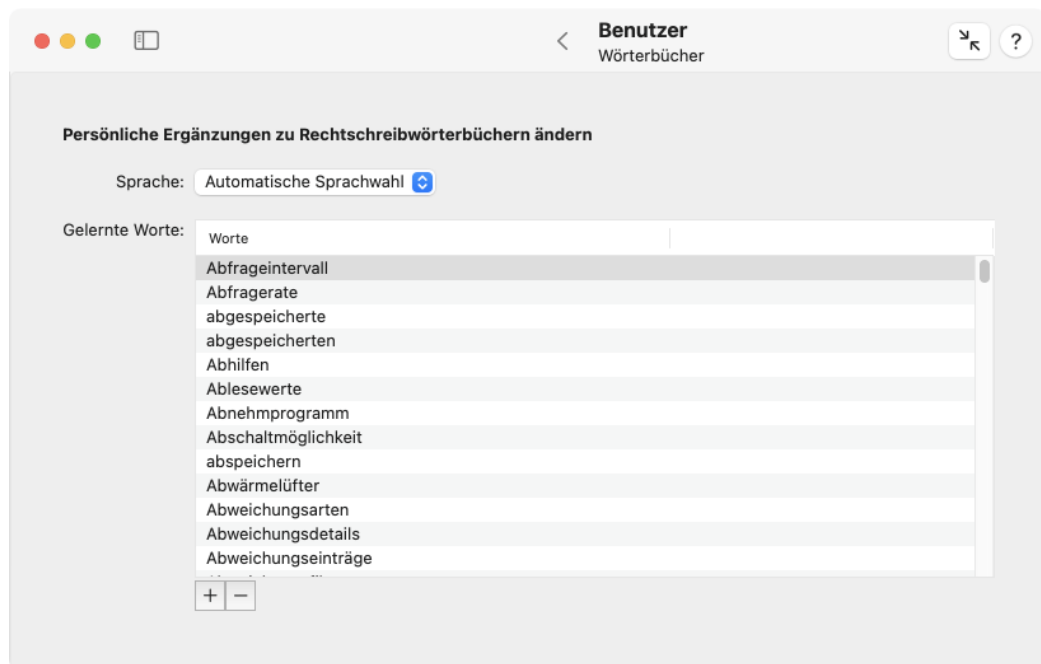


Abbildung 5.4: Rechtschreibwörterbücher

TinkerTool System kann Ihnen den Zugriff auf Ihr persönliches Verzeichnis von Worten geben, die Sie der Rechtschreibprüfung des Systems hinzugefügt haben. Wenn nötig, können Worte geändert, hinzugefügt oder entfernt werden. Führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Wörterbücher** auf der Einstellungskarte **Benutzer**.
2. Verwenden Sie das Aufklappmenü **Sprache**, um das Wörterbuch zu wählen, mit dem Sie arbeiten möchten.
3. Ändern Sie ein Wort in der Tabelle **Gelernte Worte**, indem Sie es doppelklicken, oder drücken Sie den Knopf [+], um ein neues Wort hinzuzufügen, oder wählen Sie ein oder mehrere Worte und drücken Sie den Knopf [-], um diese zu löschen.

Zusätzlich zu den Wörterbüchern für die Sprachen, die Sie normalerweise verwenden, stellt macOS ein weiteres Wörterbuch bereit, das von TinkerTool System unter der Bezeichnung **Automatische Sprachwahl** aufgeführt wird. Hierbei handelt es sich um ein mehrsprachiges Wörterbuch, auf das zugegriffen wird, wenn die Rechtschreibprüfung nicht auf eine feste Sprache eingestellt wird.

Aktuelle Versionen von macOS haben möglicherweise technische Probleme, alle offenen Programme darüber zu informieren, dass Sie Änderungen an ihren persönlichen Rechtschreibwörterbüchern vorgenommen haben. Um sicherzustellen, dass alle Programme von den Änderungen erfahren, die an Ihrer Rechtschreibwortliste erfolgt sind, melden Sie sich ab und wieder an. Sie sollten es vermeiden, die Wortliste gleichzeitig von mehreren Programmen aus zu ändern. Einige oder alle Änderungen könnten ignoriert werden.

5.1.5 Reparatur

Launchpad zurücksetzen

Das **Launchpad**, das dazu konzipiert ist, den Programmstarter von Apples Mobilgeräten nachzuahmen, hat keine für den Benutzer zugänglichen Einstellungen. Es erkennt selbstständig und kontinuierlich alle auf dem Mac vorhandenen Programme mit grafischer Benutzerschnittstelle und richtet entsprechende Startsymbole ein. Der Benutzer kann nur die Zuordnung zu Gruppen und die Verteilung auf verschiedene Bildschirmseiten steuern. In der Praxis können Probleme mit der vollautomatischen Einrichtung auftreten, z.B. wenn falsche oder doppelte Symbole gezeigt werden oder Programme fehlen. Die interne Datenbank, die von Launchpad geführt wird, könnte in diesem Fall beschädigt sein. Falls dieses Problem auftritt, kann Launchpad für den aktuellen Benutzer-Account auf Werkeinstellung zurückgestellt werden. Beachten Sie, dass hierbei eine eventuell von Ihnen angepasste Anordnung von Symbolen und deren Verteilung auf Gruppen und Bildschirmseiten verlorengeht.

Falls Sie Launchpad für Ihren Benutzer-Account zurücksetzen möchten, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Reparatur** auf der Einstellungskarte **Benutzer**.
2. Betätigen Sie den Knopf **Jetzt zurücksetzen** im Abschnitt **Launchpad zurücksetzen**.

TinkerTool System führt Sie durch den Rückstellvorgang.

„Help Viewer“ reparieren

Einige Versionen von macOS haben interne Defekte, die bewirken können, dass das in macOS eingebaute Programm **Help Viewer** zum Betrachten von Hilfeseiten ausfällt. Help Viewer verhält sich wie ein unsichtbares Programm und wird jedesmal dann verwendet, wenn Sie das elektronische Handbuch irgendeines Programms über sein Menü **Hilfe** öffnen. Danach erscheint ein schwebendes Fenster, das so tut, als wäre es Teil des laufenden Programms. In Wirklichkeit wird das Fenster vom Programm Help Viewer dargestellt, obwohl es nicht mit einem Dock-Symbol oder eigener Menüleiste in Erscheinung tritt.

Falls Sie Probleme mit dem Hilfefenster haben, egal ob Sie Programme von Apple oder anderen Anbietern verwenden, wird dies üblicherweise durch Defekte des Programms Help Viewer ausgelöst. Typische Symptome sind:

- Es erscheint überhaupt kein Hilfefenster.

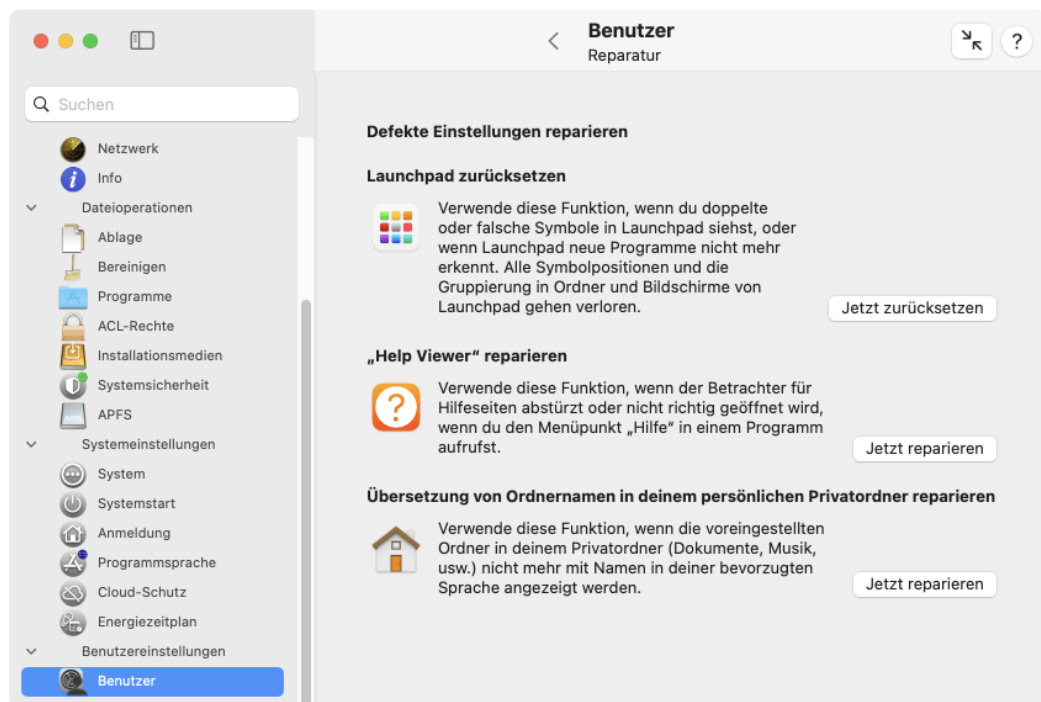


Abbildung 5.5: Reparaturfunktionen

- Eine sehr lange Zeit vergeht, bis das Hilfefenster erscheint.
- Das Hilfefenster wird kurz sichtbar, aber dann stürzt das Programm Help Viewer ab.
- Help Viewer reagiert nicht mehr auf Suchanfragen.

TinkerTool System kann das Programm Help Viewer vorübergehend reparieren, so dass es einige Zeit läuft. Führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Reparatur** auf der Einstellungskarte **Benutzer**.
2. Betätigen Sie den Knopf **Jetzt reparieren** im Abschnitt **„Help Viewer“ reparieren**.

Übersetzung von Ordernamen in Ihrem persönlichen Privatordner reparieren

Falls Ihre persönlichen Spracheinstellungen auf eine andere Sprache als Englisch eingestellt sind, verwendet der Finder übersetzte Namen für die meisten Systemordner und die vorgefertigten Ordner in Ihrem Privatordner. Beispielsweise wird der Ordner **Desktop** als **Bureau** angezeigt, falls Französisch Ihre bevorzugte Sprache ist. Auf Deutsch heißt der Ordner **Schreibtisch**.

Wenn Sie einen der vorgefertigten Ordner entfernt und dann wieder neu angelegt haben, oder falls Sie einen Benutzer-Account aktualisiert haben, der ursprünglich unter Kontrolle von Mac OS X 10.1 Puma angelegt wurde, funktioniert diese automatische Übersetzung nicht richtig. Um dies zu reparieren, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Unterpunkt **Reparatur** auf der Einstellungskarte **Benutzer**.
2. Betätigen Sie den Knopf **Jetzt reparieren** im Abschnitt **Übersetzung von Ordernamen in Ihrem persönlichen Privatordner reparieren**.

Dies betrifft nur Ordner in Ihrem eigenen Privatordner, keine Systemordner oder Ordner anderer Benutzer-Accounts.

5.1.6 Indexdatenbank von Apple Mail löschen

In manchen Fällen passiert es, dass Suchfunktionen innerhalb des Mail-Programms von macOS nicht mehr richtig funktionieren, bzw. nicht mehr das vollständige Suchergebnis liefern. Bestimmte Nachrichten werden nicht mehr gefunden. Wenn dieser Fall eintritt, gilt dies meist auch für die Suche nach E-Mails über die Spotlight-Funktion außerhalb des Programms.

Fast immer ist eine Beschädigung der Indexdatenbank des Mail-Programms Auslöser für solche Probleme. Ein Löschen der Daten und ein Neuaufbau des Index kann ein solches Problem beheben. TinkerTool System stellt eine solche Löschfunktion zur Verfügung. Mail sorgt beim nächsten Start von selbst für einen Neuaufbau der Indexdatenbank. Hierbei erscheint eine Nachricht, dass alle E-Mails neu importiert werden müssen. Nach Bestätigung werden alle weiteren Schritte vollautomatisch durchgeführt.

Bitte beachten Sie, dass dieser Importvorgang mehrere Stunden Zeit benötigen kann, je nach dem wie viele Postfächer und Nachrichten Sie mit dem Mail-Programm verwalten. Während des Imports können Sie nicht mit dem Mail-Programm arbeiten. Sie können jedoch mit einem zweiten Gerät (z.B. einem iPhone) auch in dieser Zeit immer noch auf den Mail-Server mit den Nachrichten zugreifen, falls es sich um einen IMAP-Server handelt.

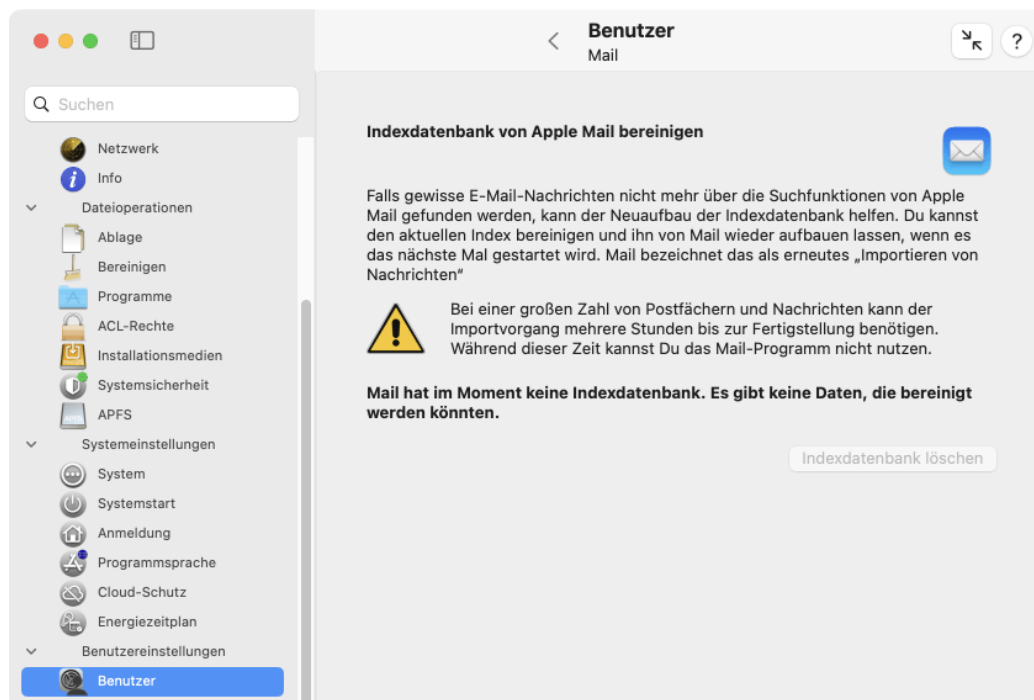


Abbildung 5.6: Indexdatenbank von Apple Mail bereinigen

TinkerTool System zeigt in einer fett markierten Statusmeldung an, ob eine Indexdatenbank für Ihren Benutzer-Account vorhanden und wie groß diese ist. Liegt die Indexdatenbank vor, können Sie das Mail-Programm beenden und die Daten löschen lassen. Klicken Sie hierzu auf den Knopf **Indexdatenbank löschen**. Der Neuaufbau des Index wird als Importieren von Daten automatisch durchgeführt, wenn Sie das nächste Mal Mail starten.

5.1.7 Info

Der Unterpunkt **Info** kann dazu genutzt werden, fortgeschrittene Daten über den aktuellen Benutzer-Account anzuzeigen, die im Programm Systemeinstellungen nicht sichtbar werden. Beachten Sie, dass diese Anzeige nur zu Informationszwecken dient. Sie können sie nicht verwenden, um Daten zu ändern. Es werden die folgenden Daten aufgeführt:

- Der Kurzname des Benutzers.
- Die Identifikationsnummer des Benutzers. Diese Nummer wird in allen Teilen des Kernbetriebssystems verwendet, um diesen Account eindeutig zu identifizieren.
- Die Mitgliedschaft in der Primärgruppe. Die Gruppe wird mit ihrem vollen Namen und der Gruppenidentifikationsnummer angezeigt.
- Ein Foto, das mit diesem Account verbunden ist. In professionellen Umgebungen wird es sich üblicherweise um ein Passbild des Benutzers handeln. Es wird auf dem Anmeldeschirm und Programmen wie Kontakte, Mail, Nachrichten und anderen verwendet, um grafisch auf diesen Benutzer Bezug zu nehmen.
- Der UNIX-Pfad des Privatordners. Dies ist der Ordner, in dem alle persönlichen Daten und Dokumente des Benutzers gespeichert werden. Sie können den Ordner vom Finder öffnen lassen, indem Sie auf das Symbol mit dem Vergrößerungsglas drücken.
- Die anfängliche Shell, die als Standard für diesen Account eingerichtet ist. Die Shell ist das Programm, das die Benutzersitzung steuert, wenn der Benutzer eine Sitzung im Textmodus beginnt, zum Beispiel durch Öffnen eines Terminal-Fensters.
- Die Information, ob der Benutzer Verwaltungsberechtigung hat oder nicht.
- Die vollständige Liste von Benutzergruppen, in denen der Benutzer direktes Mitglied ist. Gruppenidentifikationsnummer, der Kurzname der Gruppe, der volle Gruppenname und der einzigartige Gruppenidentifikationscode werden für jede Mitgliedschaft aufgeführt. Indirekte Mitgliedschaften (eine Gruppe ist dazu eingerichtet, verschachtelt Mitglied einer anderen Gruppe zu sein) werden nicht aufgelistet.

Ist der Benutzer Mitglied einer Benutzergruppe, die nicht mehr vorhanden ist, wiederholen die Spalteneinträge für Name und Voller Name die numerische ID in der Form <GID: ID>.

5.2 Arbeiten mit Einstellungskarten aus TinkerTool

Nachdem Sie ein Exemplar von TinkerTool in TinkerTool System integriert (Abschnitt 1.6 auf Seite 22) haben, können Sie mit den Einstellungskarten von TinkerTool direkt aus dem System-Programm heraus arbeiten, so dass Sie nicht mehr beide Programme getrennt voneinander starten müssen, um Zugriff auf deren vollen Funktionsumfang zu haben.

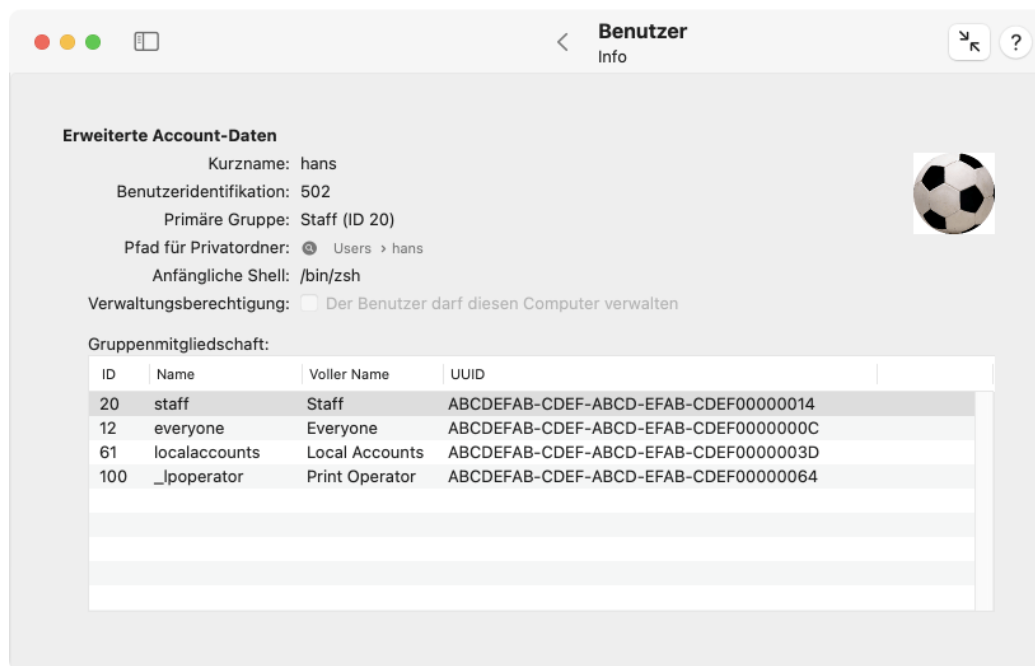


Abbildung 5.7: Info

Einstellungskarten von TinkerTool gewähren Ihnen Zugriff auf fortgeschrittene Einstellungen, die in macOS eingebaut, aber im normalen Programm Systemeinstellungen oder in den Einstellungsfenstern der jeweiligen Programme (wie Safari) nicht sichtbar werden. Um einen dieser fortgeschrittenen Einstellungswerte zu ändern, führen Sie die folgenden Schritte durch:

1. Wählen Sie eine der zusätzlichen Einstellungskarten in der Rubrik **Benutzereinstellungen** in der Seitenleiste von TinkerTool System.
2. Ändern Sie die Einstellungen mit den Bedienelementen auf der Karte, die geöffnet wurde.
3. Lesen Sie die Zeile in der linken unteren Ecke der Karte, um festzustellen, wann die Änderungen wirksam werden.

Kapitel 6

Arbeiten in der macOS-Wiederherstellung

6.1 Allgemeine Informationen

Um mit dem Programm **TinkerTool System für macOS-Wiederherstellung** arbeiten zu können, müssen Sie zunächst die Wiederherstellungsversion von macOS starten, die zu Ihrem jeweiligen Betriebssystem gehört und danach über einen Befehl im Programm Terminal das Notfallwerkzeug aufrufen. Ausführliche Informationen über diese beiden Schritte finden Sie im Kapitel Die Einstellungskarte Notfallwerkzeug (Abschnitt 2.8 auf Seite 108).

Wenn Sie auf dieser Einstellungskarte den Fragezeichen-Knopf drücken (Kurzhilfe) werden Sie unter anderem einen Internet-Link finden, auf dem Apple die aktuellsten Informationen zur Nutzung der macOS-Wiederherstellung zusammengefasst hat.

Wenn sich TinkerTool System auf dem gleichen Volume befindet, wie Ihr Betriebssystem, können Sie das Notfallwerkzeug grundsätzlich nutzen. Es sind keine besondere Installation oder andere Vorkehrungen erforderlich.

6.1.1 Das Hauptmenü des Programms

Nach dem Start über das Programm Terminal erscheint das Hauptfenster von **TinkerTool System für macOS-Wiederherstellung**. Es enthält drei Teile:

- die Anzeige der aktuellen Weltzeit,
- ein Menü, in dem durch Anklicken verschiedener Knöpfe die einzelnen Funktionen aufgerufen werden können,
- eine Statuszeile, die bestätigt, auf welchem Betriebssystem-Volume das Programm gerade arbeitet.

Falls mehrere Betriebssysteme auf Ihrem Mac vorhanden sind, sollten Sie vor dem Aufruf von Wartungsfunktionen prüfen, ob in der Statuszeile unten das richtige Betriebssystem-Volume angezeigt wird. Beachten Sie die Abhängigkeiten zwischen Speicherort und Betriebssystem, die im Kapitel Die Einstellungskarte Notfallwerkzeug (Abschnitt 2.8 auf Seite 108) beschrieben sind.

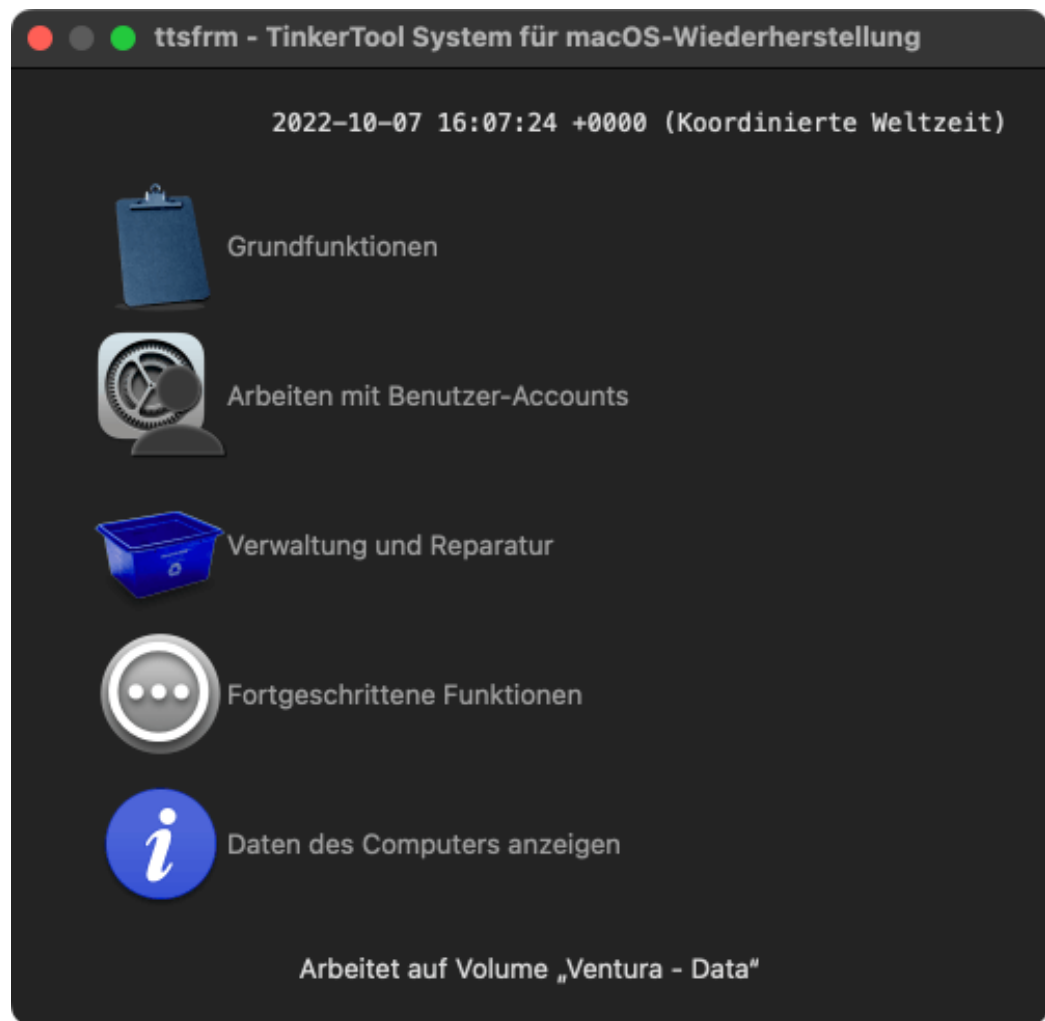


Abbildung 6.1: Das Hauptmenü von TinkerTool System für macOS-Wiederherstellung (ttsfrm)

Um eine Funktion auszuwählen, klicken Sie einfach auf das entsprechende Symbol oder dessen Bezeichnung. Die Funktionen der einzelnen Menüpunkte sind in den folgenden Abschnitten beschrieben:

- Grundfunktionen (Abschnitt 6.2 auf Seite 299)
- Arbeiten mit Benutzer-Accounts (Abschnitt 6.3 auf Seite 300)
- Verwaltung und Reparatur (Abschnitt 6.4 auf Seite 303)
- Fortgeschrittene Funktionen (Abschnitt 6.5 auf Seite 308)
- Abrufen von Informationen (Abschnitt 6.6 auf Seite 309)

6.1.2 Beenden des Programms

Um das Programm zu beenden, wählen Sie den Menüpunkt **ttsfrm > ttsfrm beenden**. Sie können auch die Tastenkombination **⌘ + Q** betätigen, genau wie im normalen Betrieb von macOS. Der Computer lässt sich über das Apfel-Menü neu starten oder ausschalten.

6.2 macOS-Wiederherstellung: Grundfunktionen

Das Dialogfenster **Grundfunktionen** öffnet sich nach Anklicken des entsprechenden Punktes im Hauptmenü. Es kann mit dem Knopf **Schließen** wieder geschlossen werden.

6.2.1 Reparieren des Temporärordners des Systems

Diese Funktion ist für Fälle gedacht, in denen der Hauptordner des Betriebssystems für vorübergehend abgespeicherte Objekte gelöscht wurde. Falls dieser Ordner fehlt, können viele Teile des Systems nicht mehr länger arbeiten. Einige Anwendungen zeigen möglicherweise eine Fehlermeldung an, dass der Ordner mit dem Namen **/tmp** nicht gefunden wurde. In diesem Fall sollten Sie den Ordner neu anlegen, bzw. reparieren lassen. Betätigen Sie hierzu einfach den Knopf **Reparieren**. Der Knopf lässt sich nur dann drücken, wenn eine Reparatur nötig und möglich ist.

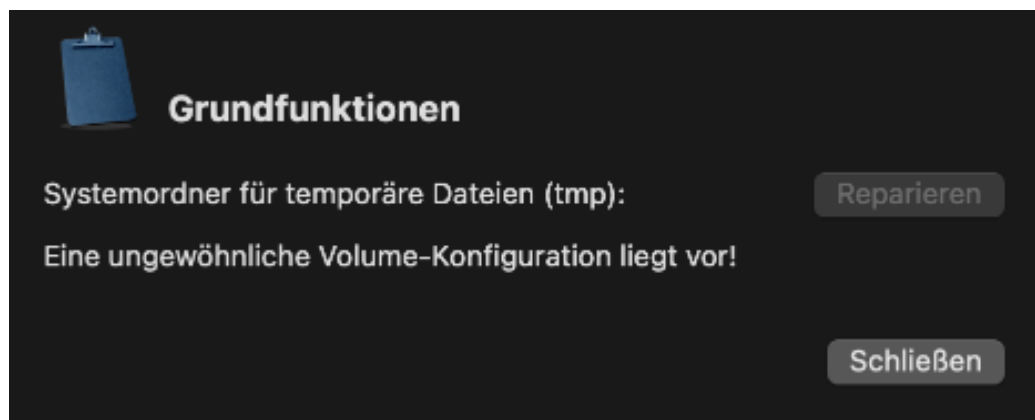


Abbildung 6.2: Grundfunktionen

6.3 macOS-Wiederherstellung: Arbeiten mit Benutzer-Accounts

6.3.1 Auswahl des zu bearbeitenden Benutzer-Accounts

Alle Funktionen, die im Hauptmenü unter dem Stichwort **Arbeiten mit Benutzer-Accounts** zu finden sind, erfordern es als ersten Schritt, den jeweiligen Account auszuwählen. Nach dem Anklicken des Menüpunktes erscheint ein Dialogfenster mit dem Menüknopf **Benutzer**. Wählen Sie dort einen Benutzer anhand seines kurzen Account-Namens aus.

Der Menüknopf **Benutzer** enthält nur diejenigen Benutzer, die ihren Privatordner am üblichen Ablageort haben, d.h. im Ordner **Benutzer:innen (/Users)** des Betriebssystems. Andere Benutzer, bzw. deren Daten sind in der macOS-Wiederherstellung im Allgemeinen nicht zugreifbar.

Das Dialogfenster kann mit dem Knopf **Schließen** wieder geschlossen werden.

6.3.2 Deaktivieren von beschädigten Einstellungsdateien

Sie können **TinkerTool System für macOS-Wiederherstellung** anweisen, alle Einstellungsdateien („Präferenzen“) eines Benutzers zu durchsuchen und alle Dateien, die von außen als beschädigt erkannt werden, automatisch zu deaktivieren. Hierbei wird nichts gelöscht. Die beschädigten Dateien werden durch Umbenennen inaktiv geschaltet, so dass sie für macOS und die Programme, die die betroffenen Einstellungen verwenden, nicht mehr wirksam werden können. Dies entspricht einer stark vereinfachten Version der Funktion **Benutzer (Abschnitt 5 auf Seite 283) > Einstellungen > Dateien prüfen** aus TinkerTool System.

1. Klicken Sie im Hauptmenü auf **Arbeiten mit Benutzer-Accounts**.
2. Wählen Sie einen Benutzer-Account über den Menüknopf **Benutzer** aus.
3. Wählen Sie im Menüknopf **Funktion** den Punkt **Fehlerhafte Einstellungsdateien deaktivieren**.
4. Klicken Sie auf **Starten**.
5. Warten Sie bis das Endergebnis der Prüfung, bzw. Reparatur auf dem Bildschirm angezeigt wird.

6.3.3 Deaktivieren aller Caches eines Benutzers

Wie im Kapitel Caches (Abschnitt 2.2 auf Seite 29) beschrieben, kann in Einzelfällen ein beschädigter Cache-Inhalt zu Fehlern bei der Ausführung von Programmen führen. **TinkerTool System für macOS-Wiederherstellung** kann die persönlichen Standard-Caches eines Benutzer-Accounts auf Wunsch komplett deaktivieren. Hierbei wird nichts gelöscht, so dass der wertvolle Cache-Inhalt im Zweifelsfall wieder gerettet werden kann, um eine hohe Geschwindigkeit des Systems zu gewährleisten. Führen Sie die folgenden Schritte durch, um die persönlichen Standard-Caches eines Benutzers vorübergehend oder dauerhaft zu deaktivieren:

1. Klicken Sie im Hauptmenü auf **Arbeiten mit Benutzer-Accounts**.
2. Wählen Sie einen Benutzer-Account über den Menüknopf **Benutzer** aus.

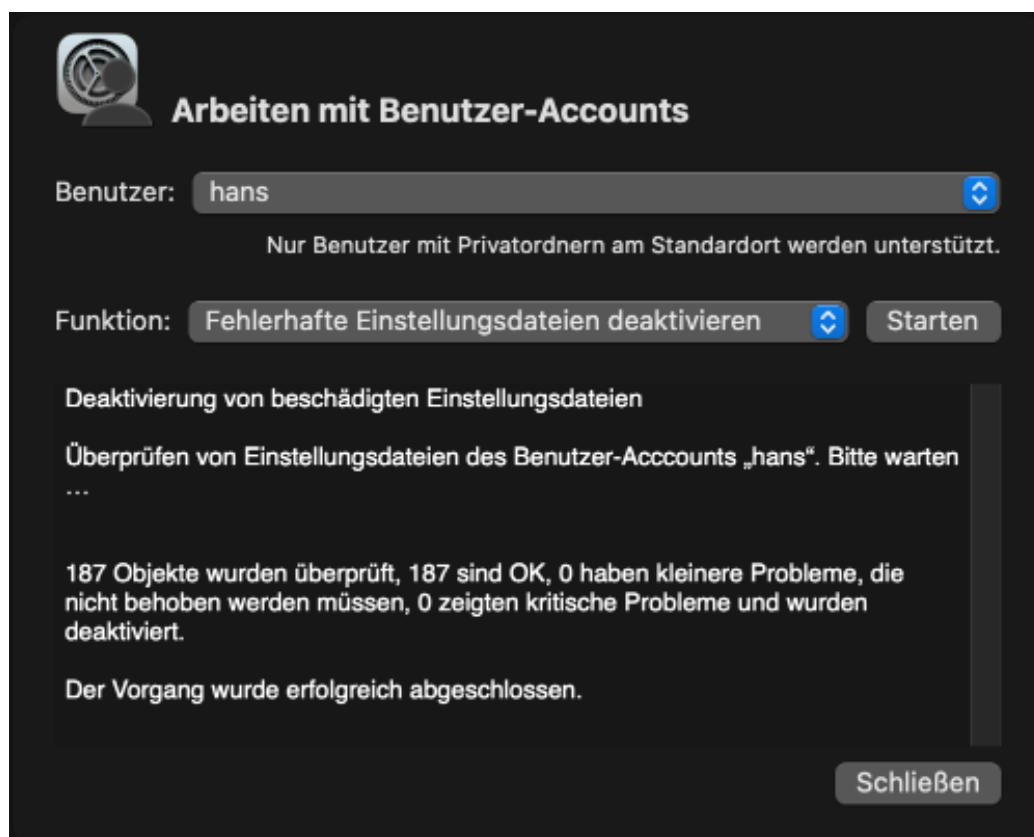


Abbildung 6.3: Arbeiten mit Benutzer-Accounts

3. Wählen Sie im Menüknopf **Funktion** den Punkt **Alle Caches eines Benutzers deaktivieren**.
4. Klicken Sie auf **Starten**.
5. Warten Sie bis das Endergebnis der Deaktivierung auf dem Bildschirm angezeigt wird.

6.3.4 Reaktivieren aller Caches eines Benutzers

Nach dem Entfernen von Cache-Inhalten arbeiten macOS und viele Programme langsamer, da die Caches wieder aufgebaut werden müssen. Sollte das Deaktivieren von Caches (aus dem vorigen Abschnitt) nicht zum gewünschten Erfolg geführt haben, können Sie die betroffenen Daten per Knopfdruck wieder komplett herstellen, so dass kein Geschwindigkeitsverlust auftritt.

1. Klicken Sie im Hauptmenü auf **Arbeiten mit Benutzer-Accounts**.
2. Wählen Sie einen Benutzer-Account über den Menüknopf **Benutzer** aus.
3. Wählen Sie im Menüknopf **Funktion** den Punkt **Alle Caches eines Benutzers reaktivieren**.
4. Klicken Sie auf **Starten**.
5. Warten Sie bis das Endergebnis der Reaktivierung auf dem Bildschirm angezeigt wird.

6.3.5 Deaktivieren aller Einstellungen eines Benutzers

Einstellungen eines Benutzers können in einer Weise beschädigt sein, so dass die Form der Daten von außen gesehen immer noch korrekt erscheint, jedoch die interne Bedeutung der Daten fehlerhaft ist. In seltenen Fällen kann dies dazu führen, dass Programme fehlerhaft oder gar nicht mehr arbeiten. Sollte sich ein solcher Fehler nicht auf die Einstellungen eines bestimmten Programms isolieren lassen, so ist es als letzte Maßnahme zur Fehlersuche manchmal wünschenswert, sämtliche Einstellungen eines Benutzers vorübergehend zurückzusetzen. Alle Programme, die dieser Benutzer startet, laufen danach mit „frischen“ Werkseinstellungen. Bei der Deaktivierung von Einstellungen werden die Daten nicht wirklich gelöscht, so dass sie sich im Zweifelsfall wiederherstellen lassen.

1. Klicken Sie im Hauptmenü auf **Arbeiten mit Benutzer-Accounts**.
2. Wählen Sie einen Benutzer-Account über den Menüknopf **Benutzer** aus.
3. Wählen Sie im Menüknopf **Funktion** den Punkt **Alle Einstellungen eines Benutzers deaktivieren**.
4. Klicken Sie auf **Starten**.
5. Warten Sie bis das Endergebnis der Deaktivierung auf dem Bildschirm angezeigt wird.

6.3.6 Reaktivieren aller Einstellungen eines Benutzers

Sollte sich herausstellen, dass die Deaktivierung aller Einstellungen (aus dem vorigen Abschnitt) nicht zum gewünschten Erfolg geführt hat, so können die Einstellungen (zum Stand des Deaktivierungsvorgangs) komplett wiederhergestellt werden. Führen Sie hierzu die folgenden Schritte durch:

1. Klicken Sie im Hauptmenü auf **Arbeiten mit Benutzer-Accounts**.
2. Wählen Sie einen Benutzer-Account über den Menüknopf **Benutzer** aus.
3. Wählen Sie im Menüknopf **Funktion** den Punkt **Alle Einstellungen eines Benutzers reaktivieren**.
4. Klicken Sie auf **Starten**.
5. Warten Sie bis das Endergebnis der Reaktivierung auf dem Bildschirm angezeigt wird.

6.4 macOS-Wiederherstellung: Verwaltung und Reparatur

6.4.1 Deaktivieren von beschädigten Systemeinstellungsdateien

Sie können **TinkerTool System für macOS-Wiederherstellung** anweisen, alle systemweiten Einstellungsdateien („Präferenzen“), die unabhängig von Benutzern gelten, zu durchsuchen und alle Dateien, die von außen als beschädigt erkannt werden, automatisch zu deaktivieren. Hierbei wird nichts gelöscht. Die beschädigten Dateien werden durch Umbenennen inaktiv geschaltet, so dass sie für macOS und die Programme, die die betroffenen Einstellungen verwenden, nicht mehr wirksam werden können. Dies entspricht einer stark vereinfachten Version der Funktion **Benutzer (Abschnitt 5 auf Seite 283) > Einstellungen > Dateien prüfen** aus TinkerTool System, beschränkt auf systemweit geltende Einstellungen.

1. Klicken Sie im Hauptmenü auf **Verwaltung und Reparatur**.
2. Wählen Sie im Menüknopf **Funktion** den Punkt **Fehlerhafte Systemeinstellungsdateien deaktivieren**.
3. Klicken Sie auf **Starten**.
4. Warten Sie bis das Endergebnis der Prüfung, bzw. Reparatur auf dem Bildschirm angezeigt wird.

6.4.2 Deaktivieren systembezogener Caches

Dies entspricht der Funktion **Deaktivieren aller Caches eines Benutzers** aus dem Menü **Arbeiten mit Benutzer-Accounts**, jedoch werden hier alle Caches deaktiviert, die systemweit für alle Benutzer aktiv sind. Führen Sie die folgenden Schritte durch, um alle systemweit geltenden Caches vorübergehend außer Kraft zu setzen:

1. Klicken Sie im Hauptmenü auf **Verwaltung und Reparatur**.
2. Wählen Sie im Menüknopf **Funktion** den Punkt **Systembezogene Caches deaktivieren**.
3. Klicken Sie auf **Starten**.

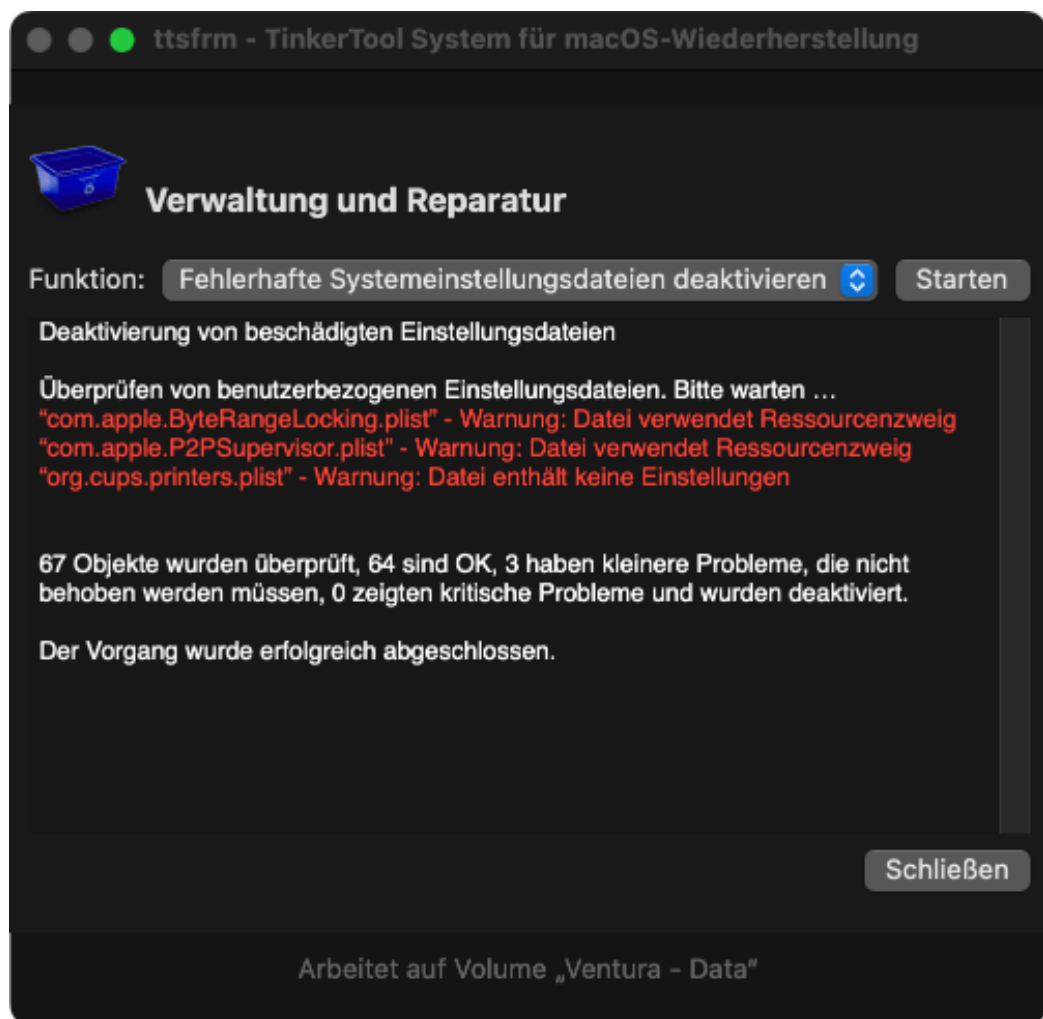


Abbildung 6.4: Verwaltung und Reparatur

4. Warten Sie bis das Endergebnis der Deaktivierung auf dem Bildschirm angezeigt wird.

Detaillierte Hinweise zur Funktion von Caches finden Sie im gleichnamigen Kapitel (Abschnitt 2.2 auf Seite 29).

6.4.3 Reaktivieren systembezogener Caches

Nach Löschen von System-Caches arbeiten macOS und viele Programme langsamer, da die Caches wieder aufgebaut werden müssen. Sollte das Deaktivieren von Caches (aus dem vorigen Abschnitt) nicht zum gewünschten Erfolg geführt haben, können Sie die betroffenen Daten per Knopfdruck wieder komplett herstellen, so dass kein Geschwindigkeitsverlust auftritt.

1. Klicken Sie im Hauptmenü auf **Verwaltung und Reparatur**.
2. Wählen Sie im Menüknopf **Funktion** den Punkt **Systembezogene Caches reaktivieren**.
3. Klicken Sie auf **Starten**.
4. Warten Sie bis das Endergebnis der Reaktivierung auf dem Bildschirm angezeigt wird.

6.4.4 Zurücksetzen von gemanagten Einstellungen

Falls Ihr Computer Teil eines macOS-Netzwerks ist, in dem Management-Funktionen zum Einsatz kommen, sind Situationen denkbar, in denen das Management nicht wie erwartet funktioniert: Eine Beschränkung, die per Management vorgegeben wird, wird auf einem Computer eventuell nicht aktiv, oder umgekehrt bleibt eine Einstellung, die im Management nicht mehr vorgegeben wird, auf einem Computer trotzdem noch gesperrt. Solche Probleme lassen sich lösen, indem alle gemanagten Einstellungen zurückgesetzt werden. Falls das System immer noch mit dem gemanagten Netz verbunden ist, wird der Computer die Einstellungen erneut lernen und mit dem aktuellen Stand erneut aktiv werden lassen. Falls das System nicht mehr mit dem Netz verbunden ist, werden die gemanagten Einstellungen entsperrt und lassen sich danach wieder lokal ändern. Führen Sie die folgenden Schritte durch, um die gemanagten Einstellungen zurückzusetzen:

1. Klicken Sie im Hauptmenü auf **Verwaltung und Reparatur**.
2. Wählen Sie im Menüknopf **Funktion** den Punkt **Verwaltete Einstellungen zurücksetzen**.
3. Klicken Sie auf **Starten**.
4. Warten Sie bis das Endergebnis der Rücksetzung auf dem Bildschirm angezeigt wird.

6.4.5 Anmeldebildschirm zurücksetzen

Technische Probleme mit der Zuverlässigkeit des Anmeldebildschirms können in der Praxis auftreten. Es ist technisch möglich, den Anmeldebildschirm durch fehlerhafte Einstellungen in eine Situation zu versetzen, in der eine Anmeldung an der grafischen Oberfläche unmöglich wird. Das System kann dadurch weitgehend unbrauchbar werden. Sie können das Problem lösen, indem Sie sämtliche Einstellungen des Anmeldeschirms auf die Werkeinstellung zurücksetzen. Führen Sie hierzu die folgenden Schritte durch:

1. Klicken Sie im Hauptmenü auf **Verwaltung und Reparatur**.
2. Wählen Sie im Menüknopf **Funktion** den Punkt **Anmeldebildschirm zurücksetzen**.
3. Klicken Sie auf **Starten**.
4. Warten Sie bis das Endergebnis der Rücksetzung auf dem Bildschirm angezeigt wird.

6.4.6 Entfernen von angepassten Startobjekten

Verschiedene Anwenderprogramme, die systemnahe oder hardwarenahe Leistungen erbringen, installieren oft zusätzliche Dienste im Betriebssystem, die danach bei jedem Systemstart automatisch im Hintergrund aktiviert werden. Wir bezeichnen solche Dienste als *angepasste Startobjekte*. Wird ein solches Programm „unsauber“ entfernt, d.h. ohne den offiziellen Deinstallierer des Herstellers zu verwenden, verbleiben oft veraltete Startobjekte im System, die nicht mehr benötigt werden. Diese Objekte verbrauchen möglicherweise Ressourcen oder können sogar Probleme auslösen. Auch bei Verwendung des macOS-Migrationsassistenten kann es passieren, dass unabsichtlich unpassende Startobjekte von einem alten auf einen neuen Computer übernommen werden.

Mit **TinkerTool System für macOS-Wiederherstellung** können Sie alle gängigen Typen von systemweiten, angepassten Startobjekten anzeigen und bei Bedarf entfernen lassen.

Der Begriff „angepasst“ soll in diesem Fall andeuten, dass es sich um ein Startobjekt handelt, das nicht zum offiziellen Lieferumfang von macOS gehört, sondern das von einem Drittanbieterprogramm installiert wurde. Das Dienstprogramm unterstützt mit Absicht keine Manipulation an eingebauten Startobjekten, die Bestandteil von macOS sind.



Sie sollten diese manuelle Entfernung von Startobjekten nur in Notfällen nutzen, wenn Sie wissen, dass ein bestimmtes Objekt für technische Probleme sorgt und nicht anderweitig (z.B. mit einem Deinstallierer des Herstellers) entfernt werden kann. Aus technischen Gründen kann das selbständige Dienstprogramm keine gegenseitigen Abhängigkeiten zwischen Startobjekten erkennen oder entscheiden, ob ein Startobjekt einen eventuell wichtigen Dienst erbringt.

Führen Sie die folgenden Schritte durch, um angepasste Startobjekte von Hand zu entfernen:

1. Klicken Sie im Hauptmenü auf **Verwaltung und Reparatur**.
2. Wählen Sie im Menüknopf **Funktion** den Punkt **Angepasste Systemstartobjekte entfernen**.
3. Klicken Sie auf **Starten**.
4. Es erscheint nun ein weiteres Dialogfenster, das drei Tabellen mit verschiedenen Typen von Startobjekten enthält.

Der erste Abschnitt enthält Objekte, die in einer Form gespeichert sind, die sowohl von Mac OS X 10.4 Tiger, als auch von neueren Versionen von macOS verwendet werden können. Diese Objekte werden in der Regel im Klartext beschrieben und orientieren sich hierbei an Beschreibungstexten des jeweiligen Herstellers. Der zweite Abschnitt enthält „modernere“ Objekte, die nicht mit Tiger kompatibel sind und bei jedem Start von macOS im

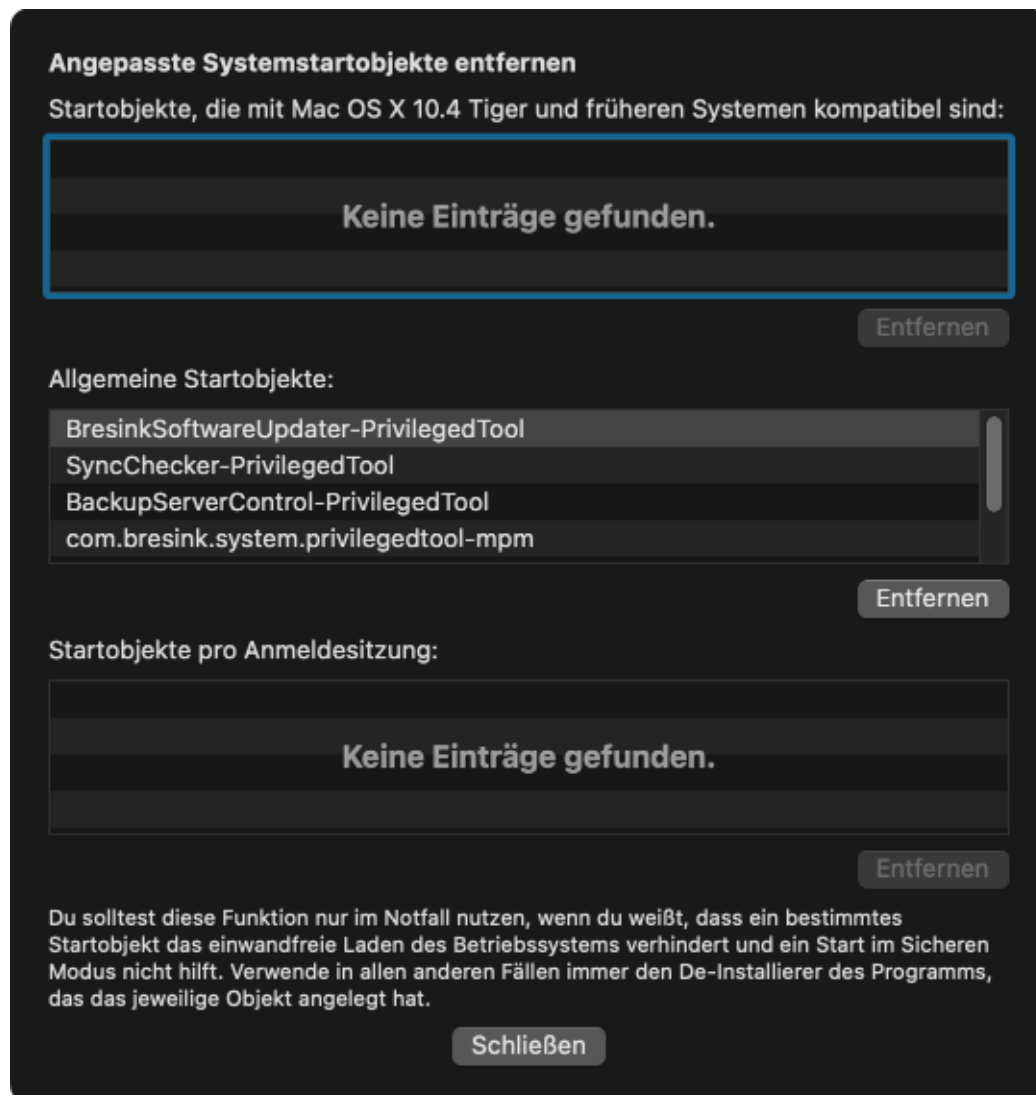


Abbildung 6.5: Angepasste Systemstartobjekte entfernen

Hintergrund aktiv werden. Der dritte Abschnitt listet Objekte auf, die ebenso im Hintergrund laufen, aber nicht beim Systemstart, sondern bei jedem Öffnen einer neuen Anmeldesitzung aktiv werden. Beachten Sie, dass es sich beim dritten Punkt nicht um Anmeldeobjekte von Benutzern handelt, sondern um systemweite Dienste pro Benutzer, die von den einzelnen Benutzern nicht verändert werden können. Im zweiten und dritten Abschnitt werden eindeutige Bezeichnungen für die einzelnen Objekte verwendet, die sich an ein bestimmtes, von Apple vorgegebenes Schema halten. Möglicherweise sind die Tabellen einiger Abschnitte leer, wenn keine entsprechenden Objekte auf Ihrem Computer installiert sind.

Sie können ein oder mehrere Startobjekte auswählen und danach den Knopf **Entfernen** unter der jeweiligen Tabelle drücken. Die Objekte werden sofort entfernt. Das Dialogfenster kann mit dem Knopf **Schließen** geschlossen werden.

6.5 macOS-Wiederherstellung: Fortgeschrittene Funktionen

6.5.1 Abschalten der automatischen Anmeldung

In manchen Fällen kann ein Programm, das sich im Normalbetrieb nicht abschalten lässt (wie Finder oder Dock), ein technisches Problem auf Ihrem Computer auslösen. Dieses Problem wird noch größer, wenn die automatische Anmeldung eines Benutzers eingeschaltet ist, das fehlerhafte Programm also nach jedem Einschaltvorgang von selbst aktiv wird. Um ein solches Problem unter Zuhilfenahme eines zweiten Benutzer-Accounts beheben zu können, lässt sich die automatische Anmeldung eines Benutzers beim Systemstart über **TinkerTool System für macOS-Wiederherstellung** abschalten:

1. Klicken Sie im Hauptmenü auf **Fortgeschrittene Funktionen**.
2. Wählen Sie im Menüknopf **Funktion** den Punkt **Automatische Anmeldung abschalten**.
3. Klicken Sie auf **Starten**.
4. Warten Sie bis das Endergebnis der Abschaltung auf dem Bildschirm angezeigt wird.

Die automatische Anmeldung lässt sich in macOS über **Systemeinstellungen > Benutzer:innen & Gruppen > Automatisch anmelden als ...** bei Bedarf später wieder einschalten.

6.5.2 Erneuten Lauf des Einrichtungsassistenten erzwingen

Es ist möglich, Konfigurationsänderungen am Betriebssystem vorzunehmen, so dass unabsichtlich alle vorhandenen Benutzer-Accounts mit Verwaltungsrechten (Administrator) deaktiviert werden. Dies ist eine sehr kritische Situation, da Sie möglicherweise den Zugriff auf das System verlieren, sich aber auch nicht mehr authentifizieren können, um dieses Problem zu beheben. Die einfachste Lösung, eine solche Situation zu bereinigen, besteht darin, das Betriebssystem dazu zu zwingen, seinen Einrichtungsassistenten noch einmal laufen zu lassen, also das Programm, das üblicherweise gestartet wird, wenn Sie den Computer das erste Mal installiert oder aktualisiert haben. Der macOS-Einrichtungsassistent erlaubt es Ihnen, den primären Administrator-Account wieder anzulegen, ohne dass dabei andere Daten verloren gehen oder geändert werden.

Um das System dazu zu zwingen, den Einrichtungsassistenten beim nächsten Start des Computers erneut laufen zu lassen, führen Sie die folgenden Schritte durch:

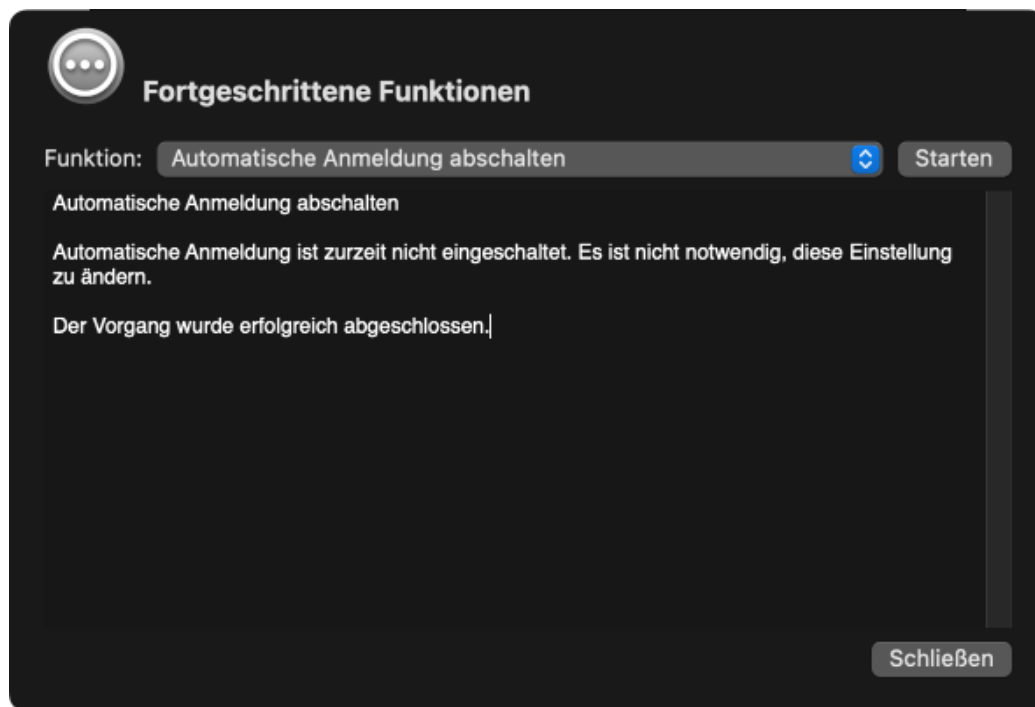


Abbildung 6.6: Fortgeschrittene Funktionen

1. Klicken Sie im Hauptmenü auf **Fortgeschrittene Funktionen**.
2. Wählen Sie im Menükopf **Funktion** den Punkt **Einrichtungsassistent beim nächsten Systemstart laufen lassen**.
3. Klicken Sie auf **Starten**.
4. Warten Sie, bis das Hilfsprogramm bestätigt, dass die notwendigen Schritte abgeschlossen sind.

Danach können Sie `ttsfrm > ttsfrm beenden` aufrufen und im Apple-Menü den Computer neu starten, um das System den Einrichtungsassistenten starten zu lassen.

6.6 macOS-Wiederherstellung: Abrufen von Informationen

Oft ist es nützlich, auch im Wiederherstellungsbetrieb interne technische Daten von Computer, Betriebssystem und Programmversion abrufen zu können. Dies ist über die Menüs **Daten des Computers anzeigen** und **Über TinkerTool System für macOS-Wiederherstellung** möglich.

6.6.1 Hardware- und Systemdaten

Hardware-Daten über Computer, Prozessor und Speicherausstattung sowie Daten über das gerade laufende Recovery-Betriebssystem können wie folgt abgerufen werden:

1. Klicken Sie im Hauptmenü auf **Daten des Computers anzeigen**.

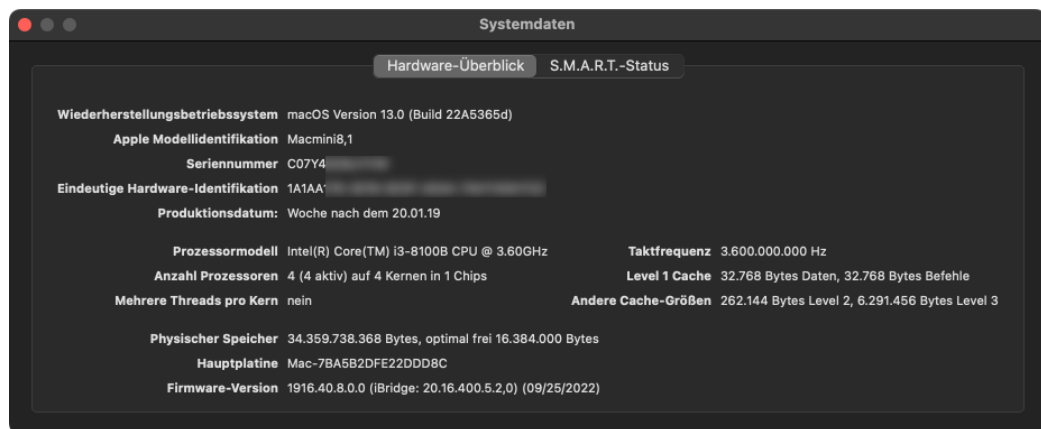


Abbildung 6.7: Hardware-Überblick

2. Stellen Sie sicher, dass der Karteireiter **Hardware-Überblick** ausgewählt ist.

Dies entspricht einer vereinfachten Version der Funktion **Info > Mac** in TinkerTool System.

6.6.2 S.M.A.R.T.-Status von Festplatten

Alle modernen Festplatten verwenden eine Diagnosetechnik nach einem Industriestandard, der den Namen *S.M.A.R.T. (Self Monitoring, Analysis, and Reporting Technology; Technik zur Selbstüberwachung, Analyse und Bericht)* trägt. Die Technik wurde 1992 eingeführt, um auf den Verschleiß von Festplatten frühzeitiger reagieren zu können. Festplatten, die sich an den S.M.A.R.T.-Standard halten, überwachen sich mit einem eigenen Mikroprozessor selbst und erlauben, dass das Betriebssystem Messwerte anfordert, die anzeigen, ob sich Betriebswerte so verändert haben, dass die Platte in näherer Zukunft ausfallen könnte. In diesem Fall kann die Festplatte ausgetauscht werden, bevor Daten verloren gehen. Die Messergebnisse werden vom Diagnoseprozessor der Platte zu einem einfachen Ja/Nein-Wert, dem sogenannten *S.M.A.R.T.-Status* zusammengefasst. Er kann folgende beiden Werte annehmen:

- **Überprüft:** Der Diagnoseprozessor des Laufwerks schätzt aufgrund der beobachteten Messwerte, dass das Laufwerk die nähere Zukunft überleben wird.
- **Ausfall:** Die Messwerte deuten an, dass das Laufwerk seine erwartete Lebenszeit erreicht hat. Es sollte schnellstmöglich ausgetauscht werden, um Datenverlust vorzubeugen.

Beachten Sie, dass der S.M.A.R.T.-Zustand keine Aussage darüber macht, ob das Laufwerk zurzeit in Ordnung ist, oder ob ein Defekt vorliegt. Es handelt sich nicht um ein Testergebnis im engeren Sinn. Der S.M.A.R.T.-Zustand ist nur eine Empfehlung, die einschätzt, wie sich die Festplatte in der näheren Zukunft wahrscheinlich verhalten wird. Die Empfehlung basiert auf den beobachteten Messdaten des Laufwerks und den Erfahrungswerten des jeweiligen Festplattenherstellers.

Gehen Sie wie folgt vor, um den jeweiligen S.M.A.R.T.-Zustand der angeschlossenen Festplatten anzeigen zu lassen:

1. Klicken Sie im Hauptmenü auf **Daten des Computers anzeigen**.

2. Stellen Sie sicher, dass der Karteireiter **S.M.A.R.T.-Status** ausgewählt ist.

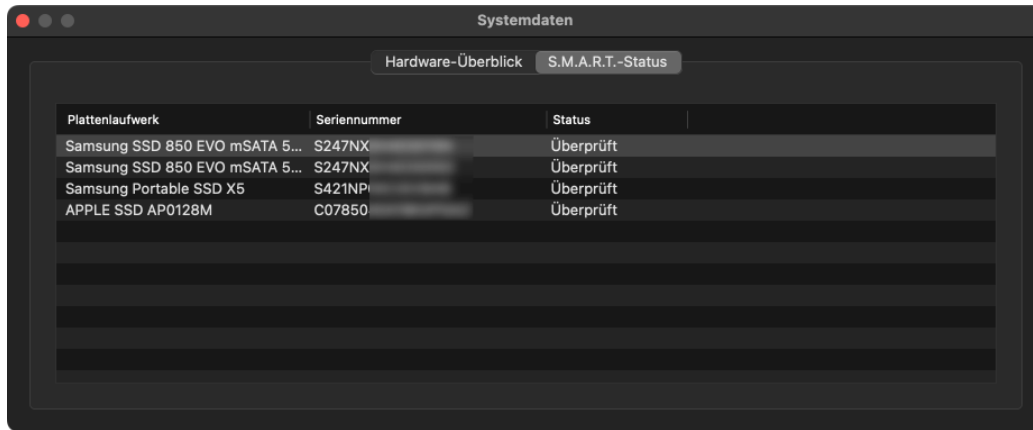


Abbildung 6.8: S.M.A.R.T.-Status

Die meisten externen Festplatten sind über einen Bridge-Chip angeschlossen, der die Daten zwischen dem SATA-Standard und dem Standard der verwendeten Anschlussart (z.B. USB oder FireWire) „übersetzt“. Aufgrund von technischen Einschränkungen sind diese Bridge-Chips nicht in der Lage, S.M.A.R.T.-Daten zu übertragen. Sie können den S.M.A.R.T.-Zustand von Festplatten daher nur von denjenigen Platten abrufen, die direkt über einen SATA-Bus oder per NVMe mit dem Computer verbunden sind. Ein Thunderbolt-Anschluss darf zwischengeschaltet sein und verhält sich neutral. Er behindert den Austausch von Diagnosedaten nicht.

6.6.3 Versionsdaten von TinkerTool System für macOS-Wiederherstellung

Sie können die Versionsnummer des Dienstprogramms und rechtliche Hinweise abrufen, indem Sie den Menüpunkt **ttsfrm > Über TinkerTool System für macOS-Wiederherstellung** auswählen.

Kapitel 7

Allgemeine Hinweise

7.1 Registrierung und Freischalten des Programms

TinkerTool System 8 ist elektronisch vertriebene Software, die nach dem „Erst prüfen, dann kaufen“-Prinzip angeboten wird. Sie können das Programm kostenlos herunterladen und prüfen, ob es sich für Ihre Bedürfnisse eignet. Es kann zwischen zwei unterschiedlichen Betriebsarten gewählt werden, die **Testmodus** und **Demomodus** heißen.

7.1.1 Testmodus

Der Testmodus erlaubt Ihnen, die Software **ohne jede Einschränkung** zu nutzen, egal ob Sie eine Registrierung besitzen oder nicht. Nur die folgende Einschränkung gilt:

Sie können das Programm lediglich sechs (6) Mal pro Computer starten. Nach sechs Startvorgängen endet der Testmodus und kann für kein Exemplar des Programms, das die von Ihnen getestete Versionsnummer trägt, wieder eingeschaltet werden. Nach Ende der Testzeit fällt das Programm in den Demomodus.

Um den Testmodus aktivieren zu können, müssen allerdings bestimmte Voraussetzungen erfüllt sein. Um zu prüfen, ob Ihr Computer zum Test der aktuellen Programmversion berechtigt ist, muss er per Internet eine Erlaubnis von uns anfordern. Diese Erlaubnis wird als *Ticket für den Testmodus* bezeichnet. Das Ausstellen eines solchen Tickets erfolgt in der Regel umgehend, innerhalb weniger Sekunden. Um ein Ticket zu erhalten, müssen die folgenden Bedingungen erfüllt sein:

- Damit das Ticket abgespeichert werden kann, müssen Sie dazu berechtigt sein, als Verwalter des Computers (Administrator) arbeiten zu können. macOS fragt möglicherweise nach Name und Kennwort eines Systemverwalters.
- Der Computer muss zumindest während der Ticketanforderung mit dem Internet verbunden sein. Für den Test und weiteren Betrieb des Programms ist keine Internetverbindung erforderlich.
- Die Verbindung zum Internet darf Datenverkehr für https-Verbindungen (verschlüsselte Web-Kommunikation) nicht blockieren.
- Sie müssen dem Programm gestatten, Daten über
 - Art und Versionsnummer des Programms,

- eine Identifikation Ihres Computers (z.B. eine Seriennummer der Hardware),
- eine Identifikation Ihrer Internet-Verbindung (z.B. die IP-Adresse) an uns zu senden, mit der Erlaubnis, diese Angaben zu speichern.

Das Programm fragt ausdrücklich nach dieser Erlaubnis, bevor Daten gesendet und ein Ticket angefordert wird. Ist ein gültiges Ticket eingegangen, wird es auf Ihrem Computer gespeichert und das Programm dadurch sofort für den Test freigeschaltet.

7.1.2 Demomodus

Ohne gültige Registrierung (und nachdem die kostenlose Testzeit abgelaufen ist), arbeitet das Programm nur im Demobetrieb:

- Ein Fenster mit dem Hinweis **Demonstrationsmodus** erscheint jedes Mal, wenn das Programm gestartet wird.
- Das Fenster **Demonstrationsmodus** erscheint ebenso, wenn Sie versuchen, eine Funktion zu verwenden, die nicht in der folgenden Liste aufgeführt ist. Die Funktion wird blockiert, so dass sie nicht genutzt werden kann.

Die folgenden Funktionen von TinkerTool System können im Demomodus genutzt werden:

- Reparieren des gemeinsamen Benutzerordners
- Beurteilung der RAM-Größe im Verhältnis zur typischen Arbeitslast
- Entfernen alter Notfallwerkzeuge (alleingestelltes Dienstprogramm)
- Anzeige von Systemdaten
- Anzeige von Prozessordaten
- Anzeige von Systemmanagementdaten
- Anzeige der Liste für sichere Downloads (Malware-Schutz)
- Anzeige der Sperrlisten für App Nap, HiDPI und Programmstarts
- Zugriff auf klassische Protokolle und Berichte
- Analyse des Dateiinhalts
- Anzeige von Spotlight-Metadaten für Dateien
- Analyse der Sicherheitseinschätzung für Programme
- Berechnung wirksam werdender Berechtigungen
- Setzen von Benutzereinstellungen um die Sprache bestimmter Programme zu überschreiben
- Übersicht und Analyse der für den aktuellen Benutzer selbststartenden Jobs
- Anzeige verschiedener Definitionen für freien Speicherplatz auf Volumes
- Ändern der Startsprache
- Anzeige erweiterter Benutzer-Account-Daten
- Zurücksetzen aller Systemwerte, die möglicherweise geändert wurden, auf Werkeinstellungen

7.1.3 Uneingeschränkte Nutzung

Wenn Sie die Software dauerhaft einsetzen möchten, müssen Sie die von Ihnen benötigte Anzahl von Nutzungslizenzen bestellen. Für jede Nutzungserlaubnis erhalten Sie eine sogenannte Registrierung, mit der Sie das Programm vom Demonstrationsmodus in den Normalbetrieb freischalten können.

Ein Weitervertrieb oder Vermietung des Programms oder seiner Lizenz an Dritte ist ohne vorherige schriftliche Genehmigung nicht gestattet. Insbesondere dürfen Sie die Registrierung nicht an jemand anders weitergeben. Die genauen vertraglichen Bestimmungen zur Nutzung der Software können angezeigt oder ausgedruckt werden, wenn Sie das heruntergeladene Softwarepaket öffnen.

7.1.4 Bestellung von Registrierungen

Die Bestellung von Registrierungen zu TinkerTool System erfolgt über unseren Vertriebspartner und erfolgt üblicherweise per Internet. Die Lieferung ist weltweit möglich. Die Zahlung kann in über 130 verschiedenen Währungen mit vielen in der jeweiligen Region gängigen Zahlungsmitteln erfolgen.

Um genaue Details über die Abwicklung der Bestellung zu erfahren, verwenden Sie bitte die folgende Internet-Seite von TinkerTool System 8:

<https://www.bresink.com/osx/301031383/order-de.html>

Für erste schriftliche Informationen können Sie alternativ auch den Menüpunkt **Hilfe > Registrierung erwerben ...** im Programm aufrufen.

7.1.5 Verschiedene Arten von Registrierungen

Die Registrierungsdaten, die benötigt werden, um das Programm voll freizuschalten, können in drei unterschiedlichen Formen an Sie ausgeliefert worden sein:

- als **Registrierungsschlüssel**, d.h. eine Folge von Buchstaben und Zahlen, die sich einfach speichern und notieren lässt. Umgangssprachlich bezeichnen viele Anwender dies oft als „Seriennummer“, obwohl der Begriff nicht wirklich zutrifft.
- als **Registrierungsdatei**, von macOS üblicherweise mit einem Eintrittskartensymbol dargestellt. Die Aktivierung erfolgt hier durch Doppelklick oder Laden der Datei.
- als Paar aus **Registrierungsname** und **Registrierungsschlüssel**: Statt in einer einzelnen Zeichenfolge wird die Registrierung als zweiteiliger Text geliefert. Name und Schlüssel gehören zusammen und müssen beide eingegeben werden.

Was für Sie zutrifft, sollte einfach zu erkennen sein. Die unterschiedlichen Arten der Registrierung ergeben sich durch die lange historische Entwicklung der Software. In vielen Fällen hängt die Art der Auslieferung vom Datum Ihrer Bestellung ab:

- ab 01.12.2024 werden in der Regel einfache Registrierungsschlüssel geliefert,
- vom 01.06.2016 bis 24.10.2024 wurden Registrierungsdateien geliefert,
- vom 01.05.2001 bis 31.05.2016, in besonderen Lizenzsituationen (wie zum Beispiel Presse-Exemplaren), sowie beim Wechsel zwischen den beiden anderen Verfahren im Herbst 2024 werden Paare aus Name und Schlüssel geliefert.

Die notwendige Vorgehensweise zur Freischaltung unterscheidet sich, je nach dem welche Art von Registrierung Sie erhalten haben. Die nachfolgenden Abschnitte beschreiben alle Vorgehensweisen zur Freischaltung im Detail. Nur eine der Vorgehensweisen gilt für Sie.

7.1.6 Freischalten der Software mit einem einfachen Registrierungsschlüssel

Falls der Schlüssel zusammen mit einem lesbaren Registrierungsnamen ausgeliefert wurde, ist dies nicht der richtige Abschnitt für Sie. Schauen Sie in diesem Fall weiter unten bei „Freischalten der Software mit einem Paar aus Name und Schlüssel“.

Das Freischalten der Software über einen einzelnen Schlüsselcode erfordert, dass Ihr Computer mit dem Internet verbunden ist. (Falls Sie keine Internet-Verbindung haben, ist eventuell eine alternative Lösung möglich, allerdings nur in bestimmten Fällen. Nehmen Sie für weitere Informationen Kontakt mit uns auf.) Sie sollten Ihren Registrierungsschlüssel vom Software-Händler erhalten haben, nachdem Ihre Bestellung ordnungsgemäß abgewickelt wurde. Beachten Sie, dass der Schlüsselcode einen Wert darstellt und deshalb an einem sicheren Platz archiviert werden sollte, z.B. als Ausdruck auf Papier oder durch Speichern in einem Passwort-Manager. Falls Sie mehrere Lizenzen für das gleiche Programm bestellt hatten, erhalten Sie für jedes Exemplar einen getrennten Schlüssel.

Führen Sie die folgenden Schritte durch, um das Programm freizuschalten:

1. Starten Sie das Programm. Das Fenster **Demonstrationsbetrieb** erscheint. Drücken Sie auf den Knopf **Freischalten** (Falls das Programm bereits läuft und Sie das Demofenster schon geschlossen haben, können Sie auch den Menüpunkt **TinkerTool System > TinkerTool System freischalten** ... auswählen.) Es erscheint das Fenster **Registrierung und Aktivierung**.
2. Drücken Sie im Fenster auf den Knopf **Registrier.-Schlüssel** bei der Frage, welche Art von Registrierung Sie erhalten haben.
3. Übertragen Sie den Registrierungsschlüssel exakt so, wie Sie ihn erhalten haben, in das Feld **Registrierungsschlüssel**. Sie können die Daten von Hand abtippen. Falls Ihnen die Daten jedoch auf der Bestell-Webseite oder in einer E-Mail auf diesem Computer vorliegen, ist es einfacher, den Inhalt über die Funktion **Bearbeiten > Kopieren** ( + ) und **Bearbeiten > Einsetzen** ( + ) zu übertragen.
4. Das Programm wird per Internet freigeschaltet und Sie sehen schließlich ein Fenster, das Ihre erfolgreiche Registrierung bestätigt. Bei einer Mehrfachbestellung gibt das Fenster außerdem an, den wievielten Schlüssel aus welcher Bestellung Sie verwendet haben.

Falls Ihre Internet-Verbindung nicht richtig arbeitet oder in dem seltenen Fall, dass alle Lizenz-Server technische Probleme haben, erhalten Sie eine diesbezügliche Fehlermeldung. Folgen Sie in diesem Fall den Anweisungen, die in der Meldung enthalten sind.

Die Registrierung wird für alle Benutzer-Accounts des jeweiligen Computers gültig.

7.1.7 Freischalten der Software mit einer Registrierungsdatei

Dieser Abschnitt beschreibt, wie Sie eine *Registrierungsdatei* verwenden, die Sie vom Software-Händler erhalten haben. Falls Sie stattdessen einen lesbaren Schlüssel und

vielleicht noch einen Namen erhalten haben, schauen Sie im vorigen oder im nächsten Abschnitt bei „Freischalten der Software mit einem einfachen Registrierungsschlüssel“, bzw. „Freischalten der Software mit einem Paar aus Name und Schlüssel“.

Das Freischalten der Software über eine Registrierungsdatei erfordert, dass Ihr Computer mit dem Internet verbunden ist. (Falls Sie keine Internet-Verbindung haben, ist eventuell eine alternative Lösung möglich, allerdings nur in bestimmten Fällen. Nehmen Sie für weitere Informationen Kontakt mit uns auf.) Sie sollten Ihre Registrierungsdatei vom Software-Händler erhalten haben, nachdem Ihre Bestellung ordnungsgemäß abgewickelt wurde. Beachten Sie, dass diese Datei einen Wert darstellt und deshalb an einem sicheren Platz archiviert werden sollte, z.B. indem Sie diese auf einen USB-Speicherstick kopieren, der sicher aufbewahrt wird.

Falls Sie mehrere Lizenzen für das gleiche Programm bestellt hatten, wird jede Registrierung durch eine getrennte Datei dargestellt. Der Händler hat diese in eine einzelne „Zip“-Datei gepackt. Sie können diese Zip-Datei durch Doppelklicken im Finder auspacken.

Eine Registrierungsdatei wird durch das Symbol einer „MBS-Schlüsselkarte“ dargestellt und hat einen Namen, der mit der Markierung „mbsreg“ endet. Wir nehmen an, dass Sie das Programm ausprobiert haben, bevor Sie sich dazu entschlossen haben, eine permanente Lizenz zu bestellen, so dass sich sowohl das Programm als auch die Registrierungsdatei jetzt auf Ihrem Computer befinden. Führen Sie die folgenden Schritte durch, um das Programm freizuschalten:

1. Doppelklicken Sie die Registrierungsdatei im Finder.
2. Das Programm wird gestartet, falls es noch nicht läuft, es wird per Internet freigeschaltet und Sie sehen schließlich ein Fenster, das Ihre erfolgreiche Registrierung bestätigt. Das ist alles.

Falls Ihr Betriebssystem von einem technischen Problem betroffen ist, so dass es das Programm aus irgendeinem Grund nicht finden kann, können Sie die Registrierungsdatei auch manuell vom Programm aus laden:

1. Starten Sie das Programm. Das Fenster **Demonstrationsbetrieb** erscheint. Drücken Sie auf den Knopf **Freischalten** (Falls das Programm bereits läuft und Sie das Demofenster schon geschlossen haben, können Sie auch den Menüpunkt **TinkerTool System > TinkerTool System freischalten ...** auswählen.) Es erscheint das Fenster **Registrierung und Aktivierung**.
2. Drücken Sie den Knopf **Aus Datei laden ...** im unteren Bereich des Fensters.
3. Wählen Sie im Navigationsdialog die Registrierungsdatei aus und betätigen Sie den Knopf **Öffnen**, um sie zu laden.
4. Das Programm wird per Internet freigeschaltet und Sie sehen schließlich ein Fenster, das Ihre erfolgreiche Registrierung bestätigt. Dabei wird auch ein Bestätigungscode angegeben. *Hinweis: Dieser Code ist kein Schlüssel, der sich eingeben lässt.*

Falls Ihre Internet-Verbindung nicht richtig arbeitet oder in dem seltenen Fall, dass alle Lizenz-Server technische Probleme haben, erhalten Sie eine diesbezügliche Fehlermeldung. Folgen Sie in diesem Fall den Anweisungen, die in der Meldung enthalten sind.

Die Registrierung wird für alle Benutzer-Accounts des jeweiligen Computers gültig.

7.1.8 Freischalten der Software mit einem Paar aus Name und Schlüssel

Dieser Abschnitt beschreibt, wie Sie eine Lieferung nutzen, die ein Paar aus *Registrierungsname* und *Registrierungsschlüssel* enthält. Falls Sie stattdessen einen *einzelnen Schlüssel* oder eine *Registrierungsdatei* vom Software-Händler erhalten haben, verwenden Sie bitte einen der vorigen beiden Abschnitte.

Bitte beachten Sie, dass das Datenpaar, das Sie erhalten haben, einen Wert darstellt und an einem sicheren Ort archiviert werden sollte, zum Beispiel als Ausdruck auf Papier. Der Code zum Freischalten besteht aus zwei Teilen, dem *Registrierungsnamen* und dem *Registrierungsschlüssel*.

Eingeben des Datenpaares von Hand

Gehen Sie wie folgt vor, um das Programm zur vollständigen Nutzung freizuschalten, wenn Sie Registrierungsname und Registrierungsschlüssel erhalten haben:

1. Starten Sie das Programm. Das Fenster **Demonstrationsbetrieb** erscheint. Drücken Sie auf den Knopf **Freischalten** (Falls das Programm bereits läuft und Sie das Demofenster schon geschlossen haben, können Sie auch den Menüpunkt **TinkerTool System > TinkerTool System freischalten ...** auswählen.) Es erscheint das Fenster **Registrierung und Aktivierung**.
2. Drücken Sie den Knopf **Name und Schlüssel**, wenn Sie nach der Art der Registrierung gefragt werden. Es erscheinen Felder zur Eingabe der Daten.
3. Übertragen Sie den Registrierungsnamen exakt so, wie Sie ihn erhalten haben, in das Feld **Registrierungsname**. Sie können die Daten von Hand abtippen. Falls Ihnen die Registrierungs-Mail jedoch auf diesem Computer vorliegt, ist es einfacher, den Inhalt über die Funktion **Bearbeiten > Kopieren** ( + ) und **Bearbeiten > Einsetzen** ( + ) zu übertragen. Beachten Sie bitte, dass Sie keine zusätzlichen Leerzeichen oder Leerzeilen mitkopieren. Sie müssen außerdem auf exakt übereinstimmende Groß- und Kleinschreibung achten.
4. Übertragen Sie auf die gleiche Weise den Registrierungsschlüssel in das Feld **Registrierungsschlüssel** des Programms.
5. Wählen Sie mit den Knöpfen bei **Aktivieren für**, ob die Freischaltung nur für den aktuellen Benutzer-Account oder für alle Benutzer dieses Computers erfolgen soll.
6. Betätigen Sie die Schaltfläche **Speichern**.

Wurden beide Teile richtig eingegeben, wird im Fenster **Registrierung und Aktivierung** Ihre Registrierungsbescheinigung mit Einzelheiten zu Ihrer Nutzungslizenz angezeigt. Sie können das Fenster danach schließen. Wurde ein Teil des Codes falsch eingegeben, wird eine Fehlermeldung angezeigt. Überprüfen Sie in diesem Fall beide Teile des Codes auf exakte Übereinstimmung mit den Daten, die Ihnen zugesandt wurden.

7.1.9 Aktivieren einer Crossgrade- oder Upgrade-Registrierung

Wir bieten möglicherweise spezielle Lizenzen an, die es Ihnen erlauben, von einem anderen Produkt auf die aktuelle Version von TinkerTool System zu wechseln. In diesem besonderen Fall kann es passieren, dass zwei Registrierungen eingegeben werden müssen, um die Anwendung freizuschalten: eine für das aktuelle Programm und eine für das Programm, das Sie früher verwendet haben. Die Schritte sind genau dieselben, wie in den vorigen Abschnitten beschrieben, Sie müssen diese nur zweifach ausführen. Bitte achten Sie darauf, die beiden Registrierungen nicht miteinander zu verwechseln.

- Falls Sie für das Vorprodukt einen einfachen Registrierungsschlüssel bekommen haben, übertragen Sie ihn in das entsprechende Feld im Upgrade-Abschnitt des Fensters und lassen Sie das dortige Namensfeld leer.
- Falls Sie für das Vorprodukt eine Registrierungsdatei bekommen haben, ziehen Sie die Datei vom Finder auf das Fenster.
- Falls Sie für das Vorprodukt ein Paar aus Name und Schlüssel bekommen haben, übertragen Sie die Daten in die beiden Felder im Upgrade-Abschnitt des Fensters.

Falls sich das Vorprodukt noch auf Ihrem Computer befindet und freigeschaltet ist, werden Sie nicht nach einem Kaufnachweis für das Vorprodukt gefragt.

7.1.10 Freischaltung zurücknehmen

Sie können die Freischaltung jederzeit zurücknehmen. Gehen Sie hierzu wie folgt vor:

1. Wählen Sie den Menüpunkt **TinkerTool System > Registrierung verwalten ...**
2. Betätigen Sie die Schaltfläche **Registrierung entfernen**.

7.1.11 Vorgehen bei Aktualisierungen und Migrationen

Sie müssen sich normalerweise nicht um Ihre Registrierung kümmern, falls Sie Ihr Exemplar des Programms durch eine kostenlose Aktualisierung (Update) ersetzen. Ziehen Sie einfach das Symbol der neuen Version in den gleichen Ordner, in dem Sie die frühere Version gespeichert haben. Der Finder fragt Sie, ob das alte Exemplar ersetzt werden soll. Nachdem die neue Version kopiert wurde, können Sie diese einfach starten und Ihre Registrierung ist immer noch vorhanden.

Wenn Sie auf einen neuen Computer migrieren, könnte die Situation anders sein: Falls das Programm durch eine personalisierte Registrierung freigeschaltet wurde (mit einem Registrierungsnamen), können Sie einfach Apples Migrationsassistent verwenden, um alle Dateien Ihres Systems zu übertragen. Ihre Registrierung bleibt dabei weiterhin erhalten und muss nicht erneut eingegeben werden.

Falls jedoch das Programm über eine *Registrierungsdatei* oder einen *einzelnen Schlüssel* freigeschaltet wurde (kein sichtbarer Registrierungsname), müssen Sie Ihre Registrierung noch einmal aktivieren, wie in der Anleitung in diesem Kapitel beschrieben.

7.1.12 Ein Kombi-Ticket für Upgrade-Lizenzen anlegen

Wie oben erläutert, müssen Sie in manchen Fällen das Programm erneut registrieren, wenn Sie auf einen neuen Computer umziehen. Dies erfordert üblicherweise, dass Sie Ihre

Registrierungsdaten erneut bereitstellen, und im Falle eines Upgrades auch einen zweiten Schlüssel (oder eine Registrierungsdatei oder ein Name-/Schlüsselpaar) für ein früheres Produkt vorweisen müssen, um zu beweisen, dass Sie zur Nutzung des Upgrades berechtigt sind.

Um diese lästigen beiden Schritte zu vermeiden, können Sie die zwei Registrierungen in eine Einzeldatei zusammenfassen. Diese Datei kann dann einfach in einem einzelnen Schritt geladen werden, wann immer es notwendig wird, die Software erneut zu registrieren. Um ein solches *Ein-Schritt-Upgrade-Ticket* anzulegen, führen Sie die folgenden Schritte durch:

1. Stellen Sie sicher, dass das Programm erfolgreich über eine Upgrade-Lizenz freigeschaltet worden ist.
2. Rufen Sie den Menüpunkt **TinkerTool System > Registrierung verwalten ...** auf.
3. Klicken Sie auf den Knopf **Ein-Schritt-Upgrade-Ticket anlegen ...** im Fenster zur Produktregistrierung.
4. Folgen Sie den Anweisungen, um den Ordner auszuwählen, in dem die neue Datei gespeichert werden soll.

Sie sollten die Datei an einem sicheren Ort archivieren. Sie können die Datei später einfach doppelklicken, um Ihre Upgrade-Lizenz auf diesem oder einem anderen Computer zu reaktivieren. Es werden nicht mehr zwei getrennte Registrierungen benötigt.

7.1.13 Arbeiten mit Volumenlizenzen

Wenn Sie Nutzungsberechtigungen für eine Organisation mit einer großen Anzahl von Computern benötigen, kann eine einzelne Volumenlizenz effizienter eingesetzt werden, als wenn Sie getrennte Lizenzen für jedes System einzeln haben. Je nach Produkt bieten wir möglicherweise *Standortlizenzen* an (zur Nutzung auf allen Computern einer Organisation an einem zusammenhängenden geografischen Standort), oder auch *globale* Lizenzen (zur Nutzung auf allen Computern einer Organisation weltweit).

Beachten Sie die folgenden Hinweise, wenn Sie mit einer Volumenlizenz arbeiten, die nach Juni 2016 geliefert wurde:

1. Kunden mit Volumenlizenzen können die neueste Standardversion der Software von der offiziellen Webseite herunterladen.
2. Ein Exemplar des Programms muss mit der Registrierungsdatei der Volumenlizenz registriert werden, wobei das normale Verfahren verwendet wird, das in diesem Kapitel beschrieben ist.
3. Bei diesem Exemplar schaltet der Administrator eine spezielle Funktion des Programms ein, um eine *Datei zur automatischen Registrierungsanforderung für Volumenlizenzen* zu erstellen.
4. Wird das Programm auf einen anderen Computer der Organisation kopiert, muss die Anforderungsdatei ebenso in einem bestimmten Ordner mitkopiert werden.
5. Beim ersten Start dieser zusätzlichen Kopie registriert sie sich automatisch und aktiviert die Lizenz.

Das heißt, statt nur das Programmpaket zu kopieren, muss nur eine einzige zusätzliche Datei auf den Zielcomputer mit übertragen werden. Beachten Sie, dass jeder Computer eine funktionierende Internet-Verbindung benötigt, wenn das Programm das erste Mal gestartet wird.

Anlegen einer Anforderungsdatei für Automatische Volumenlizenzierung

Stellen Sie sicher, dass das Programm bereits auf einem Computer registriert ist. Führen Sie dann die folgenden Schritte durch:

1. Starten Sie das Programm und öffnen Sie das Menü **TinkerTool System**.
2. Halten Sie die Optionstaste (alt-Taste, ) fest und wählen Sie den Menüpunkt **Fortgeschrittene Registrierungsfunktionen** aus. Ein Fenster mit einer Liste von Wahlmöglichkeiten öffnet sich.
3. Wählen Sie den Punkt **Auto-Registrierungsanforderung für Standortlizenz oder globale Lizenz anlegen** und drücken Sie den Knopf **Start**.
4. Es öffnet sich ein Navigationsdialog, der nach einem Zielordner fragt, um die Datei zu sichern. Geben Sie einen Ordner Ihrer Wahl an.
5. Das Programm legt die Anforderungsdatei in diesen Ordner. Der Dateiname endet mit der Markierung **mbsalicreq**. *Sie dürfen die Datei nicht umbenennen*. Archivieren Sie die Datei an einem sicheren Ort, so dass Sie diese später auf andere Computer Ihrer Organisation verteilen können.

Verwenden der Datei zur automatischen Registrierungsanforderung

Jedes Mal wenn Sie die Software auf einem neuen Computer Ihrer Organisation installieren möchten, können Sie das Programm sich selbst registrieren lassen:

1. Kopieren Sie das Programmpaket auf den Zielcomputer.
2. Kopieren Sie die Datei zur automatischen Registrierungsanforderung in den Ordner **/Users/Shared (Benutzer:innen > Geteilt)** des Zielcomputers.

Das ist alles. Das Programm registriert sich automatisch sobald es gestartet wird. Wenn die Volumenlizenz per Internet bestätigt werden konnte, wird die Auto-Registrierungsdatei automatisch gelöscht, so dass sie nicht in falsche Hände fallen kann.

7.2 Wichtige technische Hinweise

7.2.1 Abhilfen bei bestimmten Problemen

Apples Genehmigungsfunktion zur Einbindung von Sicherheitskomponenten ist sehr unzureichend: Mit macOS 13 Ventura führte Apple neue Abläufe ein, mit der Administratoren über das Programm Systemeinstellungen steuern müssen, ob sie einem Programm genehmigen, Anmeldeobjekte im System zu installieren oder beim Start des Programms gleichzeitig ein Hilfsprogramm zur Privilegtrennung zu starten. Diese Funktionen sind unzureichend und von zahlreichen technischen Defekten betroffen. Dies kann Auswirkungen auf TinkerTool System 8 haben, da es aus Sicherheitsgründen grundsätzlich immer die modernste Form von Privilegtrennung verwendet, die eine macOS-Version vorschreibt. Unter anderem gibt es folgende Probleme:

(A) Apple suggeriert fälschlicherweise, TinkerTool System würde ein ständig laufendes Hintergrundprogramm hinzufügen: Im Programm Systemeinstellungen gibt Apple an, Genehmigungen für Anmeldeobjekte wären für Hintergrundobjekte erforderlich, die Apps hinzufügen, „um Aufgaben ausführen zu können, wenn sie nicht geöffnet sind.“ Diese Beschreibung ist falsch, bzw. unvollständig. Die Genehmigung ist auch für Programme wie

TinkerTool System 8 erforderlich, die die Sicherheit durch Privilegtrennung erhöhen, indem sie ein Hilfsprogramm laufen lassen, *nur wenn das Hauptprogramm geöffnet ist*.

Abhilfe: Wir haben Apple über diesen Fehler informiert und hoffen, dass er in zukünftigen Versionen von macOS behoben wird.

(B) Netzwerkadministratoren können die notwendige Genehmigung nicht beim Start des Programms erteilen, sondern nur über die Systemeinstellungen: Beim ersten Start von TinkerTool System 8 blendet macOS eine Benachrichtigung ein, mit der Administratoren erlauben können, dass TinkerTool System ein Hilfsprogramm zur Privilegtrennung verwendet. Dies muss mit dem Kennwort eines Administrators genehmigt werden. Die Kennworteingabe funktioniert jedoch nur für lokal eingerichtete Accounts von Administratoren, nicht für im Netzwerk eingerichtete Accounts von Administratoren.

Abhilfe: Wir haben Apple über diesen Fehler informiert und hoffen, dass er in zukünftigen Versionen von macOS behoben wird. Erteilen Sie als Ersatzlösung die Genehmigung über **Systemeinstellungen > Anmeldeobjekte > Im Hintergrund erlauben** und nicht über die eingeblendete Benachrichtigung.

(C) Wenn Sie mehrere Exemplare von TinkerTool System 8 in ungewöhnlicher Weise auf Ihrem Computer speichern, kann das Dienstmanagement von macOS überfordert sein: Derzeitige Versionen von macOS sind nicht in der Lage, Situationen zu verarbeiten, bei denen mehrere Exemplare von TinkerTool System auf Ihrem Computer vorhanden sind. (Sicherungskopien in Time Machine zählen nicht.)

Abhilfe: Speichern Sie nur ein Exemplar von TinkerTool System auf Ihrem Computer.

(D) Das Verarbeiten von Hintergrundobjekten funktioniert in macOS 13.1 nicht: Falls Sie macOS 13.1 nutzen, funktionieren einige Teile der Benutzerschnittstelle zur Genehmigung von Hintergrundobjekten überhaupt nicht.

Abhilfe: Apple hat bestätigt, dass es sich um einen bekannten Defekt von macOS 13.1 handelt. Wir empfehlen, mindestens macOS 13.3.1 oder höher einzusetzen.

Die Datenschutzfunktion von macOS, die TinkerTool System vollen Plattenzugriff genehmigt, kann scheitern wenn Sie mehrere Exemplare der gleichen Generation von TinkerTool System auf Ihrem Computer speichern: Wie im Kapitel Grundlegende Bedienungshinweise: Datenschutzeinstellungen Ihres Mac (Abschnitt 1.3 auf Seite 8) beschrieben, müssen Sie TinkerTool System die Genehmigung für Festplattenvollzugriff erteilen, bevor Sie alle Funktionen des Programms nutzen können. Falls Sie jedoch mehrere Kopien von TinkerTool System 8 auf Ihrem Mac haben, kann diese Genehmigung unerwartet fehlschlagen. TinkerTool System zeigt möglicherweise an, dass es eine notwendige Genehmigung nicht hat, obwohl sie bereits früher erteilt wurde.

Abhilfe: Dies ist ein bekannter Konstruktionsfehler der Datenschutzfunktion von macOS. Die Schutzfunktion kann verwirrt werden wenn sie mit mehreren Exemplaren des gleichen Programms arbeitet. Führen Sie die folgenden Schritte aus, um sicherzustellen, dass macOS dem richtigen Exemplar der Software die Genehmigung gibt:

1. Suchen Sie alle Exemplare von TinkerTool System auf Ihrem Computer, z.B. mit Spotlight.
2. Löschen Sie alle überflüssigen Kopien und behalten Sie das richtige Exemplar.
3. Gehen Sie in den Systemeinstellungen zu **Datenschutz & Sicherheit > Festplattenvollzugriff**, melden Sie sich als Administrator an und entfernen Sie den Eintrag für TinkerTool System, falls vorhanden.
4. Fügen Sie den Eintrag für TinkerTool System wieder hinzu.

Beachten Sie, dass Sie Sicherungskopien von TinkerTool System auf Time Machine-Platten grundsätzlich behalten können. Dies gilt jedoch möglicherweise nicht für Datensicherungsprogramme von fremden Anbietern.

Die Größenangaben von APFS-Schnappschüssen auf inaktiven Betriebssystem-Volumes kann falsch sein: Aktuelle Versionen von macOS sind nicht in der Lage, die private Größe von APFS-Schnappschüssen zu bestimmen, falls die Schnappschüsse zu einem Volume einer anderen macOS-Installation auf Ihrem Computer gehören. In diesem Fall erhalten Sie möglicherweise eine private Größe von Null und eine Hochwassermarke an der Position 4,61 Exabyte.

Abhilfe: Es gibt keine bekannte Abhilfe. Apples Festplattendienstprogramm ist auch von diesem Problem betroffen.

Wird bei der Abfrage des Systemprotokolls ein Zeitintervall angegeben, können bestimmte Versionen von macOS fehlerhafte Daten liefern, wenn das Zeitintervall einige Sekunden um den Startvorgang eines Apple-Prozessors herum liegt: Wenn Sie die Funktion **Info > Protokolle** verwenden, um das Systemprotokoll auszuwerten und dabei ein Zeitintervall angeben, das sekundengenau auf den Startvorgang eines Macs mit Apple-Chips zielt, liefert macOS oft ein unvollständiges oder leeres Protokoll als Ergebnis.

Abhilfe: Dies ist ein Defekt in aktuellen Versionen von macOS. Es ist im Moment unbekannt, wann und ob Apple diesen Fehler beheben wird. Zur Abhilfe können Sie versuchen, das Zeitintervall um einen geringen Wert zu verschieben, z.B. auf 10 Sekunden nach dem Start des Computers. In den meisten Fällen liefert macOS danach den korrekten Auszug aus dem Protokoll. Macs mit Intel-Prozessor sind grundsätzlich nicht von dem Problem betroffen.

7.3 Versionshistorie

7.3.1 Release 8.98 (Build 250122)

- Die Liste der Macintosh-Baureihen beim Herunterladen von Komponenten zum Anlegen von macOS-Installationsmedien ist aktualisiert worden.
- Die Schnittstelle der Einstellungskarte, um Benutzerdaten gegen iCloud-Zugriff zu schützen, wurde leicht verändert. Dies sollte Benutzer davon abhalten, irrtümlicherweise iCloud-Funktionen in aktivem Zustand („an“) zu sperren.
- Diese Version fügt eine Umgehung eines Problems in manchen Versionen von macOS hinzu, bei denen die Gesundheitsüberwachung für Flash-Speicher und SSDs fälschlicherweise den magnetischen Plattenteil von Fusion Drives mit einschließt.
- Einige technische Details in den Referenzhandbüchern wurden aktualisiert.

7.3.2 Release 8.97 (Build 241121)

- Neue Bedienerschnittstelle für Funktionen zur vereinfachten Lizenzregistrierung und Produktaktivierung hinzugefügt, die in näherer Zukunft zur Verfügung stehen werden.
- Es wurde ein Problem behoben, bei dem die Funktion zum Löschen eines ausgewählten Time Machine-Schnappschusses auf APFS-Medien eine erfolgreiche Entfernung bestätigt hat, obwohl der Vorgang in Wirklichkeit nicht durchgeführt wurde.

7.3.3 Release 8.96 (Build 240910)

- Es wurde ein Problem behoben, bei dem Statusbenennungen für bestimmte Konfigurationseinstellungen auf englisch statt in der vom Benutzer gewählten Sprache angezeigt werden konnten.
- Es wurde ein Problem behoben, beim dem das Ändern des Standardbenutzernamens für Netzwerkanmeldungen nicht richtig funktioniert hat.
- Es wurde ein Problem behoben, bei dem die Funktion zur Diagnose von Kopiervorgängen im Finder keine Erlaubnis von macOS erhalten hat, den Finder zu steuern.
- Es wurde ein Problem behoben, bei dem manche Tabellen ihre vom Benutzer gewählten Spaltenbreiten beim Neustarten des Programms nicht beibehalten haben.
- Diese Version berücksichtigt die Verfügbarkeit von macOS 15 Sequoia und TinkerTool System 9.

7.3.4 Release 8.95 (Build 240731)

- Unterstützung für alternative Vorabversionen zukünftiger Betriebssysteme wurde hinzugefügt.
- Neue Funktion hinzugefügt, um Farb-Tags zu Dateisystemobjekten hinzuzufügen, die auf Netzwerk-Servern gespeichert sind (siehe Fehler > Tags). Dies kann als Behelfslösung für defekte Versionen des macOS-Finders verwendet werden, die dazu nicht mehr in der Lage sind.
- Beim Anzeigen undokumentierter Spotlight-Attribute für Dateien behandelt TinkerTool System jetzt Fälle, in denen Spotlight absichtlich ungültige Datums- und Zeitangaben gespeichert hat, transparenter.

7.3.5 Release 8.94 (Build 240712)

- Neue Funktion hinzugefügt um die Statuseinblendungen für Feststelltaste und Diktat neben der Schreibmarke abzuschalten (siehe Einstellungen bei System Verschiedenes, nur macOS Sonoma oder höher)
- Neue Funktion hinzugefügt um den Vorschlagsassistenten für Emojis neben der Schreibmarke abzuschalten (nur macOS Sonoma oder höher)
- Neue Funktionen hinzugefügt, um bei der Analyse von Dateien weitere nicht dokumentierte Spotlight-Attribute zu beschreiben. Mehr als 20 Attribute wurden hinzugefügt (siehe Karte für Ablage Inhalt).
- Neue Funktionen hinzugefügt, um bei der Sicherheitsanalyse von Programmen weitere Sandbox-Ausnahmen zu beschreiben. Mehr als 80 Befugniseinträge wurden hinzugefügt (siehe Programme Sicherheitsprüfung).
- Die Erkennung neuer Typen von Temporärdateien wurde für das Prüfen und Bereinigen von Einstellungen hinzugefügt (Karte Benutzer). Dies betrifft auch TinkerTool System für den Wiederherstellungsmodus.
- Der Eintrag um abzuschätzen, ob ein Programm über den App Store lizenziert wurde, ist von der Karte für die Sicherheitsprüfung von Programmen entfernt worden. Aufgrund von Änderungen im App Store ist eine verlässliche Analyse nicht mehr möglich.

- Die Richtlinie das Entfernen von Apps, die im App Store gekauft wurden, nicht über den Deinstallationsassistenten zu erlauben, ist nicht mehr in Kraft.

7.3.6 Release 8.93 (Build 240612)

Diese Fassung fügt vorläufige Unterstützung für zukünftige Versionen von macOS hinzu.

7.3.7 Release 8.92 (Build 240515)

- Neue Funktion hinzugefügt, um den macOS-Dienst zur Zeitsynchronisation zurückzusetzen (auf der Einstellungskarte Fehler). Dies kann das Betriebssystem in Fällen reparieren, in denen es immer wieder falsche Werte für Datum und Uhrzeit einstellt.
- Die Filtereinstellungen beim Abrufen von Protokolleinträgen aus der macOS-Protokolldatenbank erlauben nun die Verwendung von Bezeichnern und Namen, die Leerzeichen enthalten.
- Die allgemeinen Symbole zur Anzeige von erfolgreichen oder fehlgeschlagenen Vorgängen wurde im gesamten Programm modernisiert. Sie entsprechen nun besser der Gestaltung aktueller macOS-Versionen.
- Interne Modifikationen und Aktualisierungen, die notwendig sind, um sich an Änderungen in aktuellen Versionen von macOS anzupassen.
- Es wurde ein Problem behoben, bei dem es möglich war, die Einstellungskarte für den Energiezeitplan zu verlassen, ohne Änderungen zu sichern.
- Es wurde ein Problem insbesondere auf langsamen Computern behoben, bei dem die Abfrage von Einträgen aus der macOS-Protokolldatenbank manchmal mit einer Fehlermeldung beantwortet wurde, dass ein möglicher Syntaxfehler vorliegt.

7.3.8 Release 8.91 (Build 240417)

- Neue Funktion hinzugefügt, um Protokolle für bestimmte Prozessexemplare zu trennen, bzw. zu extrahieren nachdem Anfragen an die macOS-Protokolldatenbank gemacht wurden.
- Die Bedienerschnittstelle um mit der macOS-Protokolldatenbank zu arbeiten wurde leicht überarbeitet.
- Es wurde ein Problem behoben, bei dem die Optionen zum Auslesen von Quellprogramm- und „Signpost“-Daten aus der macOS-Protokolldatenbank nicht wie erwartet funktioniert haben.
- Die Fehlerbehandlung wurde für Fälle geändert, in denen Apple Wartungszugriff auf den Software-Aktualisierungsdienst in Betriebssystemen, die nach März 2024 veröffentlicht wurden, sperrt.
- Einige Änderungen in der internen Architektur des Programms.

7.3.9 Release 8.9 (Build 240214)

- Die Funktionen, um mit Spotlight zu arbeiten, wurden komplett neu geschrieben um die aktuellen Betriebssystemversionen zu unterstützen. Die entsprechende Bedienerschnittstelle wurde neu entworfen.
- Neues Detailfenster hinzugefügt, wenn der Spotlight-Index eines Volumes untersucht wird.
- Verlaufsanzeige hinzugefügt, wenn ungeschützte Benutzer-Caches verworfen oder wiederhergestellt werden.
- Neue Diagnosefunktionen hinzugefügt, um zu ermitteln, ob und warum macOS beim Verarbeiten inaktiver Benutzer-Caches langsam ist.
- Alle Tabellen, in denen Markierungspunkte genutzt werden, um ja/nein-Zustände anzuzeigen, verwenden jetzt größere Punkte für bessere Lesbarkeit.

7.3.10 Release 8.89 (Build 240111)

- Neue Funktion zur Autorisierung privilegierter Vorgänge hinzugefügt. Das Programm erlaubt nun die Authentifizierung von Benutzern mit Verwaltungsrechten in zusätzlichen Sonderfällen, die vorher nicht zulässig waren:
 - Autorisierung innerhalb einer laufenden Anmeldesitzung eines Nicht-Administrators
 - Autorisierung durch Administratoren mit leeren Kennworten in Betriebssystemen, die das nicht generell sperren
 - Autorisierung in Fällen, in denen mehrere Benutzer angemeldet sind, der betroffene Benutzer sich aber nicht in der vordersten Konsolsitzung befindet
- Administratoren können falls gewünscht auf die vorherigen strengeren Autorisierungsrichtlinien zurückkehren
- Neue Funktionen zur Karte Energiezeitplan hinzugefügt, die es erlauben, sich wiederholende Ereignisse in komplexeren Konfigurationen zu definieren. Es ist jetzt möglich, beliebige Kombinationen von Wochentagen zum Auslösen von Energiesteuerungsereignissen zu verwenden.
- Neuer Auffrischungsknopf auf der Karte zum Bereinigen von Zeitlupenbildschirm-schonern hinzugefügt (nur macOS Sonoma).
- Die Liste von Systemdiensten, die Speicherplatz automatisch bereinigen, wurde aktualisiert.
- Kleine Änderungen bei der Präsentation von Daten auf der Karte zur Auswertung der RAM-Größe
- Es wurde ein Problem behoben, bei dem das Layout eingebundener TinkerTool-Karten in bestimmten Betriebssystemversionen und Sprachen nicht wie erwartet war.

7.3.11 Release 8.88 (Build 231116)

- Neue Funktion hinzugefügt, um große Dateien von optionalen Apple Zeitlupenbildschirmschonern sofort zu entfernen, falls nötig (nur macOS 14 oder höher).
- Unterstützung neuer Technik bei Hintergrundobjekten für zukünftige Versionen von macOS hinzugefügt.
- Unterstützung für den Lüftertest bei Macs mit M3-Prozessoren hinzugefügt.
- Alle Funktionen, die vom Benutzer gewählte Dateien durchsuchen oder ändern, wurden daraufhin überarbeitet, dass Konflikte mit iCloud oder Cloud-Lösungen anderer Anbieter vermieden werden. Das Öffnen betroffener Ordner löst keine von macOS durchgeführten automatischen Downloads synchronisierter Daten mehr aus.
- Aktualisierte Unterstützung für das Bereinigen von Speicherabzügen des Systemkerns.

7.3.12 Release 8.87 (Build 231024)

- Neue Funktion hinzugefügt, um Verlaufseinträge des Benutzers aus dem „Gehe zu Ordner“-Dialog des Finders zu entfernen.
- Die Funktion, um Berechtigungen im Privatordner eines Benutzer-Accounts zurückzusetzen wurde komplett neu geschrieben:
 - Die Genauigkeit, mit der die empfohlenen Rechteeinstellungen eines frischen macOS-Benutzer-Accounts wiederhergestellt werden, ist noch höher geworden.
 - Die Datumsangaben von Ordnern werden nur noch verändert wenn notwendig.
 - Dateien, die dem Betriebssystem gehören, sind nun im Rücksetzvorgang inbegriffen.
 - Ein neuer Erinnerungsdiallog macht den Benutzer darauf aufmerksam, dass Cloud-Synchronisation vermieden werden sollte, während der Rückstellvorgang läuft.
- Unterstützung für neue Authentifizierungssituationen hinzugefügt, die in macOS Sonoma vorhanden sind.
- Die Schnellhilfefunktion wurde aktualisiert, um Apples neueste Hinzufügungen zu den macOS-Bedienungshandbüchern zu berücksichtigen.
- Viele kleine Änderungen und Optimierungen in der Bedienerschnittstelle.
- Es wurde ein Problem behoben, bei dem TinkerTool System für den Wiederherstellungsmodus (ttsfrm) auf Macs mit Apple-Chips eine irreführende Fehlermeldung anzeigen konnte.

Hinweis: Benutzer, die TinkerTool in TinkerTool System einbinden möchten, müssen aus technischen Gründen auf TinkerTool 9.6 oder höher aktualisieren.

7.3.13 Release 8.86 (Build 230925)

- Volle Unterstützung für macOS 14 Sonoma wurde hinzugefügt.
- Neue Optionen zum Zurücksetzen der Datenschutzeinstellungen hinzugefügt, für Ortungsdienste, Bewegung & Fitness (nur macOS 14 oder höher) und Zugriff auf Passkeys für Webbrowser.
- Neue Funktionen für Software-Entwickler hinzugefügt, wenn eine Sicherheitsprüfung für ein einzelnes Programm ausgeführt wird, das nicht für den Vertrieb über den App Store konzipiert ist: Es kann getestet werden, ob ein Programm bereit ist, entweder zu Apples Beglaubigungsdienst („Notarisierung“) eingesandt zu werden, oder auf Computern von Endkunden ausgeführt zu werden. Diese Funktion ist nur für macOS 14 oder höher verfügbar.
- Benutzer können nun auch zurück zum Übersichtsmenü einer Karte mit Unterpunkten gelangen, indem sie die Karte in der Seitenleiste anklicken.
- Aufgrund von Architekturänderungen in neueren Macintosh-Modellen und macOS-Versionen musste die Funktion zum Abschalten des Systemintegritätsschutzes per Mausklick aus dem Notfalldienstprogramm (ttsfrm) entfernt werden.
- Es wurde ein Problem behoben, bei dem der aktuelle Zustand des Systemintegritätsschutzes auf Macs mit Apple-Chips möglicherweise nicht korrekt angezeigt wurde.

7.3.14 Release 8.85 (Build 230816)

- Neue Funktion zum Monitortest hinzugefügt. Es ist jetzt möglich, ein sich bewegendes schwarzes Raster mit einer Gittergröße von 1 oder 2 physischen Pixeln über den Farbflächen einzublenden. Dies macht es noch leichter, hängende oder tote Pixel auf hochauflösenden Bildschirmen zu erkennen.
- Die Umgehung eines Konstruktionsfehlers in macOS Ventura wurde hinzugefügt, die das Erstellen von Installationsmedien für ältere Versionen von OS X oder macOS verhindern konnte.
- Weitere Unterstützung für zukünftige Versionen von macOS hinzugefügt.
- Einige Arbeitsabläufe auf der Karte Installationsmedien wurden geändert um die Effizienz zu verbessern.
- Die Anleitung auf der Karte Notfallwerkzeug zum Arbeiten mit TinkerTool System in Wiederherstellungssystemen von macOS verwendet nun spezielle Markierungen, um Leerzeichen im notwendigen Terminal-Befehl besser hervorzuheben.

7.3.15 Release 8.8 (Build 230712)

- Neue Funktion hinzugefügt um Zeitangaben für Dateisystemobjekte zu ändern. Dies beinhaltet, falls verfügbar, die Zeit der letzten Änderung, des letzten Zugriffs, der letzten Datensicherung und das Erstellungsdatum. Zusätzlich wird die Zeit der letzten Statusänderung eingeblendet.
- Neue Funktion hinzugefügt um die überarbeiteten Beta-Test-Abläufe von macOS zu unterstützen. Auf der Info-Karte wurde die Anzeige Freigabestatus der Seite Betriebsumgebung durch ein Feld Systemupdatequelle ersetzt.

- In das Ergebnis des macOS-Tests zum Netzwerkantwortverhalten wurde ein neues Feld Leerlauf Latenz hinzugefügt.
- Weitere Unterstützung für zukünftige Betriebssysteme wurde hinzugefügt.
- Viele kleine Änderungen in der Benutzeroberfläche, um auf neue Entwicklungen in macOS zu reagieren.
- Es wurde ein Problem behoben, bei dem der Test von Finder-Kopiervorgängen nicht durchgeführt werden konnte, weil macOS das verhindert hat.

7.3.16 Release 8.7 (Build 230614)

- Neue Funktion hinzugefügt, um verwaiste Berechtigungseinträge in Zugriffssteuerungslisten auf einem lokalen Volume zu erkennen und zu bereinigen. Verwaiste ACLs beziehen sich auf Accounts, die auf dem System nicht mehr vorhanden sind.
- Neue Funktion hinzugefügt, um den wahren Typ von Dateisystemobjekten darzustellen, die vom Finder als Alias präsentiert werden.
- Neue Funktion hinzugefügt, um verwaiste Dateien, die keinen bekannten Eigentümer mehr haben, anderen Benutzer-Accounts zuzuweisen. Dies ist eine alternative Möglichkeit zu der seit Jahren bekannten Funktion, solche Dateien automatisch zu entfernen.
- Neue Funktion hinzugefügt, um das Betriebssystem in Fällen zu reparieren, in denen macOS den erfolgreichen Start von TinkerTool System aufgrund von beschädigten Einstellungen für Hintergrundobjekte nicht zulässt. Die entsprechende Situation wird automatisch erkannt.
- Vorläufige Unterstützung für zukünftige Betriebssysteme wurde hinzugefügt.
- Es wurde ein Kompatibilitätsproblem mit bestimmten Versionen von macOS behoben, bei denen das Löschen eines Time Machine-Schnappschuss immer mit Fehlercode 2 abgewiesen wurde, falls das Sicherungsziel ein APFS-Volume war.

7.3.17 Release 8.6 (Build 230515)

- Neue Funktion hinzugefügt, um die automatische Defragmentierung von APFS-Volumes auf magnetischen Platten zu prüfen, einzuschalten oder abzuschalten.
- Neue Funktionen hinzugefügt, um Benutzer durch die Einschränkungen von macOS 13 zu führen, die die Programmgenehmigung für Hintergrundobjekte und Festplattenvollzugriff betreffen.
- Die Info-Karte zeigt nun auch die Versionsnummer von Apples XProtect Antivirus-Software an, zusätzlich zur Version der Malware-Definitionsdateien.
- Die Sicherheitsrichtlinie für den Zugriff auf den Energiezeitplan wurde geändert: Wie in früheren Versionen der Systemeinstellungen ist eine getrennte Administrator-Authentifizierung nicht mehr erforderlich.
- Die Funktionen zum Überprüfen der Integrität der EFI-Firmware und der Broadcom-Ethernet-Firmware auf Intel-basierten Macs müssen bis auf Weiteres entfernt werden. Aktuelle Versionen von macOS 13 sind nicht mehr in der Lage, solche Prüfungen korrekt durchzuführen.

7.3.18 Release 8.5 (Build 230418)

- Aufgrund neuer Einschränkungen in macOS-Entwicklungswerkzeugen hat sich die interne Architektur des Programms geändert. Benutzer, die TinkerTool aus TinkerTool System heraus nutzen möchten, müssen aus technischen Gründen auf TinkerTool 9.3 oder höher aktualisieren.
- Unterstützung für die neue Architektur in macOS 13 zur Steuerung privilegierter Vorgänge wurde wiederhergestellt. Aufgrund von Einschränkungen in macOS 13 kann es bei manchen Betriebssystemversionen erforderlich sein, den Computer neu zu starten wenn TinkerTool System zum allerersten Mal gestartet wird.
- Unterstützung für das Bereinigen veralteter Installationen von automatisch startenden Jobs wurde wiederhergestellt.
- Die Hauptkategorien in der Seitenleiste des Programms werden nun klarer hervorgehoben.
- Neue Funktion hinzugefügt um System-XPC-Dienste, programm-eingebettete Daemons und programm-eingebettete Agents in der Liste automatisch startender Jobs darzustellen.
- Neue Funktion hinzugefügt um die Build-Nummern verfügbarer macOS-Versionen anzugeben, wenn die Liste der von Apple zum Download angebotenen Installationsprogramme dargestellt wird.
- Neue Funktion hinzugefügt um zu erkennen, ob die von Apple veröffentlichten Größenangaben in der Liste der zum Download angebotenen Installationsprogramme plausibel sind. Falls nicht, wird die Speicherplatzmenge automatisch korrigiert.
- Neue Funktion hinzugefügt um zu erkennen, warum das Erstellen von Installationsmedien von Macs mit Apple-Chips möglicherweise verweigert wird.
- Neue Funktion hinzugefügt um zu erkennen, ob Volumes von Apples LIFS-Technik (Live File Provider File System) verarbeitet werden, damit angegeben werden kann, dass diese nicht mit den Volume-Ausschlusstabellen von macOS kompatibel sind, die auf der Karte System dargestellt sind.
- Einige kleine Änderungen und Klarstellungen in der Benutzeroberfläche und im Benutzerhandbuch.
- Es wurde ein Problem behoben, bei dem die reparierte Version der Installations-App für macOS 10.12 bei der Erstellung von Installationsmedien als ungültige Software abgelehnt wurde.

7.3.19 Release 8.4 (Build 230315)

- Neue Funktion hinzugefügt, um die Benutzer-Accounts von FileVault zu verwalten.
- Neue Funktion hinzugefügt, um den persönlichen Wiederherstellungsschlüssel von FileVault zu überprüfen.
- Neue Funktion hinzugefügt, um die Benutzer-Accounts anzuzeigen, die ein gegebenes APFS-Volume entschlüsseln können.

- Neue Funktion hinzugefügt, um zu ermitteln, welche Benutzer-Accounts als Eigentümer eines APFS-Volumes gelten (nur auf Macs mit Apple Silicon). „APFS-Volumen-Eigentum“ wird benötigt, um die Startsicherheitsrichtlinien einer macOS-Installation zu ändern, um macOS-Installationen oder Updates durchzuführen oder den Vorgang „Alle Inhalte löschen“ auszulösen.
- Unterstützung für zukünftige Versionen von macOS 13 hinzugefügt.
- Die Einstellung, um beim Wechsel zwischen den Karten des Programms automatisch die Überblicksmenüs mit den Unterfunktionen einzublenden, ist nun standardmäßig auf aktiv geschaltet. Erfahrene Benutzer können diese Option jederzeit wieder über das Einstellungsfenster abschalten.
- Die Funktion, um Ventura-„Hintergrundobjekte“ zu analysieren wurde erweitert, um auch sehr komplexe Situationen unterstützen zu können.
- Die Formulierungen zur Beschreibung der unterschiedlichen Arten von Wiederherstellungssystemen auf Macs mit Apple-Chips wurden für bessere Klarheit geändert.
- Falls die Installation der Sicherheitskomponente beschädigt wurde, liefert das Programm jetzt die genaue technische Ursache zusammen mit jeweils passenden Anleitungen, wie das Problem zu beheben ist.
- Es wurde ein Problem behoben, bei dem das Anklicken des Knopfes zum Analysieren von Ventura-„Hintergrundobjekten“ in manchen Fällen keine Wirkung zu haben schien.

7.3.20 Release 8.3 (Build 230215)

- Neue Funktion hinzugefügt, um Inhaltscaching-Server im lokalen Netz zu erkennen und zu fern-analysieren. Solche Server können Probleme mit macOS-Softwareaktualisierungen verursachen.
- Neue Funktion hinzugefügt, um das macOS-Dienste-Management für Hintergrundobjekte zurückzusetzen. Dies ist für Benutzer hilfreich, die mit sich wiederholenden Benachrichtigungen über hinzugefügte Hintergrundobjekte überflutet werden, oder die unrichtige Einträge für diese Objekte in Systemeinstellungen sehen.
- Neue und einzigartige Funktion hinzugefügt, um die von macOS verwaltete Liste von Hintergrundobjekten zu analysieren. Dies erlaubt es, die verwirrenden und oft fehlerhaften Einträge in den Systemeinstellungen besser zu verstehen.
- Die Liste der Baureihen zum Herunterladen von IPSW-Dateien wurde aktualisiert.
- Die Liste der von Apple bereitgestellten System-Jobs wurde aktualisiert.
- Der Punkt zum Reparieren von Funktionen der macOS-Netzwerkbedienerschnittstelle, die durch das 11.2-Update beschädigt werden konnte, wurde entfernt. Er wird in macOS 13 Ventura nicht mehr benötigt.

7.3.21 Release 8.2 (Build 230123)

- Neue Funktion hinzugefügt um IPSW-Dateien von Apple herunterzuladen. IPSW-Dateien können genutzt werden, um eine Vollwiederherstellung mit Rückstellen auf den Werkszustand im DFU-Modus auf Macs mit Apple-Chips durchzuführen.

- Neue Funktion hinzugefügt um die Nachrichtenindexdatenbank von Apple Mail zu löschen. Dies ist hilfreich, um Probleme zu beheben, wenn das Suchen nach E-Mail-Nachrichten nicht mehr richtig funktioniert und unvollständige Ergebnisse liefert.
- Das aktuell in Time Machine ausgewählte Zeitintervall für Datensicherungen und der Verschlüsselungsmodus werden nun auf der Karte für Time Machine angezeigt.
- Die Bedienerschnittstelle für den Status von Flash-Laufwerken wurde überarbeitet. Dies erlaubt es, die Karte Diagnose mit geringerer Höhe anzuzeigen, wodurch Probleme vermieden werden, bestimmte Bedienungselemente auf kleinen Bildschirmen zu erreichen.
- Es wurde ein Layout-Problem auf der Karte „Benutzer > Defekte Einstellungen reparieren“ behoben wenn die Karte auf ihr Minimum verkleinert wurde.
- Interne Änderungen für Funktionen mit Internet-Zugriff, was die Kompatibilität mit Firewalls von Drittanbietern verbessert.

7.3.22 Release 8.14 (Build 221220)

- Da viele Benutzer durch die schlechte Qualität von macOS 13.1 verwirrt sind, fügt diese Version weitere Schutzmaßnahmen gegen Defekte im Betriebssystem hinzu und stellt zusätzliche Benutzerführung bereit.
- Es wird Schutz gegen Fälle hinzugefügt, in denen das Programm für automatische Suche nach Software-Updates konfiguriert ist, aber eine Netzwerk-Firewall die notwendigen Internet-Verbindungen sperrt. In bestimmten Fällen konnte dies zu einer unerwarteten Programmbeendigung statt einer Fehlermeldung führen.

7.3.23 Release 8.12 (Build 221214)

Diese Version fügt weitere Abhilfen für Defekte von macOS 13.1 hinzu.

7.3.24 Release 8.11 (Build 221212)

Dies ist ein Notfall-Update, das nötig geworden ist, da Apple eine Fassung von macOS 13.1 mit mehreren kritischen Defekten veröffentlicht hat. Diese Defekte können unter bestimmten Umständen verhindern, dass TinkerTool System 8 erfolgreich startet.

Wir rüsten die Sicherheitskomponente von TinkerTool System 8 auf Technik von macOS 10.12 Sierra zurück, um bestimmte neue Funktionen von macOS 13 zu vermeiden, die im Moment nicht verwendbar sind. In den letzten 6 Monaten war Apple nicht in der Lage, Systemdienste bereitzustellen, die die Spezifikationen von Ventura einhalten.

7.3.25 Release 8.1 (Build 221205)

- Neue Einstellungskarte hinzugefügt, um wieder Zugriff auf den Energiezeitplan von macOS zu erhalten. Wie in älteren Versionen des Programms Systemeinstellungen können die Funktionen des Mac zum zeitgesteuerten Einschalten, Herunterfahren, Ruhezustand oder Neustart innerhalb einer Woche mit wenigen Mausklicks eingerichtet werden.
- Zusätzlich kann der macOS-Energiezeitplan für Einmaltermine eingesehen und vollständig verändert werden.

- Eine Symbolleiste wurde dem Hauptsteuerungsfenster hinzugefügt. Sie bringt macOS dazu, die Titelleiste des Fensters in einer gefälligeren Darstellung anzuzeigen.
- Optionale Bedienungselemente wurden von der Seitenleiste in die Symbolleiste verlagert.
- Die Punkte in der Seitenleiste berücksichtigen nun automatisch die allgemeine Einstellung des Benutzers für die Anzeigegröße von Seitenleisten.
- Die Punkte in der Seitenleiste behalten nun beim Neustart des Programms ihre Statusinformationen bei, welche Unterpunkte ein- oder ausgeklappt dargestellt werden.
- Eine neue Benutzereinstellung wurde hinzugefügt, die es erlaubt, beim Umschalten zwischen Einstellungskarten immer die Funktionsübersicht zu bevorzugen, anstatt den zuletzt benutzten Unterpunkt zu öffnen.
- Alle Internet-Links in der Schnellen Kontexthilfe wurden aktualisiert, da Apple endlich das Benutzerhandbuch für macOS Ventura veröffentlicht hat.
- Diese Version behebt ein Problem, bei dem die allgemeine Reset-Funktion möglicherweise für die Karte Cloud-Schutz nicht wie erwartet funktioniert hat.

7.3.26 Release 8.0 (Build 221019)

- Volle Unterstützung für macOS Ventura hinzugefügt. TinkerTool System 8 kann nur mit macOS 13 oder höher eingesetzt werden. Es erlaubt die Integration von TinkerTool 9.
- Das Programm verwendet eine komplett neue Bedieneroberfläche, die an die Stilvorgaben des Programms „Systemeinstellungen“ angelehnt ist. Dies gilt auch für die Stichwortsuche von Funktionen.
- Das Fenster des Programms ist nun in der Größe anpassbar. Bei Tabellen mit vielen Spalten ist die frühere Zusatzfunktion „in getrenntem Fenster zeigen“ nicht mehr notwendig.
- Es ist ein neuer Knopf vorhanden, um das Fenster auf die geringstmögliche Größe für die gerade verwendete Karte zu optimieren.
- Das Hilfsprogramm für privilegierte Vorgänge verwendet nun die neuesten Ventura-Technologien. Es muss beim Erststart nicht mehr installiert, sondern nur noch genehmigt werden.
- Falls Sie TinkerTool in TinkerTool System integrieren, werden dessen Einstellungskarten ebenso über die Suchfunktion zugreifbar.
- Die Funktion zum Scannen von Netzwerk-Ports musste entfernt werden. Die nötigen Komponenten sind nicht mehr in macOS 13 enthalten.
- Die Funktion zum vollautomatischen Bereinigen fehlerhafter Hintergrund-Dienste ist vorübergehend gesperrt. Ventura verwendet neue Techniken zur Steuerung von Diensten, die noch nicht ausgereift sind. Es ist geplant, dieses Feature später wieder zur Verfügung zu stellen, wenn macOS 13 die notwendige Zuverlässigkeit erreicht hat.

TinkerTool System 8 ist der Beginn einer neuen Produktlinie. Der obenstehende Abschnitt listet Änderungen in Bezug auf TinkerTool System 7, Version 7.91 auf. Für weitere Informationen über die Versionshistorie von TinkerTool System 7 verwenden Sie bitte das entsprechende Programm.

Anhang A

Aufgaben und Lösungen

A.1 Wo ist diese Funktion jetzt?

Informationen für Benutzer, die von TinkerTool System 7 umgestiegen sind

Falls Sie ein Upgrade von macOS 11 Big Sur oder macOS 12 Monterey auf macOS 13 Ventura oder höher vorgenommen haben und nach fehlenden Funktionen in TinkerTool System 8 suchen, verwenden Sie bitte die untenstehende Tabelle, um zu erfahren, weshalb bestimmte Funktionen nicht mehr vorhanden sein können, bzw. ob sich deren Aufruf verändert hat.

Tabelle A.1: Vergleich der Orte der verschiedenen Funktionen

Früherer Platz	Aktueller Status
Fehler > Netzwerk Bedienelemente	<i>entfernt</i> , da in macOS 13 nicht mehr benötigt
Netzwerk > Portscan	von Apple aus macOS 13 <i>entfernt</i>
Info > Systemdaten	Info > Mac
Info > Systemdaten > Betriebsumgebung	Info > Betriebsumgebung
Info > Klass. Protokolle & Berichte	Info > Klassische Protokolle & Berichte
Info > Klass. Protokolle & Berichte > Server-Protokolle	<i>entfernt</i> , da macOS Server von Apple eingestellt
Systemicherheit > EFI-Firmware	<i>entfernt</i> , da die zugrundeliegende Funktion in macOS 13 im Moment defekt ist
Systemicherheit > Broadcom® Ethernet	<i>entfernt</i> , da die zugrundeliegende Funktion in macOS 13 im Moment defekt ist
Installations-Medien	Installationsmedien
APFS > Getrenntes Fenster	<i>entfernt</i> , da mit TinkerTool System 8 überflüssig
System > Einstellungskarten	<i>entfernt</i> , da in Systemeinstellungen und Archivierungsprogramm enthalten
System > Versch.	System > Verschiedenes
Systemstart > Geschützte Optionen	<i>entfernt</i> , da auf modernen Macs gesperrt und nicht mehr sinnvoll
Systemstart > Sprache	<i>für macOS 14 entfernt</i> , da in modernen Systemversionen nicht mehr notwendig
Programm-Sprache	Programmsprache

Alle Punkte, die hier nicht aufgeführt sind, haben ihren Platz und Namen beibehalten.

A.2 Sollte ich regelmäßige Wartungsarbeiten durchführen?

Die kurze Antwort lautet: Nein.

macOS ist so konstruiert, dass es keine Art irgendeiner regelmäßig durchgeführten Wartung benötigt. Alle Aufräumarbeiten werden bereits automatisch vom Betriebssystem erledigt. Unter normalen Umständen, müssen Sie sich um technische Details nicht kümmern, was der üblichen Philosophie von Apple-Produkten entspricht. Sich wiederholende Aufgaben, wie das Überwachen von Druckern oder das Löschen veralteter Absturzberichte werden bereits von Dienstprogrammen im Hintergrund erledigt. Andere Aufgaben, wie das Defragmentieren von Festplatten, werden als Nebenwirkung normaler Vorgänge durchgeführt oder komplett vermieden, indem moderne Technologien zum Einsatz kommen.

Aus diesen Gründen brauchen Sie **keine der Funktionen von TinkerTool System in regelmäßigen Abständen laufen zu lassen**. Mit Absicht enthält das Programm keinen Terminplan, „Autopiloten“ oder ähnliche Funktionen.

In einigen Fällen können per Terminplan ausgeführte Wartungsmaßnahmen Ihrem Computer sogar schaden. Dies gilt insbesondere für die meisten Cache-Bereinigungsfunktionen. Das Bereinigen von Caches kann eine wichtige Maßnahme bei der Fehlersuche sein, falls Ihr Computer tatsächlich von einem Software-Problem betroffen ist, aber es hat immer schädliche Nebenwirkungen, da das System und die Programme die Caches wieder neu aufbauen müssen, was je nach Fall Tage dauern kann. Während dieser Zeit läuft das System langsamer als üblich, da die Cache-Daten neu geholt oder neu berechnet werden müssen. Zusammenfassend gesagt ergibt das Bereinigen von Caches ohne triftigen Grund überhaupt keinen Sinn. Es führt dazu, dass Ihr Computer schlechter arbeitet. Aus diesem Grund führte TinkerTool System neue Funktionen ein, die zur Fehlersuche im Cache dienen, jedoch das Bereinigen von Caches vermeiden, wenn es nicht absolut notwendig ist.

Das heißt nicht, dass macOS überhaupt keine Wartung benötigen würde. Aber Sie müssen sie nicht regelmäßig durchführen. Wartung ist nur dann nötig, wenn es auch etwas zu reparieren gibt.

Es kann zahlreiche Ursachen für technische Probleme mit einem Computer geben, auf dem macOS läuft, die Wartungsarbeiten notwendig machen:

- Frühe Versionen des Betriebssystems enthalten möglicherweise Defekte („Bugs“), die noch nicht behoben sind.
- Das Betriebssystem kann allgemeine Konstruktionsfehler enthalten, bei denen eine Behebung nicht geplant ist, aber die trotzdem Probleme verursachen.
- Schlecht geschriebene Installationsprogramme von Drittanbietern können Teile des Systems beschädigen.
- Während des Arbeitens mit Verwalterberechtigungen könnten Sie einen Bedienungsfehler gemacht haben.
- Sie möchten fortgeschrittene Funktionen des Systems nutzen, aber haben nicht die notwendigen Kenntnisse, diese auf der UNIX-Befehlszeile abzurufen.

In allen diesen Fällen kann TinkerTool System Ihnen weiterhelfen.

Falls Sie unsicher sind, wann Sie eine bestimmte Wartungsfunktion von TinkerTool System einsetzen sollten, betätigen Sie den Hilfeknopf in der oberen rechten Ecke der jeweiligen Einstellungskarte.

A.3 Wie kann ich das System reparieren, wenn macOS durcheinandergewürfelten Text bei der Verwendung bestimmter Schriftarten zeigt?

In fast allen Fällen wird das Problem durch technische Probleme des Schriftregistrierungsservers von macOS ausgelöst. Es kann behoben werden, indem man dieses Subsystem dazu zwingt, seine Caches neu aufzubauen. Führen Sie die folgenden Schritte durch:

1. Prüfen Sie, ob nur ein bestimmter Benutzer-Account oder alle Benutzer-Accounts von diesem Problem betroffen sind. Stellen Sie sicher, dass Sie als derjenige Benutzer angemeldet sind, bei dem das Problem auftritt.
2. Öffnen Sie die Einstellungskarte **Caches**.
3. Öffnen Sie den Unterpunkt **Schrift-Caches**.
4. Falls nur der aktuelle Account betroffen ist, wählen Sie den Punkt **Schrift-Caches für den Benutzer ... bereinigen**. Falls alle Benutzer betroffen sind, wählen Sie den Punkt **Schrift-Caches des Benutzers und des Betriebssystems bereinigen**.
5. Drücken Sie den Knopf **Schrift-Caches bereinigen**.

Weitere Informationen: Die Einstellungskarte Caches (Abschnitt 2.2 auf Seite 29).

A.4 Wie kann ich die tatsächlichen Zugriffsrechte auf eine Datei oder einen Ordner anzeigen lassen?

Da die Anzeige von Zugriffsrechten im Finder sehr verwirrend oder sogar falsch ist, kann Ihnen TinkerTool System dabei helfen, die echten Zugriffsrechte einer Datei oder eines Ordners auszulesen. Führen Sie die folgenden Schritte durch:

1. Öffnen Sie die Einstellungskarte **ACL-Rechte**.
2. Wählen Sie den Unterpunkt **Zugriffsrechte zeigen oder einstellen**.
3. Ziehen Sie das in Frage kommende Objekt vom Finder in das Feld **Datei oder Ordner**.

Die Berechtigungseinstellungen werden in der Tabelle **Zugriffsrechte und Eigentümer** angezeigt.

Weitere Informationen: Die Einstellungskarte ACL-Rechte (Abschnitt 3.4 auf Seite 192).

A.5 Was sollte ich tun, wenn macOS die Online-Hilfe nicht mehr öffnen kann?

Das Programm zur Anzeige von Hilfetexten in Anwendungen (Online-Dokumentation) leidet unter mehreren technischen Defekten, so dass es von Zeit zu Zeit ausfallen kann. Um es zu reparieren, führen Sie die folgenden Schritte durch:

1. Öffnen Sie die Einstellungskarte **Benutzer**.
2. Wählen Sie den Unterpunkt **Reparatur**.
3. Drücken Sie auf den Knopf **Jetzt reparieren** in der Rubrik „**Help Viewer**“ reparieren.

Weitere Informationen: Die Einstellungskarte Benutzer (Abschnitt 5 auf Seite 283).

A.6 Freischalten des Programms

Wenn Sie TinkerTool System 8 uneingeschränkt nutzen möchten, müssen Sie eine Registrierung erwerben, die bestätigt, dass Sie eine Lizenz zur dauerhaften Nutzung haben.

1. Rufen Sie im Programm den Menüpunkt **TinkerTool System > TinkerTool System freischalten** auf. Das Fenster **Registrierung und Aktivierung** erscheint.
2. Wählen Sie aus, welche Art von Registrierung Sie haben. Seit Ende 2024 ist dies in der Regel **Registrier.-Schlüssel**.
3. Übertragen Sie den gelieferten Schlüsselcode in das Feld **Registrierungsschlüssel**.
4. Klicken Sie auf **Speichern**.
5. Bestätigen Sie Ihr Einverständnis, dass das Programm eine Internet-Verbindung herstellen darf.
6. Warten Sie einige Sekunden, bis Ihre Registrierung bestätigt wurde.

Die Bestätigung wird angezeigt. Sie können das Fenster danach schließen. Weiterführende Informationen: Registrierung und Freischalten des Programms (Abschnitt 7 auf Seite 313)

Index

/Local/Default, 27

/tmp, 299

4k, 130

5k, 130

A

Abhilfe, 321

Ablaufverfolgung, 137

Abmeldung, 33

abschalten, 239

Abschottung, 86

absoluter Pfad, 158

Absturz, 86

Absturzbericht, 132, 167

Access Control Entry, 195

Access Control List, 192, 195

Account, 272

Account-Name, 214

accountsKeychain, 75

ACE, 195

ACL, 192, 195

ACL entfernen, 203

Active Directory, 28

Adams, Carlisle, 248

Ad-Hoc-Signatur, 190

Administrator, 3, 5, 135, 308

Adobe® Flash®, 129

adressierbarer Speicher, 124

Advanced Host Controller Interface, 96

Änderungsrate, 46

AFP, 198

Agent, 260

AHCI, 96

aktivieren, 318

Aktivitätsbezeichner, 138

Aktualisierung, 17, 18, 319

Alias, 145, 153, 173

Amazon, 276

Analyse, 164

analysieren, 153

Anbieterkennung, 122

Anbieterkennzeichnung, 124

Andere, 192

Andere (Benutzer), 270

anhängen, 195

anlegen, 195

Anleitung drucken, 109

Anmeldebildschirm, 305

Anmeldeobjekt, 4, 76, 183, 261

Anmeldeverfahren, 247

Anmeldezeit, 103

Antwortverhalten, 120

Anwendungs-Sandbox, 186

Apfelmenü, 271, 287

APFS, 39, 198, 223, 228

APFS-Container, 223, 228

APFS-Rolle, 230

APFS-Schlüssel, 230

APFS-Schnappschuss, 49, 64

APFS-Volume, 229

APFS-Volumegruppe, 228

App Nap, 130

App Store, 68, 73, 244

Apple Configurator, 219

Apple Diagnose, 258

Apple File System , 39, 228

Apple Filing Protocol, 198

Apple GPU-Kern, 124

Apple T2, 125

Apple TV, 176

Apple-Chip, 122, 218, 257

Apple-Chip-Problem, 133

AppleDouble, 90, 165

Apple-Menü, 271

Apple-Modellidentifikation, 122

AppleShare, 198

App-Updates, 68

Arbeitsumfang, 89

Archiv, 167

Archivordner, 287

ASCII, 149

ATA8-ACS2, 95

Attribut, 148, 165, 195

aufheben, 148

auflösen, 173

Auftragsverarbeitungsvertrag, 276

Aufzeichnungsformat, 93
Aufzeichnungsschicht, 93
Ausfall, 310
ausführbare Datei, 193
ausführen, 193, 241
Auslagerung, 89
Auslagerungsspeicher, 87, 89
ausmustern, 286
ausschalten, 271
Auswahlknopf, 12
auswerfen, 93, 176
auswerten, 87
Automation, 21
automatische Aktivierung, 34
automatische Anmeldung, 308
Automatische Benachrichtigung, 17
automatische Sprachwahl, 291
Automator, 227
Autopilot, 336
Autoradio, 175
Autorisierung aufheben, 5
Azure Active Directory, 28

B

Baseband-Verarbeitung, 134
Batterie (Karte), 279
Bedrohung, 130
Befugnis, 186
Beglaubigung, 186, 189
bekannter Fehler, 321
Benutzer ausblenden, 272
Benutzer-Account, 170, 294, 300
Benutzerdienst-Anmeldeobjekt, 261
Benutzereinstellung, 283
Benutzerfoto, 294
Benutzergruppe, 294
Benutzerliste, 269
Benutzerordner, 211
Benutzerordner, gemeinsamer, 29
Benutzersitzung, 252, 269
benutztes Objekt, 287
Berechtigung, 192, 250
bereinigen, 164
Bereinigung, 224
Bericht, 13, 15, 132, 164, 182
Bestätigen, 15
Bestätigung, 164
bestellen, 315
Bestellnummer, 122
Beta-Programm, 69
Betriebssystem, 3
Betriebssystemversion, 126

bevorzugte Sprache, 273
Bildpunkt, 105
Bildschirm, 105
Bildschirmfreigabe, 253
Bildschirmschoner, 176
Block, 87
Blu-Ray Disc, 93
böswillige Software, 129
Bookmark, 146, 156
Bridge-Chip, 311
BridgeOS, 101, 125
Buchführung, 103
Build-Nummer, 126
Byte, 149

C

CA, 189
Cache, 26, 29, 300, 303
Cache-Bereinigung, 31
Cache-Größe, 122, 124
Cache-Server, 69
Cache-Speicher, 89
CBC128, 248
CD, 93
Certificate Authority, 189
CIFS, 198
Cipher Block Chain, 248
Codesigning, 186, 225
Common Unix Printing System, 255
Computer, 122
Computereinstellung, 287
computerweit, 181
CPU, 260
Creator Code, 148
CSR, 18
csrutil, 20
CUPS, 255
Customer System Restriction, 18

D

Daemon, 260
dark wake, 258
Darstellungseinstellung, 165
Darwin, 126
Datei, 12
Dateiname, 158
Dateinamenserweiterung, 153
Dateiserver, 198, 247
Dateisystem, 12, 90, 165
Dateizweig, 162
Datenbank, 137
datenlose Datei, 159, 213

Datenschutz, 20, 185
Datenzweig, 162
Datum, 81
deaktivieren, 285, 300
Defragmentieren, 336
Defragmentierung, 232
Deinstallationsassistent, 180
deinstallieren, 180
Demomodus, 17, 313
Demonstrationsfenster, 314
Desktop Services Store, 165
DFU-Modus, 219
Dialogfenster, 13
Dienste-Management, 75
Dienste-Menü, 289
Dienstleistungsmarken, ii
Differential Privacy, 134
Diffie-Hellman, 248
digitales Siegel, 189
Directory, 153
Disk Image, 187
Diskmedien, 93
Display, 105
DMG, 187
DNS, 116
DNS-Auflöser, 26
DNS-Name, 284
Dock, 308
Dockmenü, 12
Domain Name Service, 116
Download, 186, 187
drahtlos, 248
Drahtlos-Diagnose, 134
Drosseln, 239
Druckauftrag, 255
drucken, 126, 182
Druckerprogramm, 227
Druckverlauf, 255
dsimport, 28
.DS_Store, 165
dtrace, 19
durcheinandergewürfelter Text, 35
Durchmesser, 93
durchqueren, 193, 195
DVD, 93
DVD+R, 95
DVD-ROM, 95

E

Effizienzkernel, 124
eigene Berechtigung, 199
Eigenschaftsliste, 283

Eigentümer, 170, 192, 196
Ein-/Ausgabe, 239
ein-/ausschalten, 245
Einbenutzerbetrieb, 111
Eingabeassistent, 256
eingeschränkt, 19
Einheit (für Speichergröße), 222
Einheiten, 16
einmaliges Energieereignis, 280
Einrichtungsassistent, 308
Einschalttaste, 256
Ein-Schritt-Upgrade-Ticket, 320
Einstellungen, 13, 180
Einstellungsdatei, 300, 303
Einstellungsdomäne, 283
Einstellungskarte, 1, 10, 22
Einstellungssystem, 283
empfohlener freier Speicher, 89
emulieren, 165
Energie sparen (Karte), 279
Energiesparen, 239
Energiezeitplan, 279
entfern timer Platte, 175
entfernen, 15
entfernen (Registrierung), 319
Erkennungsmerkmal, 129
erlauben, 195
erst prüfen, dann kaufen, 313
erteilen, 193
erweiterte Attribute, 90
Erweitertes Attribut, 162
erweitertes Attribut, 195
Erweiterung, 12
Erweiterungssteckplatz, 125
Erzeugercode, 148
everyone, 193
ExFAT, 198, 242
expliziter Eintrag, 197
externes Laufwerk, 311

F

Familiennummer, 124
Farbfeld, 122
Farb-Tag, 81
FAT, 90, 162, 198
FAT32, 198
Fenster, herausgleitendes, 13
Fenstergröße, 11
Fernseher, 175
fester Link, 145
Festplatte, 239, 310
Festplattendienstprogramm, 84, 217, 222

Festplattenvollzugriff, 21
 File-Server, 90, 270, 286
 FileVault, 227, 253, 265, 269
 FileVault-Benutzer, 265
 Finder, 90, 145, 153, 158, 165, 170, 175, 199,
 222, 250, 285, 287–289, 292, 294, 308
 Finder Kopieren, 92
 Finder-Tag, 162
 Finger-Protokoll, 118
 FireWire, 311
 Firma, 250
 Firmlink, 229
 Firmware, 93, 125, 218, 256
 firmware, 126
 Flash-Speicher, 95, 96
 fork, 162
 Format, 90, 93
 Fragezeichen, 11
 Fragment, 232
 Framework, 93
 freier Speicher, 89
 freischalten, 318
 Freispeichergröße, 124
 FTP, 198
 Fusion Drive, 98, 230

G

Gatekeeper, 152, 187
 Gebläse, 101
 GECOS, 214
 geerbter Eintrag, 197
 Gegenanzeige, 11
 gehärtete Laufzeit, 186
 Gehäuse, 125
 Gehäusefarbe, 122
 Gehäusemodell, 122
 Gehe zu Ordner, 288
 gelerntes Wort, 290
 gelockt, 147
 gemanagte Einstellungen, 305
 gemeinsam verwendeter Speicher, 89
 Generalschlüssel, 265
 Gerät, 170
 Geschwindigkeitstest, 120
 Gesundheit (Flash-Speicher), 98
 geteilt (Benutzerordner), 29
 gleichzeitiger Lauf, 274
 globale Lizenz, 320
 Google, 276
 Grafikchip, 89
 Grammatik, 290
 grüner Pfeil, 33

Grundfunktionen, 299
 Gruppe, 294
 Gruppeneigentümer, 192
 Gültigkeitsprüfung, 8
 GUID, 206
 Guizhou, 276

H

hängendes Pixel, 105
 Hardware, 309
 Hardware-Identifikation, 122
 Hauptfenster, 8
 Hauptplatine, 124
 Hauptspeicher, 86
 Help Viewer, 291
 Hersteller, 93
 heruntergeladen, 187
 herunterladen, 18, 315
 Hexadezimalziffer, 149
 HFS, 90, 148
 HFS+, 39, 198
 HiDPI, 130
 Hierarchie, 284
 Hilfefenster, 11
 Hilfeknopf, 2
 Hilfsprogramm, 3
 Hintergrunddienst, 258
 Hintergrundobjekt, 4, 75
 Hintergrundprogramm, 239, 252
 Hitze, 259
 Hochgeschwindigkeits-Cache, 31
 Hochwassermarke, 235
 Höchstleistungskern, 124
 Hohe Auflösung, 130
 Host-Name, 272
 HTML, 126
 https, 313
 Hypervisor, 219, 221

I

iCloud, 134, 265, 276
 Icon-Caches, 36
 Identifikationsnummer, 294
 IEEE 1003, 192
 immer an, 256
 Importieren (E-Mail), 293
 INACTIVE-plist, 286
 Indexdatenbank, 293
 Info, 122, 294
 Inhalt, 153
 Inhaltscaching-Server, 69
 inkrementelle Sicherung, 39

inspizieren, 93
Installationsmedium, 216
Installationsprogramm, 156, 183
Installer, 216
Integrität, 284
intelligente Deaktivierung, 31
interner Cache, 31
Internet, 12, 18, 152
Internet-Adresse, 187
Internet-Plugin, 129
Internet-Protokollversion 6, 250
Internet-Verbindung, 120
Internet-Wiederherstellung, 216
iOS-Stil, 133
iPad-Aktualisierung, 134
IP-Adresse, 272
iPhone-Aktualisierung, 134
iPod, 169
IPSW-Datei, 218
IPv6, 250
ISO-Datei, 221
iXcellerate, 276

J

Java™, 129
Jeder, 193
Jobstatus, 262

K

kanonische Sortierung, 203
Karte, 13
Karteireiter, 10
Kategoriebezeichner, 138
Kennwort, 269, 287
Kern, 259
Kern (Prozessor), 122
Kernel, 86
Kernel Panic, 133
Kernel-Erweiterung, 258
Kibi, 16
Klartextübertragung, 248
Klon, 235
Kollision, 113
komprimiert, 167
komprimierter Auslagerungsspeicher, 89
komprimierter Speicher, 87
Konsole, 135, 227
Kontexthilfe, 11
Kopiervorgang, 92
kritischer Vorgang, 15
Kühlung, 101
Kurzname, 214, 247, 294

L

langsames Antwortverhalten, 134
langsames Herunterfahren, 134
Launchpad, 291
LDAPv3, 28
Leistung, 86, 259
lesen, 193
LIFS, 242
Link, 12, 145
Linux, 175
Liste für sichere Downloads, 129
Live File Provider File System, 242
Lizenz, 315
locate, 28
Lock, 147
löscherbarer Speicher, 222
löschen, 196, 286
Löschen (Platte), 84
löschen (Schnappschüsse), 66
Löschen (Server), 81
löschen (Sicherungsdaten), 52
Löschung, 157, 164
Löschungsstärke, 181
Logic Board, 124
lokaler Benutzer, 270
lokaler Schnappschuss, 49, 64
Lüfter, 101

M

Mac App Store, 68
Mac OS, 145, 173, 175, 284
Mac OS 7, 153
Mac OS Extended, 39
Mac OS X 10.1, *siehe* Mac OS X Puma
Mac OS X 10.4, *siehe* Mac OS X Tiger
Mac OS X Puma, 292
Mac OS X Tiger, 306
MAC-Adresse, 113, 286
macFUSE, 242
Macintosh, 124
Macintosh File System in User Space, 242
macOS 10.12, *siehe* macOS Sierra
macOS 10.14, *siehe* macOS Mojave
macOS 10.15, *siehe* macOS Catalina
macOS 11, *siehe* macOS Big Sur
macOS 12, *siehe* macOS Monterey
macOS 13, *siehe* macOS Ventura
macOS 14, *siehe* macOS Sonoma
macOS 15, *siehe* macOS Sequoia
macOS Big Sur, 2, 39
macOS Catalina, 2
macOS Mojave, 2, 20

- macOS Monterey, 2
 - macOS Sequoia, 2
 - macOS Server, 26
 - macOS Sierra, 190, 221
 - macOS Sonoma, 2, 3, 176, 190, 256, 268, 271, 275
 - macOS Ventura, 2, 3, 268, 271
 - macOS-Bookmark-Datei, 156
 - macOS-Wiederherstellung, 297
 - Mail, 293
 - Malware, 129
 - Malware-Schutz, 129
 - Managementeinträge, 124
 - Marketing-Name, 122
 - Markierung, 246
 - Markierungen (Markup), 288
 - mbsalicreq-Datei, 321
 - mbsetupuser, 105
 - mbsreg-Datei, 317
 - Medium Access Control, 113
 - mehrsprachig, 273, 291
 - Memory Management Unit, 87
 - Metadaten, 153
 - Metadatenpeicher, 244
 - Microsoft Azure, 276
 - Migrationsassistent, 306, 319
 - Minimieren (Fenster), 11
 - Mitgliedschaft, 294
 - MMU, 87
 - Mobilcomputer, 270
 - mobiler Benutzer, 270
 - Mobilgerät, 169
 - Modellbezeichnung, 122
 - Modellnummer (Prozessor), 124
 - Monitor, 105
 - MS-DOS, 162, 165
 - Multicast, 114
 - Musik, 29
- N**
- named fork, 162
 - NAS, 39
 - NetBoot, 216
 - Netz, 247
 - Netzbenutzer, 270
 - Netzqualität, 120
 - Netzteil, 126
 - netzweit, 181
 - Netzwerk, 81
 - Netzwerkdienstprogramm, 112
 - Neulauf, 308
 - Neustart, 271
 - Neuzuweisung, 41, 57
 - NFS, 92
 - NFSv2, 198
 - NFSv3, 198
 - NFSv4, 198
 - Notarisierung, 186, 189
 - Not-Aus, 133
 - Notfallwerkzeug, 108
 - Notfall-Wiederherstellungssystem, 216
 - NTFS, 198, 242
 - nur hinzufügen, 194
 - Nutzungsdauer, 103
 - Nutzungserlaubnis, 315
 - NVMe, 96, 98, 311
 - NVRAM, 19, 264
- O**
- öffentlicher Ordner, 194
 - Öffnen mit, 288
 - Öffnen-Dialog, 12
 - Open Directory, 273
 - Open Directory Server, 26
 - Operationen (ACL), 203
 - optische Disk, 93
 - optisches Laufwerk, 93
 - Ordner, 12, 153, 196
 - Ordnernebene, 196
 - Ordnerhierarchie, 158
 - Ortsangabe, 12
- P**
- Paket, 153
 - Paketinhalt, 153
 - Paketverfolgung, 116
 - Papierkorb, 157, 175, 182, 287
 - Parameter-RAM, 264
 - Partei, 192
 - Partition, 84, 90
 - Partitionierung, 223
 - PC, 124
 - persönlicher Cache, 31
 - Pfad, 12, 158, 294
 - Pfeilnavigation, 13
 - physischer Datenträger, 228
 - Ping, 114
 - Pixel, 105
 - Platte, 90, 175
 - Plattenabbild, 187
 - Plattenplatz, 245
 - Plattenschreibaktivität, 134
 - Plattenspeicher, 16
 - plist, 283

POSIX, 158, 214, 251
POSIX.1e, 192
POSIX-Berechtigung, 192, 197
post mortem, 178
Primärgruppe, 294
Priorität, 239
Prioritätsliste, 273
Privatgröße (APFS), 234
Privatordner, 170, 211, 270, 286, 292, 294
Privatsphäre, 138
privilegierter Vorgang, 3
proaktives Ereignis, 135
Problem, 321
Produktionswoche, 122
Profil, 277
Programmabsturzbericht, 132
Programmaktivität, 133
Programme-Ordner, 289
Programmsprache, 274, 275
Programmstillstandsbericht, 133
Programmvorfall, 135
Property List, 283
Protokoll, 132
Protokoll (Time Machine), 53
Protokollarchiv, 139
Protokolldatei, 167
Protokollierung, 137
Prozess, 86, 89
Prozessexemplare, 143
Prozessor, 122, 309
Prozessoraktivität, 133
Prozessor-Cluster, 124
Prozessorkern, 259
Prozessormodell, 122
Punkt-Unterstrich, 165

Q

Quarantäne, 151, 165, 186

R

RAM, 86, 124, 260
Random Access Memory, 86, 124
Recht, 192, 195
Rechte reparieren, 211
Rechte zurückstellen, 211
Rechtetrennung, 4
Rechtschreibprüfung, 290
Recovery Mode, 109
Registrierung, 17, 315
Registrierung und Aktivierung, 316–318
Registrierungsbescheinigung, 318
Registrierungsname, 318

Registrierungsschlüssel, 318
relativer Pfad, 159
reparieren, 269, 291
Replizieren (APFS), 235
reservierter Speicher, 89
resident, 194
resource fork, 162
Ressourcenweig, 162, 165
restricted, 19
Retina, 130
RFC 952, 116
RFC 2307, 28
Richtlinie, 248
root, 105
root-Benutzer, 18
rootless, 18
Rosetta, 222
Rotationsgeschwindigkeit, 93
rotes Schild, 21
rückgängigmachen, 17
Ruhezustand, 271
Ruhezustandszeitgeber, 239
runden, 16

S

sandbox-geschützt, 20
SATA, 311
SATA-Bus, 96
Schalter, 125
Schicht, 93
Schlosssymbol, 147
Schlüsselbund, 73
Schnappschuss, 223
Schneller Benutzerwechsel, 8
Schrägstrich, 13
schreiben, 193
Schreibmarke, 256
Schreibschutz, 157
Schrift-Cache, 34
Schriftregistrierungsserver, 34
Schriftsammlung, 35
Schriftzeichen, 34
Schubfach, 93
Schule, 250
Schutz, 129, 147
Schutzmechanismus, 15
Seeding Program, 126
Seite, 87
Seitenleiste, 10
Self Monitoring, Analysis, and Reporting Technology, 310
Sensoren, 124

- Seriennummer, 122
- Server, 81, 181
- Serverbetrieb, 259
- Services für Macintosh, 248
- Session, 93
- set group identification, 194
- set user identification, 194
- Setup Assistant, 308
- SGID, 194
- Shell, 294
- shoebox app, 181
- Sichere Enklave, 230
- sicherer Modus, 258
- Sicherheit, 3, 15, 20, 151, 194, 289
- Sicherheitseinschätzung, 187
- Sicherheitskomponente, 4
- Sicherheitsprüfung, 8
- Sicherheitsstandard, 18
- Sicherheits-Updates, 129
- sichtbar, 164
- Sichtbarkeit, 148, 165
- Sidecar, 230
- Signatur, 129
- Signatur (Prozessor), 124
- Signpost, 142
- Simultanes Multithreading, 122
- Sitzung, 93
- S.M.A.R.T., 310
- Smart Queue Management, 120
- Smartcard, 7
- SMB, 92, 198
- SMBIOS, 125
- SMC, 101, 124
- SoC, 125
- Socket, 114
- Softwareaktualisierung, 17, 18
- Software-Entwickler, 260
- Softwareupdate, 3
- softwareupdate (Befehl), 68
- Softwareupdate (Karte), 68
- Solid-State-Laufwerk, 95
- source, 142
- Speicher, 86, 124, 309
- Speicher, löscher, 224
- Speicherabzug, 178
- Speichergröße, 16, 260
- Speicherkapazität, 93
- Speichermanagementeinheit, 86
- Speicherplatz, 222
- Speicherraum, 86
- Speichersteckplatz, 125
- Speicherverbrauch, 46, 133
- spezielles Recht, 192
- Spindelmotor, 239
- Spotlight, 21, 28, 153, 175, 243, 293
- Spotlight-Kommentar, 162
- Spotlight-Sperre, 246
- Sprache, 268, 273
- SQM, 120
- SSD, 95
- SSD-Verschlüsselung, 125
- Staging, 37
- Standard, 17, 269
- Standardeinstellungen, 17
- Standortlizenz, 320
- Start (von Programmen), 183
- Startdienste, 289
- Startobjekt, 306
- Startsprache, 268
- Startumgebungsbeschränkung, 275
- Startzeit, 128
- Statistik, 86, 103
- Statistik (Time Machine), 44
- Status, 29
- Steckbrücke, 125
- Steckverbinder, 125
- Stepping, 124
- Steuerungsfenster, 8
- Stichwortsuche, 11
- sticky, 194, 206
- Stiftsymbol, 199
- Stillstandsbericht, 133
- Subsystembezeichner, 138
- Suche, 243
- Suche (E-Mail), 293
- Suchfeld, 11
- Suchindex, 293
- SUID, 194, 206
- Support-Richtlinie, 2
- Symbol, 12, 288
- Symbol-Caches, 36
- symbolischer Link, 90, 145, 156, 204
- Symboleiste, 10
- Synchronisation, 81, 286
- System Integrity Protection, 18
- System Management BIOS, 125
- System Management Controller, 101, 124
- System on a chip, 125
- Systemabsturz, 133
- Systemanforderungen, 3
- Systemdaten, 122
- Systemeinstellungen, 4, 68, 76, 129, 130, 170, 176, 239, 245, 268, 269, 273, 294, 295
- Systemgerät, 125

Systeminformationen, 122, 286
Systemintegritätsschutz, 18, 31, 37, 126
Systemkern, 126, 178, 257
SystemLoad, 103
Systemplatine, 125
Systemprotokoll, 132
Systemstart, 256
Systemstartsprache, 268
Systemupdatequelle, 126
Systemverwalter, 3, 16, 135, 270
systemweiter Cache, 31

T

T2-Prozessor, 101
Tab, 10
Tag, 81, 162
Taktfrequenz, 124
Tastaturbelegung, 269
Tavares, Stafford, 248
Technische Hinweise, 321
Teilen, 289
Teilen & Zugriffsrechte, 199
Telefonieüberwachung, 134
Temporärordner, 299
Termin, 279
Terminal, 294
Terminplan, 336
Test, 92
Testmodus, 17, 313
TextEdit, 126
Throttling, 239
Thunderbolt, 311
Ticket für Testmodus, 313
Time Capsule, 39
Time Machine, 39, 162, 244, 269
Time Machine X, 40
Time Machine-Dateifreigabe, 39
Time-Sharing, 103
TinkerTool, 3, 22, 165, 294
TinkerTool 9, 23
TinkerTool System 1, 2
TinkerTool System 4, 2
TinkerTool System 5, 2
TinkerTool System 6, 2
TinkerTool System 7, 2
TinkerTool System 8, 2
TinkerTool System 9, 2
TinkerTool System Release 2, 2
Tippen, 256
Toneffekt, 92
totes Pixel, 105
Touch ID, 5, 7, 256

TouchID, 125
Traceroute, 116
Transportplatte, 176
Treiber, 258
Trennung, Benutzerrechte, 4
Trim-Befehl, 95
trimforce, 96
ttsfrm, 109
Typcode, 148, 165
Typmarkierung, 153

U

Überbuchung, 223
Überprovisionierung, 98
überprüft, 310
Überprüfung (Time Machine), 44, 60
Übersetzung, 292
übertragen (Rechte), 203
Übertragungsprotokoll, 90
UFS, 198
Uhrzeit, 81
umgekehrte Reihenfolge, 284
Umschalttaste, 258
umsortieren (ACL), 203
Unicode, 159
Unified Logging, 137
Universal Unique Identifier, 241, 286
universeller einzigartiger Bezeichner, 241
UNIX, 192, 198
Unix, 28, 103
UNIX-Pfad, 12
unknown, 193
unsichtbar, 148
untätig, 259
Unterordner, 196
Update, 319
Uptime, 128
URL, 187
USB, 311
USB-Flash-Laufwerk, 217
UTF-8, 159
UUID, 214, 241, 286

V

Vereinheitlichte Protokollierung, 137
vererben, 195
Vererbung, 196
verfügbarer Speicher, 222
Vergrößerungsglas, 285, 294
Verknüpfung, 154
verschlüsselte Sicherung, 39
Verschlüsselung, 265

Version, 272
 versteckt, 148, 164, 175
 Vertrauen, 152
 Vertrauensprüfung, 134
 vertraulich, 135, 193, 245
 Vertrieb, 315
 verwaist, 167, 170
 verwaiste Zugriffssteuerungsliste, 209
 Verwalter, 270, 308, 313
 Verwalterautorisierung, 16
 verweigern, 193, 195
 verwerfen, 33
 Verzeichnis, 26
 Verzeichnisdienst, 25, 214, 270
 Verzeichnisdienstserver, 16, 203
 Verzeichnisknoten, 26
 VFAT, 198
 Virens Scanner, 129
 Virtuelle Maschine, 219, 221
 virtueller Speicher, 86
 Vollbildmodus, 11
 voller Name, 214
 Vollzugriff, 201
 Volume, 243
 Volume (Time Machine), 43, 59
 Volume-Eigentum, 230
 Volumenlizenz, 320
 Vorabtestprogramm, 126
 Vordefinieren von Rechten, 205
 Vorschaubild, 162

W

Währung, 315
 Warenzeichen, ii
 Wartung, 25
 Web-Browser, 126, 255
 Web-Cache, 30
 WebDAV, 198
 Web-Schnittstelle, 255
 Web-Seite, 18
 Werkseinstellung, 17, 314
 Werkzustand, 219
 whois, 117
 wiederherstellen, 33
 Wiederherstellungs-Betriebssystem, 108
 Wiederherstellungspunkt, 49, 64
 Wiederherstellungsschlüssel, 231, 265
 Wiederherstellungssystem, 19, 49, 64, 258
 Wiederherstellungs-Volume, 216
 wiederkehrendes Energieereignis, 279
 Windows, 175, 198
 wirksames Zugriffsrecht, 206

WLAN-Schnittstelle, 248
 Wörterbuch, 290
 wortreich, 257

X

Xcode, 73
 XID, 234
 XProtect, 129, 220

Z

Zahlung, 315
 Zeichen, 34
 Zeit, 81
 Zeitattribute, 150
 Zeitintervall für Datensicherung, 39
 Zeitlupe, 176
 Zeitplan, 279
 ZFS, 198
 Ziehen, 13
 Ziehen und Ablegen, 180
 Zip-Registrierungsdatei, 317
 Zugriffsrecht, 192, 195, 199, 205
 Zugriffsrechtsfilter, 251
 Zugriffssteuerungseintrag, 195
 Zugriffssteuerungsliste, 192, 195
 zurücknehmen (Registrierung), 319
 zurücksetzen, 17
 zurückstellen, 17
 Zwangslöschung, 157
 Zweig, benannter, 162
 Zwei-Wege-Zufallsschlüssel, 248