Dokumentation 0912-1979/2

TinkerTool System 7

Referenzhandbuch

Marcel Bresink
Software-Systeme

MBS

Version 7.99, 1. Oktober 2024. Deutsche Ausgabe.
MBS-Dokumentation 0912-1979/2

© Copyright 2003 – 2024 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 7? . . . 1
1.1.1 Die verschiedenen Funktionsbereiche von TinkerTool System 7 . . . 2
1.1.2 Systemanforderungen . . . 3
1.2 Die Sicherheitsrichtlinien von TinkerTool System . . . 3
1.2.1 Sicherheitsarchitektur . . . 3
1.2.2 Bestätigen eines privilegierten Vorgangs . . . 4
1.2.3 Technische Details für fortgeschrittene Benutzer . . . 7
1.2.4 Entfernen alter Generationen der Sicherheitskomponente . . . 7
1.3 Grundlegende Bedienungshinweise . . . 8
1.3.1 Das Steuerungsfenster von TinkerTool System . . . 8
1.3.2 Suche nach Funktionen per Stichwort . . . 10
1.3.3 Verwenden der Touch Bar . . . 10
1.3.4 Kontexthilfe . . . 11
1.3.5 Das Dockmenü . . . 11
1.3.6 Felder für Dateisystemobjekte . . . 11
1.3.7 Verstehen, wann Änderungen aktiv werden . . . 12
1.3.8 Allgemeine Einstellungen . . . 13
1.3.9 Kartensteuerung . . . 13
1.3.10 Sicherheit . . . 14
1.3.11 Anzeigen von Speichergrößen . . . 15
1.3.12 Andere Einstellungen . . . 15
1.3.13 Alle dauerhaften Änderungen an Systemeinstellungen rückgängig machen . . . 16
1.3.14 Suche nach Softwareaktualisierungen . . . 17
1.4 Systemintegritätsschutz . . . 17
1.4.1 Technischer Hintergrund . . . 17
1.4.2 Abschalten des Schutzes . . . 18
1.5 Datenschutzeinstellungen Ihres Mac . . . 19
1.5.1 Hintergrundinformationen . . . 19
1.5.2 Datenschutzeinstellungen, die TinkerTool System betreffen . . . 20
1.5.3 Ändern der Datenschutzeinstellungen . . . 20
1.6 TinkerTool in TinkerTool System 7 einbinden . . . 21
1.6.1 Einbindung einschalten . . . 21
1.6.2 Einbindung abschalten . . . 22

2 Systemwartung **23**
2.1 Die Einstellungskarte Wartung . . . 23
2.1.1 Verzeichnis-Cache . . . 23
2.1.2 Verzeichnisdaten exportieren . . . 24

2.1.3 Locate-Datenbank . . . 26
2.1.4 Gemeinsamer Benutzerordner . . . 27
2.2 Die Einstellungskarte Caches . . . 27
2.2.1 Ungeschützte und geschützte Caches . . . 29
2.2.2 Verwenden der Cache-Wartungsfunktionen . . . 29
2.2.3 Schrift-Caches . . . 31
2.2.4 Symbol-Caches . . . 32
2.2.5 Die Staging-Ablage von Treibern . . . 33
2.3 Die Einstellungskarte Time Machine X . . . 35
2.3.1 Time Machine-Grundlagen . . . 35
2.3.2 Allgemeine Hinweise zum Arbeiten mit der Time Machine-Karte . . . 35
2.3.3 Die unterschiedlichen Versionen von Time Machine für macOS 10 und macOS 11 . . . 35
2.3.4 Wartung nach dem Austausch einer Datenquelle von Time Machine 36
2.3.5 Überprüfung und Statistik der Datensicherung . . . 39
2.3.6 Vergleich von Time Machine Sicherungsschnappschüssen . . . 42
2.3.7 Arbeiten mit lokalen APFS-Schnappschüssen . . . 45
2.3.8 Löschen von Time Machine-Sicherungsdaten . . . 48
2.3.9 Auslesen von Time Machine-Protokollen . . . 49
2.4 Die Einstellungskarte Time Machine . . . 51
2.4.1 Wartung nach dem Austausch einer Datenquelle von Time Machine (Moderner Betrieb) . . . 52
2.4.2 Überprüfung der Datensicherung . . . 55
2.4.3 Vergleich von Time Machine Sicherungsschnappschüssen (Moderner Betrieb) . . . 57
2.4.4 Arbeiten mit lokalen APFS-Schnappschüssen (Moderner Betrieb) . . . 60
2.4.5 Löschen von Time Machine-Schnappschüssen . . . 62
2.5 Die Einstellungskarte Fehler . . . 63
2.5.1 Beheben von Problemen mit der Softwareaktualisierung von macOS 63
2.5.2 App Store-Aktualisierungen . . . 65
2.5.3 Xcode-Schlüsselbunde . . . 68
2.5.4 Netzwerk Bedienelemente . . . 69
2.5.5 Löschen von Partitionierungsdaten auf Platten zur Lösung von Problemen mit dem Festplattendienstprogramm . . . 71
2.6 Die Einstellungskarte Diagnose . . . 73
2.6.1 RAM-Größe auswerten . . . 73
2.6.2 Finder Kopieren testen . . . 77
2.6.3 Optische Disks inspizieren . . . 80
2.6.4 SSDs . . . 82
2.6.5 Flash-Zustand . . . 83
2.6.6 Schnelltest mit Kühlungslüftern durchführen . . . 88
2.6.7 Anmeldezeitabrechnung . . . 90
2.6.8 Monitore testen . . . 92
2.7 Die Einstellungskarte Notfallwerkzeug . . . 94
2.7.1 Einführung in das Notfallwerkzeug . . . 94
2.7.2 Ausdrucken der Anleitung . . . 95
2.7.3 Struktur des Startbefehls . . . 95
2.7.4 Verwenden des Notfallwerkzeugs . . . 97
2.7.5 Alte Versionen des Notfallwerkzeugs . . . 97
2.8 Die Einstellungskarte Netzwerk . . . 98
2.8.1 Informationen über Netzwerkschnittstellen . . . 98
2.8.2 Routing-Tabellen und Netzwerkstatistiken . . . 99

2.8.3 Netzwerkverbindung per Echosignal prüfen 100
2.8.4 Zuordnung zwischen Host-Namen und Adressen ermitteln 101
2.8.5 Weg von Datenpaketen nachverfolgen 103
2.8.6 Datenbanken des Whois-Dienstes abfragen 103
2.8.7 Nutzerinformationen per Finger-Dienst ermitteln 104
2.8.8 Offene IPv4-Ports suchen 106
2.8.9 Antwortverhalten (nur macOS 12 oder höher) 106
2.9 Die Einstellungskarte Info 109
2.9.1 Systemdaten 109
2.9.2 Malware-Schutz 114
2.9.3 Sperrliste Programme 116
2.9.4 Klassische Protokolle und Berichte 118
2.9.5 Moderne Protokollierung und Ablaufverfolgung 123

3 Dateioperationen 129
3.1 Die Einstellungskarte Ablage 129
3.1.1 Link 129
3.1.2 Schutz 131
3.1.3 Attribute 132
3.1.4 Quarantäne 134
3.1.5 Inhalt 135
3.1.6 Zwangslöschung 136
3.1.7 Verschachtelung 137
3.1.8 Erweiterte Attribute 141
3.2 Die Einstellungskarte Bereinigen 143
3.2.1 Allgemeine Hinweise zum Löschen von Dateien 143
3.2.2 Versteckte Hilfsdateien 143
3.2.3 Protokollarchive 146
3.2.4 Absturzberichte 146
3.2.5 Verwaiste Dateien 149
3.2.6 Aliase 152
3.2.7 Entfernbare Platten 153
3.2.8 Speicherabzüge 155
3.3 Die Einstellungskarte Programme 155
3.3.1 Deinstallationsassistent 155
3.3.2 Entfernen von Software-Komponenten und zugehöriger Dateien . . 157
3.3.3 Besonderer Start von Programmen 160
3.3.4 Datenschutz 162
3.3.5 Sicherheitsprüfung 163
3.4 Die Einstellungskarte ACL-Rechte 167
3.4.1 Einführung in Berechtigungen 167
3.4.2 POSIX-Berechtigungen 168
3.4.3 Zusätzliche Berechtigungsmarkierungen 169
3.4.4 Zugriffssteuerungslisten 170
3.4.5 Zugriffsrechte zeigen oder einstellen 174
3.4.6 Wirksame Zugriffsrechte 181
3.4.7 Spezielle Rechte 181
3.4.8 Berechtigungen in einem Benutzerordner auf Standardwerte stellen 184
3.4.9 Interne Identifikationen von Benutzer- und Gruppen-Accounts finden 186
3.5 Die Einstellungskarte Installationsmedien 188
3.5.1 Betriebssysteminstallation 188
3.5.2 Notwendige Voraussetzungen 189

3.5.3 Herunterladen von Installationsprogrammen ohne den App Store . 190
3.5.4 Anlegen des Installationsmediums 191
3.5.5 Ein Installationsmedium als ISO-Datei anlegen 192
3.5.6 Reparieren der Oktober–2019-Ausgabe des Sierra-Installers 192
3.5.7 Unzuverlässiges Verhalten von macOS 11 Big Sur 193
3.6 Die Einstellungskarte Systemsicherheit 193
3.6.1 Programmintegrität 193
3.6.2 Speicherplatz 195
3.6.3 Systemprotokoll auf verdächtige Benutzeraktivität prüfen 198
3.6.4 EFI-Firmware 199
3.6.5 Broadcom® Ethernet 202
3.7 Die Einstellungskarte APFS 203
3.7.1 Überblick über APFS-Volumes 203
3.7.2 Arbeiten mit APFS-Schnappschüssen 206
3.7.3 Kopieren von APFS-Daten 207

4 Systemeinstellungen 211
4.1 Die Einstellungskarte System 211
4.1.1 Laufwerk 211
4.1.2 Volumes 213
4.1.3 Spotlight 215
4.1.4 Spotlight-Indexdatenbanken 216
4.1.5 Netz 217
4.1.6 Einstellungskarten 221
4.1.7 Zugriffsrechtsfilter für neue Dateisystemobjekte 223
4.1.8 Verschiedenes 225
4.2 Die Einstellungskarte „Immer an“-Mobilcomputer 228
4.2.1 Automatisches Einschalten 228
4.3 Die Einstellungskarte Systemstart 229
4.3.1 Hinweise zu Macs mit Apple-Prozessoren 229
4.3.2 Optionen 230
4.3.3 Job-Übersicht 232
4.3.4 NVRAM 236
4.4 Die Einstellungskarte Anmeldung 238
4.4.1 Einstellungen 238
4.4.2 Benutzer ausblenden 240
4.5 Die Einstellungskarte Programmsprache 241
4.5.1 Startsprache für ein Programm dauerhaft überschreiben 243
4.6 Die Einstellungskarte Cloud-Schutz 244

5 Benutzereinstellungen 247
5.1 Die Einstellungskarte Benutzer 247
5.1.1 Einstellungen („Präferenzen“) 247
5.1.2 Benutzte Objekte 251
5.1.3 Startdienste 252
5.1.4 Wörterbücher 254
5.1.5 Reparatur 255
5.1.6 Info 257
5.2 Arbeiten mit Einstellungskarten aus TinkerTool 257

6 Arbeiten in der macOS-Wiederherstellung 259
6.1 Allgemeine Informationen . . . 259
6.1.1 Das Hauptmenü des Programms . . . 259
6.1.2 Beenden des Programms . . . 261
6.2 macOS-Wiederherstellung: Grundfunktionen . . . 261
6.2.1 Reparieren des Temporärordners des Systems . . . 261
6.3 macOS-Wiederherstellung: Arbeiten mit Benutzer-Accounts . . . 262
6.3.1 Auswahl des zu bearbeitenden Benutzer-Accounts . . . 262
6.3.2 Deaktivieren von beschädigten Einstellungsdateien . . . 262
6.3.3 Deaktivieren aller Caches eines Benutzers . . . 262
6.3.4 Reaktivieren aller Caches eines Benutzers . . . 264
6.3.5 Deaktivieren aller Einstellungen eines Benutzers . . . 264
6.3.6 Reaktivieren aller Einstellungen eines Benutzers . . . 265
6.4 macOS-Wiederherstellung: Verwaltung und Reparatur . . . 265
6.4.1 Deaktivieren von beschädigten Systemeinstellungsdateien . . . 265
6.4.2 Deaktivieren systembezogener Caches . . . 265
6.4.3 Reaktivieren systembezogener Caches . . . 267
6.4.4 Zurücksetzen von gemanagten Einstellungen . . . 267
6.4.5 Anmeldebildschirm zurücksetzen . . . 267
6.4.6 Entfernen von angepassten Startobjekten . . . 268
6.5 macOS-Wiederherstellung: Fortgeschrittene Funktionen . . . 270
6.5.1 Abschalten der automatischen Anmeldung . . . 270
6.5.2 Erneuten Lauf des Einrichtungsassistenten erzwingen . . . 270
6.6 macOS-Wiederherstellung: Abrufen von Informationen . . . 271
6.6.1 Hardware- und Systemdaten . . . 271
6.6.2 S.M.A.R.T.-Status von Festplatten . . . 272
6.6.3 Versionsdaten von TinkerTool System für macOS-Wiederherstellung 273

7 Allgemeine Hinweise 275
7.1 Registrierung und Freischalten des Programms . . . 275
7.1.1 Testmodus . . . 275
7.1.2 Demomodus . . . 276
7.1.3 Uneingeschränkte Nutzung . . . 277
7.1.4 Bestellung von Registrierungscodes . . . 277
7.1.5 Registrieren per Datei oder per Texteingabe . . . 277
7.1.6 Freischalten der Software mit einer Registrierungsdatei . . . 277
7.1.7 Freischalten der Software mit einer Registrierungs-Mail . . . 278
7.1.8 Eingeben einer per Mail zugesandten Registrierung von Hand . . . 279
7.1.9 Eingeben einer Crossgrade- oder Upgrade-Registrierung . . . 279
7.1.10 Freischaltung zurücknehmen . . . 280
7.1.11 Vorgehen bei Aktualisierungen und Migrationen . . . 280
7.1.12 Ein Kombi-Ticket für Upgrade-Lizenzen anlegen . . . 280
7.1.13 Arbeiten mit Volumenlizenzen . . . 281
7.1.14 Anlegen einer Anforderungsdatei für Automatische Volumenlizenzierung . . . 281
7.1.15 Verwenden der Datei zur automatischen Registrierungsanforderung 282
7.2 Wichtige technische Hinweise . . . 282
7.2.1 Abhilfen bei bestimmten Problemen . . . 282
7.3 Versionshistorie . . . 284
7.3.1 Release 7.99 (Build 241001) . . . 284
7.3.2 Release 7.98 (Build 240214) . . . 284
7.3.3 Release 7.97 (Build 230822) . . . 284

7.3.4 Release 7.96 (Build 230605) 284
7.3.5 Release 7.95 (Build 230414) 284
7.3.6 Release 7.94 (Build 230207) 285
7.3.7 Release 7.93 (Build 221205) 285
7.3.8 Release 7.92 (Build 221026) 285
7.3.9 Release 7.91 (Build 221012) 285
7.3.10 Release 7.9 (Build 220913) 285
7.3.11 Release 7.9 (Build 220809) 285
7.3.12 Release 7.89 (Build 220711) 285
7.3.13 Release 7.88 (Build 220614) 286
7.3.14 Release 7.87 (Build 220509) 286
7.3.15 Release 7.86 (Build 220317) 287
7.3.16 Release 7.85 (Build 220214) 288
7.3.17 Release 7.8 (Build 220112) 288
7.3.18 Release 7.71 (Build 211122) 289
7.3.19 Release 7.7 (Build 211021) 289
7.3.20 Release 7.6 (Build 210927) 289
7.3.21 Release 7.5 (Build 210824) 290
7.3.22 Release 7.41 (Build 210721) 290
7.3.23 Release 7.4 (Build 210621) 291
7.3.24 Release 7.3 (Build 210518) 291
7.3.25 Release 7.21 (Build 210504) 292
7.3.26 Release 7.2 (Build 210414) 292
7.3.27 Release 7.12 (Build 210208) 293
7.3.28 Release 7.11 (Build 210114) 294
7.3.29 Release 7.1 (Build 201214) 294
7.3.30 Release 7.01 (Build 201119) 295
7.3.31 Release 7.0 (Build 201111) 295
7.3.32 Release 6.93 (Build 201007) 296
7.3.33 Release 6.92 (Build 200910) 297
7.3.34 Release 6.91 (Build 200804) 297
7.3.35 Release 6.9 (Build 200702) 297
7.3.36 Release 6.89 (Build 200527) 298
7.3.37 Release 6.88 (Build 200427) 298
7.3.38 Release 6.87 (Build 200422) 298
7.3.39 Release 6.86 (Build 200323) 299
7.3.40 Release 6.85 (Build 200218) 299
7.3.41 Release 6.84 (Build 200117) 300
7.3.42 Release 6.83 (Build 191211) 300
7.3.43 Release 6.82 (Build 191114) 301
7.3.44 Release 6.81 (Build 191030) 301
7.3.45 Release 6.8 (Build 191009) 302
7.3.46 Release 6.7 (Build 190916) 302
7.3.47 Release 6.6 (Build 190812) 303
7.3.48 Release 6.51 (Build 190625) 304
7.3.49 Release 6.5 (Build 190611) 304
7.3.50 Release 6.4 (Build 190508) 304
7.3.51 Release 6.3 (Build 190327) 305
7.3.52 Release 6.2 (Build 190212) 305
7.3.53 Release 6.1 (Build 190121) 306
7.3.54 Release 6.02 (Build 181122) 307
7.3.55 Release 6.01 (Build 181002) 307

7.3.56 Release 6.0 (Build 180918) 308

A Aufgaben und Lösungen **309**
A.1 Wo ist diese Funktion jetzt? 309
A.2 Sollte ich regelmäßige Wartungsarbeiten durchführen? 309
A.3 Wie kann ich das System reparieren, wenn macOS durcheinandergewürfelten Text bei der Verwendung bestimmter Schriftarten zeigt? 311
A.4 Wie kann ich die tatsächlichen Zugriffsrechte auf eine Datei oder einen Ordner anzeigen lassen? 312
A.5 Was sollte ich tun, wenn macOS die Online-Hilfe nicht mehr öffnen kann? 312
A.6 Freischalten des Programms 312

Kapitel 1

Einführung

1.1 Was ist TinkerTool System 7?

TinkerTool System 7 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 Bedieneroberfläche 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 (nur für bestimmte Betriebssystemversionen), das bei der Fehlersuche und Reparatur von macOS hilft, in Fällen, in denen die grafische 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 Bedieneroberfläche 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 „7“ weglassen. Beachten Sie allerdings, dass es in Wirklichkeit sechs 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

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 bösartigen Benutzerprogrammen abgefangen werden können. Systemverwalter von großen Systeminstallationen können die Sicherheitsrichtlinien für TinkerTool System feinanpassen, zum Beispiel indem bestimmten Klassen von Systemverwaltergruppen unterschiedliche Zugriffsrechte auf bestimmte Operationen erteilt werden. Um dies möglich zu machen, gliedert sich TinkerTool System nahtlos in die Datenbank der Sicherheitsrichtlinien von macOS ein.
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 Hilfeknopf 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 7

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 7 zu nutzen, brauchen Sie einen *Apple-Computer*, auf dem das folgende Betriebssystem installiert ist:

- macOS 11 Big Sur
- macOS 12 Monterey

Es wird empfohlen, auf die neueste Version von macOS zu aktualisieren, die von Apple verfügbar ist. Dies kann über die Funktion **Automatische Software-Aktualisierung** 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 entgegen nimmt. 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 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:
Die laufende Benutzersitzung muss einem Administrator gehören: 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. Die Anmeldesitzung, in der TinkerTool System arbeitet, muss auf diesen Benutzer angemeldet sein, oder auf einen anderen, dem ebenso Administrationsrecht erteilt wurde. Es ist also nicht möglich, einen privilegierten Vorgang von einem Benutzer-Account aus aufzurufen, der im Moment nicht als Verwalter angemeldet ist. Sie können während der Bestätigung Ihrer Identität *nicht* vom Programm aus auf einen anderen Benutzer umschalten, indem Sie dessen Name und Kennwort in TinkerTool System eingeben.

> Dies entspricht den klassischen Sicherheitsregeln, die für die ersten Generationen von macOS (damals Mac OS X) üblich waren und ist strenger als die Regeln, die moderne Versionen von macOS normalerweise für grafische Programme einsetzen. Diese Vorgehensweise ist ähnlich der, die macOS und andere Unix-Systeme für die Nutzung des Befehls *sudo* auf der Befehlszeile verwenden, der ebenso privilegierte Vorgänge einzeln freischaltet.

Wenn Sie gerade mit einem Benutzer-Account arbeiten, der keine Verwaltungsrechte hat, müssen Sie die laufende Bildschirmsitzung aber nicht unbedingt abbrechen, um mit TinkerTool System arbeiten zu können. Wenn Sie im Programm **Systemeinstellungen** den Punkt **Benutzer & Gruppen** > **Anmeldeoptionen** > **Menü für schnellen Benutzerwechsel** eingeschaltet haben, können Sie sich einfach über einen Punkt rechts oben im Menü über die grafische Oberfläche von macOS ummelden und eine zweite Sitzung als Systemverwalter starten. Sie arbeiten dann mit mehreren Bildschirmsitzungen für unterschiedliche Benutzer, zwischen denen Sie schnell hin und her schalten können.
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.

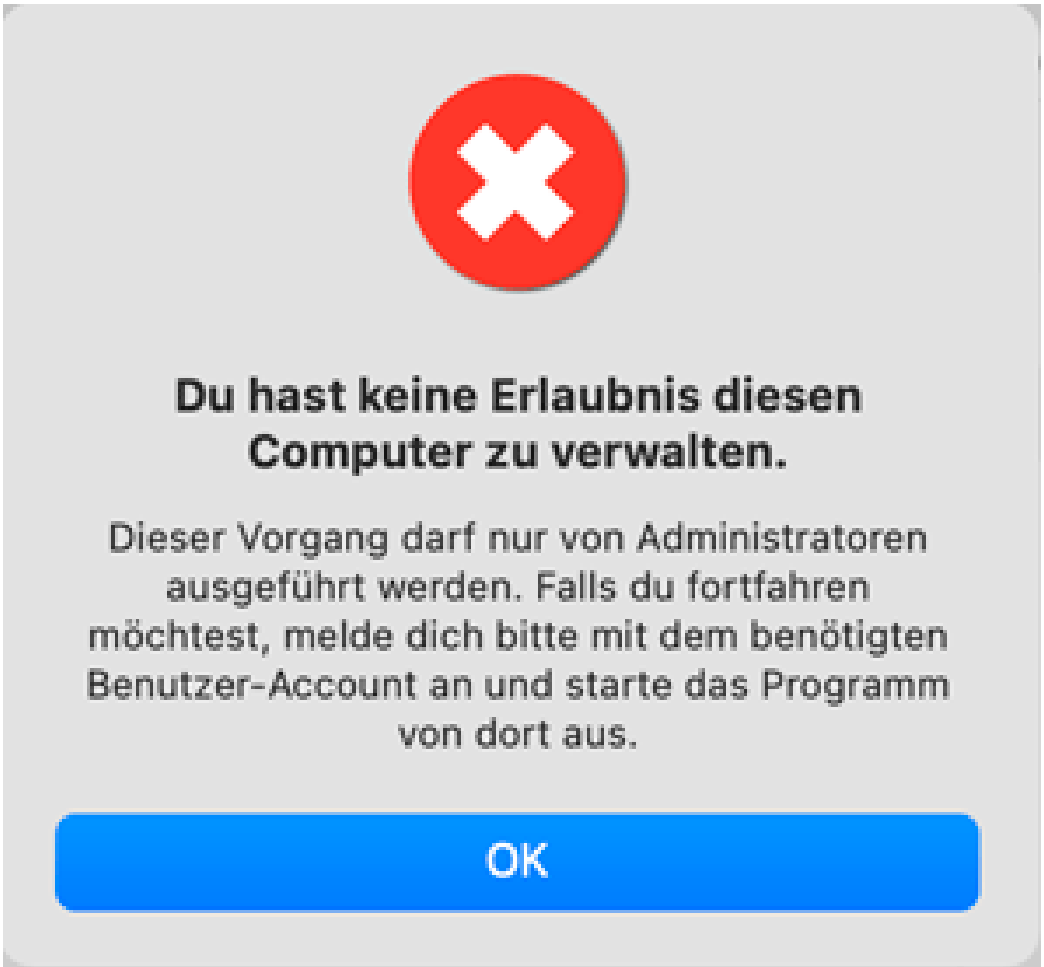

Abbildung 1.1: Die laufende Bildschirmsitzung muss auf einen Benutzer mit Verwalterrecht angemeldet sein.

> 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.

Ein Administrator darf kein leeres Kennwort haben: Obwohl es mit früheren Versionen von macOS möglich war, Benutzer-Accounts mit Verwalterrecht ohne ein Kennwort anzulegen (was konkret bedeutet, dass ein Passwort der Länge Null vorliegt), sehen aktuelle Versionen von macOS dies als Konfigurationsfehler an. Betroffene Administrator-Accounts können sich nicht mehr in allen Fällen authentifizieren und einige Systemdienste werden die Arbeit verweigern. Dies schließt die privilegierten Vorgänge mit ein, die unter Kontrolle von TinkerTool System ausgeführt werden können. Auf normalen Wegen können Accounts ohne Kennwort nicht mehr eingerichtet werden. Falls Sie noch einen solchen Account haben, der aus einer älteren Version von macOS übernommen wurde, müssen Sie für ihn ein Kennwort definieren damit ihm gestattet wird, Funktionen von TinkerTool System zu verwenden, für die privilegierte Vorgänge notwendig sind.
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. Zur Kontrolle wird auf den anstehenden Vorgang außerdem noch einmal in einer kurzen Beschreibung in der *Touch Bar* hingewiesen, so wie im abgebildeten Beispiel. Wie in macOS üblich, können Sie jederzeit wählen, ob Sie sich per Kennwort oder per Fingerabdruck identifizieren möchten.

Abbildung 1.2: Bei Computern mit Touch ID kann die Überprüfung auch per Fingerabdruck erfolgen. Die Touch Bar weist im Klartext darauf hin.

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 kön-

nen, 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.
Die folgenden Abschnitte enthalten Informationen für erfahrene Systemverwalter. Sie können beim ersten Lesen übersprungen werden.

1.2.3 Technische Details für fortgeschrittene Benutzer

Die Sicherheitskomponente wird im Ordner **/Library/PrivilegedHelperTools** abgelegt, der Apples empfohlenen Ort für solche Hilfsprogramme darstellt. Der Name der Komponente lautet **com.bresink.system.privilegedtool-ts7**. macOS startet und beendet das Programm automatisch, wie es gerade erforderlich ist, und vermeidet es, es längere Zeit im Hintergrund laufen zu lassen.
Sie können sich jederzeit dazu entscheiden, das Sicherheitsprogramm ohne Spuren zu entfernen. In diesem Fall verliert TinkerTool System seine Fähigkeit, auf privilegierte Systembereiche zugreifen zu dürfen, so dass das Programm gezwungen wird, sich ebenso abzuschalten. Führen Sie die folgenden Schritte durch, um die Komponente zu entfernen:

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

2. Wählen Sie den Menüpunkt **Zurücksetzen** > **Sicherheitskomponente entfernen** ....

3. Folgen Sie den Anweisungen, die das Programm gibt. Als letzter Schritt dieses Vorgangs beendet sich das Programm selbst.

1.2.4 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. Das Programm weist Sie jeweils darauf hin, falls eine Aktualisierung erforderlich ist und führt dann die notwendigen Schritte selbst durch.
Es kann jedoch Fälle geben, in denen sich eine aktualisierte Sicherheitskomponente so stark von den Vorgängerversionen unterscheidet, dass sie mit diesen nicht kompatibel ist und sie aus technischen Gründen nicht vollautomatisch entfernen kann. 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** ....

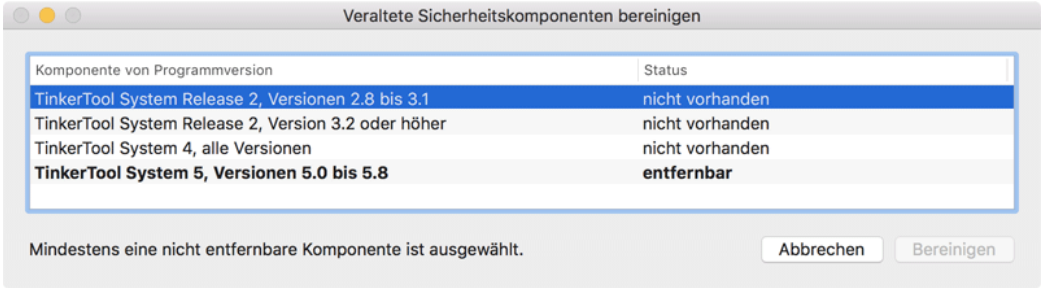

Abbildung 1.3: Veraltete Fassungen des privilegierten Hilfsprogramms können auf Wunsch bereinigt werden.

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.

1.3 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.

Das Steuerungsfenster ist in horizontale Balken unterteilt, welche die verschiedenen Funktionsbereiche des Programms darstellen. Jeder Balken enthält eine Anzahl von Symbolen, die angeklickt werden können, um eine Steuerungskarte zu öffnen, die für die jeweilige Funktionsmenge zuständig ist. Beispielsweise öffnet das Anklicken des Symbols **Info** in der Zeile **Systemwartung** eine Karte mit dem Namen **Info**, die dazu verwendet wird, um auf Detailinformationen über den Computer und das Betriebssystem zuzugreifen. Die Karten verhalten sich ähnlich wie die Punkte aus dem Programm **Systemeinstellungen** von macOS.

Alternativ können Sie auch einen der Punkte im Menü **Darstellung** wählen. Von einer Karte zur nächsten oder zur vorherigen zu wechseln ist möglich, indem Sie auf einen der beiden Pfeilknöpfe in der Symbolleiste des Steuerungsfensters klicken. Das Durchblättern der einzelnen Karten ist zudem über das Menü möglich, indem Sie **Darstellung** > **Zurück**, bzw. **Darstellung** > **Vorwärts** wählen, oder ⌘ + ← / ⌘ + → drücken. Um zurück zur Übersicht über alle Kartensymbole zu kommen, drücken Sie den Knopf mit den kleinen Punkten in der Symbolleiste des Fensters, oder wählen den Menüpunkt **Darstellung** > **Alle Karten einblenden** (⌘ + L).

Abbildung 1.4: Das Steuerungsfenster von TinkerTool System mit integriertem TinkerTool bei Ausführung auf einem mobilen Intel-basierten Mac

> Die Bedeutung der mit Pfeilen markierten Steuerungselemente folgt einer simplen Links-/Rechts-Idee. Falls Sie es bevorzugen, stattdessen in der Historie der getroffenen Auswahl zu navigieren (wie in anderen macOS-Programmen, zum Beispiel Systemeinstellungen oder Safari), ist dies auch möglich, wenn Sie eine entsprechende Benutzereinstellung einschalten (siehe unten).

Sie können auch Steuerung per Tastatur verwenden, um die verschiedenen Einstellungskarten zu öffnen. Um dies zu tun, müssen Sie sicherstellen, dass die Funktion Tastatursteuerung für Ihren Benutzer-Account eingeschaltet ist:

1. Öffnen Sie das Programm **Systemeinstellungen**.
2. Öffnen Sie die Einstellungskarte **Tastatur** und deren Karteireiter **Kurzbefehle**.
3. Sorgen Sie dafür, dass der Punkt **Bewege den Fokus mittels Tastaturnavigation zu Steuerelementen** eingeschaltet ist.

Wenn volle Tastatursteuerung eingeschaltet ist, drücken Sie die Tabulatortaste ⇥ im Steuerungsfenster von TinkerTool System, um den Tastaturfokusring in der Kartenübersicht einzublenden. Sie können danach den Fokusring mit den Pfeiltasten oder Tabulatortasten bewegen. Verwenden Sie die Leertaste, um eine Einstellungskarte zu öffnen.
Auch die einzelnen Karten können in verschiedene Funktionsbereiche unterteilt sein. Um zwischen diesen Funktionen auszuwählen, werden *Karteireiter (Tabs)* verwendet. TinkerTool System behält automatisch, welcher Reiter bei der letzten Benutzung einer Karte offen war. Bei der nächsten Verwendung der Karte wird es automatisch wieder auf den früher ausgewählten Reiter zurückgehen.

1.3.2 Suche nach Funktionen per Stichwort

TinkerTool System bietet eine hohe Zahl unterschiedlicher Funktionen an. Möglicherweise verwenden Sie diese nicht alle regelmäßig und vergessen daher, auf welcher Einstellungskarte und welchem Karteireiter sich diese befinden. Um Ihnen in diesem Fall zu helfen, können Sie nach Funktionen und Einstellmöglichkeiten per Stichwort suchen: Stellen Sie sicher, dass die Symbole für alle Einstellungskarten sichtbar sind, und tippen Sie dann das Wort für das Feature, nach dem Sie suchen, in das Suchfeld in der oberen rechten Ecke des Fensters ein. Nach dem Eintippen der ersten Buchstaben macht TinkerTool System außerdem Vorschläge, die auf Ihrer Eingabe beruhen. Sie können einen dieser Vorschläge durch Anklicken auswählen, oder indem Sie die Pfeiltasten verwenden und dann die Taste ↵ drücken. Dies öffnet die entsprechende Einstellungskarte und deren Karteireiter automatisch. Während der Suche dunkelt TinkerTool System die Übersicht der Symbole ab und beleuchtet diejenigen Punkte, die sich auf Ihr Stichwort beziehen.
Das eingegebene Suchwort kann über die Schaltfläche mit dem Kreuz im Suchfeld gelöscht werden.

1.3.3 Verwenden der Touch Bar

Falls Sie einen Mac mit Touch Bar haben, können Sie auch deren Leiste als Alternative verwenden, um zwischen Einstellungskarten zu navigieren oder nach Funktionen zu suchen. Die Elemente, um zur vorigen oder nächsten Karte zu wechseln, zur Symbolübersicht, oder zur Eingabe eines Suchwortes können auch in der Touch Bar gefunden werden.

Abbildung 1.5: Die Elemente der Symbolleiste stehen auch in der Touch Bar zur Verfügung

1.3.4 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 offenen Karteireiter zeigen. Der Hilfetext ist in die folgenden Abschnitte unterteilt:

- **Was passiert:** eine kurze Beschreibung, welche Funktion im gerade geöffneten Karteireiter 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 Web-Seiten von Apple, die aktuelle Informationen aus erster Hand über das zur Diskussion stehende Thema geben.

1.3.5 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 Karteireiter öffnen, so dass Sie die Gelegenheit haben, Einstellungen zu prüfen und anzupassen, bevor irgendetwas geschieht.

1.3.6 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:

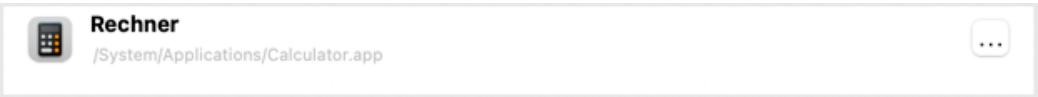

Abbildung 1.6: Pfadeingabefeld

- 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 Ihre 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.

1.3.7 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 verharrt. 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.

1.3.8 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 ⌘ + ,.

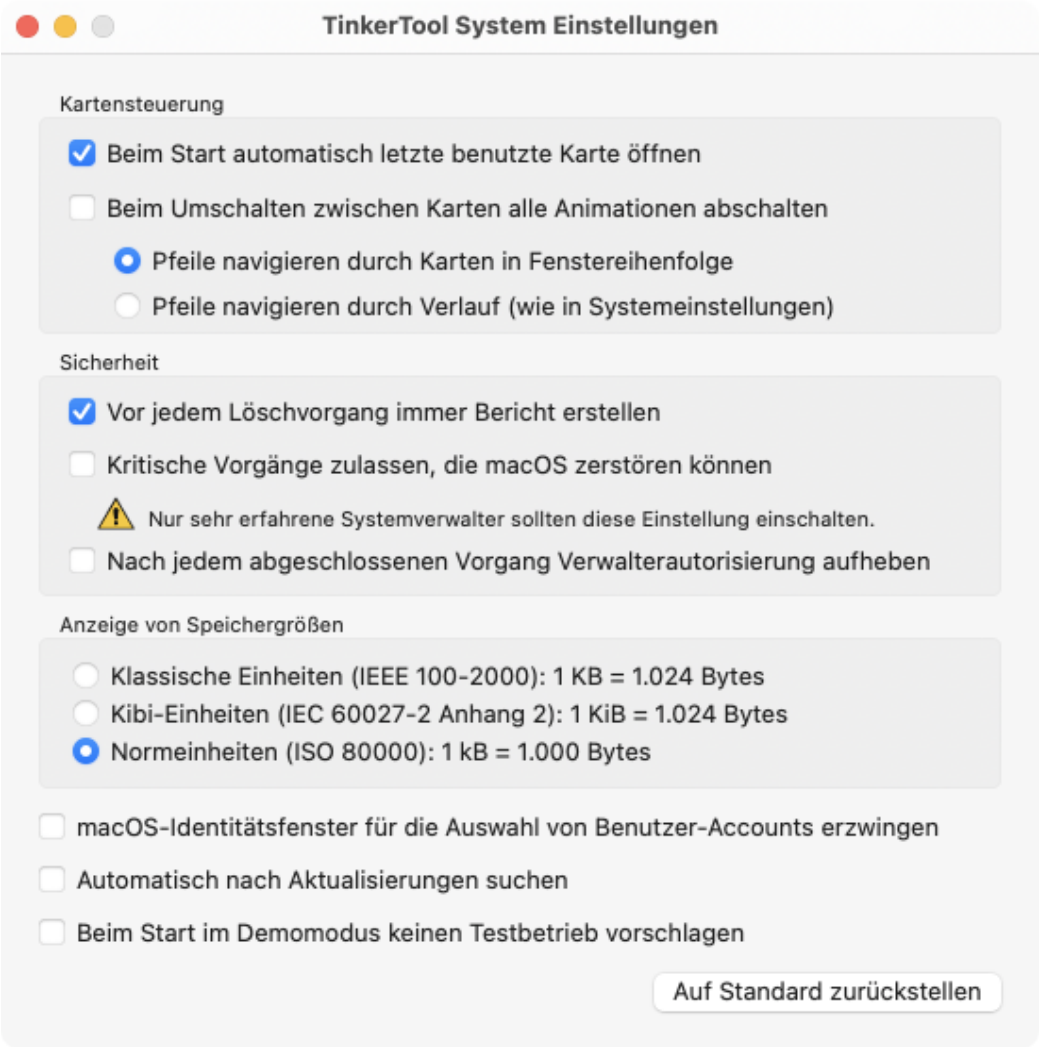

Abbildung 1.7: Das Einstellungsfenster

1.3.9 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.
Falls Sie die kurzen Animationssequenzen nicht mögen, die beim Umschalten der Symbolübersicht auf eine Karte oder beim Hin- und Herschalten zwischen verschiedenen Einstellungskarten angezeigt werden, können Sie alle Animationen deaktivieren, indem Sie den

Punkt **Beim Umschalten zwischen Karten alle Animationen abschalten** ankreuzen.

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**.

1.3.10 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 oder bei der Entfernung von Sprachunterstützungspaketen aus Programmen 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, 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 zwischenzuspeichern 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).

1.3.11 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.

1.3.12 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 interne 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 275).
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.

1.3.13 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 ⇧ + ⌘ + R 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.

1.3.14 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** > **Löschen** > **Löschen erzwingen** 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 der Anzeige Systeminformationen auf der Karte Info (Abschnitt 2.9 auf Seite 109) 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 ⌘ + R 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 Datenschutzeinstellungen 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 **Nicht betriebsbereit!** erscheint in der Symbolleiste 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 **Nicht betriebsbereit!** in der Symbolleiste 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 Datenschutzgenehmigungen erteilt werden:

- **Festplattenvollzugriff**
- **Automation** zwischen TinkerTool System und dem Finder, falls Sie die Funktion **Finder Kopieren testen** auf der Einstellungskarte Diagnose (Abschnitt 2.6 auf Seite 73) 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 **Sicherheit**.
3. Gehen Sie zum Karteireiter **Datenschutz**.
4. Klicken Sie auf das Schloss und identifizieren Sie sich als Benutzer mit Verwaltungsrechten.
5. Wählen Sie den Punkt **Festplattenvollzugriff** aus.
6. Prüfen Sie, ob ein Eintrag für **TinkerTool System** in der Tabelle vorhanden ist. Falls ja, setzen Sie ein Häkchen bei diesem Eintrag. Falls nein, drücken Sie den Knopf **+** unterhalb der Liste der Apps und fügen Sie TinkerTool System zur Tabelle hinzu.
7. Starten Sie TinkerTool System erneut.

1.6 TinkerTool in TinkerTool System 7 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 für** … 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 7* und höher kann Exemplare von *TinkerTool 8* und höher 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 **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 vorgefunden 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.

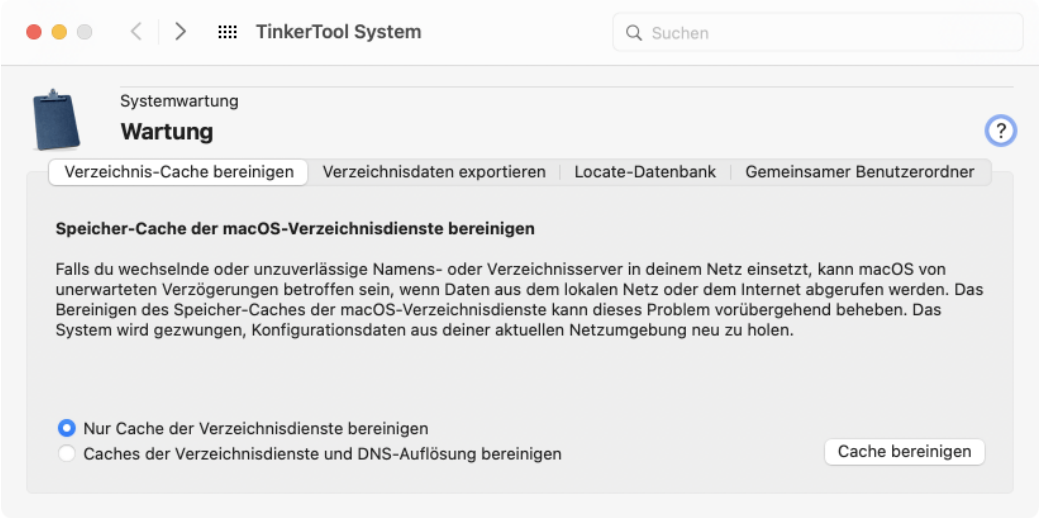

Abbildung 2.1: Verzeichnis-Cache bereinigen

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 Karteireiter **Verzeichnis-Cache** auf der Einstellungskarte **Wartung**.
2. Betätigen Sie einen der Auswahlknöpfe, um anzugeben, ob der Cache der DNS-Auflösung in den Bereinigungsvorgang 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.

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

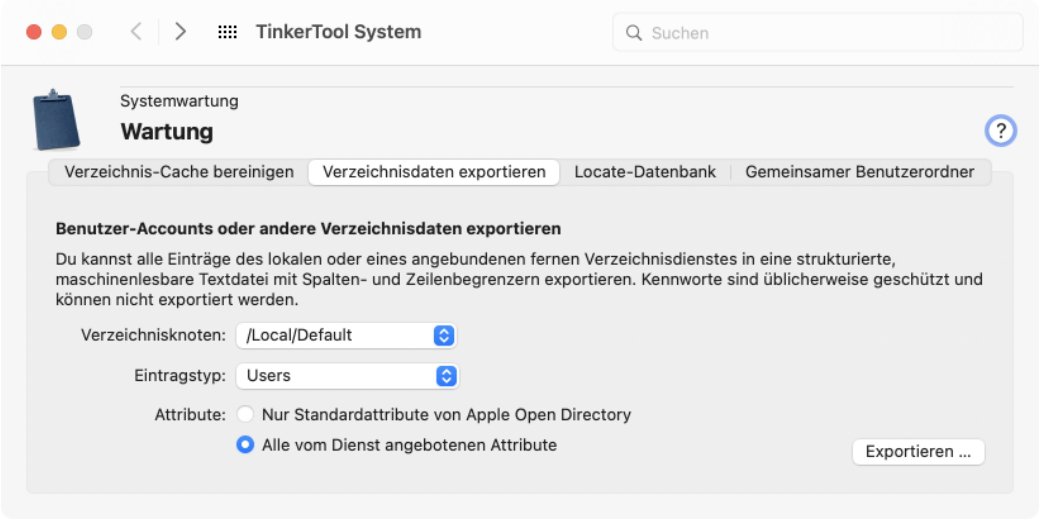

Abbildung 2.2: Exportieren von Verzeichnisdaten

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 Zieldatei 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.

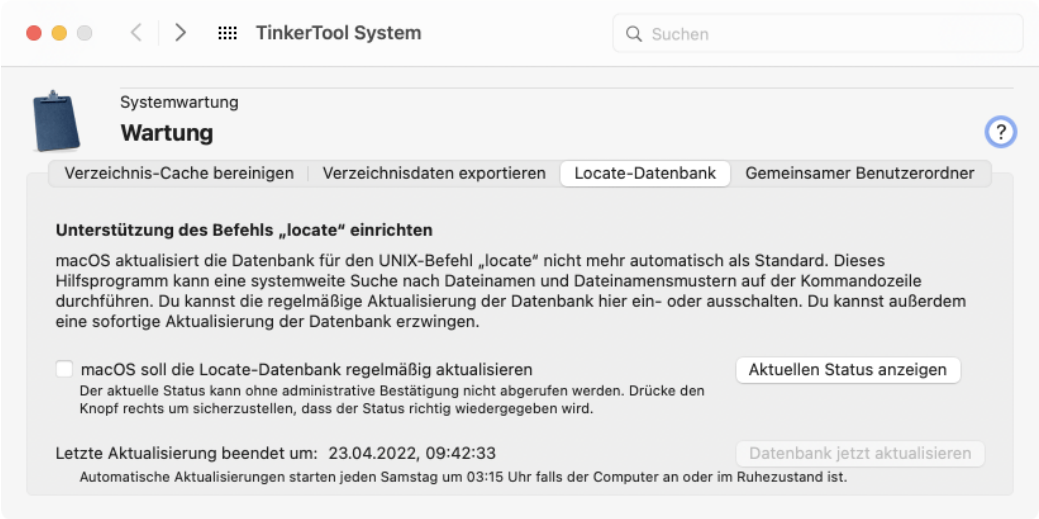

Abbildung 2.3: Locate-Datenbank

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 Karteireiter **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** > **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 iTunes versteckte Inhalte in diesem Ordner, um die Nutzungsrechte für urheberrechtlich geschützte Medien zu verwalten.

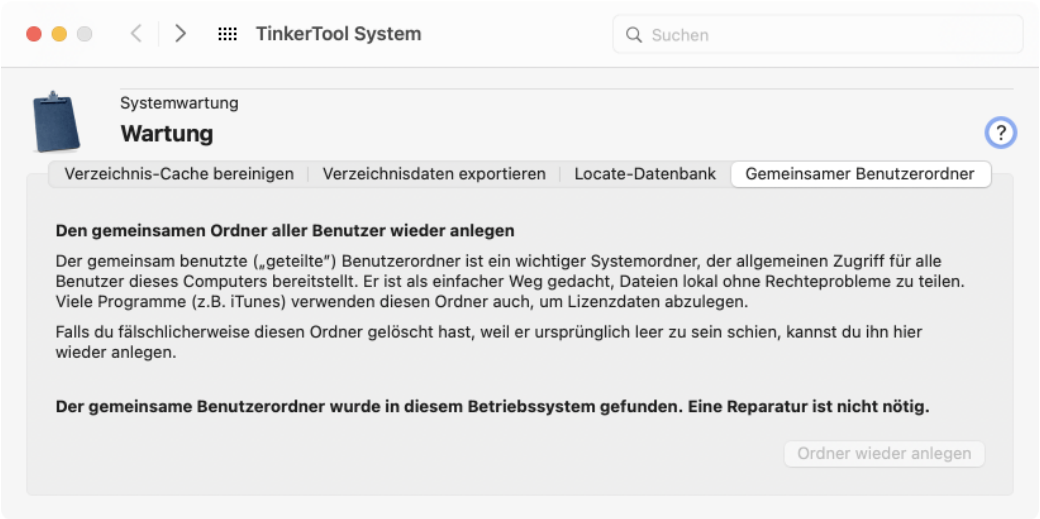

Abbildung 2.4: Gemeinsamer Benutzerordner

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 Karteireiter **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, 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, das 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.

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.

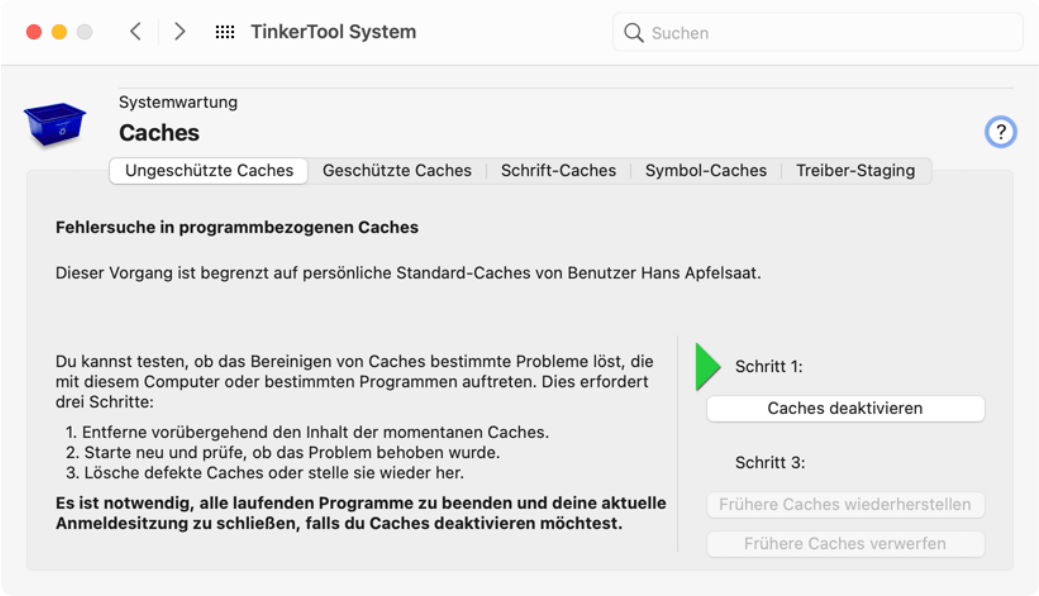

Abbildung 2.5: Ungeschützte Caches

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 des Fensters 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.

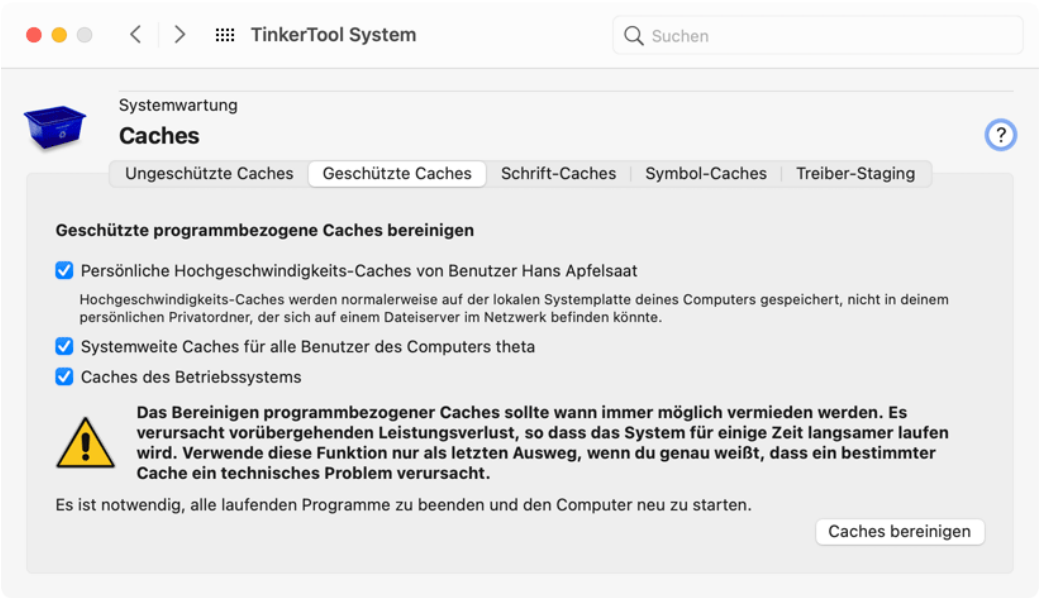

Abbildung 2.6: Bereinigen geschützter Caches

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 Schrift-

sammlung, 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.

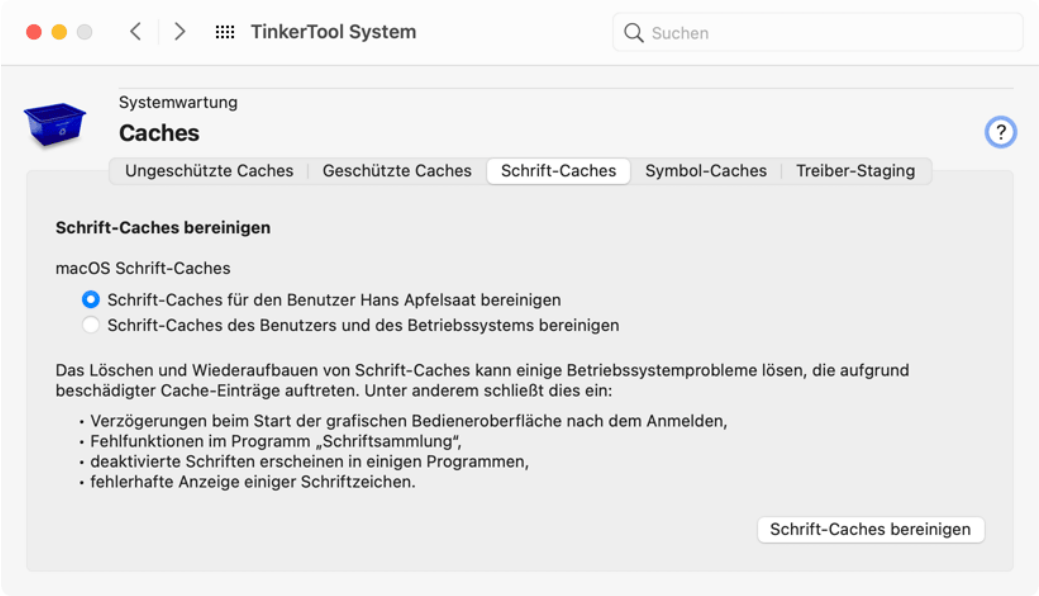

Abbildung 2.7: Schrift-Caches

Falls Sie von einem solchen Problem betroffen sind, kann TinkerTool System Sie beim Bereinigen von Schrift-Caches unterstützen. Der Bereinigungsvorgang 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 Karteireiter **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.

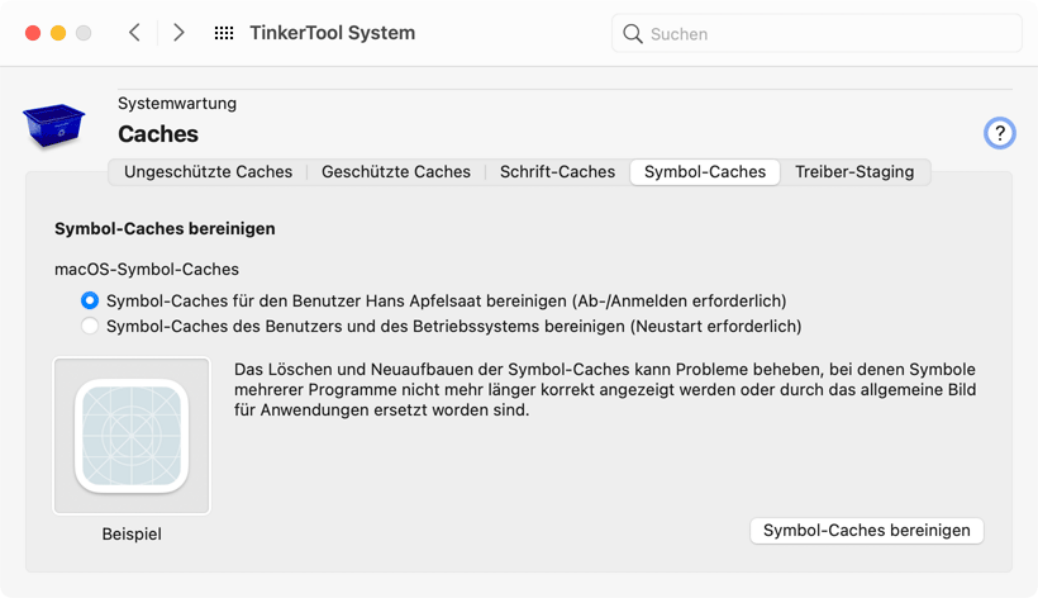

Abbildung 2.8: Symbol-Caches

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 Karteireiter **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** > **Sicherheit** > **Allgemein** 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.

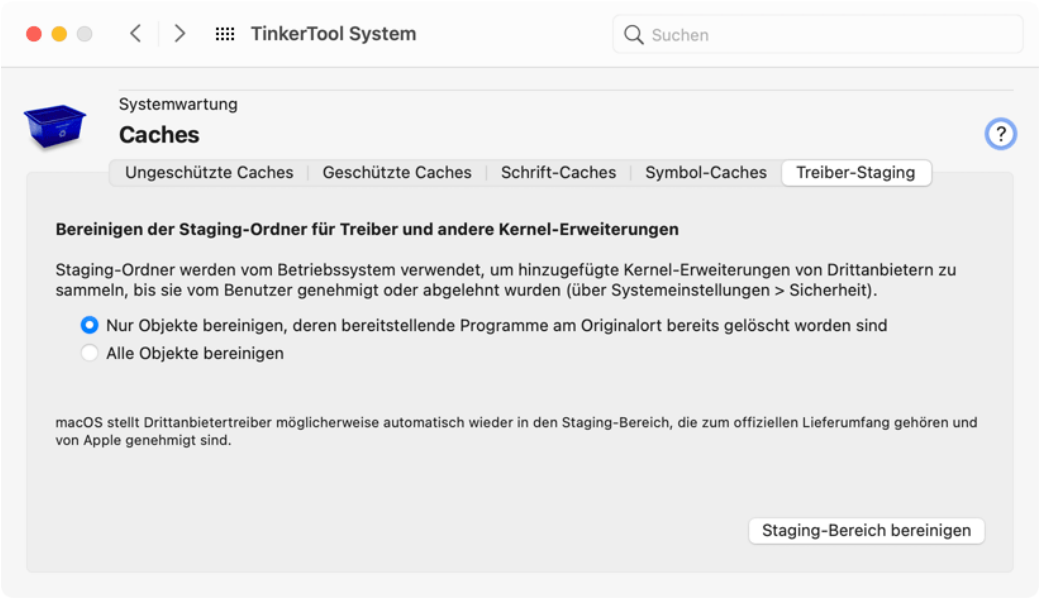

Abbildung 2.9: Treiber-Staging

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 Karteireiter **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.

2.3 Die Einstellungskarte Time Machine X

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 stündlich im Hintergrund angelegt und veraltete Dateisätze werden automatisch entfernt, wobei stündliche Sicherungen für den letzten Tag, tägliche Sicherungen für die letzte Woche 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. Ab macOS 11 schließt dies auch das Betriebssystem selbst mit ein. 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. Netzwerkbasierte 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.

2.3.3 Die unterschiedlichen Versionen von Time Machine für macOS 10 und macOS 11

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 jetzt auch Sicherungen auf das *Apple File System (APFS)* möglich. Wird Time Machine frisch auf einer Sicherungsplatte eingerichtet, wird standardmäßig APFS verwendet und es läuft im macOS 11-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 macOS 11-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 Kapitel bezieht sich auf die Karte **Time Machine X**. Wenn Sie die macOS 11-Variante verwenden, lesen Sie bitte im nächsten Kapitel (Abschnitt 2.4 auf Seite 51) weiter.
> 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.

2.3.4 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, dass 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 das 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 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 auf der Karte **Time Machine** der **Systemeinstellungen** wiedereinschalten und das Ziel für die Datensicherung neu einstellen.
Falls die lokalen Volumes des aktuellen Computers sich von denen des früheren Computers unterscheiden, *reicht die Neuzuweisung der Datensicherung alleine nicht aus*. Sie müssen auch jedes Volume neu zuordnen, was im nächsten Abschnitt behandelt wird.

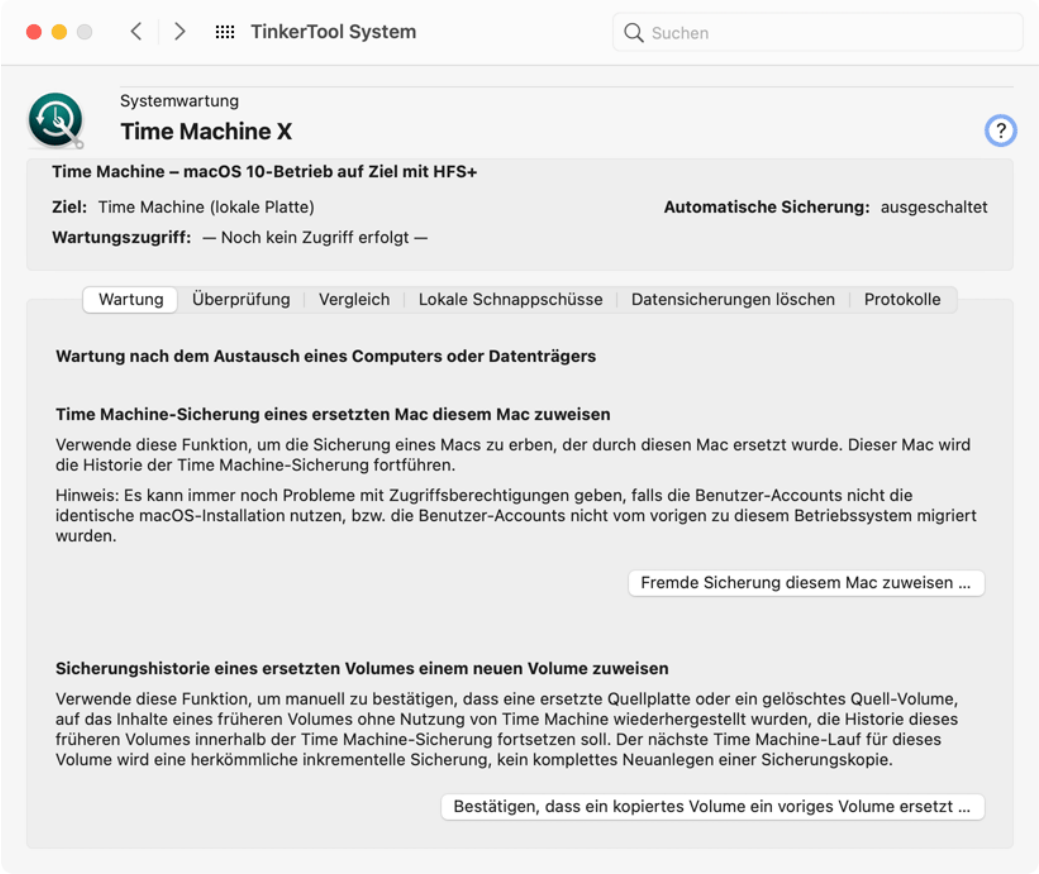

Abbildung 2.10: Wartung nach Austausch einer Time Machine-Datenquelle

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 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 diese 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.

2.3.5 Überprüfung und Statistik der Datensicherung

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

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 GB × 50 = 25,000 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 Textdatei abgespeichert werden, falls notwendig.

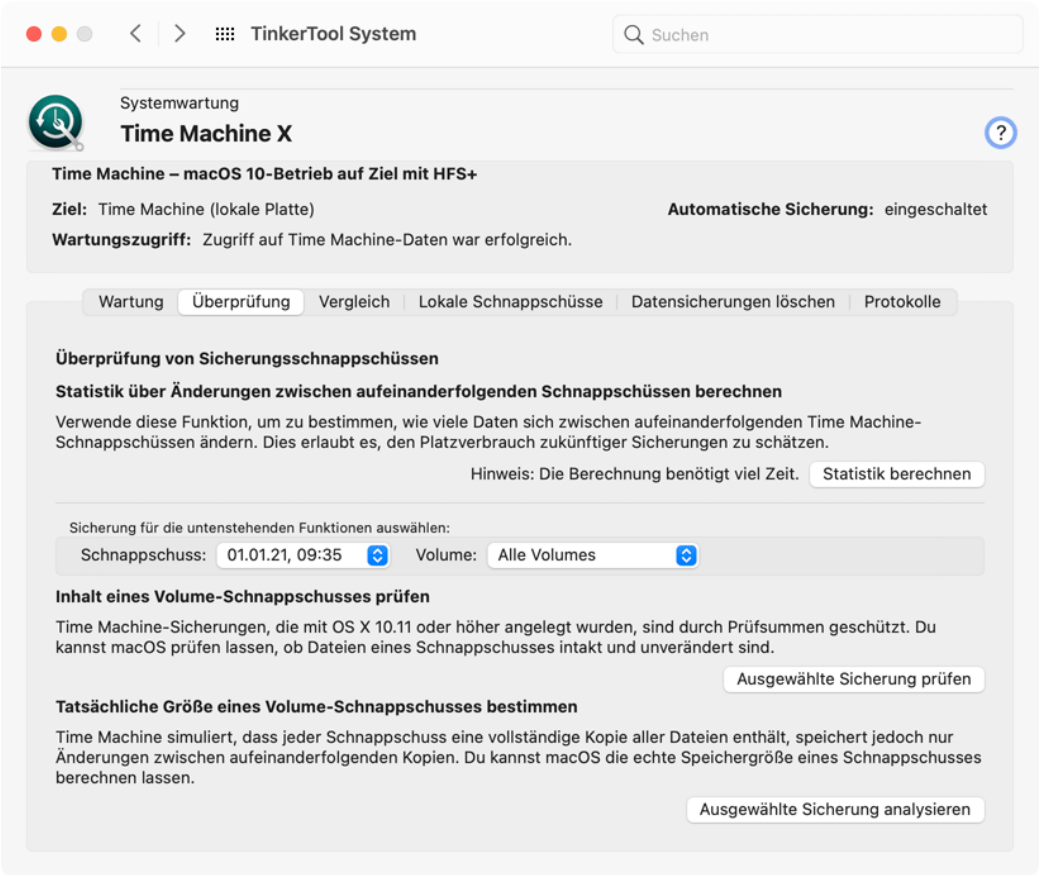

Abbildung 2.11: Funktionen zur Überprüfung und Statistik der Datensicherung

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**.

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.

Den tatsächlichen Speicherbedarf eines Volume-Schnappschusses berechnen

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.

2.3.6 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.
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**.

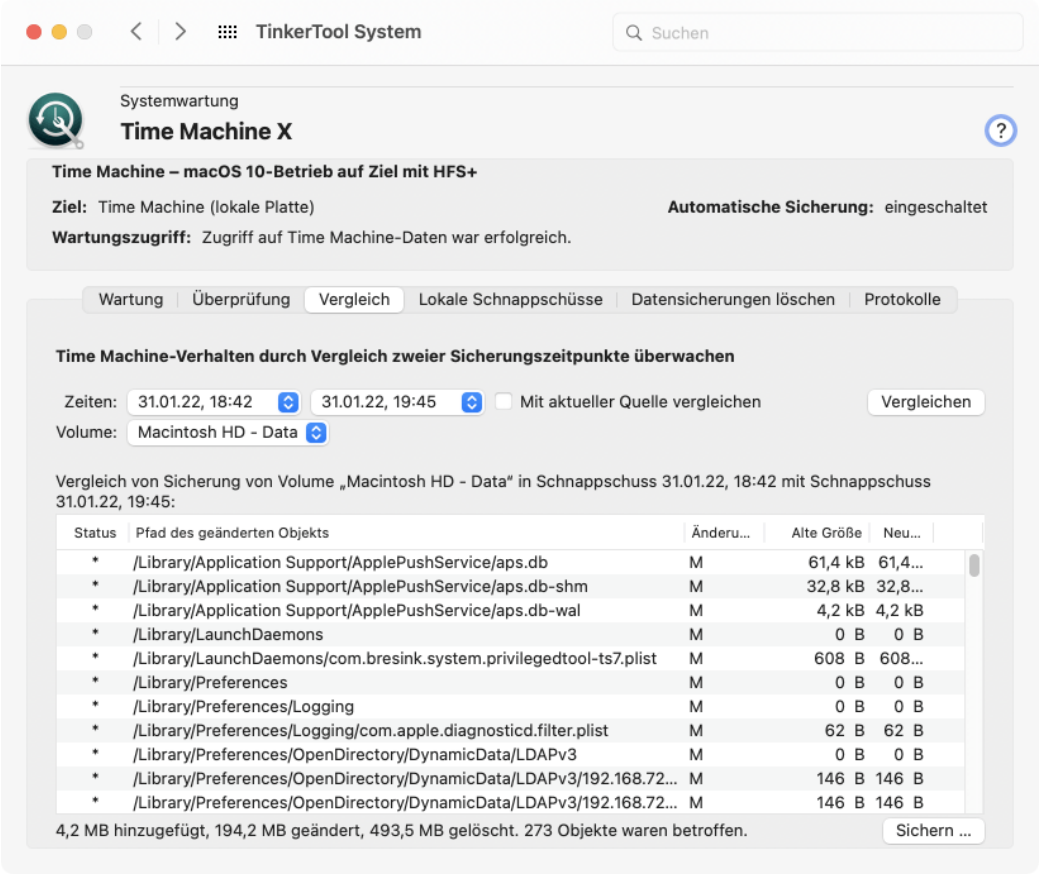

Abbildung 2.12: Time Machine prüfen

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.

2.3.7 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 Betriebsystem 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 203).

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.

- 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-

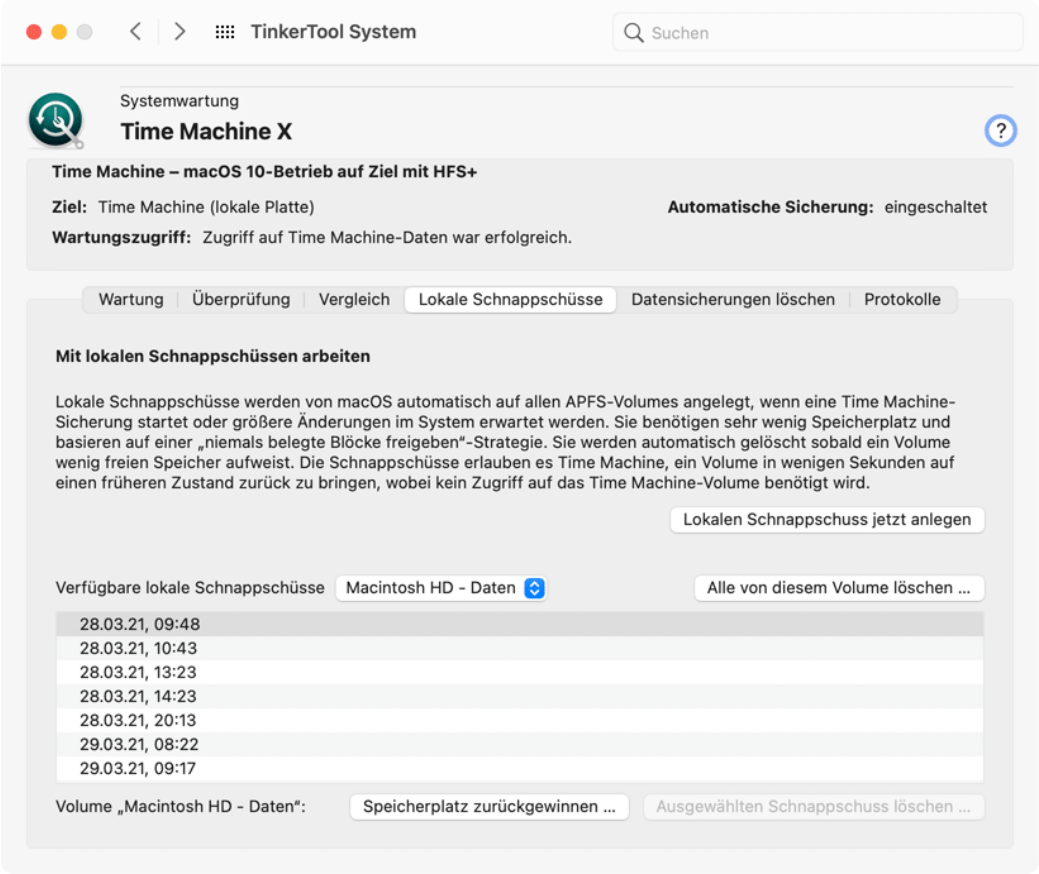

Abbildung 2.13: Arbeiten mit lokalen Schnappschüssen

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** ….

2.3.8 Löschen von Time Machine-Sicherungsdaten

Einen Sicherungsschnappschuss von der gerade aktuellen Time Machine-Platte entfernen

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 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

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** ….

2.3.9 Auslesen von Time Machine-Protokollen

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.

> 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:

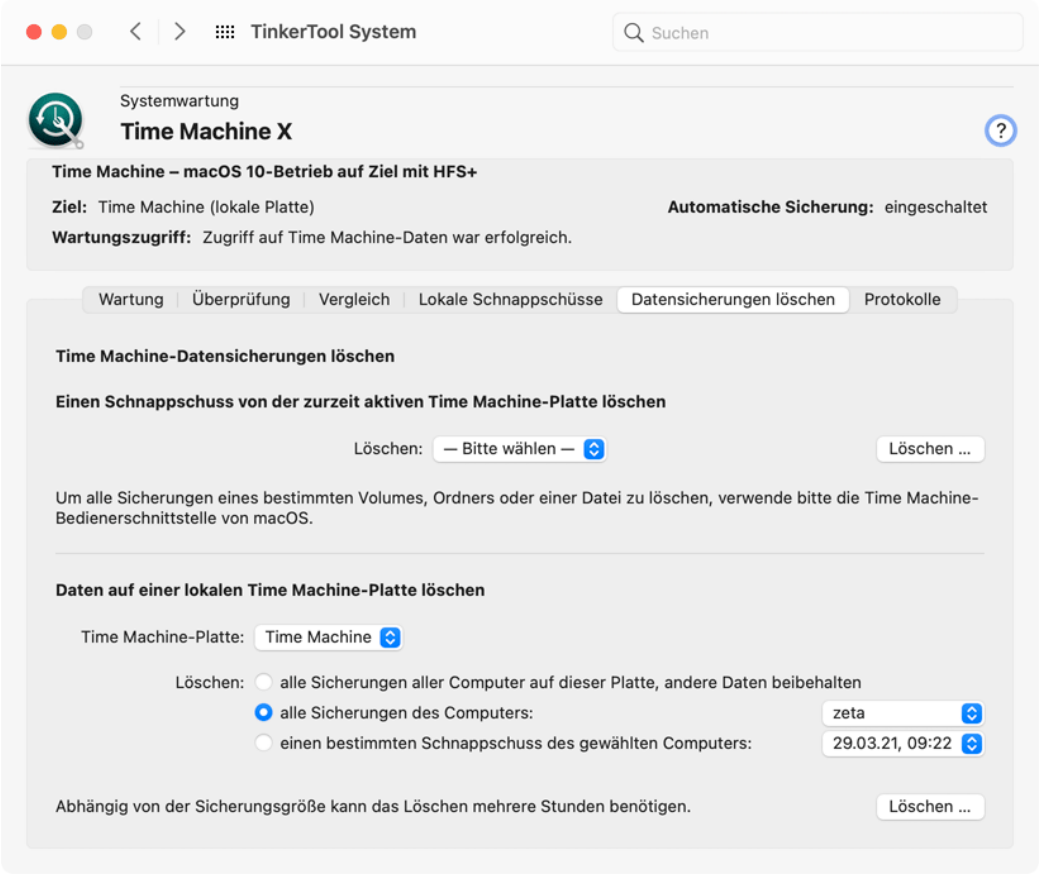

Abbildung 2.14: Löschen von Time Machine-Sicherungsdaten

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.

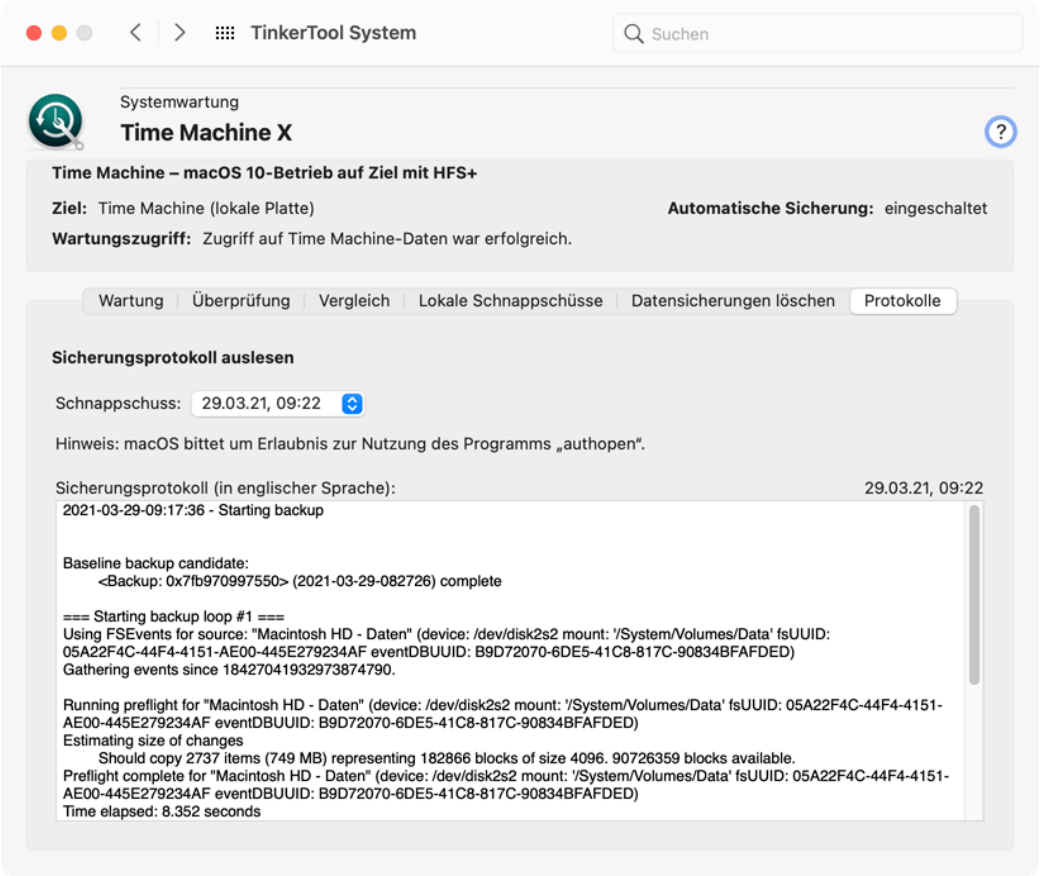

Abbildung 2.15: Zugriff auf Time Machine-Protokolle

2.4 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 2.3 auf Seite 35).
> 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.

2.4.1 Wartung nach dem Austausch einer Datenquelle von Time Machine (Moderner 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, dass 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 das 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 (Moderner 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**.
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 auf der Karte **Time Machine** der **Systemeinstellungen** wiedereinschalten und das Ziel für die Datensicherung neu einstellen.
Falls die lokalen Volumes des aktuellen Computers sich von denen des früheren Computers unterscheiden, *reicht die Neuzuweisung 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 (Moderner 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**.

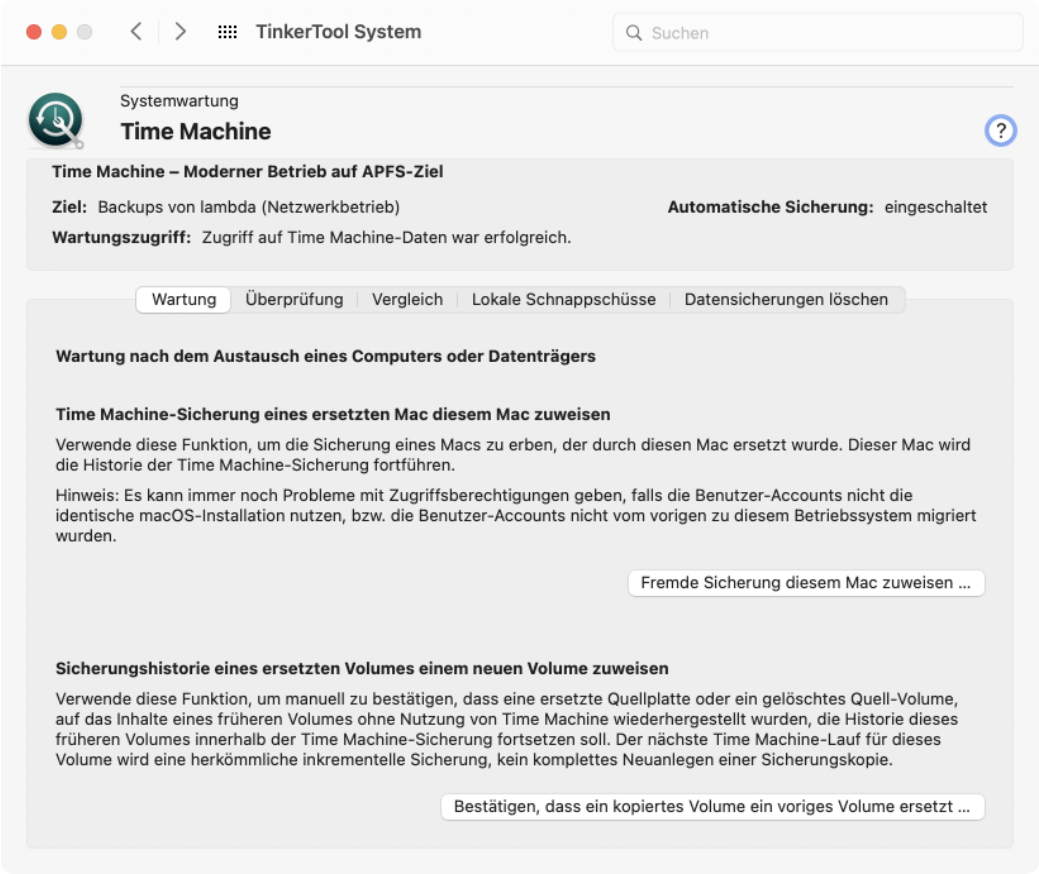

Abbildung 2.16: Wartung nach Austausch einer Time Machine-Datenquelle

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 diese 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 der Datensicherung

Den Inhalt eines Volume-Schnappschusses überprüfen (Moderner 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:

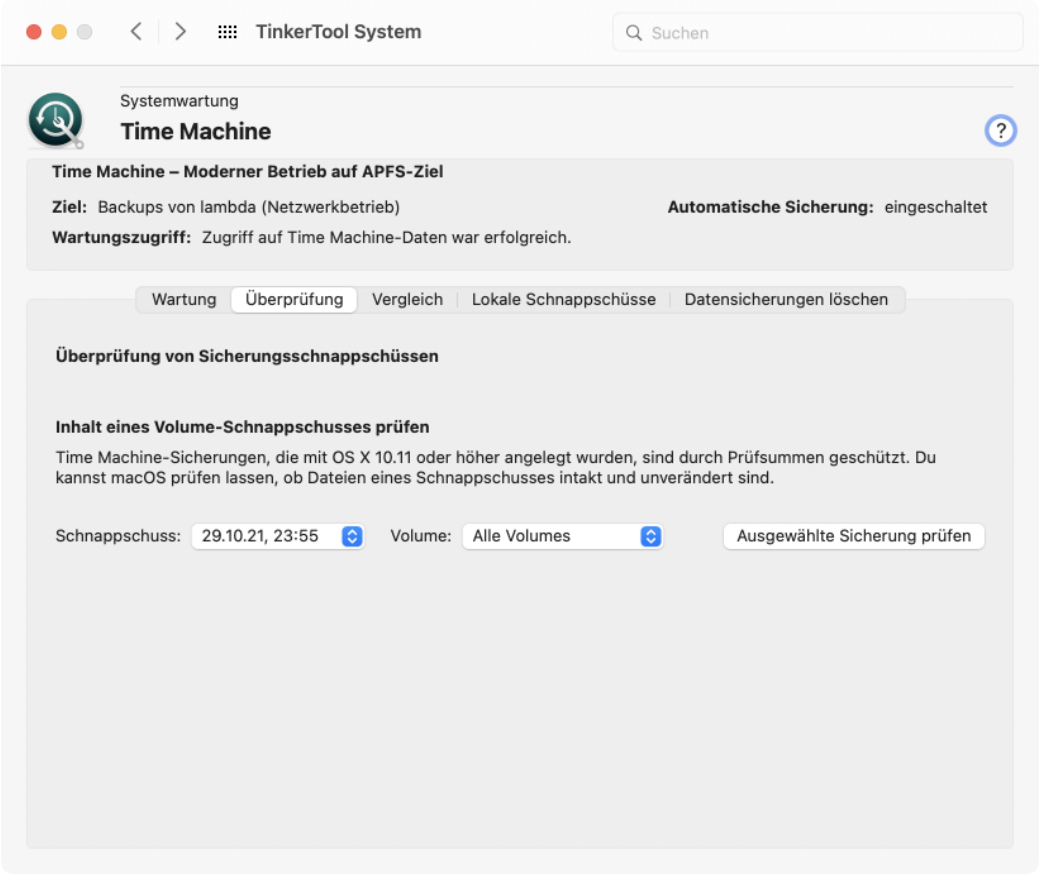

Abbildung 2.17: Funktion zur Überprüfung der Datensicherung

- **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.

2.4.3 Vergleich von Time Machine Sicherungsschnappschüssen (Moderner 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.
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,

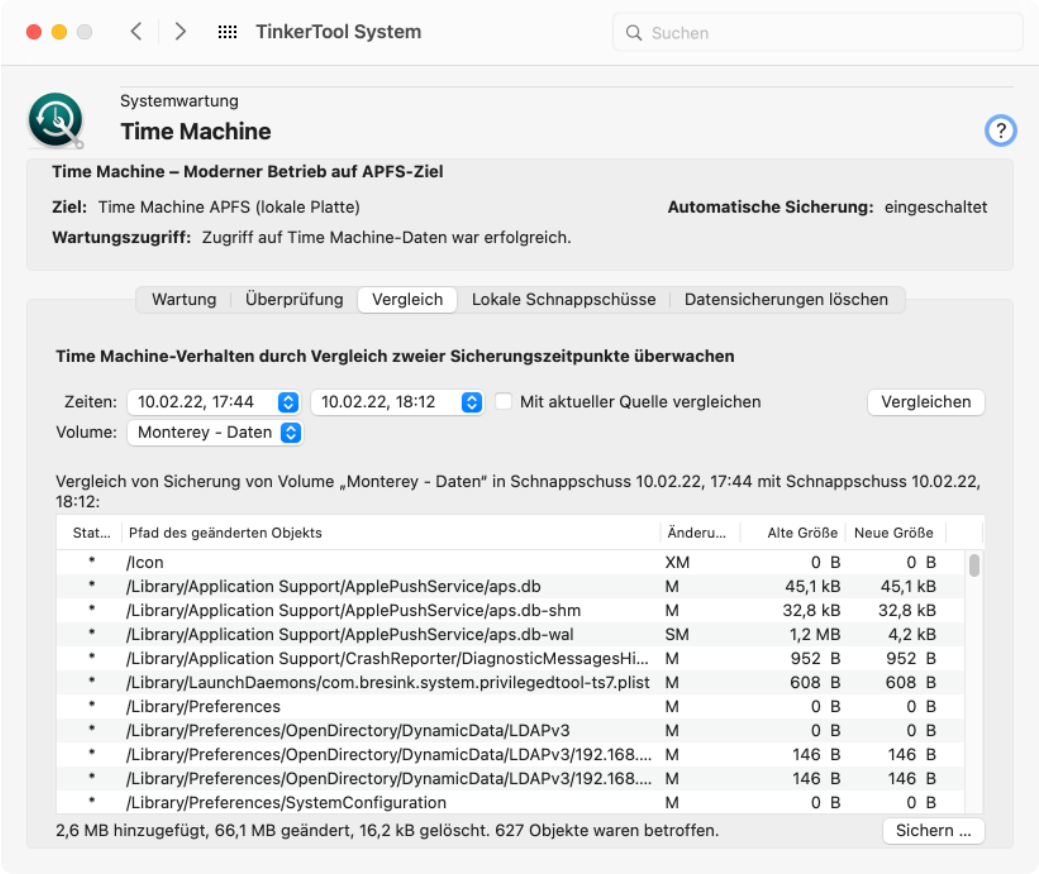

Abbildung 2.18: Time Machine prüfen

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.

- 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 (Moderner 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 Betriebsystem 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 203).

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.

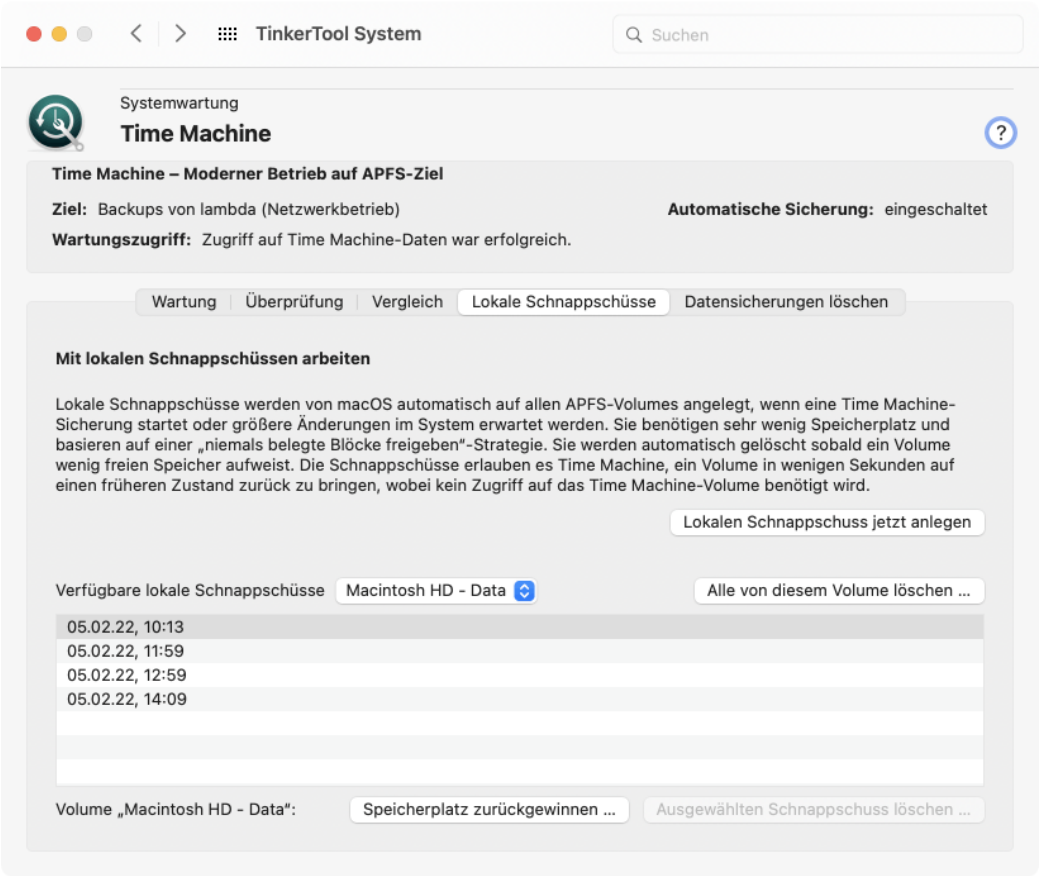

Abbildung 2.19: Arbeiten mit lokalen Schnappschüssen

- 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** ….

2.4.5 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 Klappmenü **Löschen** in der oberen Hälfte des Fensters aus.
3. Drücken Sie auf den Knopf **Löschen** … daneben.

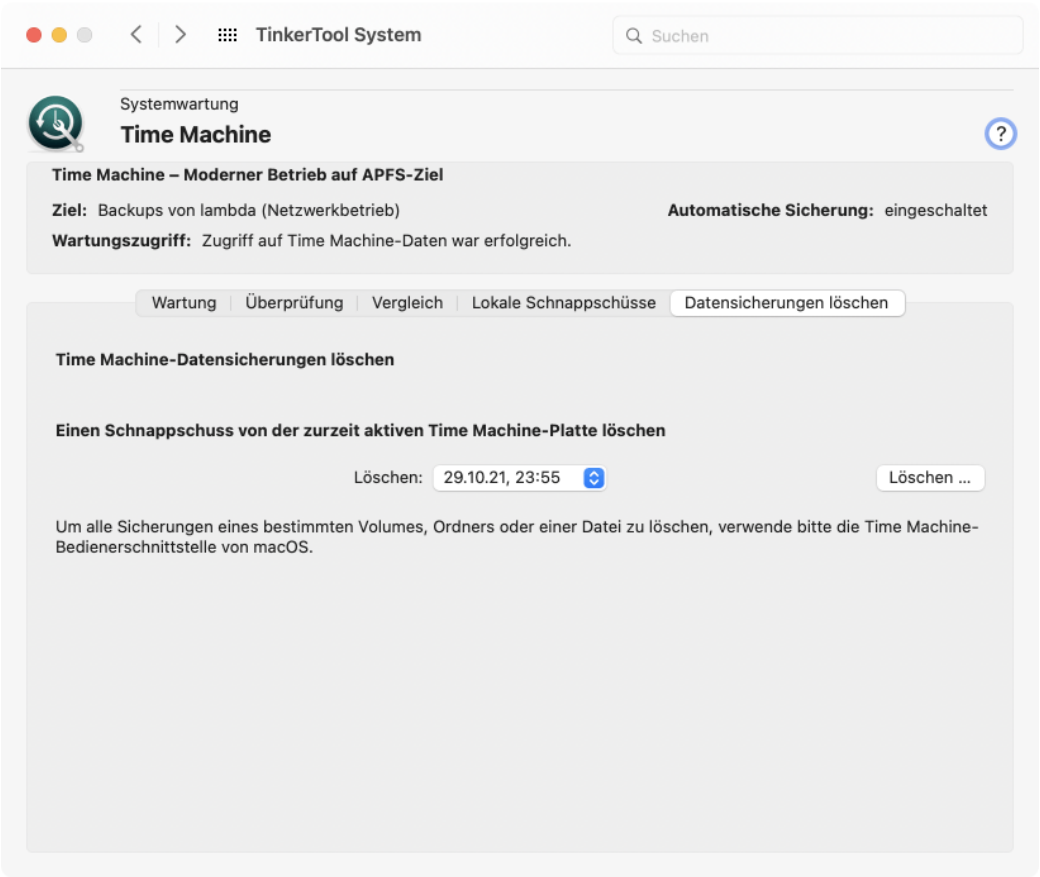

Abbildung 2.20: Löschen von Time Machine-Sicherungsdaten

2.5 Die Einstellungskarte Fehler

2.5.1 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, zwei 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 Betaprodukte 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 **Software-Update**.
> 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 2022 veröffentlicht hat, kann es passieren, dass die Funktion zum Softwareupdate nicht mehr richtig funktioniert, falls Sie ein Betriebssystem vor macOS 12 Monterey verwenden. Wenn Sie nach den neuesten Aktualisierungen auf der Karte **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 Karteireiter **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, einen Verbindung zu Apple aufzubauen und die neueste Liste verfügbarer Updates sofort zu beziehen. Führen Sie hierzu die folgenden Schritte durch:

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

2.5.2 App Store-Aktualisierungen

Das App Store-Programm führt in macOS Big Sur ein neues 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.

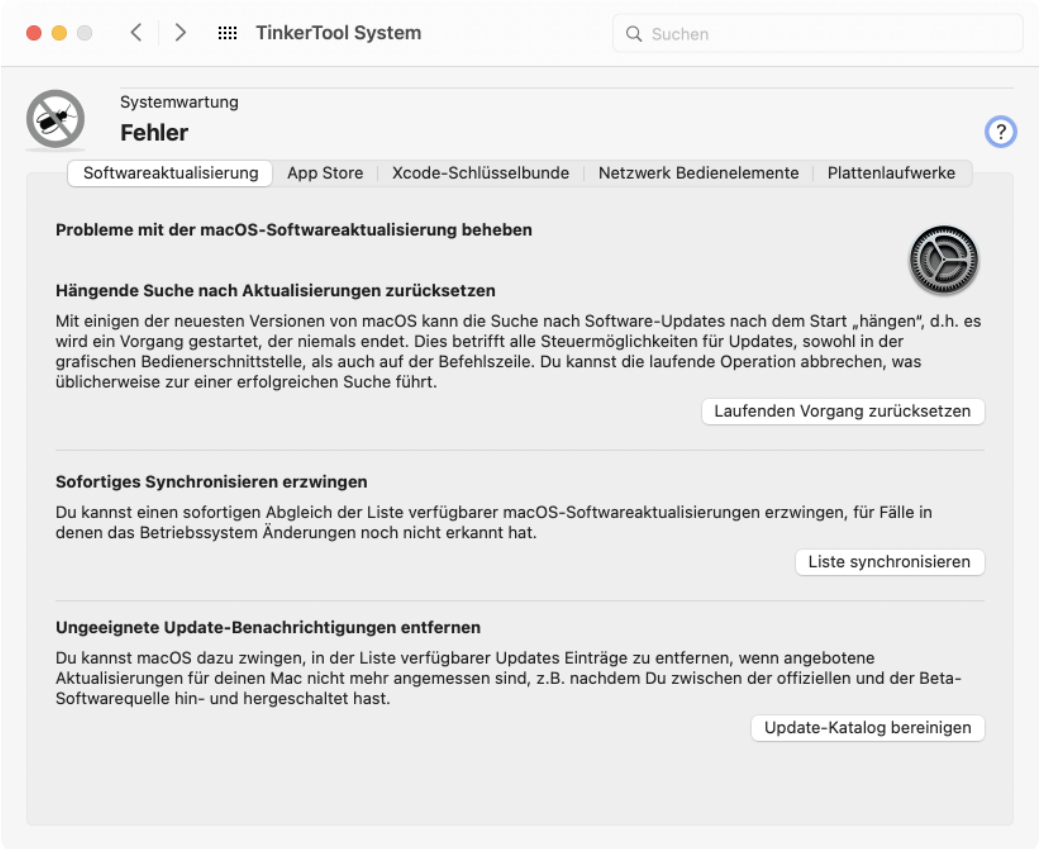

Abbildung 2.21: Beheben von Problemen mit der Softwareaktualisierung von macOS

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**).
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.

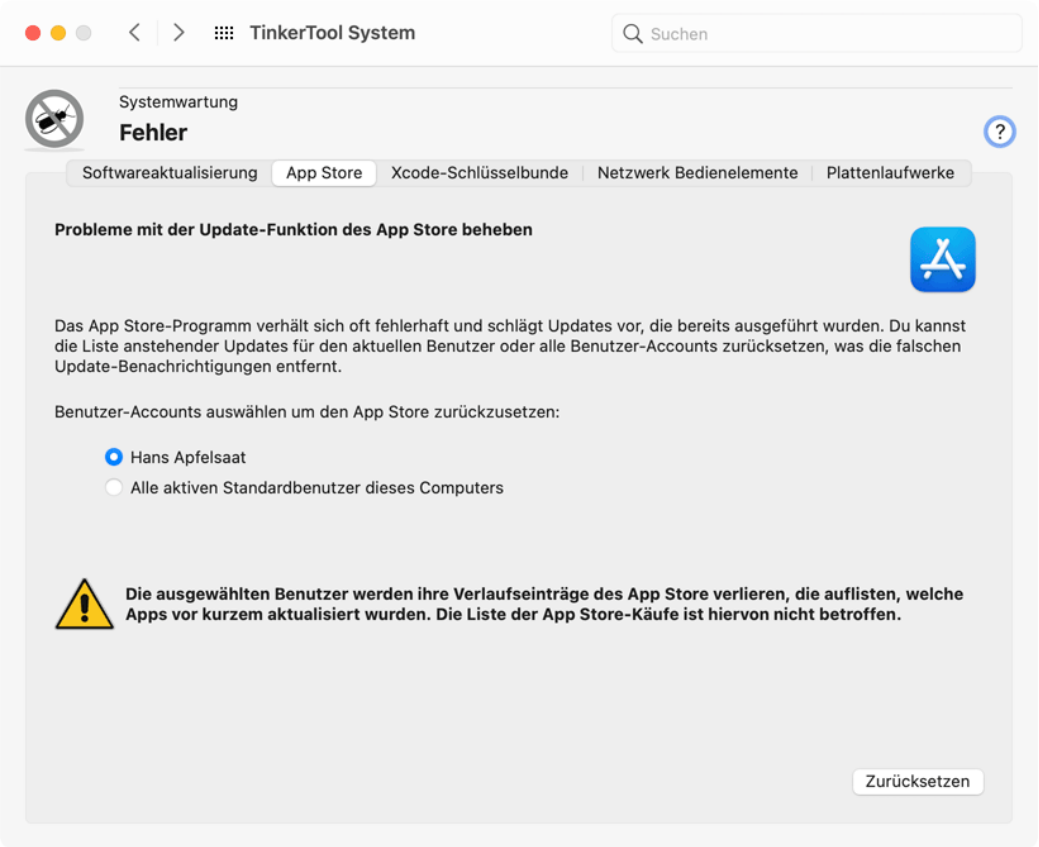

Abbildung 2.22: Das Zurücksetzen des App Store-Programms kann ungültige Update-Benachrichtigungen entfernen

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

1. Öffnen Sie den Karteireiter **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.

2.5.3 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:

- 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.

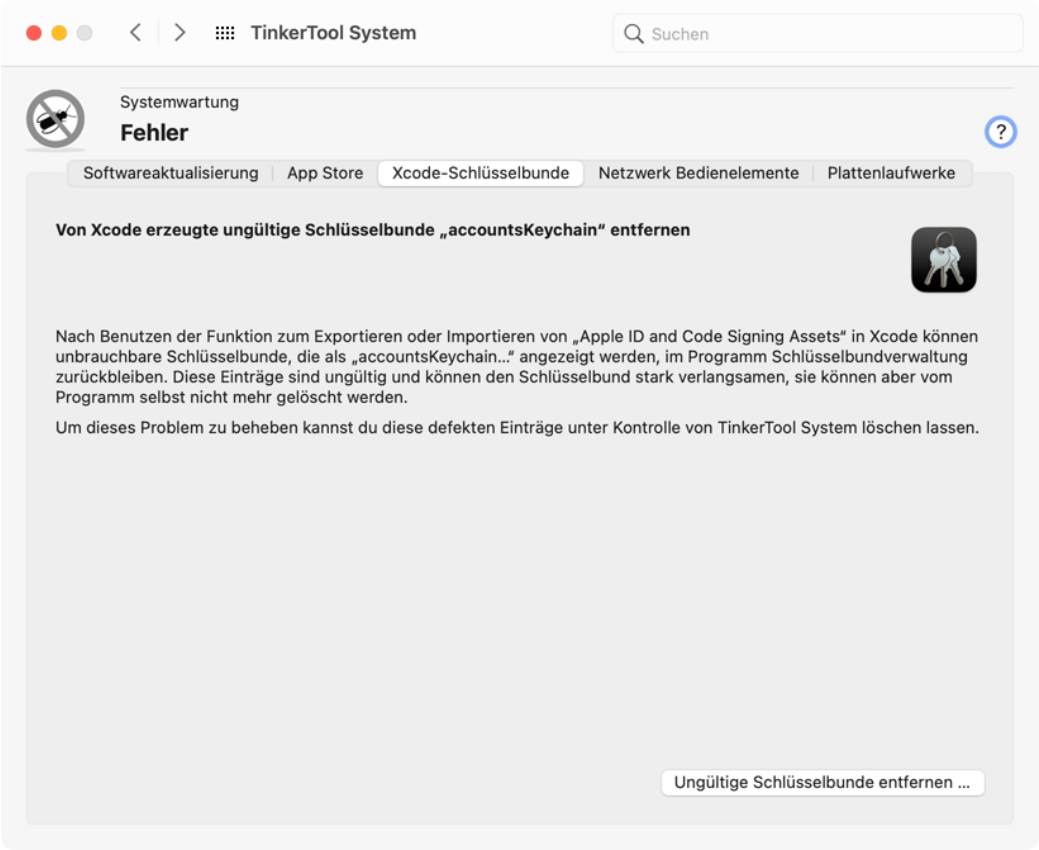

Abbildung 2.23: Von Xcode erstellte ungültige Schlüsselbunde können entfernt werden

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 Karteireiter **Xcode-Schlüsselbunde** auf der Karte **Fehler**.
2. Betätigen Sie die Schaltfläche **Ungültige Schlüsselbunde entfernen**.

2.5.4 Netzwerk Bedienelemente

Nach einem Update des Betriebssystems auf macOS 11.2 oder höher kann es passieren, dass einige Benutzer Probleme mit den grafischen Bedienelementen haben, die für Netzwerkverbindungen mit anderen Computern zuständig sind. Dies schließt die folgenden Symptome mit ein:

- Der Ordner Netzwerk des Finders fehlt.
- Der Eintrag Netzwerk in der Seitenleiste des Finders funktioniert nicht oder fehlt ebenso.
- Beim Versuch sich mit einem Server zu verbinden, erscheint kein Anmeldedialogfenster.
- AirDrop funktioniert nicht.
- Handoff funktioniert nicht.
- Das Arbeiten mit der Funktion Instant Hotspot ist nicht möglich.

Diese Probleme werden von einem Defekt im Betriebssystem ausgelöst. Die Konfiguration bestimmter Nutzer-Accounts wird möglicherweise vom macOS-Update beschädigt, so dass die betroffenen Benutzer viele Bedienelemente für den Zugriff auf Netzwerk-Computer verlieren. TinkerTool System kann diese Benutzer-Accounts für gewöhnlich reparieren, falls Sie die beschriebenen Symptome sehen.
Aus technischen Gründen ist die Reparaturfunktion auf die folgenden Benutzer-Accounts beschränkt:

- Der Account des Benutzers, der gerade mit TinkerTool System arbeitet, aber nur falls dieser Benutzer den Computer verwalten darf (Administrator).
- Alle lokalen Benutzer-Accounts des Typs „Standard“, die aktiv sind.

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**). Dieser Ordner muss die normalen, empfohlenen Berechtigungseinstellungen und einen normalen Namen aufweisen (üblicherweise den Kurznamen des Accounts). Das heißt in der Praxis, dass Sie die Reparaturfunktion nicht für roamende Netzwerkbenutzer verwenden können, wenn diese nicht Mitglied in der lokalen Gruppe der Administratoren dieses Macs sind.
Um TinkerTool System die Bedienerschnittstelle für Netzwerkfunktionen reparieren zu lassen, führen Sie die folgenden Schritte durch:

1. Verwenden Sie die Radioknöpfe bei **Benutzer-Accounts zum Überprüfen und Reparieren auswählen**, um zu bestimmen, welche Benutzer in den Vorgang mit eingeschlossen werden sollen.
2. Betätigen Sie den Knopf **Testen und reparieren**.

TinkerTool System öffnet einen Berichtsdialog, der alle ausgewählten Benutzer auflistet, sowie ob diese von dem Problem betroffen sind und was das jeweilige Ergebnis des Reparaturversuchs war.

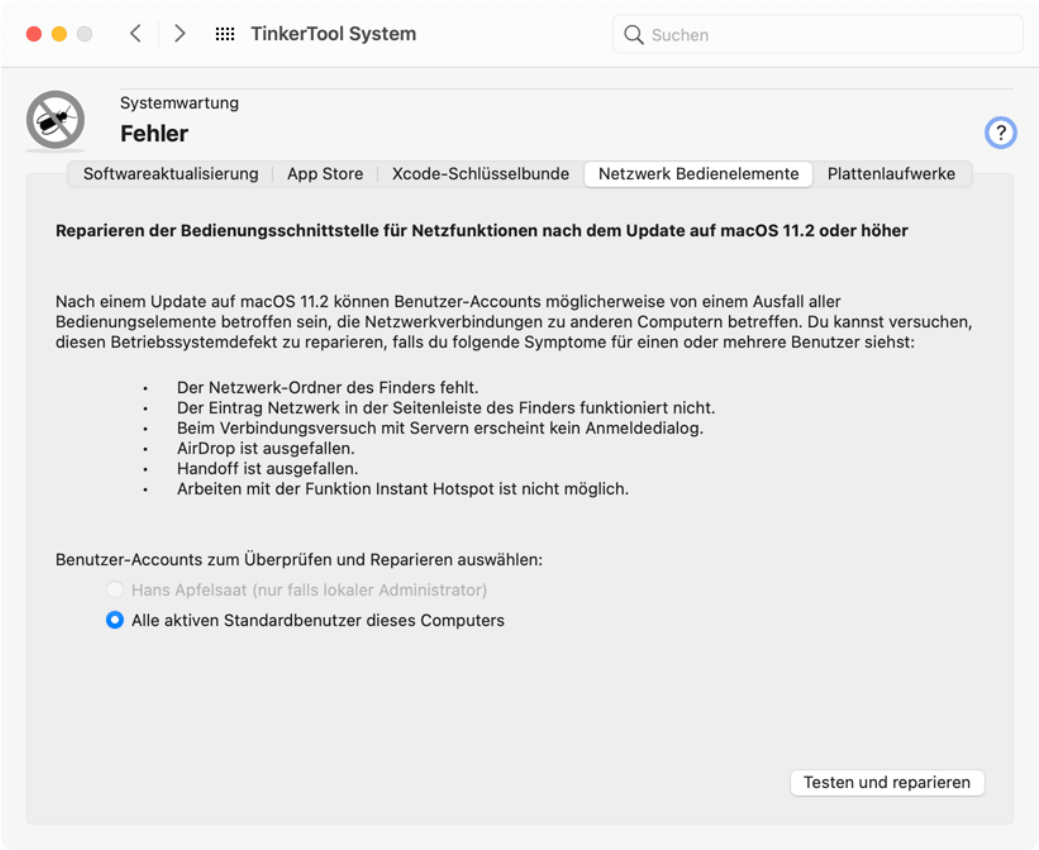

Abbildung 2.24: Ein Ausfall der Bedienungselemente für Netzwerkzugriff kann für betroffene Benutzer-Accounts repariert werden

2.5.5 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 Karteireiter **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** ....

> Seien Sie absolut sicher, die richtige Platte ausgewählt zu haben, bevor Sie den Knopf **Löschen** drücken.

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

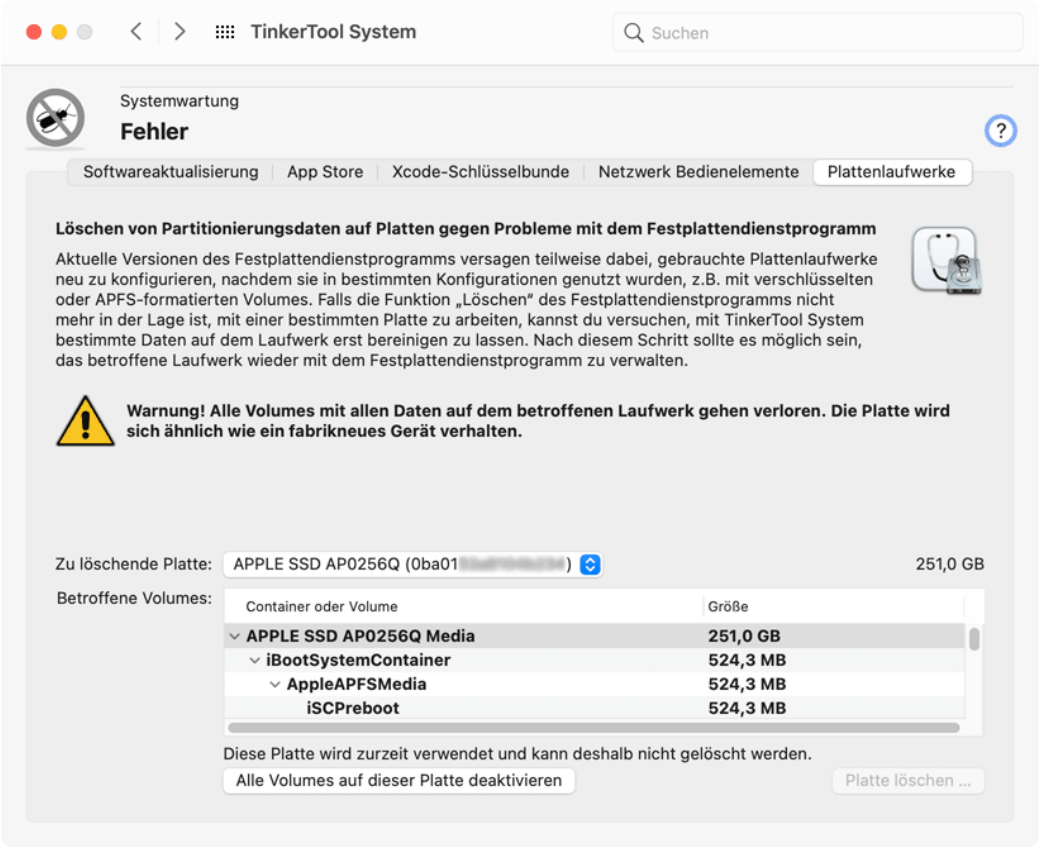

Abbildung 2.25: Bereinigen Sie Platten, die im Festplattendienstprogramm nicht mehr gehandhabt werden können

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.

2.6 Die Einstellungskarte Diagnose

2.6.1 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 zuwenig Speicher vorhanden, kann die Geschwindigkeit des Computers stark herabgesetzt werden. Ist allerdings zuviel 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 Management 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 Karteireiter **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.

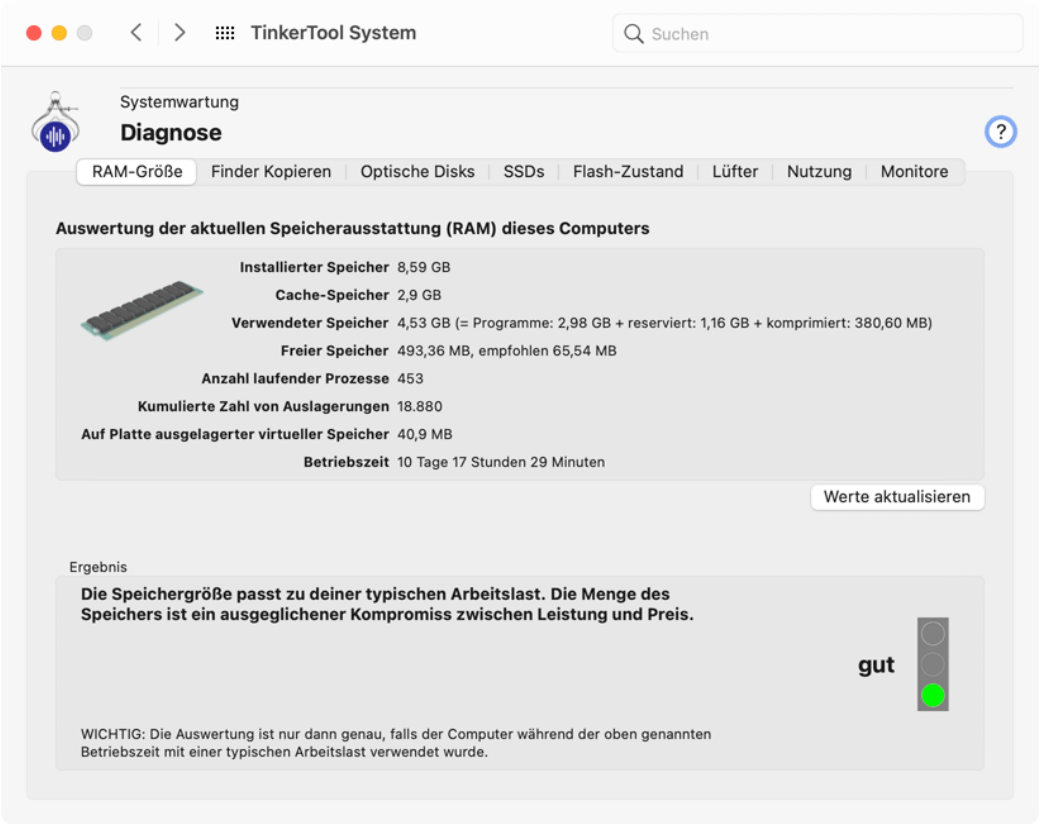

Abbildung 2.26: RAM-Größe auswerten

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 Computermodellen 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 Gesamtbewertung 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.

2.6.2 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.

> 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).

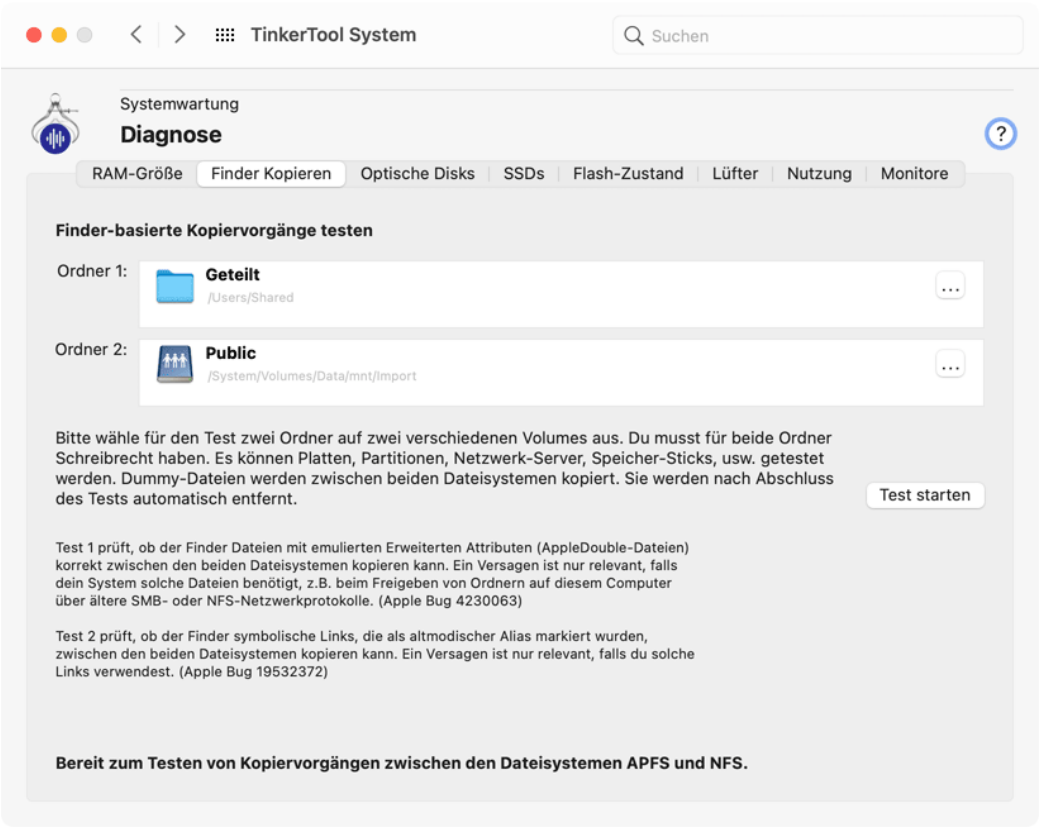

Abbildung 2.27: Dateikopiervorgänge überprüfen

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

1. Öffnen Sie den Karteireiter **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), 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.

> Falls einer der Tests fehlschlägt, während Sie zwei Datenträger mit HFS+ für den Kopiervorgang ausgewählt hatten, müssen Sie leider damit rechnen, dass auch Time

> Machine nicht korrekt arbeitet. Da der Finder indirekt an Kopiervorgängen in Time Machine beteiligt ist, kann auch dort das Sichern und Zurückladen von Daten zu einer Beschädigung kopierter Daten führen.

2.6.3 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 Karteireiter **Optische Disks** auf der Einstellungskarte **Diagnose**.
2. Falls an Ihren Computer mehrere optische Laufwerke angeschlossen sind, wählen Sie das gewünschte Laufwerk mit dem Klappmenü **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.
4. Drücken Sie den Knopf **Disk inspizieren**.

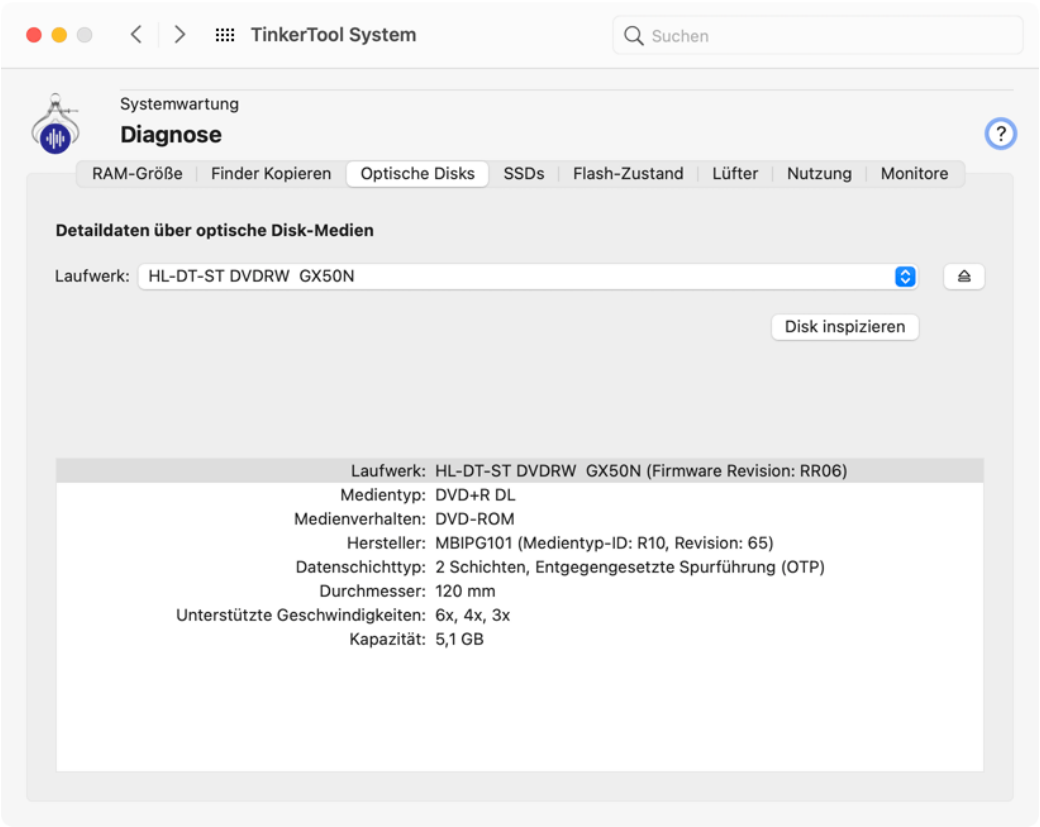

Abbildung 2.28: Optische Disks inspizieren

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.

2.6.4 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 Karteireiter **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.

2.6.5 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 Lösch-, bzw. Schreiboperationen ausführen. Wird eine bestimmte Anzahl von Neuprogrammiervorgängen überschritten, kann die Speicherzelle irgendwann nicht mehr zuverlässig zwischen dem Zustand für *0* und *1* hin- und herschalten. Das betroffene Bit „bleibt hängen“ und der gesamte Speicherblock,

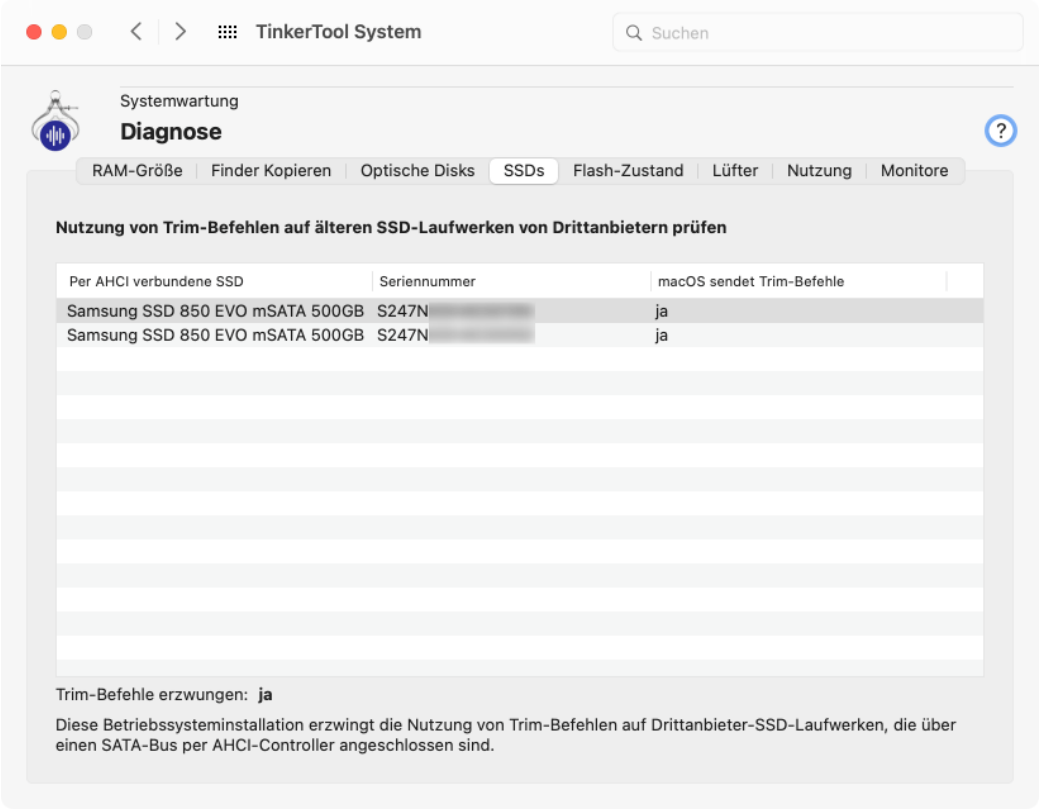

Abbildung 2.29: macOS kann Trim-Befehle an AHCI-verbundene SSDs von Drittanbietern senden

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

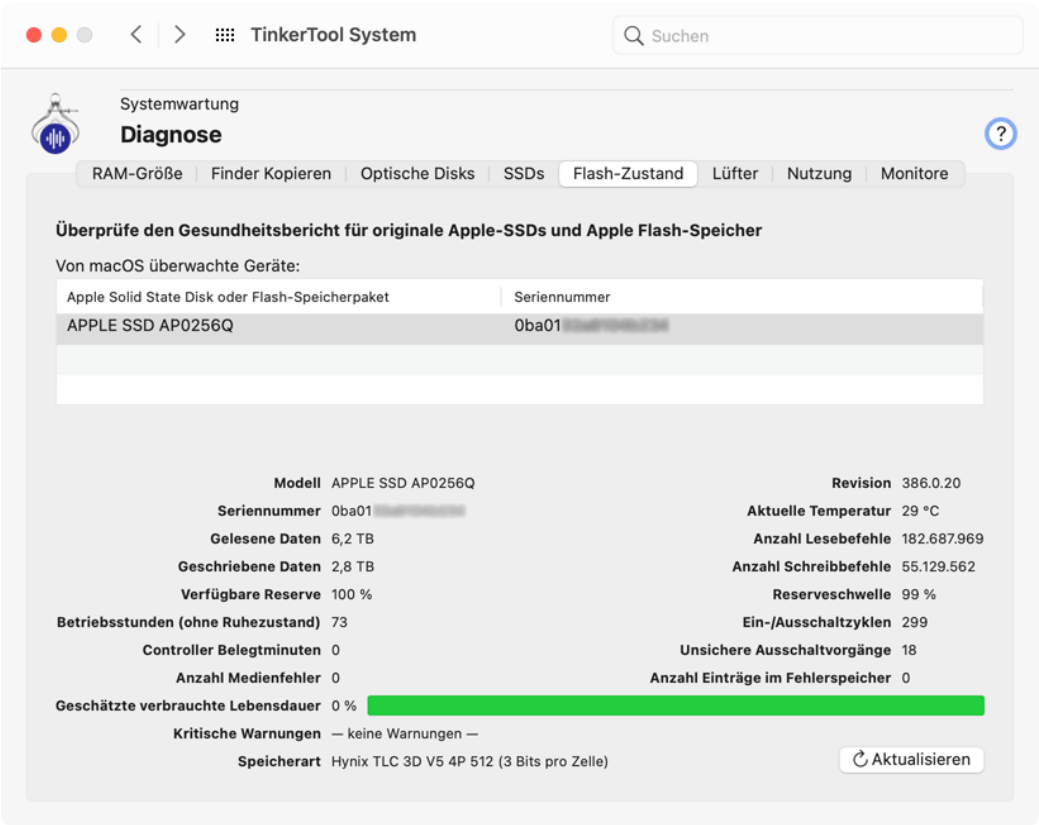

Abbildung 2.30: Überprüfen Sie den Zustand von originalem Apple-Flash-Speicher

- **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.
- **Anzahl 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 SSD in den Flash-Speicher geschrieben wurde.
- **Anzahl 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 (ohne Ruhezustand):** 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 Belegtminuten:** 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.
- **Anzahl Medienfehler:** Die Anzahl der Fehler, die im Flash-Speicher über Prüfsummenverfahren erkannt und nicht behoben werden konnten. Es wurden fehlerhafte Daten gespeichert oder geliefert.
- **Anzahl Einträge im Fehlerspeicher:** Die Anzahl interner Fehlersituationen, die der Controller während der Lebensdauer der SSD intern beobachtet und aufgezeichnet hat.
- **Geschätzte 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.

2.6.6 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 den neuesten Modellen ein *Apple T2*-Prozessor, auf dem Apples BridgeOS-Betriebssystem läuft. 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:

1. Öffnen Sie den Karteireiter **Lüfter** auf der Einstellungskarte **Diagnose**.

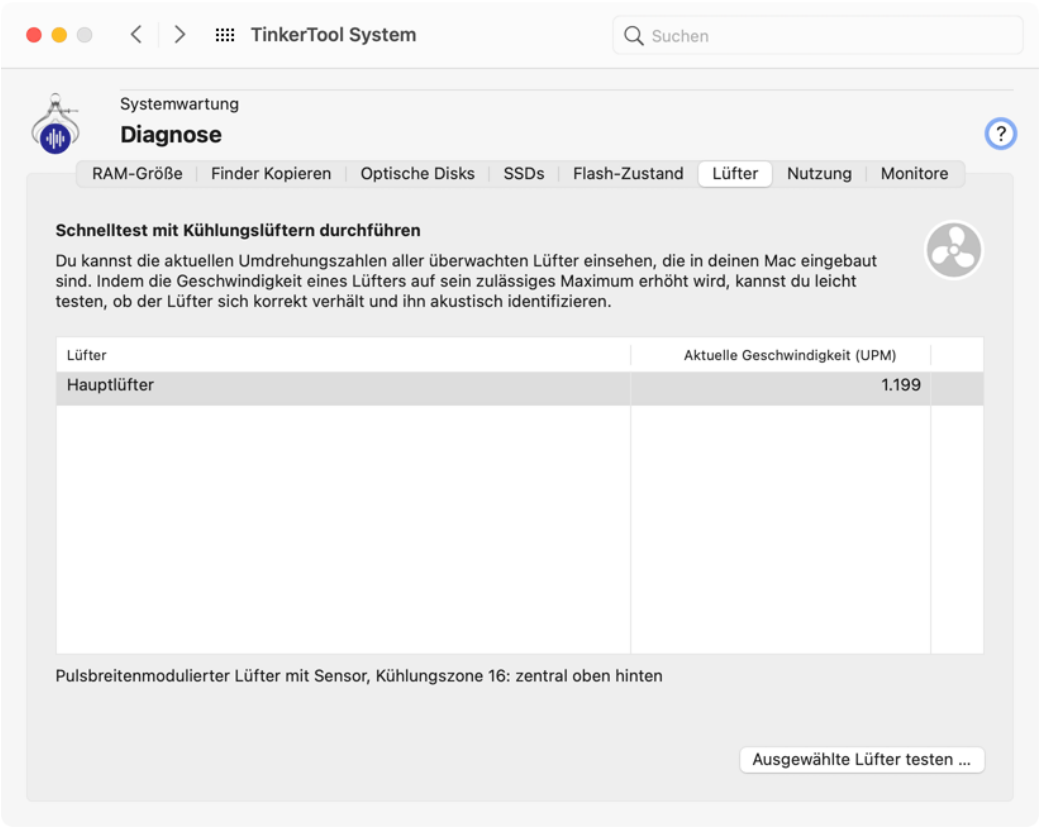

Abbildung 2.31: Kühlungslüfter des Macs überprüfen

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.

2.6.7 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.

1. Öffnen Sie den Karteireiter **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).

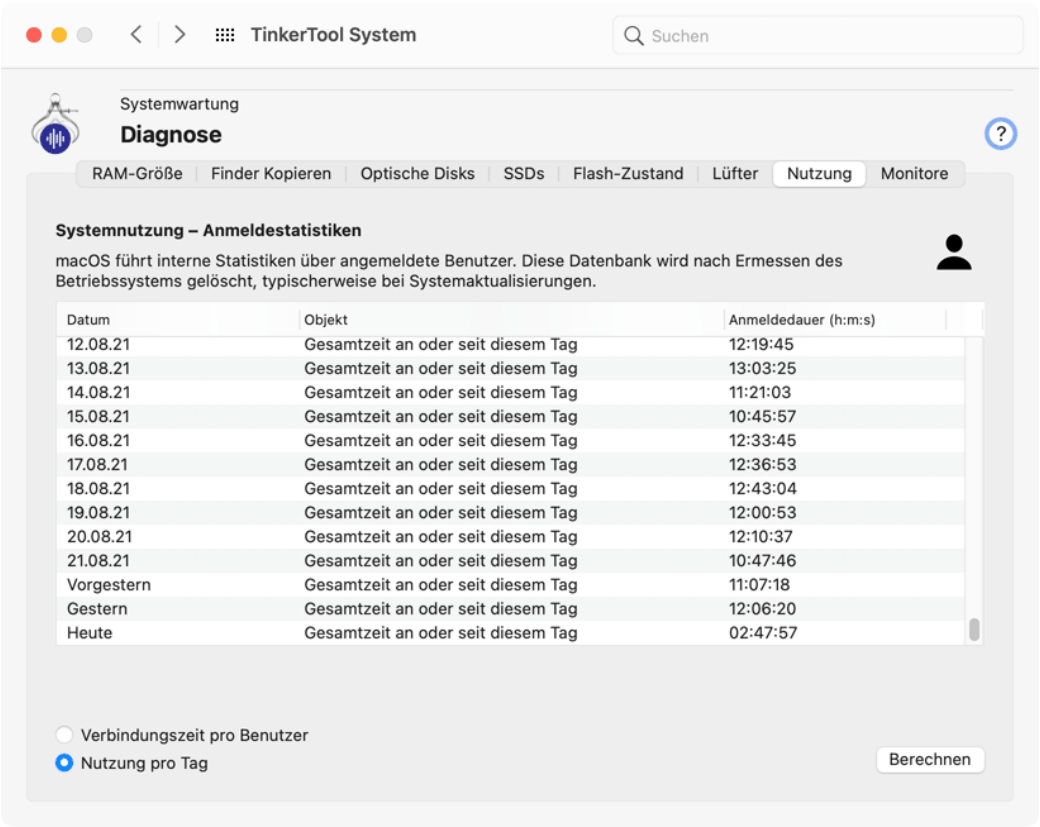

Abbildung 2.32: Rufen Sie die Statistik der Anmeldezeiten ab, die von macOS geführt wird

- 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 der Systemeinstellungen *Accountname* genannt und stimmen mit den Ordnernamen 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.

2.6.8 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

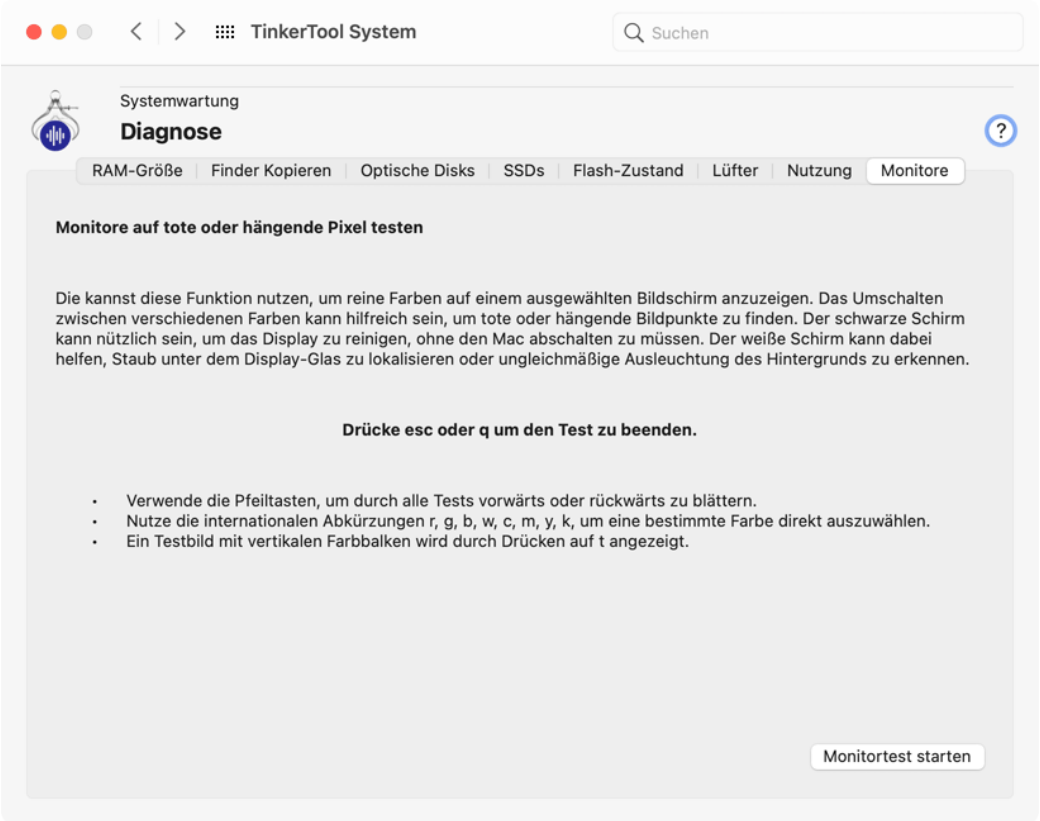

Abbildung 2.33: Angeschlossene Bildschirme können über Farbflächen getestet werden

Sie können die Testbilder wie folgt abrufen:

1. Öffnen Sie den Karteireiter **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.

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

Tabelle 2.1: Tasten zum Steuern der Testbilder

Taste	Funktion
esc oder q	Test beenden
↓ oder → oder ␣	nächstes Testbild
↑ oder ←	voriges Testbild
k	schwarz
w	weiß
r	rot
g	grün
b	blau
c	zyan
m	magenta
y	gelb
t	Testbild mit Farbbalken

2.7 Die Einstellungskarte Notfallwerkzeug

> Falls Sie einen Mac mit Apple-Chips verwenden, ist macOS 12.5 oder höher für das Notfallwerkzeug erforderlich. Die Sicherheitsfunktionen von macOS erlauben es Ihnen nicht, das Programm auf den meisten früheren Betriebssystemen zu starten.

2.7.1 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.**

2.7.2 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.

2.7.3 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"**.

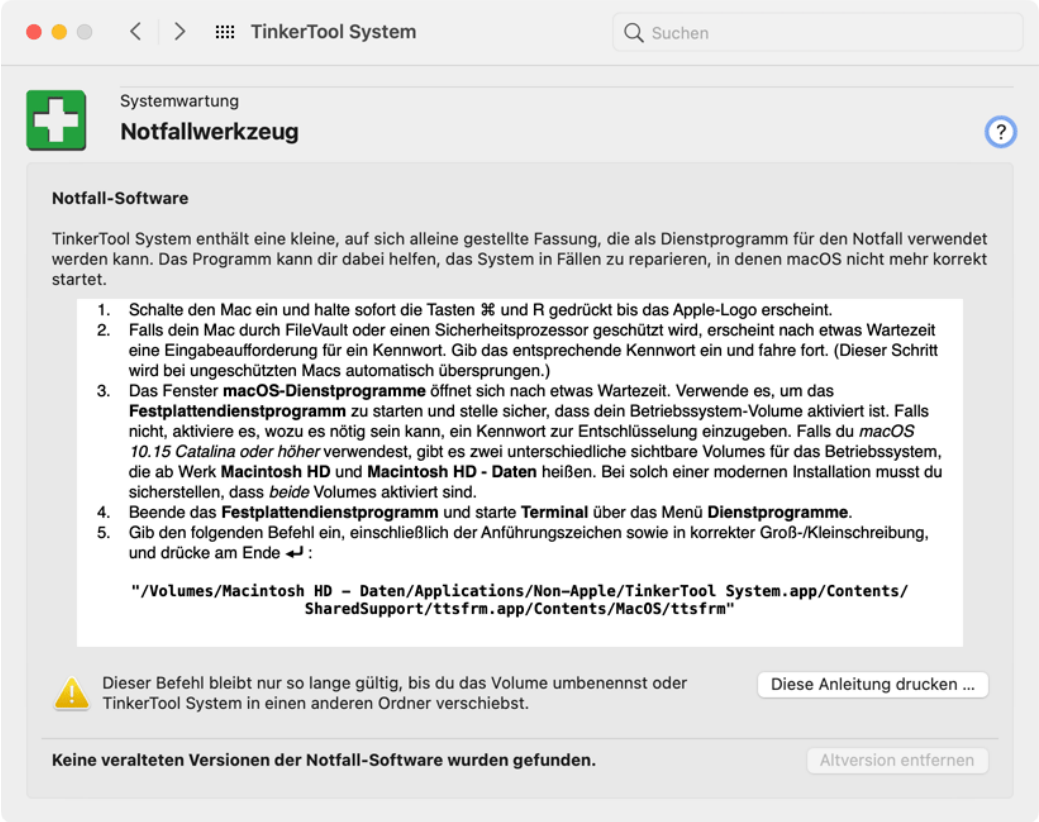

Abbildung 2.34: Notfallwerkzeug - Die im Bild gezeigte Anleitung ist individuell für jeden Computer und trifft auf Ihre Situation möglicherweise nicht zu.

6. Nach Ende des Befehls muss die Eingabetaste gedrückt werden.

Das Muster des Aufrufs lautet also

```
"/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.

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 Betriebsystem 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-Update-Volume und dessen Daten-Volume. Sie können diese Gruppierung über die Karte APFS (Abschnitt 3.7 auf Seite 203) im Detail anzeigen lassen.

2.7.4 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 259).

2.7.5 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 musst 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.

2.8 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.

2.8.1 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.

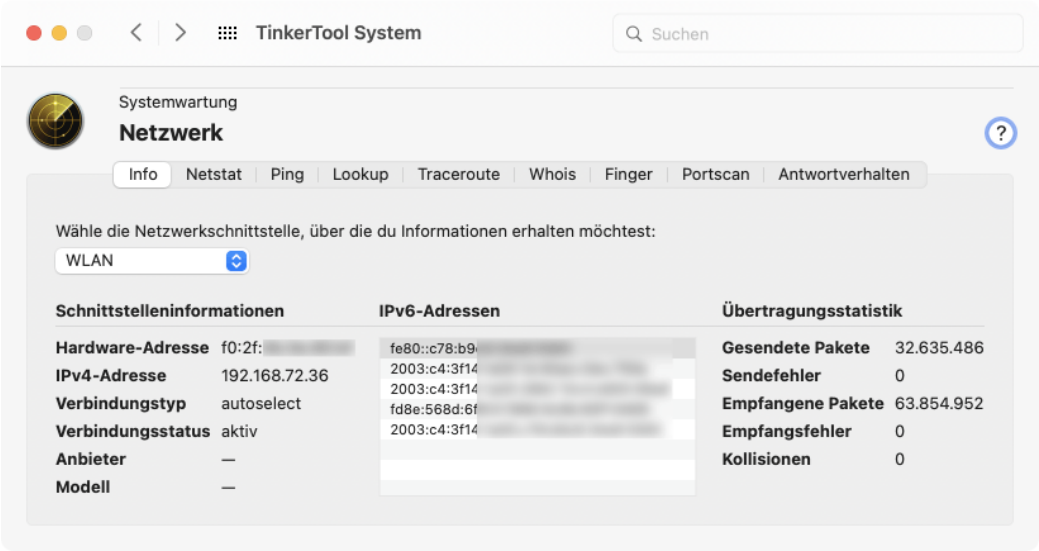

Abbildung 2.35: Detaildaten über jeden aktiven Netzwerkanschluss können ermittelt werden

Die folgende Details sind abrufbar:

- **Hardware-Adresse:** die in der Hardware vorgegeben 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.

2.8.2 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:

- 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.

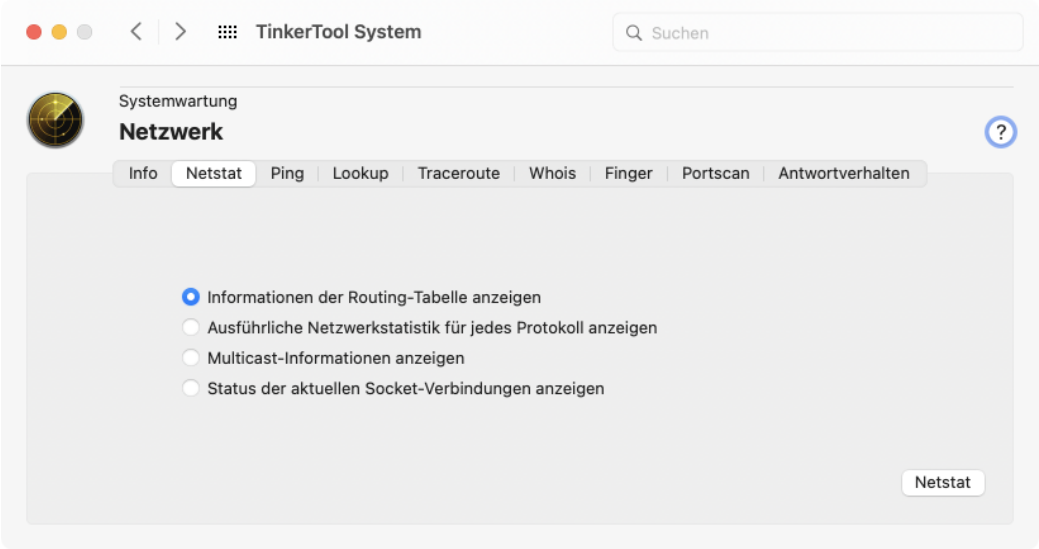

Abbildung 2.36: Statistiken und Routing-Tabellen lassen sich aus dem System auslesen

- 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.

2.8.3 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**.

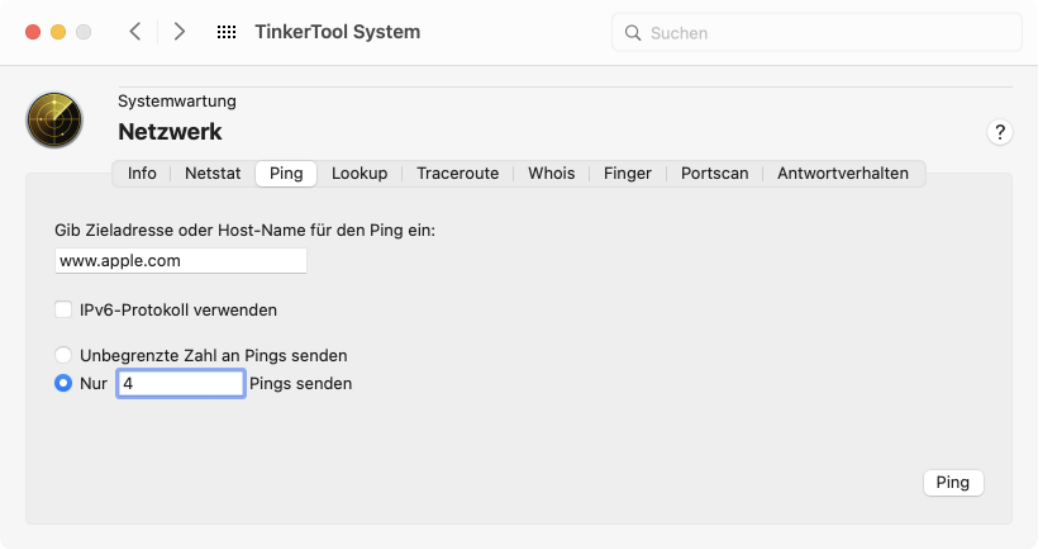

Abbildung 2.37: Um eine Verbindung zu prüfen, können Echo-Anforderungen versandt werden

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.

2.8.4 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**.

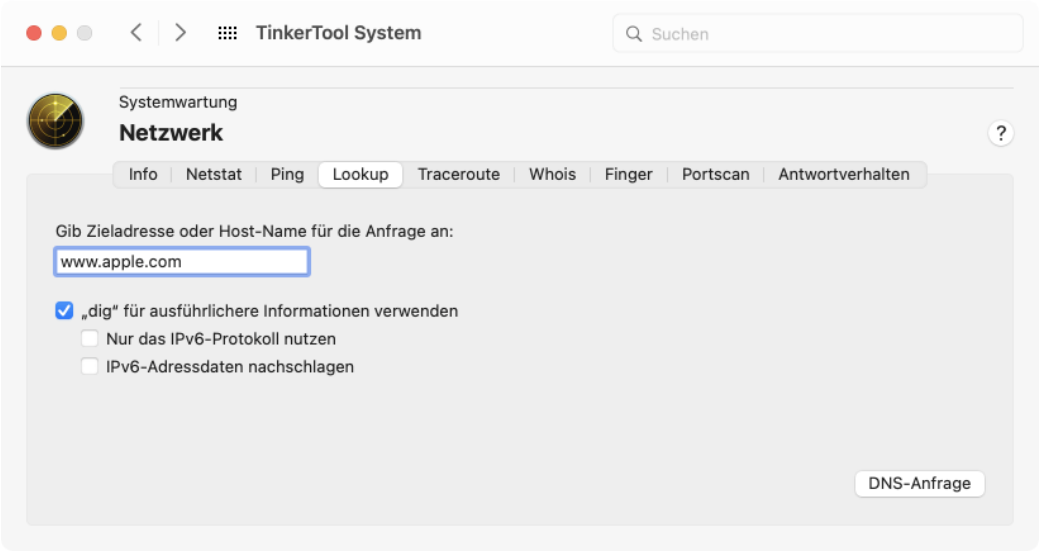

Abbildung 2.38: Die Beziehungen zwischen Namen und Adressen können abgerufen werden

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.

2.8.5 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.
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**.

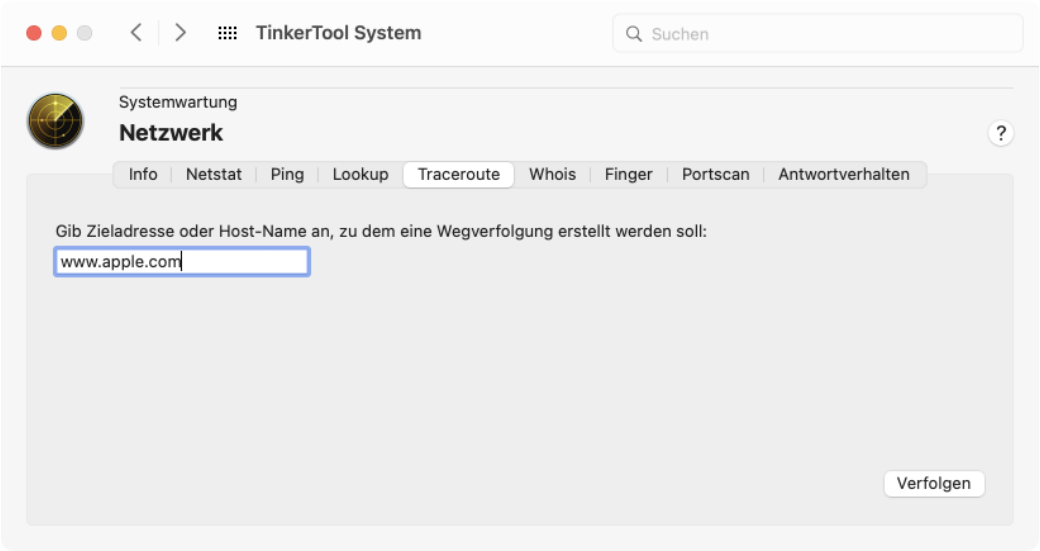

Abbildung 2.39: Der zurzeit gewählte Weg von Datenpaketen kann im Netz nachverfolgt werden

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.

2.8.6 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.

> 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**.

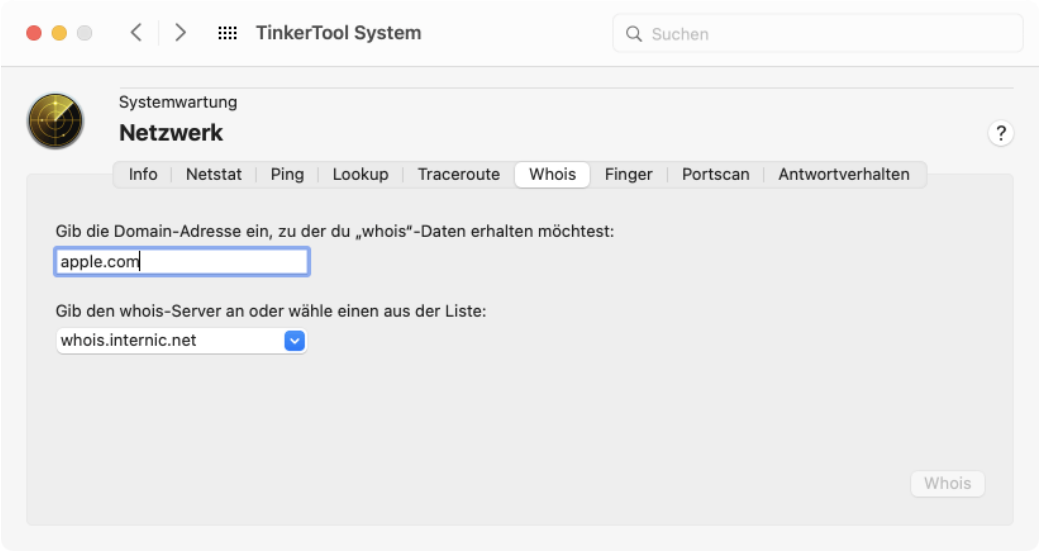

Abbildung 2.40: Der Whois-Dienst des Internet kann abgefragt werden

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.

2.8.7 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

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**.

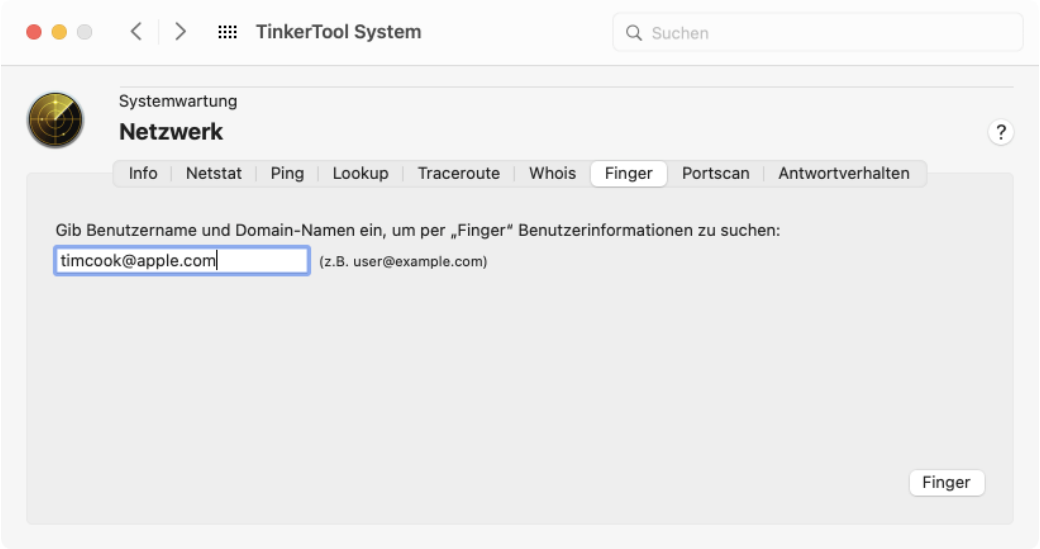

Abbildung 2.41: Daten über Netzwerkbenutzer kann der Finger-Dienst bereitstellen

> 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.

2.8.8 Offene IPv4-Ports suchen

Adressen werden benutzt, um bestimmte Geräte, bzw. deren Anschlüsse im Netzwerk ansprechen zu können. *Ports* werden benutzt, um bestimmte Kommunikationsendpunkte (Sockets) auf einem Netzwerkgerät auswählen zu können. Ein solcher Port stellt in der Regel einen bestimmten Netzwerkdienst zur Verfügung und wird über eine zugeordnete Zahl zwischen 0 und 65.535 angesprochen. Der in diesem Kapitel erwähnte Dienst DNS wird zum Beispiel üblicherweise auf Port 53 des jeweiligen Server-Computers erreicht. Ein verschlüsselnder Web-Server *(HTTP over SSL)* bietet seinen Dienst üblicherweise auf Port 443 an.
Es ist technisch möglich, zu prüfen, ob ein bestimmtes Netzwerkgerät einen Port auf einer bestimmten Nummer geöffnet hat, auch ohne dass echte Nutzdaten an diesen Port gesendet werden müssen. Dadurch lässt sich indirekt bestimmen, ob das Gerät den zu einer Nummer passenden Dienst anbietet, bzw. ob dieser Dienst erreichbar ist. Durch Durchprobieren eines Nummernbereichs lässt sich auf diese Weise ausspionieren, welche Netzwerkdienste auf einem bestimmten Gerät wahrscheinlich ansprechbar sind, ohne dass dies im Vorhinein bekannt sein muss.
Wenn ein bestimmter Dienst nicht für ein bestimmtes Netz oder für die Öffentlichkeit bestimmt ist, lässt sich aber auch umgekehrt prüfen, ob der zugehörige Port erfolgreich gesperrt, bzw. der Dienst tatsächlich nicht erreichbar ist. Das Suchen nach offenen Ports wird *Portscan* genannt. Führen Sie die folgenden Schritte durch, um einen Portscan durchzuführen:

1. Öffnen Sie den Punkt **Portscan** auf der Karte **Netzwerk**.
2. Geben Sie das gewünschte Ziel entweder per IPv4-Adresse oder per Name in das Textfeld ein und drücken Sie die Eingabetaste.
3. Wählen Sie aus, ob Sie alle denkbaren Ports oder nur einen bestimmten Port-Bereich überprüfen lassen möchten. Es ist zulässig, wenn der angegebene Bereich nur aus einer einzelnen Port-Nummer, beispielsweise „zwischen 80 und 80“ besteht.
4. Klicken Sie auf den Knopf **Scannen**.

> Warnung: Verwenden Sie diese Funktion nur, wenn Sie die Genehmigung des Eigentümers des jeweiligen Zielcomputers haben. Aufgrund der erwähnten Spionagemöglichkeiten kann es als böswilliger Akt gelten, einen Portscan auf ein Gerät in einem fremden Netzwerk durchzuführen. Der Eigentümer oder Ihr Internet-Provider könnte rechtliche oder technische Gegenmaßnahmen einleiten.

2.8.9 Antwortverhalten (nur macOS 12 oder höher)

> Diese Funktion wird von macOS 11 Big Sur nicht angeboten.

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

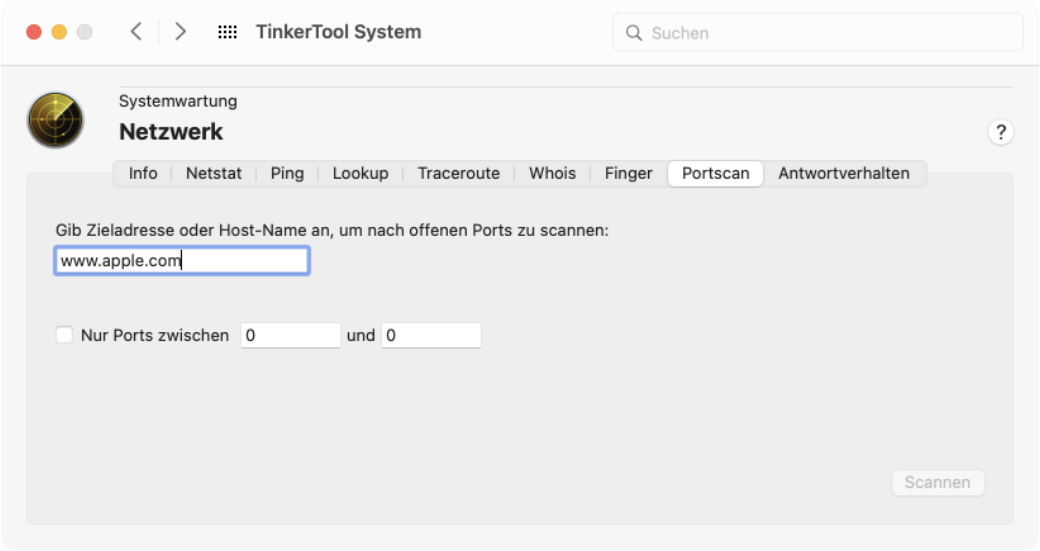

Abbildung 2.42: Es kann geprüft werden, auf welchen Ports andere Computer Netzwerkdienste anbieten

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
- **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.

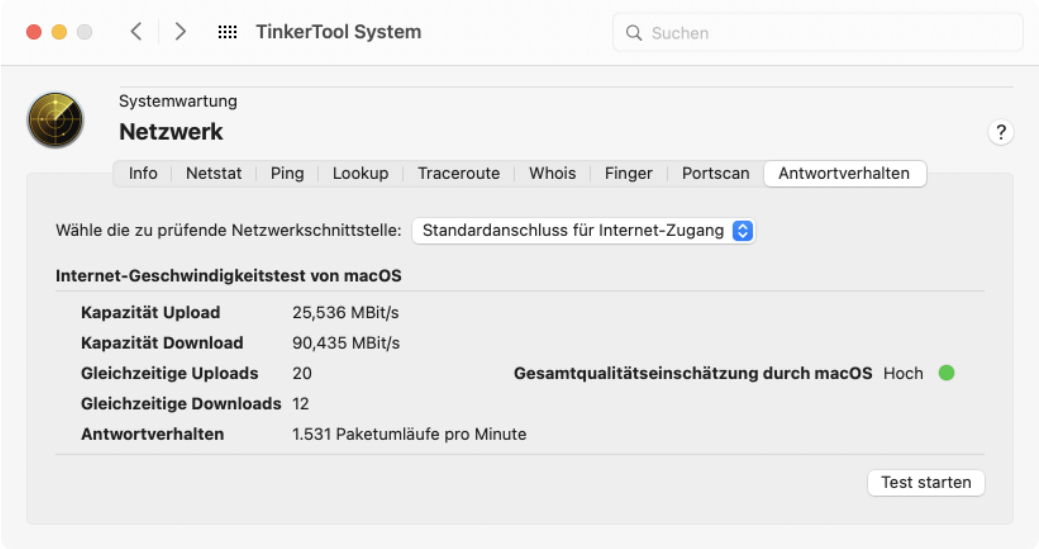

Abbildung 2.43: macOS kann das typische Antwortverhalten Ihres Netzwerks beurteilen und die Qualität einschätzen

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.

2.9 Die Einstellungskarte Info

2.9.1 Systemdaten

Der Karteireiter **Systeminformationen** 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 und ein Bild dieser Baureihe, 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.

> 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 **Prozessoren** 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 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

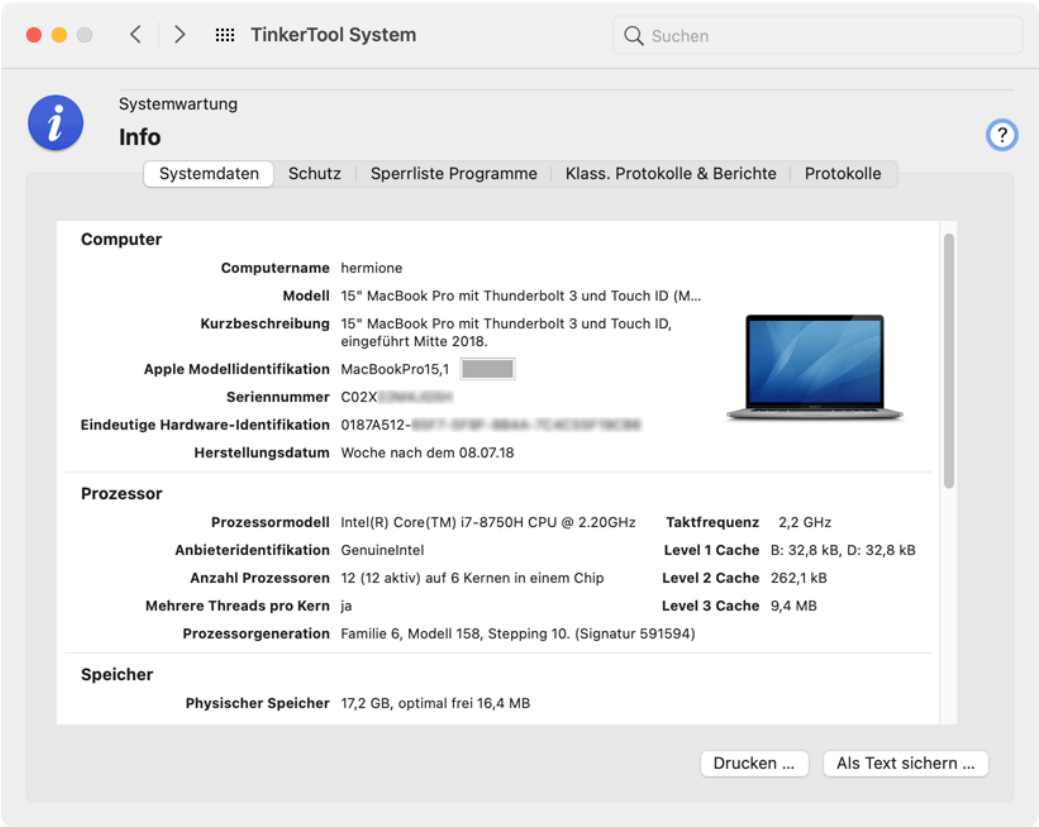

Abbildung 2.44: Systemdaten (Version für Macs mit Intel-Prozessor)

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 2.6 auf Seite 73).
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 Hilfssystem 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.

Betriebsumgebung

Der letzte Abschnitt **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 **Freigabestatus** gibt an, ob Sie eine offiziell freigegebene Version des Betriebssystems verwenden oder eine Vorabversion aus einer von Apples Software-Verteilungsaktionen *(Seeding Program)*.

> Beachten Sie, dass die Quelle des Betriebssystems bei der Definition des Freigabestatus wichtiger einzustufen ist, als dessen Versionsnummer. Wenn Sie eine bestimmte Systemversion vorab erhalten, könnte exakt das gleiche System später zu einer offiziellen Version werden. Das heißt identische Betriebssysteme können manchmal als offiziell, manchmal als Vorabexemplar angegeben sein, je nach dem, woher sie stammen.

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 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 vertrauensvolle 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 vertrauensvolle 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**.
Es ist möglich, den Inhalt des Hauptinformationsfensters 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.

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

2.9.2 Malware-Schutz

macOS enthält mehrere eingebaute Schutzmaßnahmen gegen böswillige Software *(Malware)*. Eine dieser Schutzvorrichtungen arbeitet wie ein Virenscanner, 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 **Systemdatendateien und Sicherheits-Updates installieren** auf der Einstellungskarte **App Store** 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.
Über den Karteireiter **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.
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 Schad-

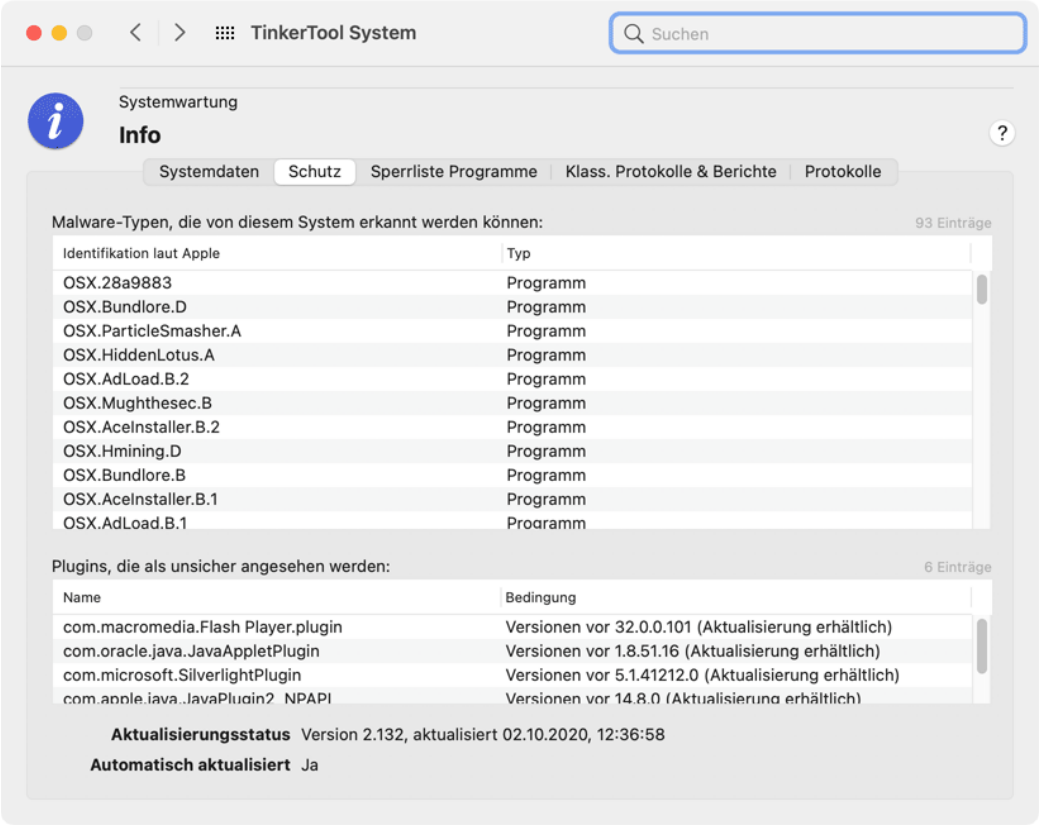

Abbildung 2.45: Malware-Schutz

software 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.

- Die Angaben in den Spalten **Typ** und **Name** können variieren, je nach dem, welche Version von macOS Sie einsetzen und welche anderen Programme auf Ihrem Computer vorhanden sind. Es kann beispielsweise eine interne technische Bezeichnung, ein englischer Name oder ein Name in der von Ihnen eingestellten Landessprache angezeigt werden.

2.9.3 Sperrliste Programme

Nachdem Sie den Karteireiter **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 **Systemdatendateien und Sicherheits-Updates installieren** auf der Einstellungskarte **App Store** 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-* 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.

Jede Tabelle hat drei Spalten mit der folgenden Bedeutung:

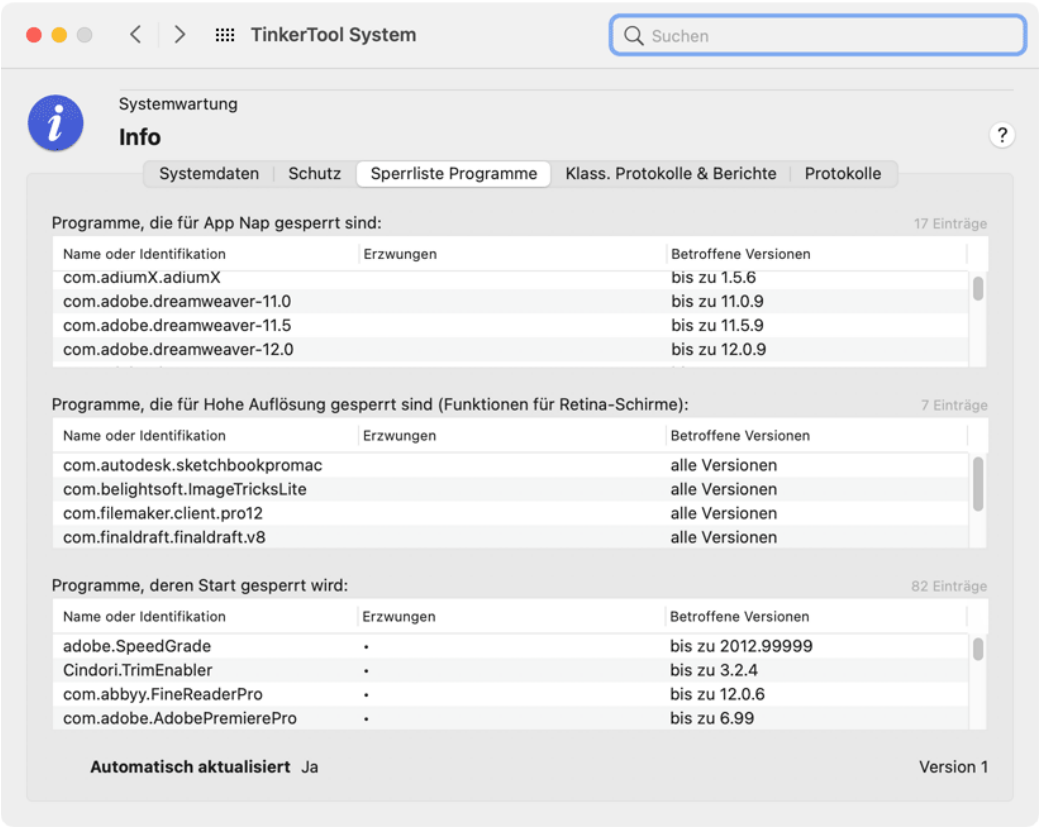

Abbildung 2.46: Sperrliste Programme

- **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. Falls ein Sperrvermerk nicht erzwungen ist, können Sie das Programm über den Finder entsperren. Hinweise hierzu finden Sie im nächsten Absatz.

- **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.

Sie können Apples Empfehlung zur Sperrung gewisser Funktionen für bestimmte Programme übergehen, falls Sie dafür einen Grund haben. Führen Sie in diesem Fall die folgenden Schritte durch:

1. Wählen Sie das betroffene Programm im Finder aus.

2. Öffnen Sie den Menüpunkt **Ablage** > **Informationen** oder drücken Sie ⌘ + I.

3. Entfernen Sie das Häkchen bei **App Nap deaktivieren**, beziehungsweise **In niedriger Auflösung öffnen**, falls verfügbar.

4. Schließen Sie das Info-Fenster.

2.9.4 Klassische Protokolle und Berichte

Nach Auswahl des Karteireiters **Klass. Protokolle & Berichte** haben Sie direkten Zugriff auf eine hohe Zahl von Protokollaufzeichnungen, die von macOS und der App macOS Server vorgehalten werden. 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.
Die möglicherweise verfügbaren Protokolle und Berichte können über drei 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.

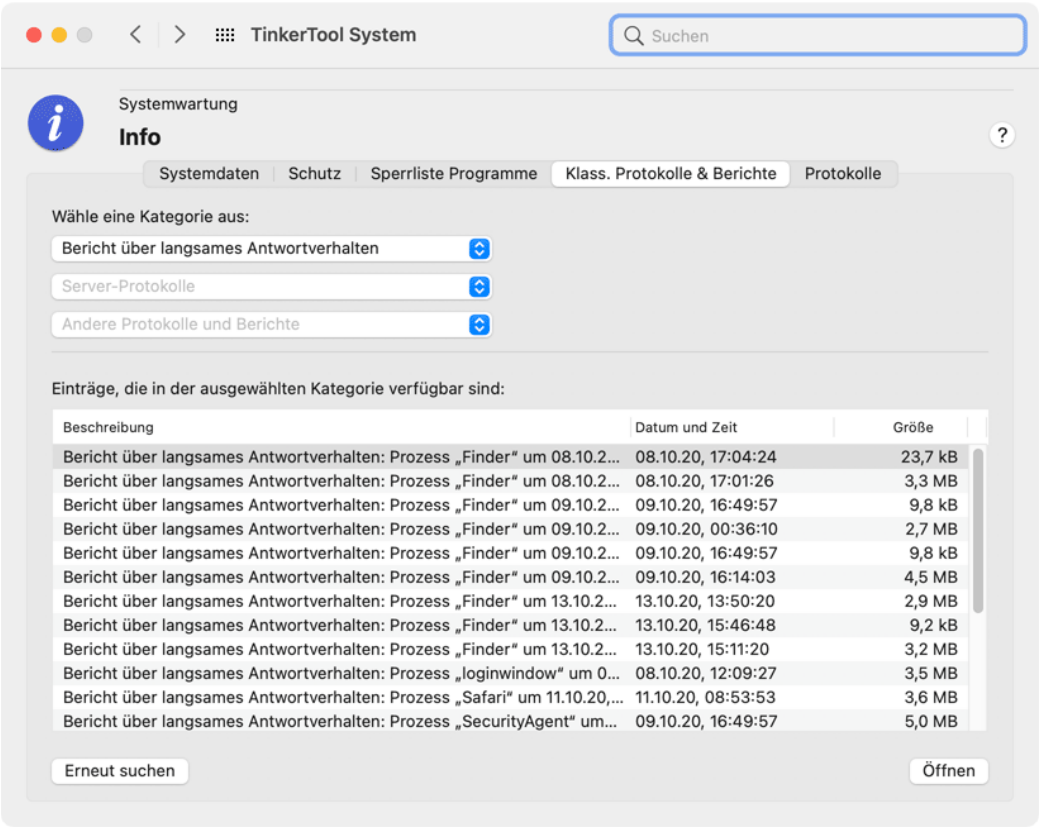

Abbildung 2.47: Protokolle und Berichte

- **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 iTunes, bzw. 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.

Das zweite Klappmenü **Server-Protokolle** erlaubt den Zugriff auf Protokolldateien, die von den Server-Funktionen von macOS geführt werden. Einige dieser Protokolle werden nur dann angelegt, wenn Sie die App macOS Server zusätzlich zu macOS installieren und dort entsprechende Server-Dienste einschalten, aber viele Protokolle beziehen sich allgemein auf Netzwerkserver-Funktionen, die in macOS enthalten sind. TinkerTool System fügt automatisch Menüpunkte zu diesem Knopf hinzu, je nach dem, welche Dienste auf Ihrem System aktiv sind. Die Namen der Protokolle und Berichte sollten selbsterklärend sein und werden an dieser Stelle nicht noch einmal wiederholt. TinkerTool System gruppiert die einzelnen Punkte in die folgenden Dienstkategorien:

- **Open Directory**: Protokolle der Open Directory-Komponenten von Client und Server
- **Profilmanager**: Protokolle des Servers zur Geräteverwaltung (Mobile Device Management, MDM)

Der dritte 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 drei 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.

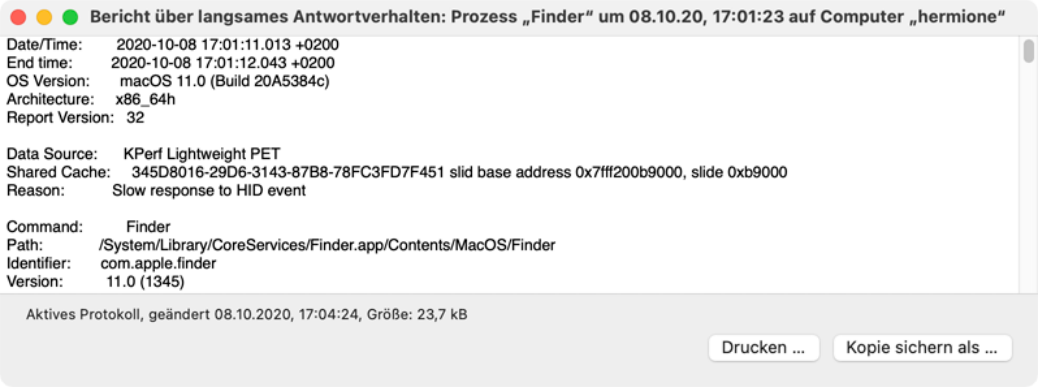

Abbildung 2.48: Der Inhalt eines Protokolls oder Berichts wird in einem getrennten Fenster angezeigt.

> 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.

2.9.5 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.
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-Protokollsubsystembezeichner** 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.
Um mit modernen macOS-Protokollen zu arbeiten, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **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 die Quelle für den Vorgang (falls zutreffend) aus. Dies kann entweder die **aktuelle Protokolldatenbank** des lokalen Computers oder **importierte Protokolldaten** sein.
4. Verwenden Sie das Aufklappmenü bei **Zeitbereich**, um entweder alle verfügbaren Protokolldaten in der gewählten Quelle auszuwählen oder ein bestimmtes Zeitintervall anzugeben. 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.

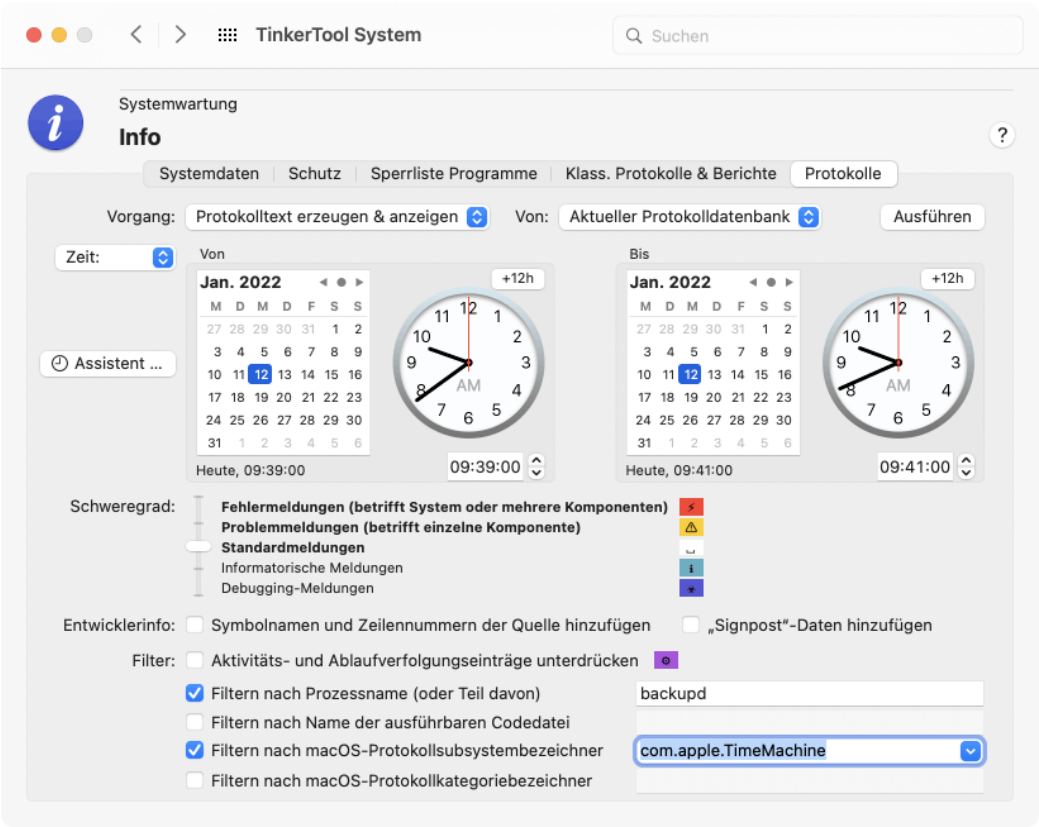

Abbildung 2.49: Arbeiten mit modernen Protokollen

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** in der oberen rechten Ecke.

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 das entsprechende Intervall mithilfe des *Zeitassistenten* einstellen. Klicken Sie hierzu auf den Knopf **Assistent** … neben den Zeiteinstellungen.
In einem zusätzlichen Dialog können Sie nun 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 aktuelle Uhrzeit oder der Systemstart per Knopfdruck gesetzt 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 eine halbe Million Zeilen.

Abbildung 2.50: Anzeige eines macOS-Protokolls

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.

> 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. TinkerTool System kann diese „zensierten“ Teile nicht sichtbar machen. Falls Sie die Farben entfernen, werden die schwarzen Bereiche mit dem Text **private** dargestellt.

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 ⌘ + F.
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.

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 der gleichen Plattenpartition 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.

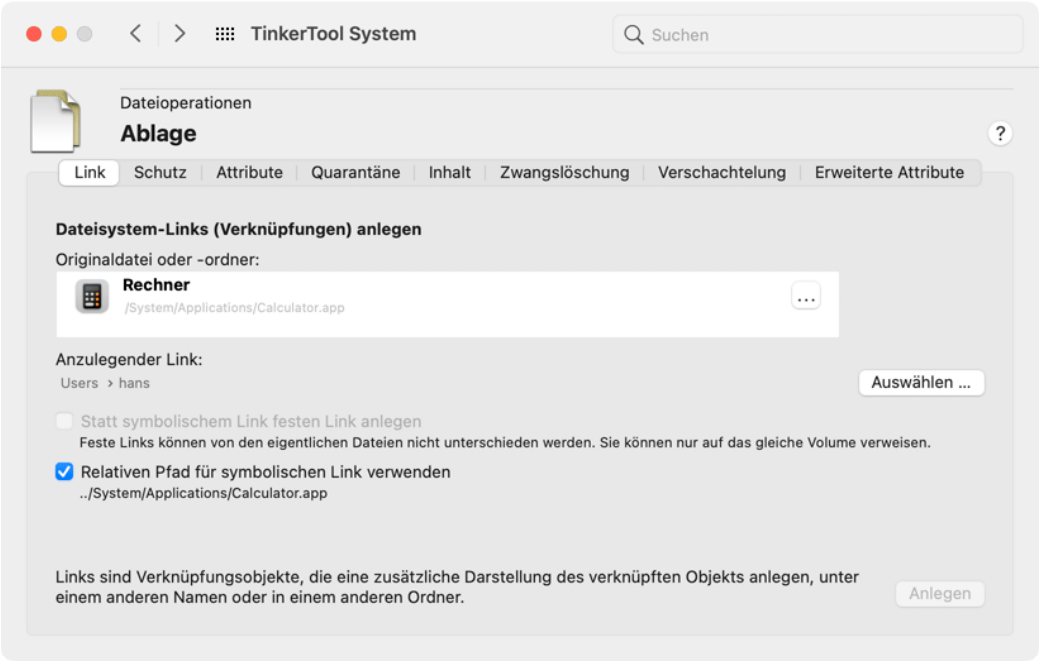

Abbildung 3.1: Link

> 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 Karteireiter **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 „gelockt“, 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.

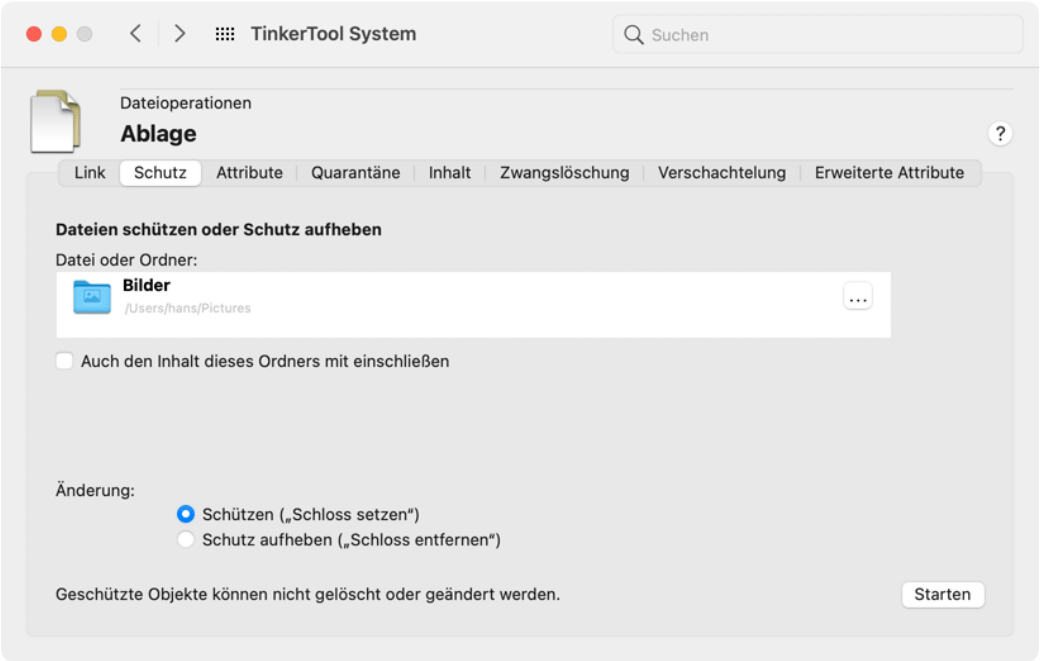

Abbildung 3.2: Schutz

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 Karteireiter **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 Karteireiter **Attribute** 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.

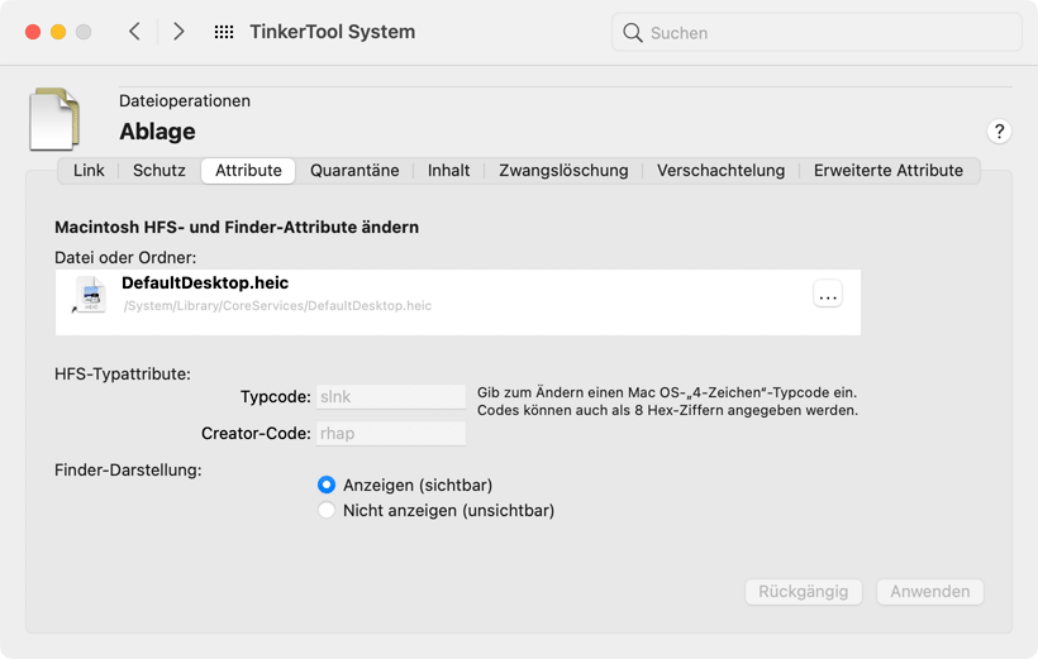

Abbildung 3.3: Attribute

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 könnten jedoch das Schwesterprogramm **TinkerTool** verwenden, um Ihre Finder-Einstellungen so zu verändern, dass der Finder auch unsichtbare Objekte anzeigt.

3.1.4 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.

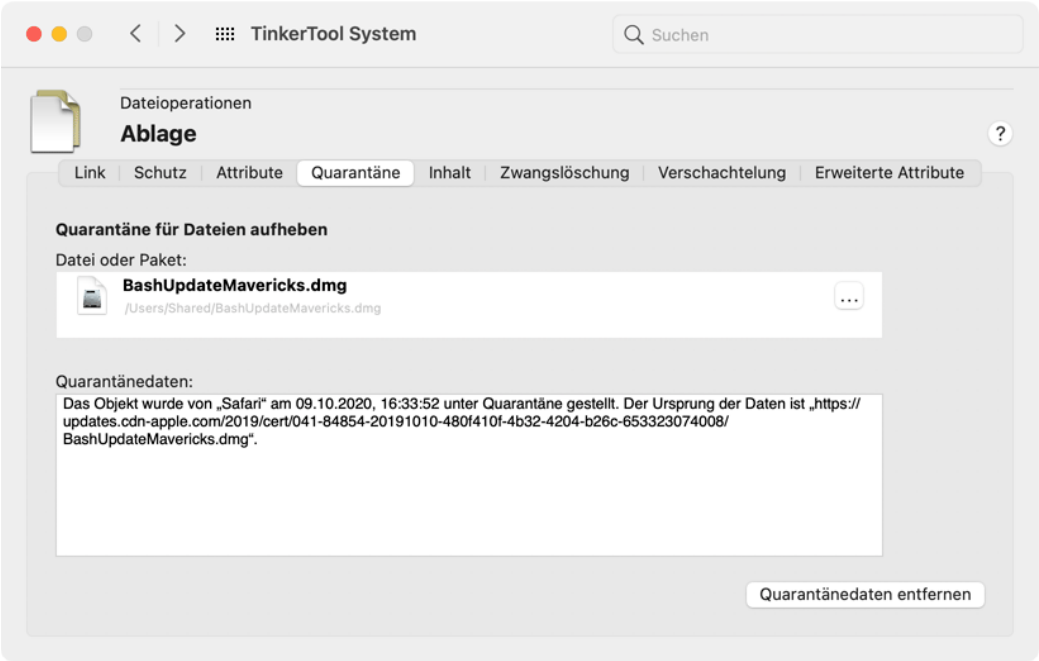

Abbildung 3.4: Quarantäne

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** > **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 Karteireiter **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**.

3.1.5 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 Karteireiter **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.

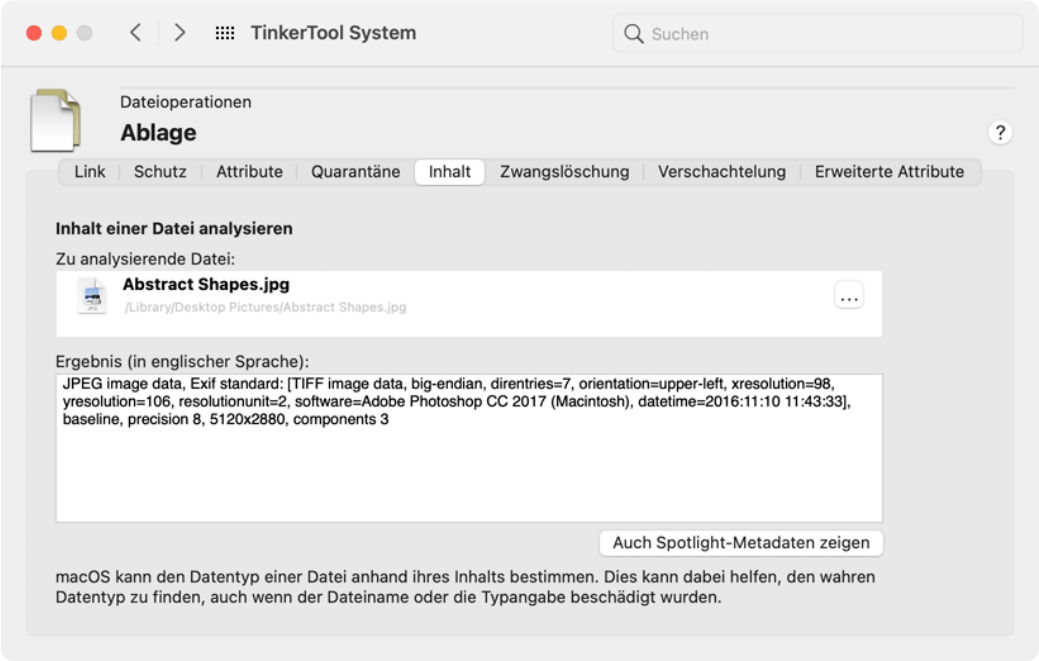

Abbildung 3.5: Inhalt

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.

3.1.6 Zwangslöschung

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

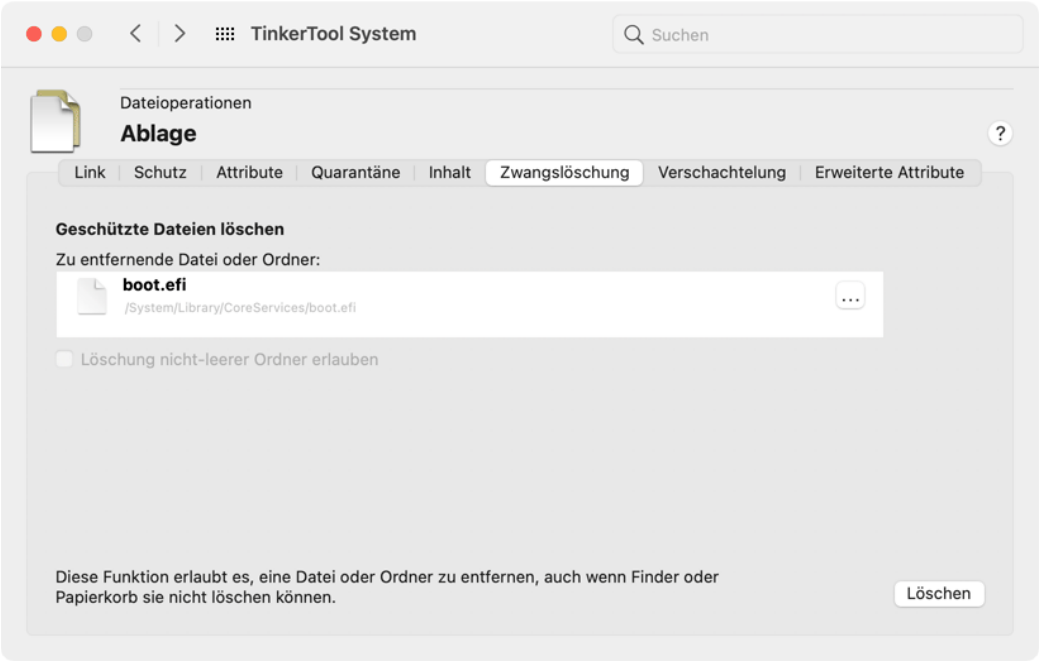

Abbildung 3.6: Zwangslöschung

tenen Objekten gelöscht werden soll. Kreuzen Sie in diesem Fall den Punkt **Löschung nicht-leerer Ordner erlauben** an.

4. Drücken Sie den Knopf **Löschen**.

3.1.7 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, 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-Volume 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 angegeben 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.

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:

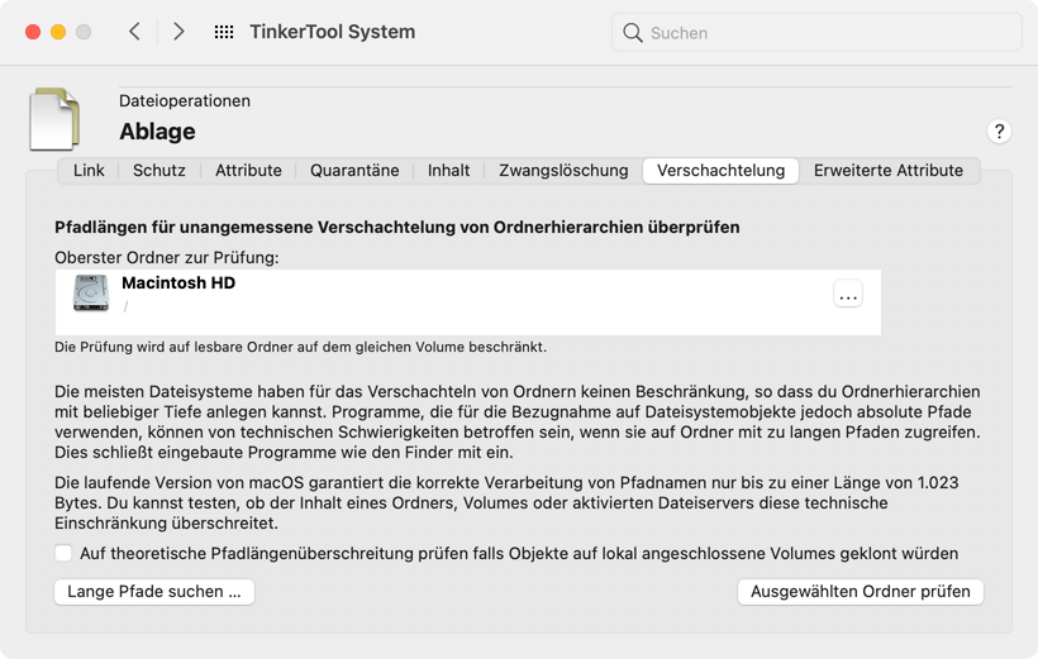

Abbildung 3.7: Suche nach absoluten Pfaden, die für viele Programme zu lang sein könnten

1. Öffnen Sie den Karteireiter **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. 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 würden** 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 Karteireiter **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 angegeben 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.

3.1.8 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 Farbetiketten im 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 Zeit-

punkten vorhanden sind, nun auf der Originalplatte gelandet. Um spätere Sicherungen 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 Leserecht für die betroffenen Ordner und Erweiterten Attribute benötigen. Zum Löschen wird entsprechend Schreibrecht benötigt.

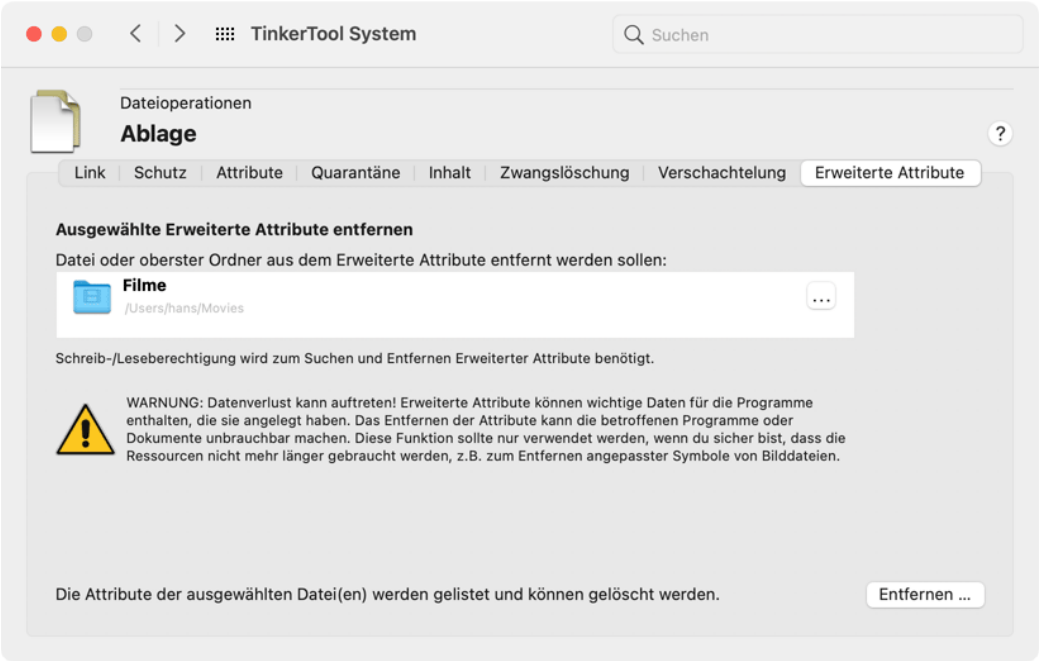

Abbildung 3.8: Erweiterte Attribute entfernen

Führen Sie die folgenden Schritte durch, um Erweiterte Attribute anzuzeigen, bzw. zu löschen:

1. Öffnen Sie den Karteireiter **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 Karteireiters 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 CD-ROM erzeugen, 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 Cover Flow), 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 129) 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 erweitere 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:

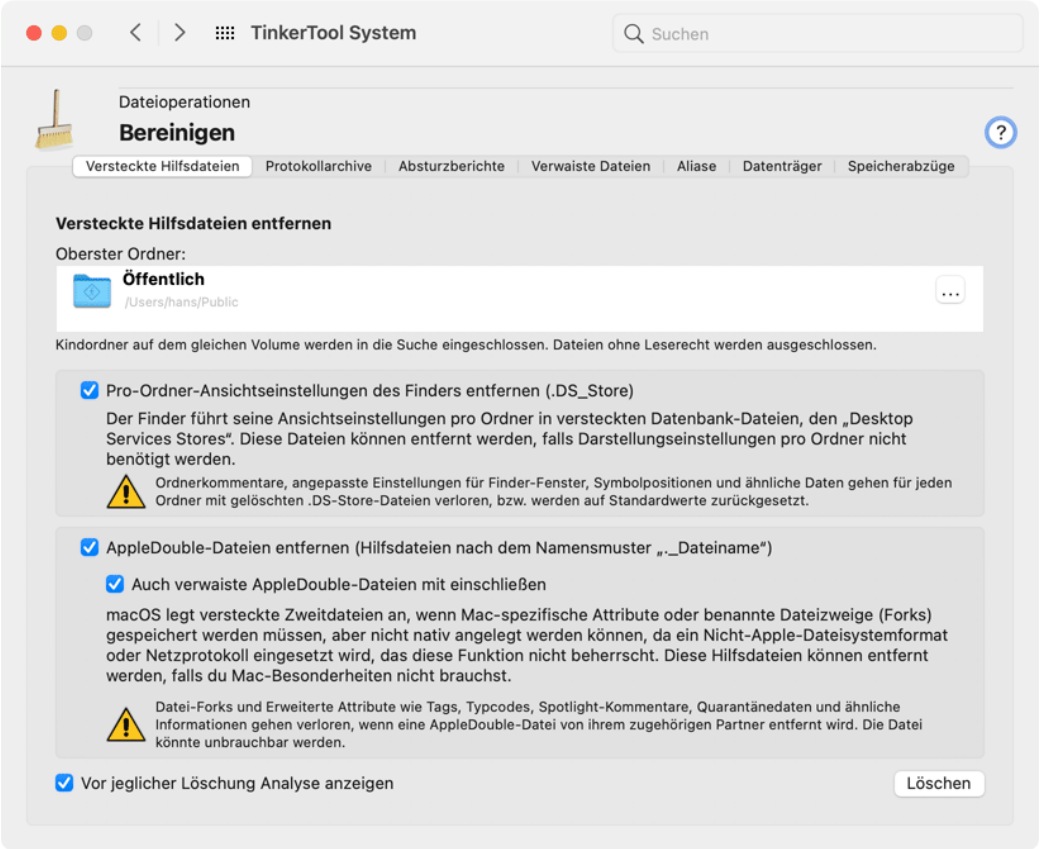

Abbildung 3.9: Versteckte Hilfsdateien

1. Öffnen Sie den Karteireiter **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 2.9 auf Seite 109) 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 Karteireiter **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

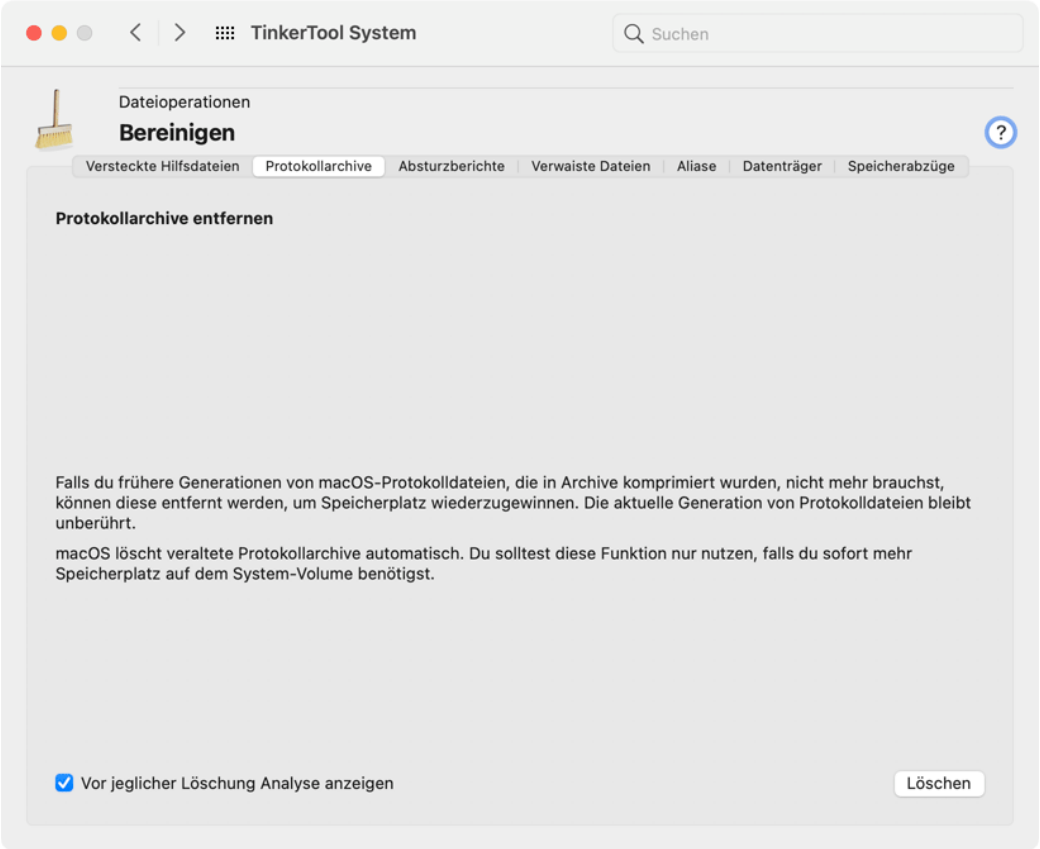

Abbildung 3.10: Protokollarchive

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.

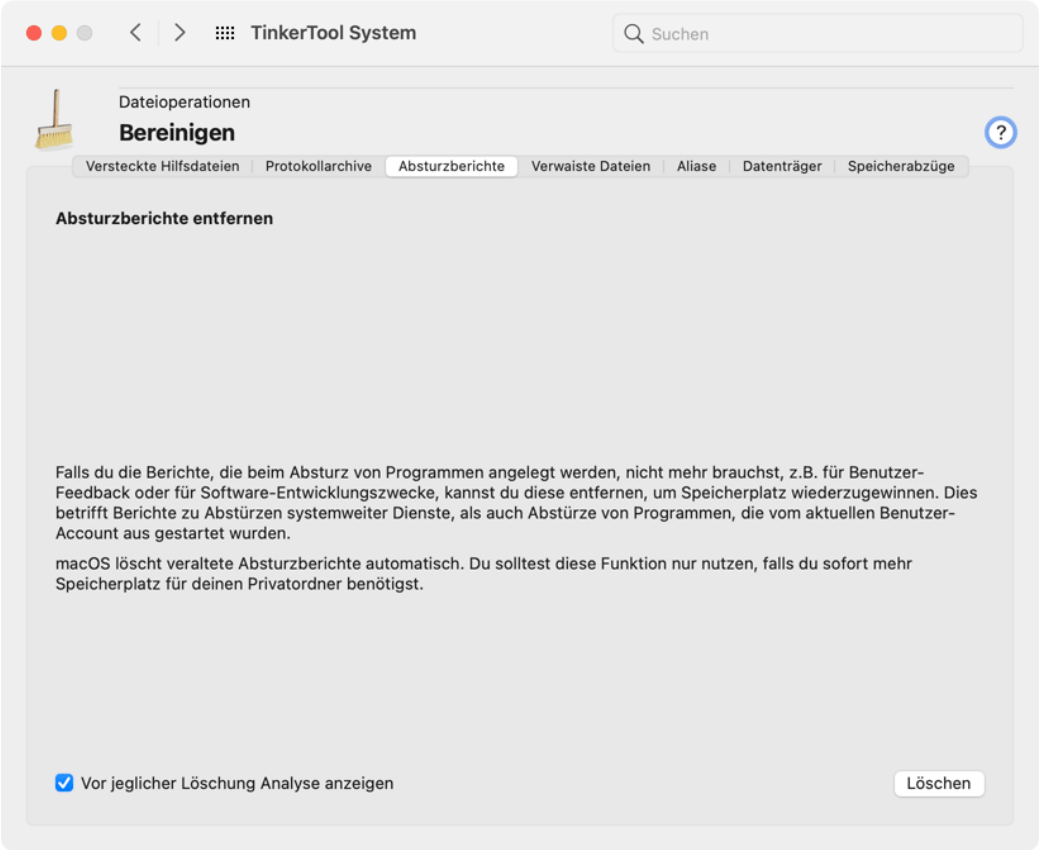

Abbildung 3.11: Absturzberichte

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 Karteireiter **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 zu löschen. 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 167) 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.

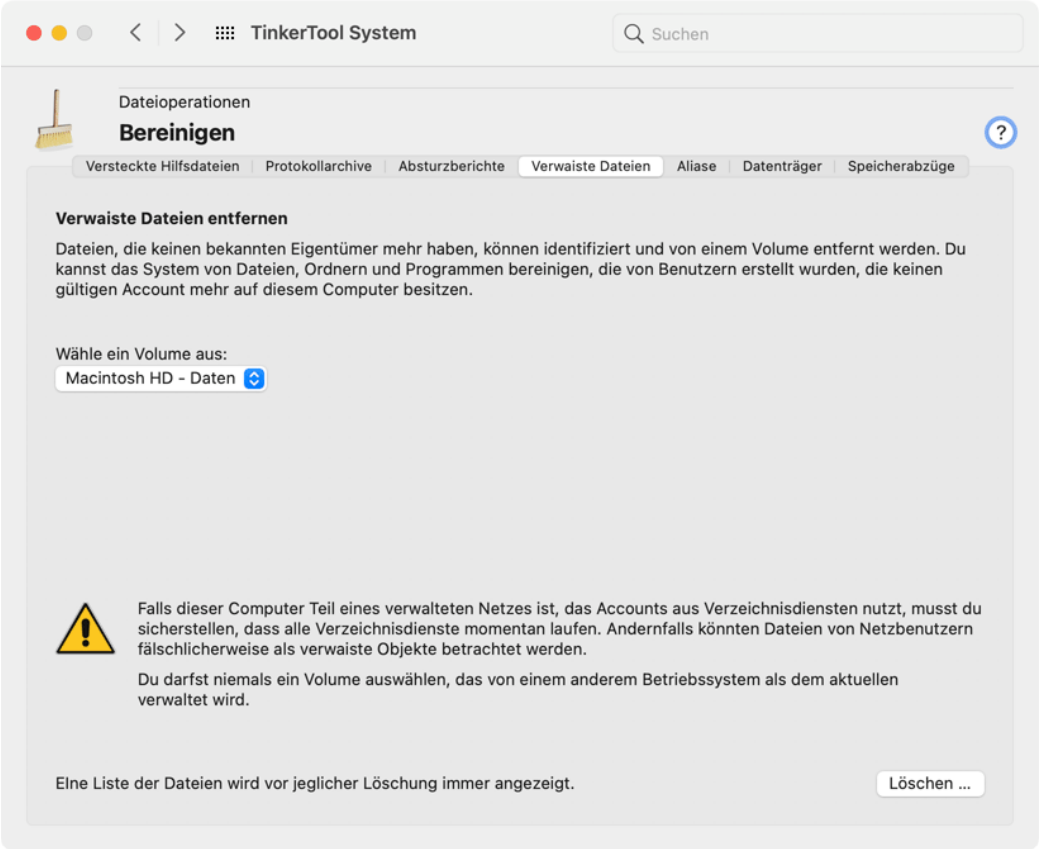

Abbildung 3.12: Verwaiste Dateien

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 und sie gegebenenfalls zu löschen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Verwaiste Dateien** auf der Einstellungskarte **Bereinigen**.
2. Drücken Sie den Knopf **Löschen** ... 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. Falls mehrere verwaiste Dateien gefunden wurden, fragt TinkerTool System Sie, ob Sie eine Liste der Dateipfade in eine Textdatei sichern möchten. Treffen Sie eine Auswahl und folgen Sie den Instruktionen.
5. Die Liste aller betroffenen Dateien und Ordner wird angezeigt. Durch Wählen oder Abwählen von Häkchen in der Spalte **Entfernen?** können Sie bestimmen, welche Objekte gelöscht und welche aufbewahrt werden sollen.
6. Drücken Sie den Knopf **Löschen** im Dialogfenster, um die ausgewählten Objekte zu löschen oder drücken Sie **Abbrechen**, um keinen Vorgang auszulösen.

Falls Sie in Punkt (4) die Entscheidung getroffen haben, eine Berichtsdatei zu erstellen, wird eine Textdatei mit der Namensendung **.txt** erstellt. Dies kann hilfreich sein, wenn Sie die verwaisten Dateien eigentlich gar nicht löschen, sondern stattdessen die Liste überprüfen und die gefundenen Objekte an einen neuen Eigentümer übergeben möchten. Die Datei enthält die vollen Pfade aller Objekte, einen pro Zeile, eingeschlossen in Anführungszeichen. Auf diese Weise kann die Datei leicht editiert und in ein Unix-Skript umgeschrieben werden, das Operationen auf den betroffenen Dateien ausführt.

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 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 129)). 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.

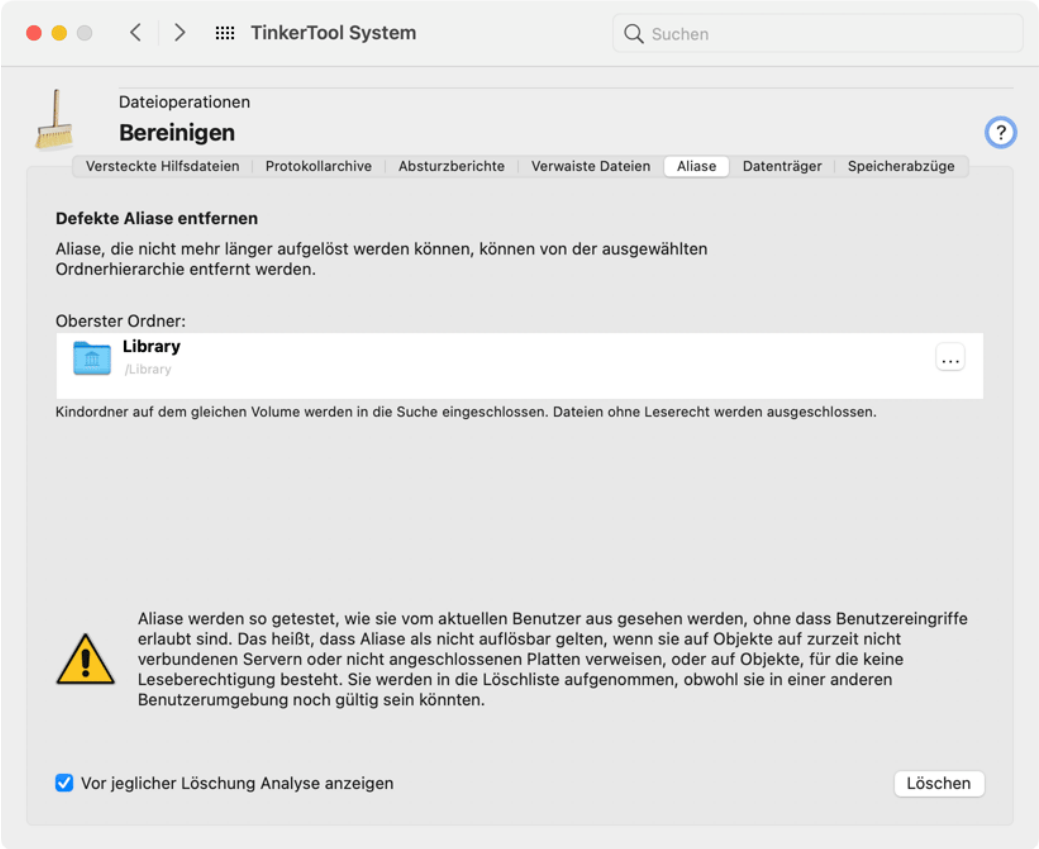

Abbildung 3.13: Aliase

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 Karteireiter **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.
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.
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 Karteireiter **Datenträger** auf der Einstellungskarte **Bereinigen**.
2. Wählen Sie die Platte über das Aufklappmenü **Entnehmbarer Datenträger** aus.
3. Drücken Sie den Knopf **Löschen**.

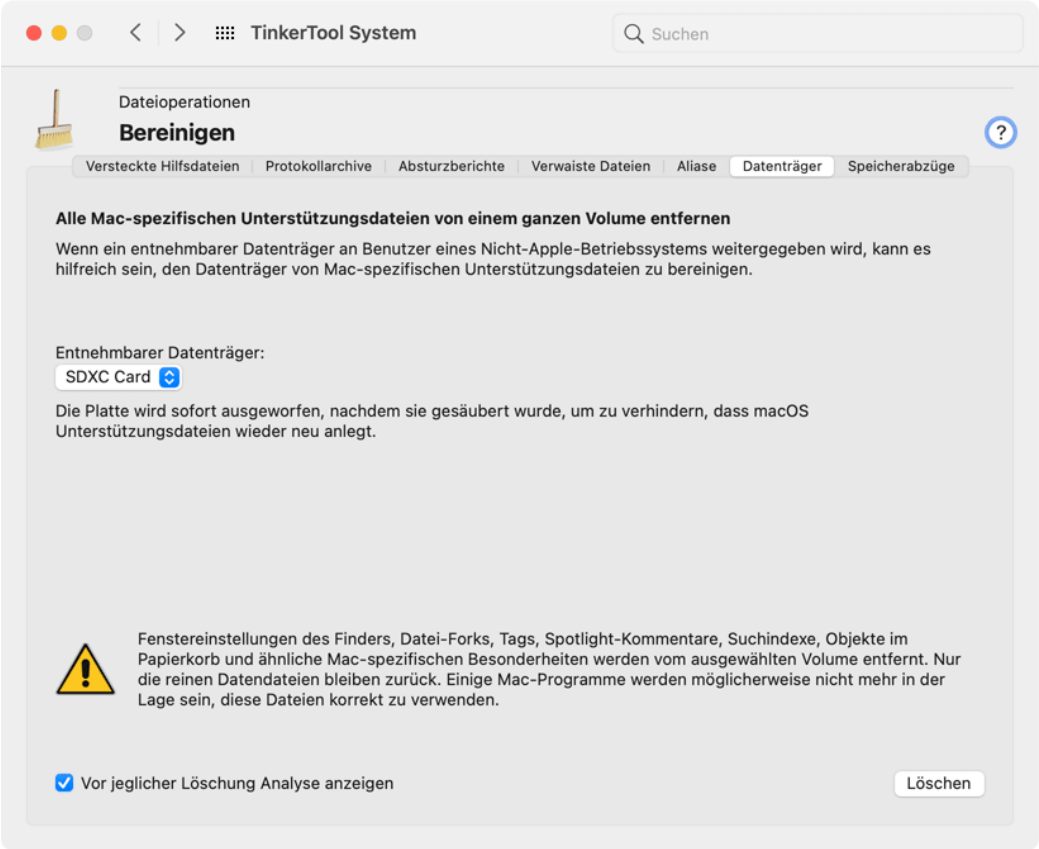

Abbildung 3.14: Entfernbare Platten

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 könnte 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 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 Karteireiter **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 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.

Für „Apps“, die im Mac App Store gekauft wurden, gelten neue, geänderte Regeln: Apps werden automatisch installiert und sollten mit dem Programm *Launchpad* entfernt werden.

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

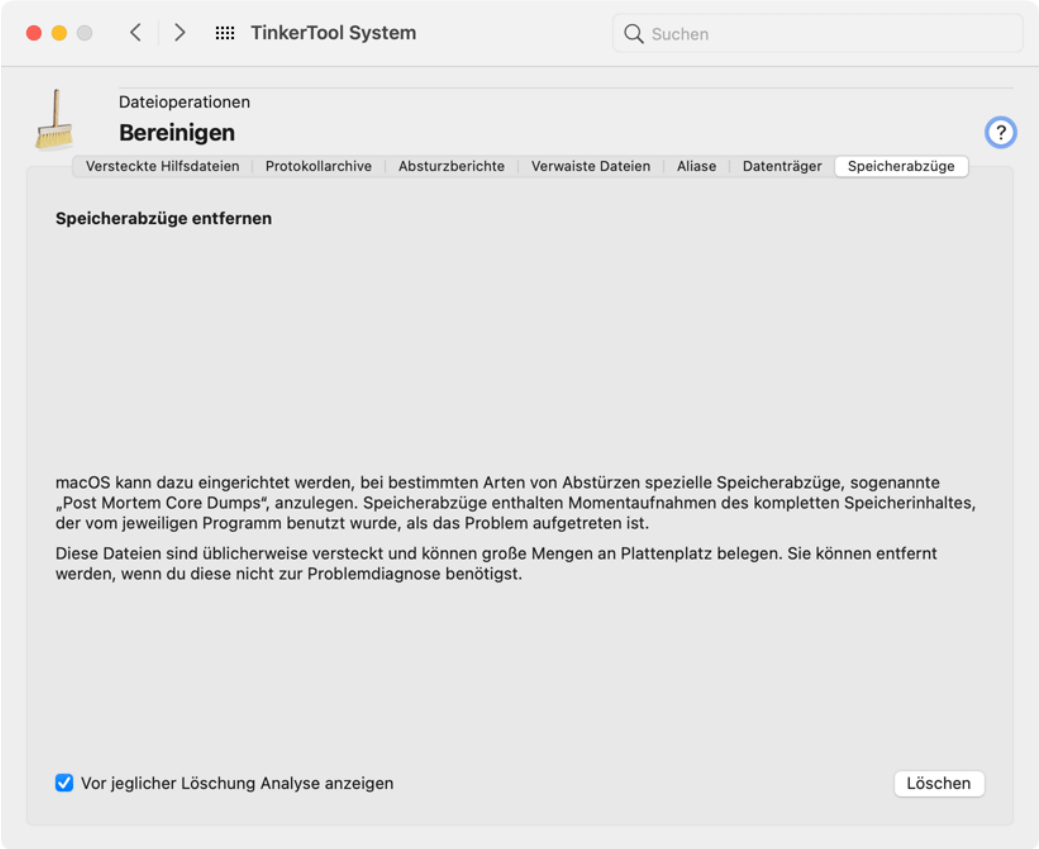

Abbildung 3.15: Speicherabzüge

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.

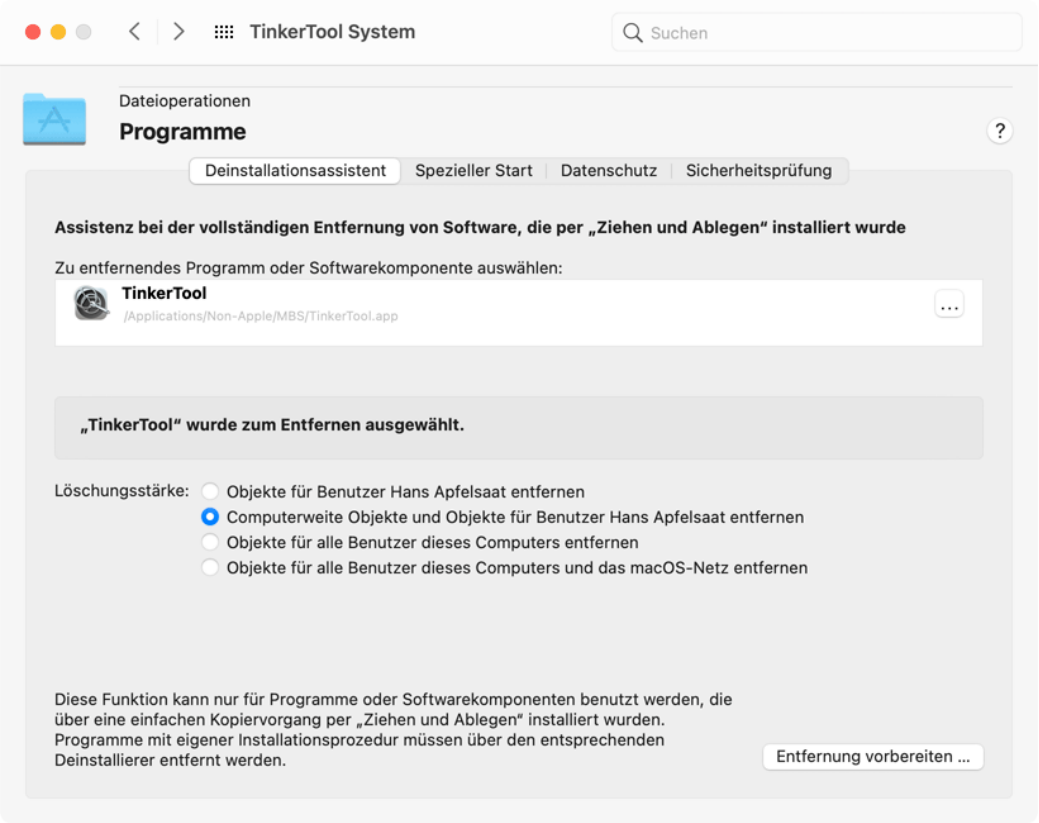

Abbildung 3.16: Deinstallationsassistent

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 Löschungsstärken, 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 Server einsetzen, die Daten in den Ordnern **Netzwerk** > **Programme** (**/Network/Applications**) und **Netzwerk** > **Library** (**/Network/Library**) ablegen.

Falls Sie die Löschungsstärken (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 Karteireiter **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 Löschungsstärken auswählen, indem Sie die Knöpfe bei **Löschungsstärke** 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 **STOP**-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 Löschungsstärken 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 Löschungsstärke 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, wozu auch Apps aus dem Mac App Store gehören, 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.

1. Öffnen Sie den Karteireiter **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.

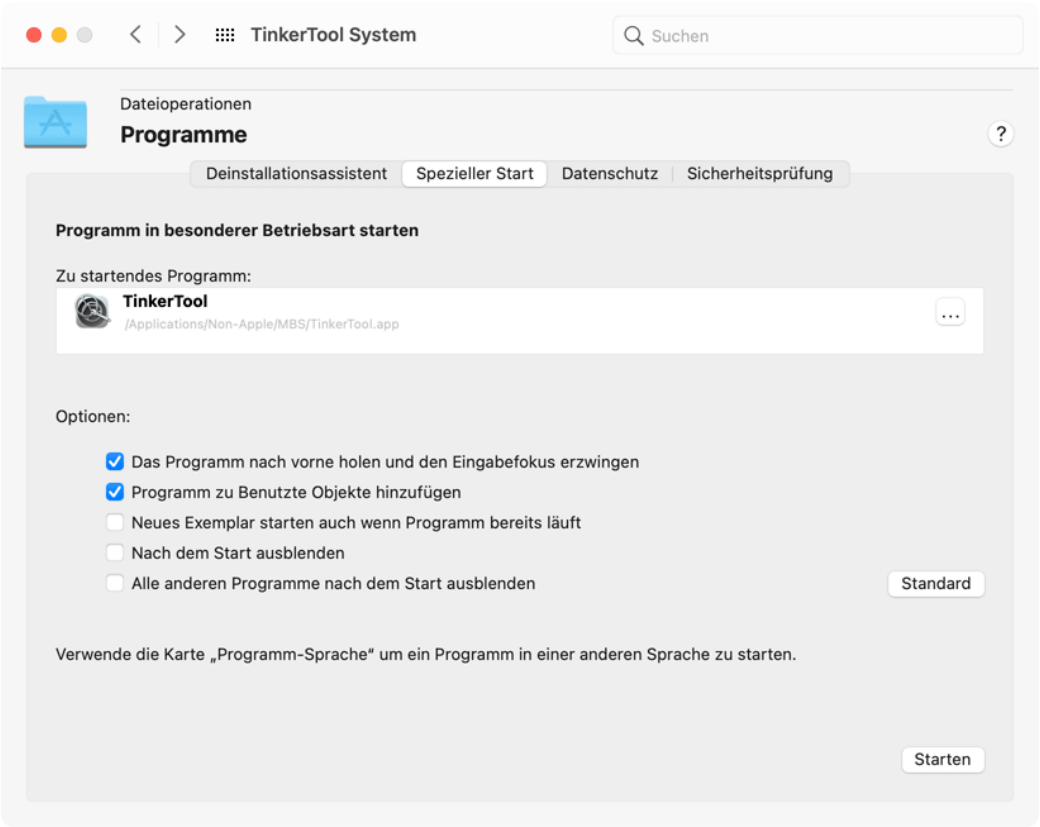

Abbildung 3.17: Programme können mit besonderen Wahlmöglichkeiten gestartet werden

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** > **Sicherheit** > **Datenschutz** 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.

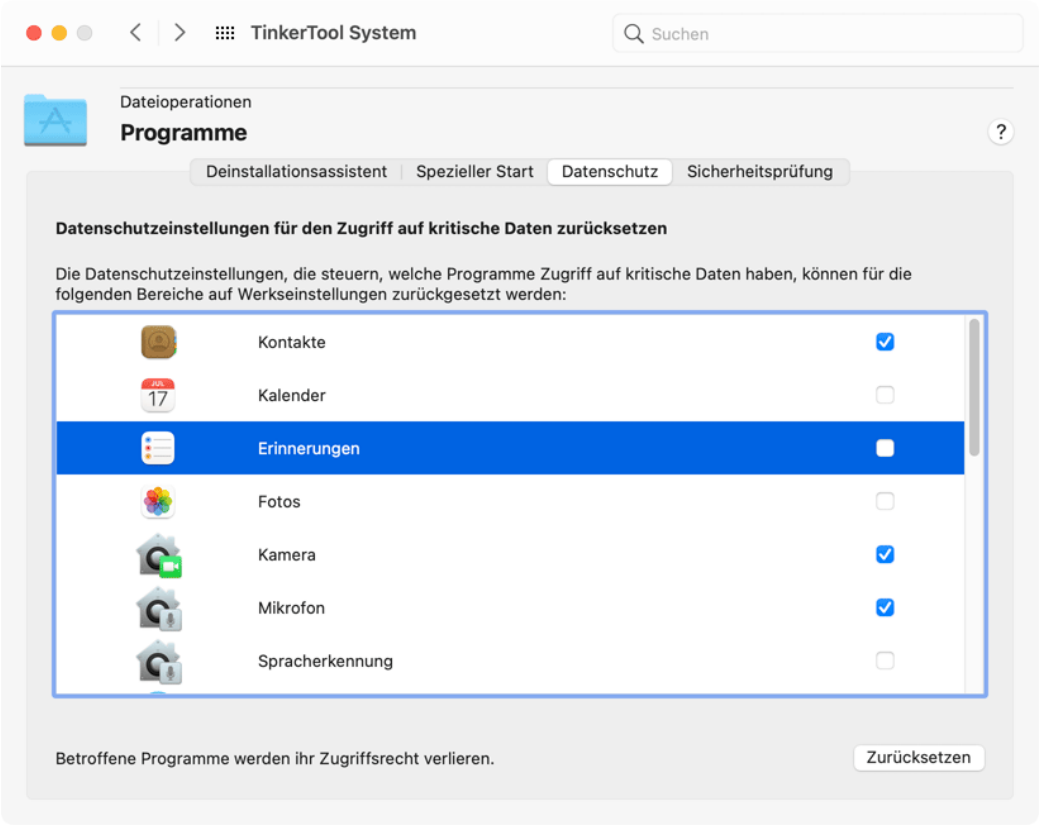

Abbildung 3.18: Datenschutzeinstellungen für Programme zurücksetzen

1. Öffnen Sie den Karteireiter **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 *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.

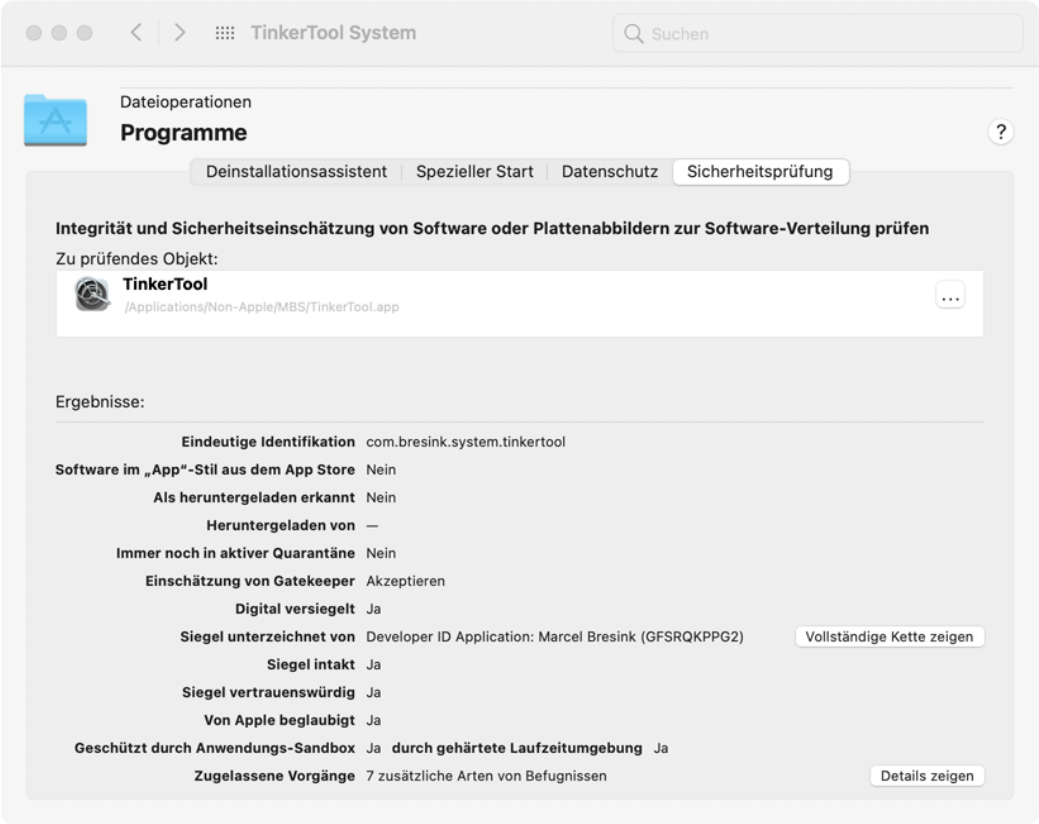

Abbildung 3.19: Sicherheitsprüfung

Das Prüfen eines Programms ist sehr einfach. Führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **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.)
- **Software im „App"-Stil aus dem App Store:** wenn dieser Eintrag auf **Ja** gesetzt ist, haben Sie ein Programm ausgewählt, das von Apple als App im App Store verkauft wurde. Solche „Apps" sind eingeschränkt, in dem Sinne, dass sie gewisse Aktionen nicht durchführen und bestimmte Funktionen von macOS nicht nutzen dürfen. Die Einschränkungen werden über einen Satz von App-Regeln durch Apple festgelegt. Die Einhaltung dieser Regeln wird zusätzlich durch ein *App Review Team* bei Apple geprüft. In den meisten Fällen garantiert diese Prüfung auch ein bestimmtes Mindestniveau der Produktqualität.
- **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.
- **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** > **Sicherheit** > **Apps-Download erlauben 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 „virenfrei“ 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 Privatordner des Benutzers auszulesen, ohne vorher den Benutzer darüber zu informieren, sind zwei Befugnisse des Typs **Lesezugriff auf angegebene Datei im Privatordner 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 eingebauter 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 einer 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.

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 berechtigungsähnlichen 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 anderen 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 Ordner 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 * 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 **Freigabe & 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 Karteireiter **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 geerbt oder explizit ist,
- die Vererbungseinstellungen.

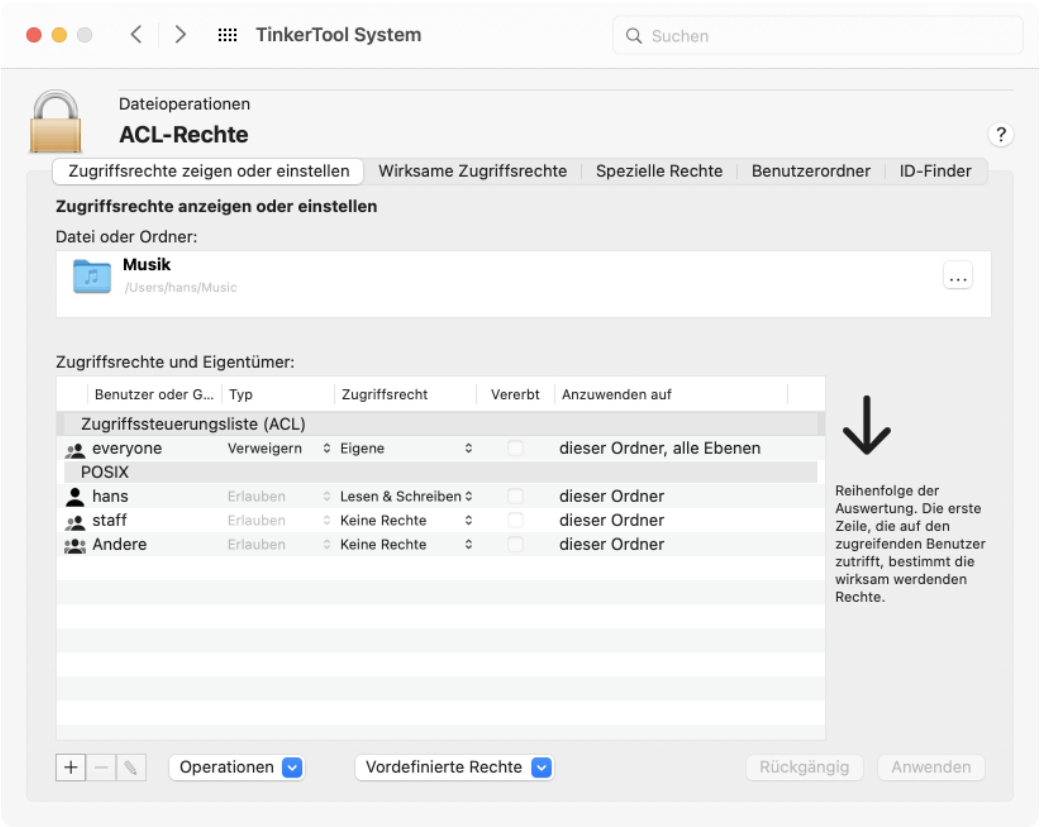

Abbildung 3.20: Zugriffsrechte zeigen oder einstellen

> 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.

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).

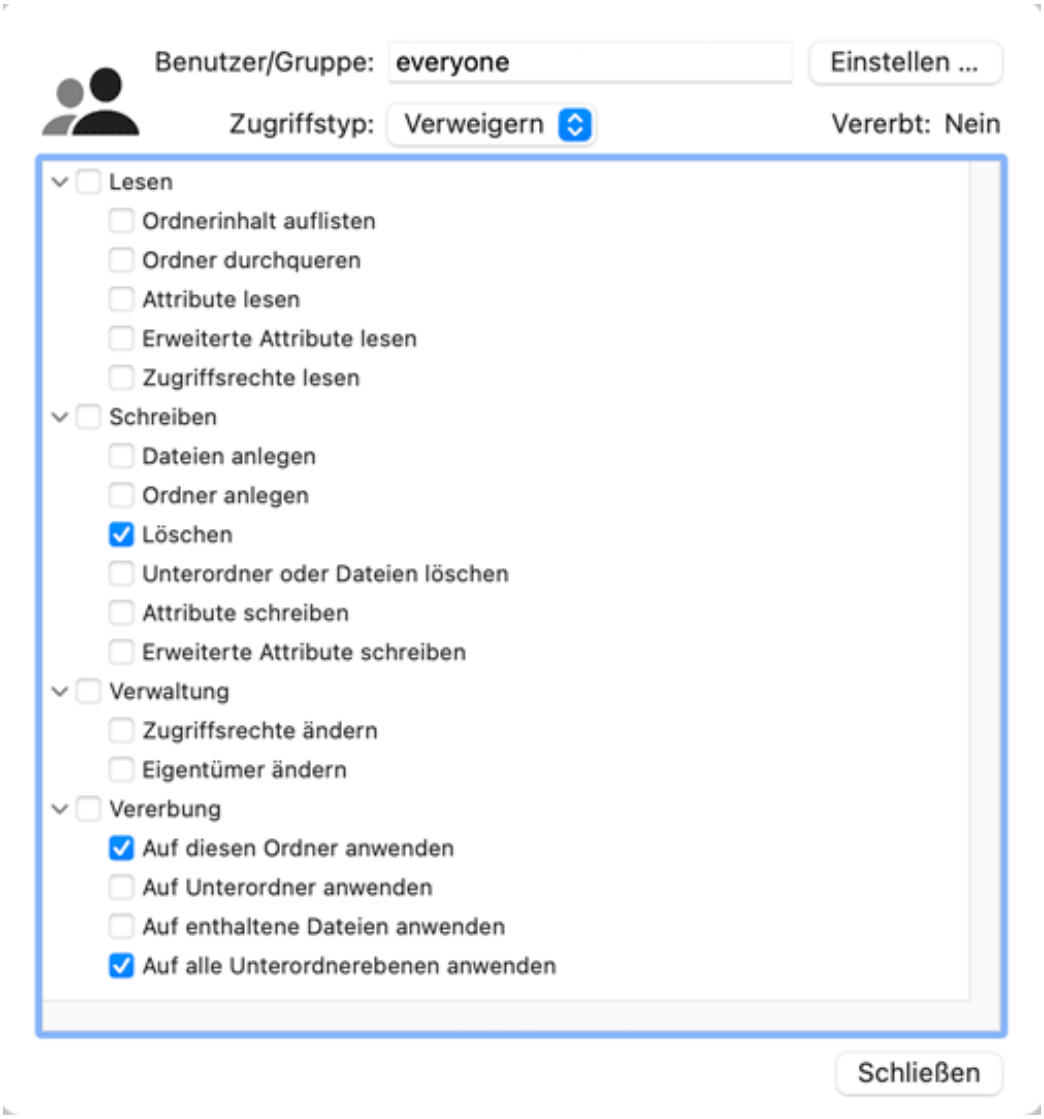

Abbildung 3.21: Berechtigungseinstellungen im Detail

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 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 129) 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 Zugrifssteuerungsliste 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 Karteireiter **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 Karteireiter **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 Karteireiter **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 Karteireiter **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.

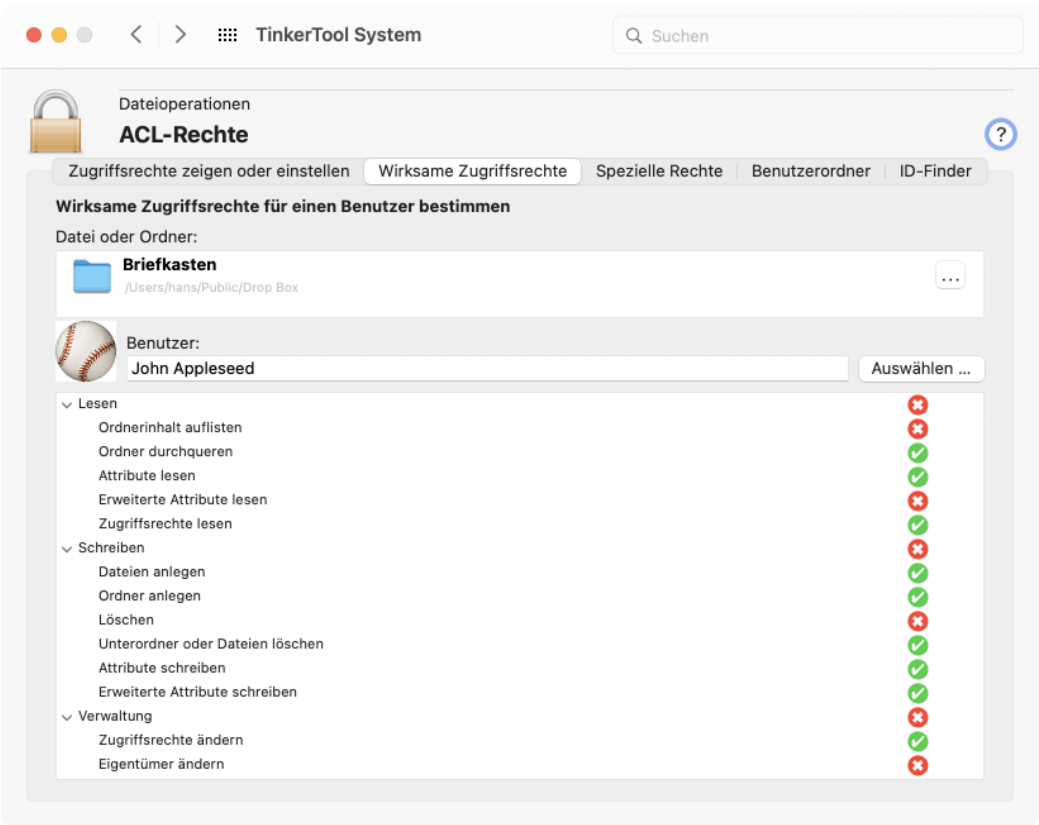

Abbildung 3.22: Wirksame Zugriffsrechte

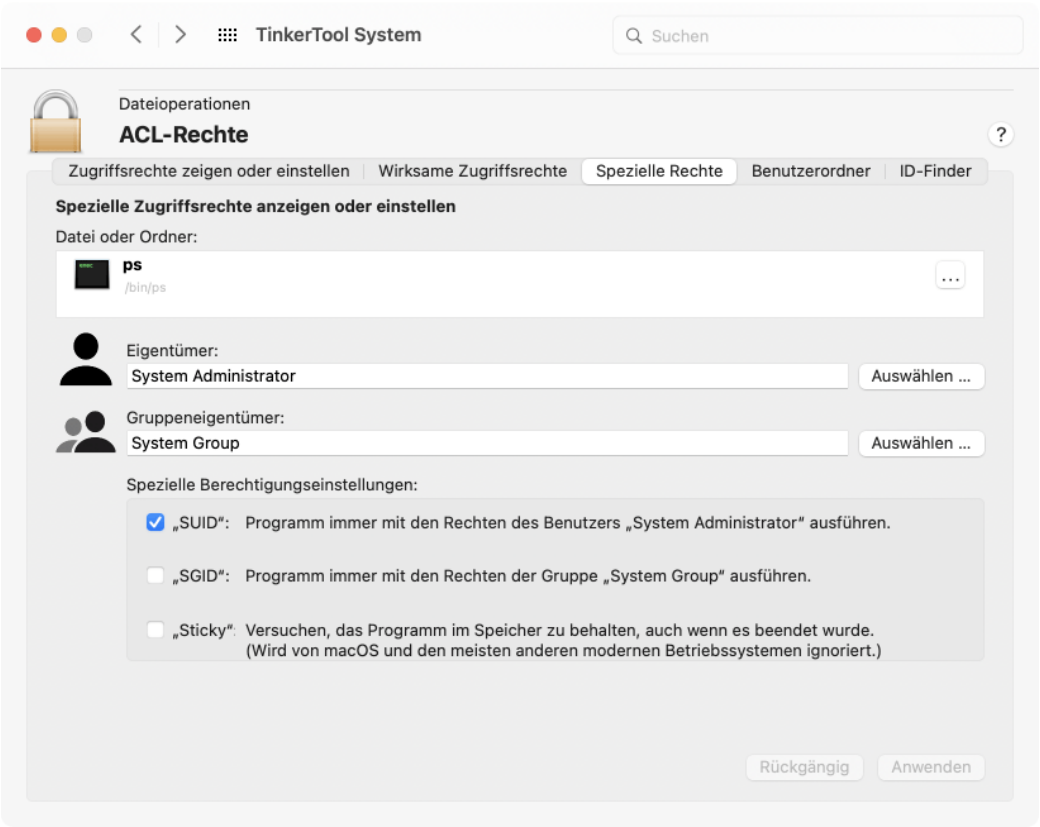

Abbildung 3.23: Spezielle Rechte

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.

3.4.8 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.

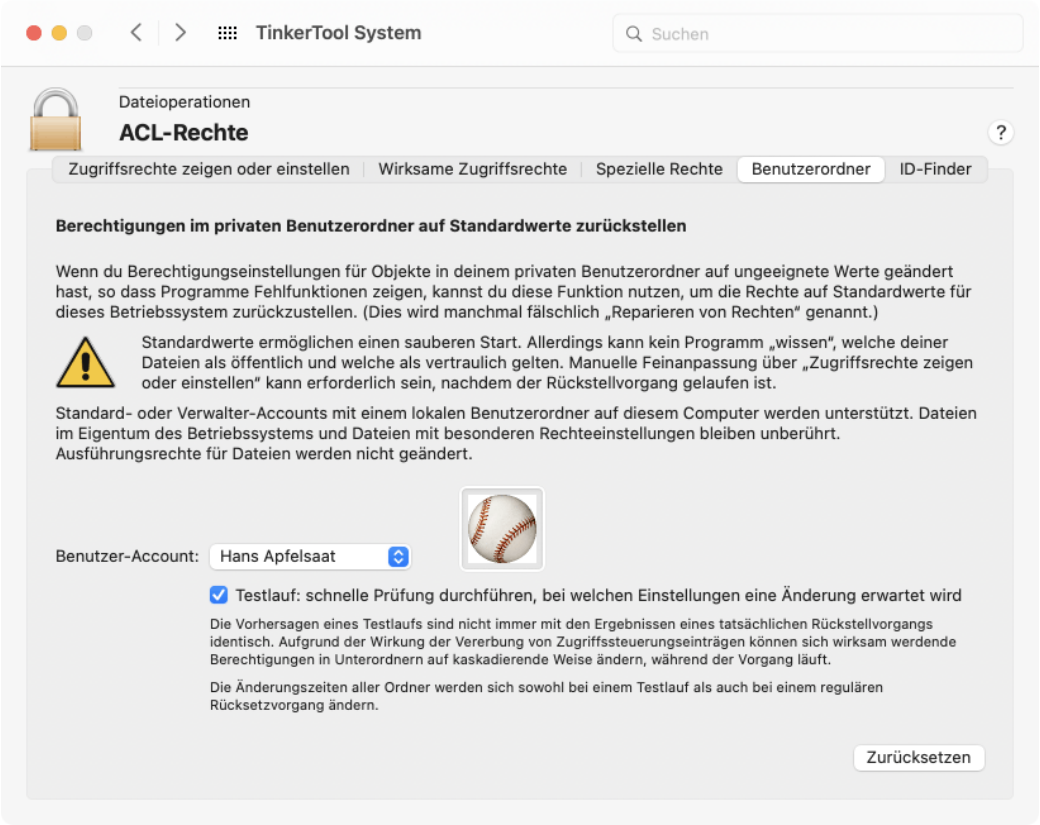

Abbildung 3.24: Verstellte Berechtigungen in einem Benutzerordner können auf Standardvorschläge zurückgestellt werden

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 dem Betriebssystem in Form der obersten Systemautorität *„root"* gehören (z.B. Teile des Spotlight-Index) oder Daten, die *Spezielle Rechte* (siehe voriger Abschnitt) aufweisen, bleiben diese aus Sicherheitsgründen immer unberührt.
- 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.
>
> Aus technischen Gründen ändert sich bei jedem Rücksetzvorgang der Eintrag *Datum der letzten Änderung* bei jedem Ordner im Benutzerordner. Dies gilt auch für einen Testlauf. Dateien sind hiervon nicht betroffen.

Um die Rechte im Privatordner eines lokalen Benutzers auf einen funktionsfähigen Vorschlag zurückzustellen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **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.

3.4.9 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.

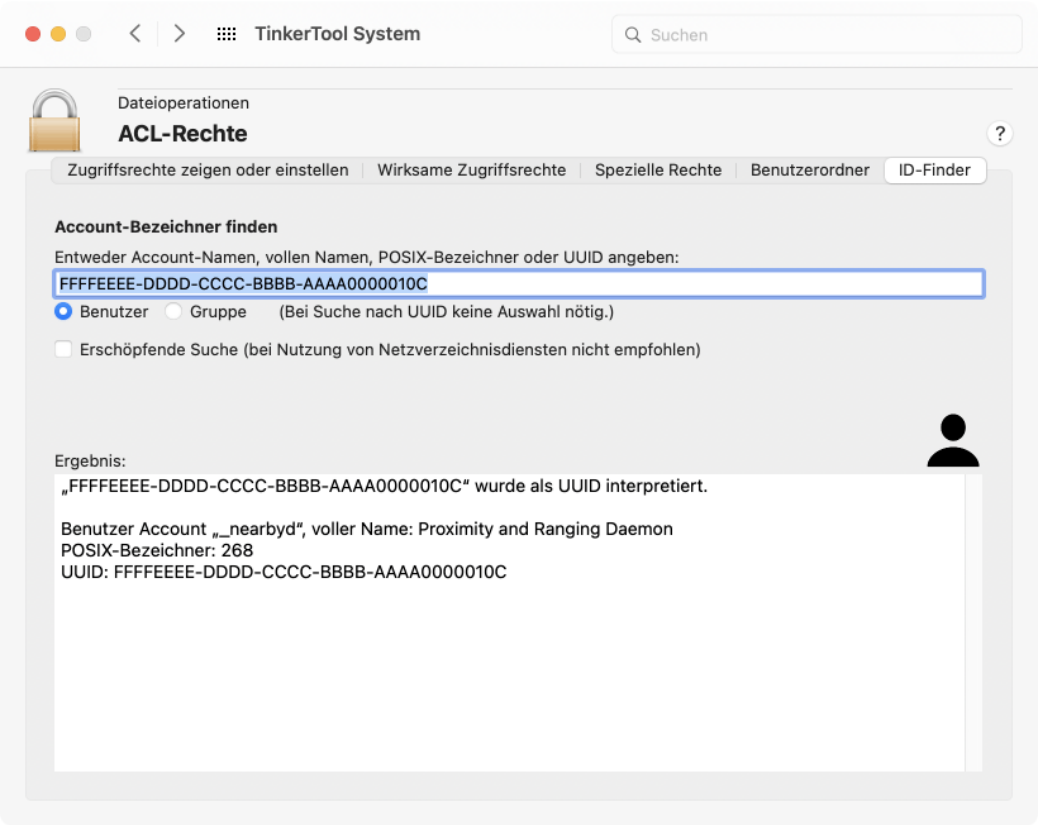

Abbildung 3.25: ID-Finder

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 Karteireiter **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 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. Das 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 Betriebssystem 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 das Festplattendienstprogramm, Terminal, oder die Funktion „Vollständige Wiederherstellung“ von 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).

- jedes plattenartige 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 **Stop**-Knopfes abgebrochen werden.

> Wenn Sie macOS 12 nutzen, werden auch die Build-Nummern der zum Herunterladen verfügbaren Betriebssysteme in der Tabelle angezeigt. Für macOS 11 bietet Apple diese Information nicht an. Die entsprechende Spalte in der Tabelle bleibt in diesem Fall leer.
> 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 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.

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 Anlegeprozesses 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.

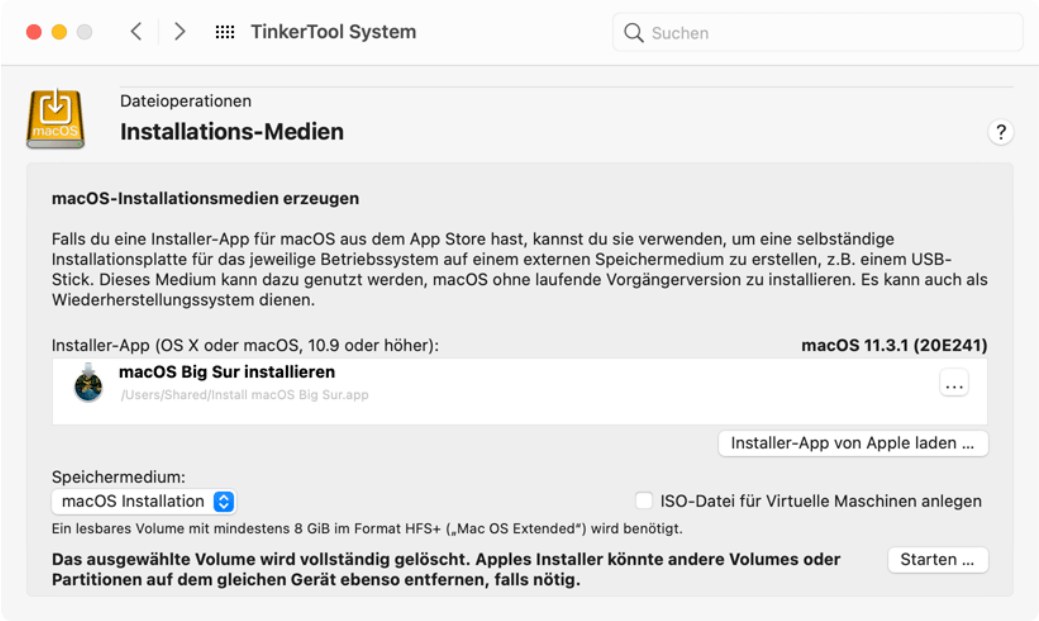

Abbildung 3.26: Ein selbständiges Installationsmedium für das Betriebssystem kann mit wenigen Mausklicks angelegt werden

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 sicher schließen und die Platte auswerfen.

3.5.5 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 Ausgabedatei 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.

3.5.6 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.

3.5.7 Unzuverlässiges Verhalten von macOS 11 Big Sur

Besonders ab Version 11.3 oder höher ist es bekannt, dass macOS Big Sur von internen Konstruktionsfehlern betroffen ist, die das erfolgreiche Anlegen von Installationsmedien unter bestimmten Umständen scheitern lassen können:

- Spotlight kann sich manchmal dazu entschließen, ein aggressives Verfahren zum Anlegen eines Index auf dem Installationsmedium zu starten, während dieses gerade erzeugt wird. Dies kann dazu führen, dass der laufende Prozess fehlschlägt.
- Die TCC-Komponente *(„Transparency, Consent, and Control“)* zum Schutz persönlicher Daten in macOS Big Sur kann manchmal entscheiden, den Zugriff auf das Installationsmedium zu verweigern, während macOS es gerade löscht. Obwohl der Benutzer seine Zustimmung signalisiert hat, dass datenschutzrelevanter Zugriff auf eine externe Platte möglich sein soll, kann diese Erlaubnis vorübergehend verlorengehen, da macOS nicht mehr erkennt, dass das gelöschte Volume immer noch das gleiche ist wie vorher.

TinkerTool System kennt dieses unzuverlässige Verhalten von macOS Big Sur und versucht automatisch, gegenzusteuern. Das Anlegen einer ISO-Datei kann intern bis zu drei Mal wiederholt werden, bevor das Programm aufgibt und eine abschließende Fehlermeldung anzeigt. Es kann manchmal helfen, weitere Versuche von Hand auszuprobieren. Das heißt, falls macOS Big Sur beim Anlegen von Installationsmedien immer noch nicht wie erwartet funktioniert, ist es manchmal überraschenderweise erfolgreich, einfach zu warten und den gleichen Vorgang später noch einmal zu versuchen.

3.6 Die Einstellungskarte Systemsicherheit

3.6.1 Programmintegrität

Auf der Einstellungskarte Programme (Abschnitt 3.3 auf Seite 155) 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-Volume. 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.

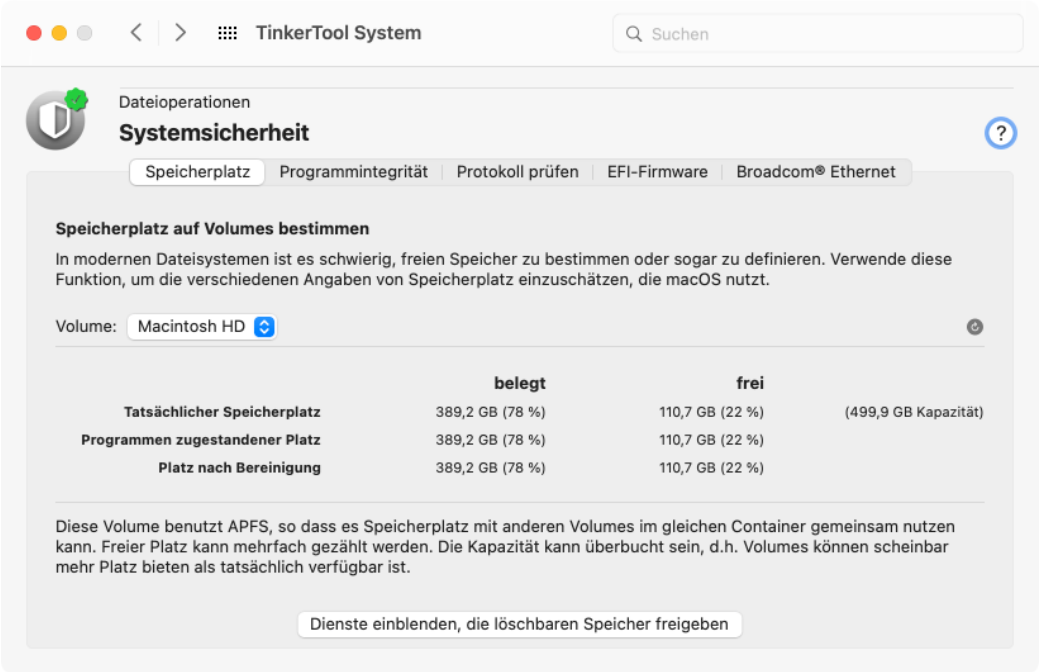

Abbildung 3.27: Alle Programme des Systems können auf Wunsch überprüft werden

1. Öffnen Sie den Karteireiter **Programmintegrität** auf der Einstellungskarte **Systemsicherheit**.

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 abzubrechen.

> 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 abzubrechen, 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 155) 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.

3.6.2 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 löschbar“ definiert ist. Ausführliche Informationen zu lokalen Time Machine-Schnappschüssen finden Sie im Kapitel Die Einstellungskarte Time Machine (Abschnitt 2.4 auf Seite 51).

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 Karteireiter **Speicherplatz** auf der Einstellungskarte **Systemsicherheit**.

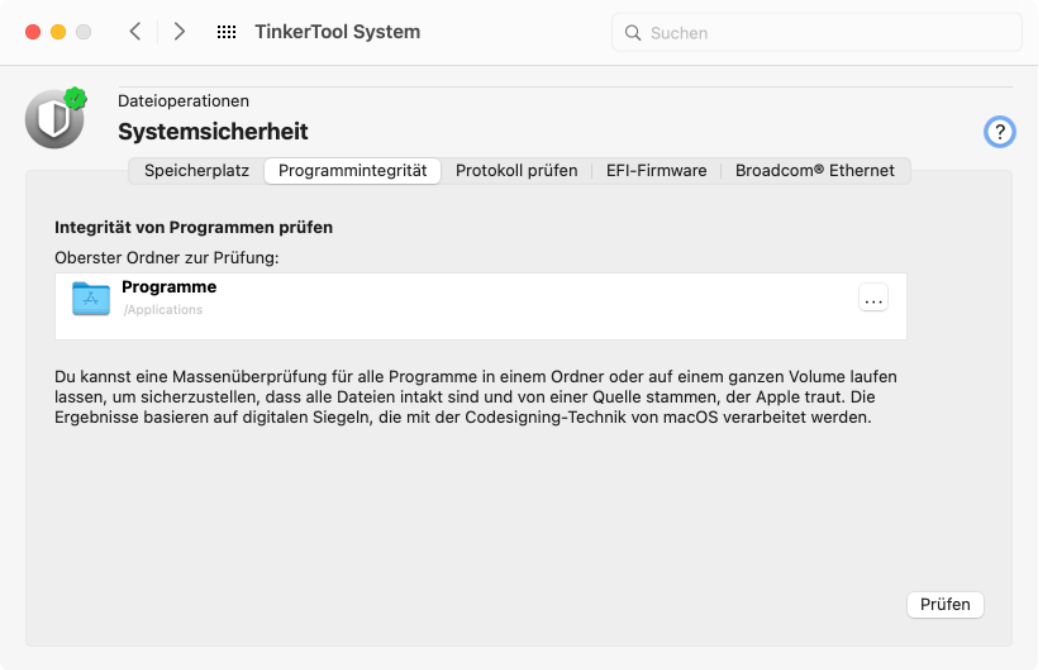

Abbildung 3.28: Freier Speicherplatz kann bei modernen Dateisystemen unterschiedlich definiert sein

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 ein Update-Schnappschuss-Volume 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.

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 zugestandener 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 *löschbarer 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.

3.6.3 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.

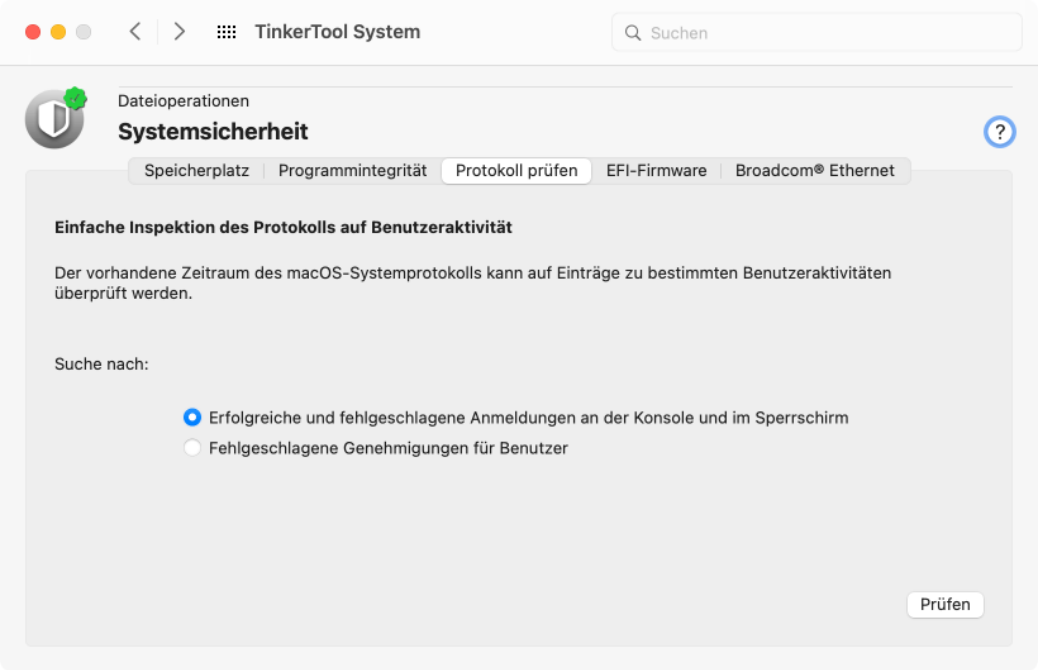

Abbildung 3.29: Das Systemprotokoll lässt sich auswerten, um mögliche Einbruchsversuche zu erkennen

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.

3.6.4 EFI-Firmware

> Auf Macs mit Apple-Chip ist diese Funktion nicht vorhanden, aber auch nicht notwendig. Solche Macs sind speziell gegen Manipulation der Firmware geschützt.

Um einen Computer zu starten und ein Betriebssystem zu laden, muss es ein weiteres Programm, eine Art Minibetriebssystem geben, das diese Aufgabe übernimmt. Dieses Programm muss fest in den Computer eingebaut sein und wird daher *Firmware* genannt. So fest ist diese Software allerdings nicht in der Hardware verankert, ansonsten könnte sie selbst nicht aktualisiert und an technische Weiterentwicklungen angepasst werden. Sie wird daher in einem speziellen, elektrisch löschbaren Speicher festgehalten, ähnlich wie Flash-Speicher. Apple aktualisiert die Firmware in regelmäßigen Abständen ohne besondere Hinweise, als Nebenaufgabe wenn auch Updates des „normalen“ Betriebssystems installiert werden.
Die Firmware ist durch mehrere Maßnahmen gegen Manipulationen geschützt. Trotzdem ist es mit etwas krimineller Energie machbar, auch in der Firmware bösartige Programme, wie z.B. Spionagefunktionen unterzubringen. Solche Angriffe auf den Computer sind schwer zu entdecken, da die Firmware im Normalbetrieb ja immer als fest eingebaut und unveränderlich gilt.
Aus Sicherheitsgründen überprüft Apple in neueren Betriebssystemversionen regelmäßig, ob die Firmware noch intakt und unverändert ist. Hierzu werden Blockprüfsummen al-

ler jemals ausgelieferten Firmware-Versionen für die jeweiligen Macintosh-Baureihen per Internet zur Verfügung gestellt und mit Prüfsummen der vorgefundenen Firmware verglichen. Solche Prüfläufe finden unsichtbar im Hintergrund statt und melden sich nur, falls eine Abweichung gefunden werden sollte. Eine Beispielwarnung ist untenstehend gezeigt.

Abbildung 3.30: macOS führt regelmäßige Integritätsprüfungen automatisch durch. Mögliche Probleme werden wie hier angezeigt.

TinkerTool System kann eine solche Prüfung manuell starten, so dass die Integrität der Firmware *sofort* überprüft und sichergestellt werden kann. Führen Sie hierzu folgende Schritt durch:

1. Öffnen Sie den Karteireiter **EFI-Firmware** auf der Einstellungskarte **Systemsicherheit**.

2. Drücken Sie den Knopf **Prüfen**.

Das Endergebnis wird danach in einem Benutzerdialog angezeigt und eine Kopie auch noch einmal im Anzeigefenster festgehalten.

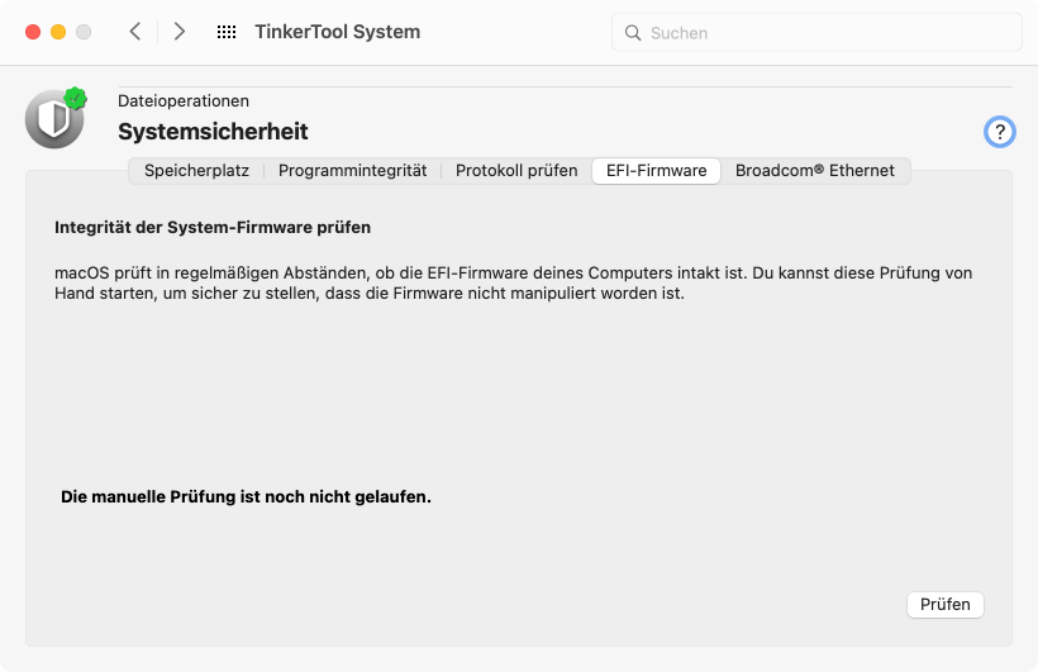

Abbildung 3.31: Die Integritätsprüfung für die Firmware kann auf Wunsch sofort wiederholt werden

> Nicht alle Macintosh-Modelle unterstützen diese Form der Firmware-Prüfung. In diesem Fall erhalten Sie von TinkerTool System einen entsprechenden Hinweis. Dies betrifft insbesondere die neuesten Baureihen, in denen der Computer durch einen unabhängigen Prozessor mit eigenem Betriebssystem (Apple BridgeOS) überwacht und geschützt wird, oder wenn es sich um einen Mac mit Apple-Prozessor handelt. In solch einem System darf macOS die Firmware nicht mehr lesen, aber erst recht nicht schreiben, so dass die Sicherheit auf anderem Wege gewährleistet ist.
> Es kann passieren, dass Apple eine neue Version von macOS veröffentlicht, die eine neue Firmware installiert, aber *keine* aktualisierte Prüfsumme für diese Firmware enthält. *In diesem besonderen Fall wird die Integritätsprüfung fehlschlagen.* Solch ein Fehler löst allerdings üblicherweise eine interne Aktualisierung der Prüfsummenliste per Internet aus, falls die Option **Systemeinstellungen** > **Softwareupdate** > **Weitere Optionen** > **Systemdatendateien und Sicherheitsupdates installieren** eingeschaltet ist, was der Standard ist. Das heißt, falls Sie eine Integritätswarnung kurz nach einem Update von macOS sehen, wiederholen Sie die Integritätsprüfung nach ein paar Stunden, um zu testen, ob es sich um einen Fehlalarm gehandelt hat.
> Ein falscher Alarm kann normal sein, wenn Sie unveröffentlichte Beta-Betriebssysteme testen.

3.6.5 Broadcom® Ethernet

> Auf Macs mit Apple-Chip ist diese Funktion nicht vorhanden, aber auch nicht notwendig. Solche Macs sind speziell gegen Manipulation der Firmware geschützt.

Ethernet-Anschlüsse der Herstellers Broadcom zeichnen sich durch die Besonderheit aus, dass auch deren Firmware auf relativ einfache Weise veränderbar ist. Die Überwachung der Firmware ist deshalb auch für diese Fälle sicherheitskritisch.

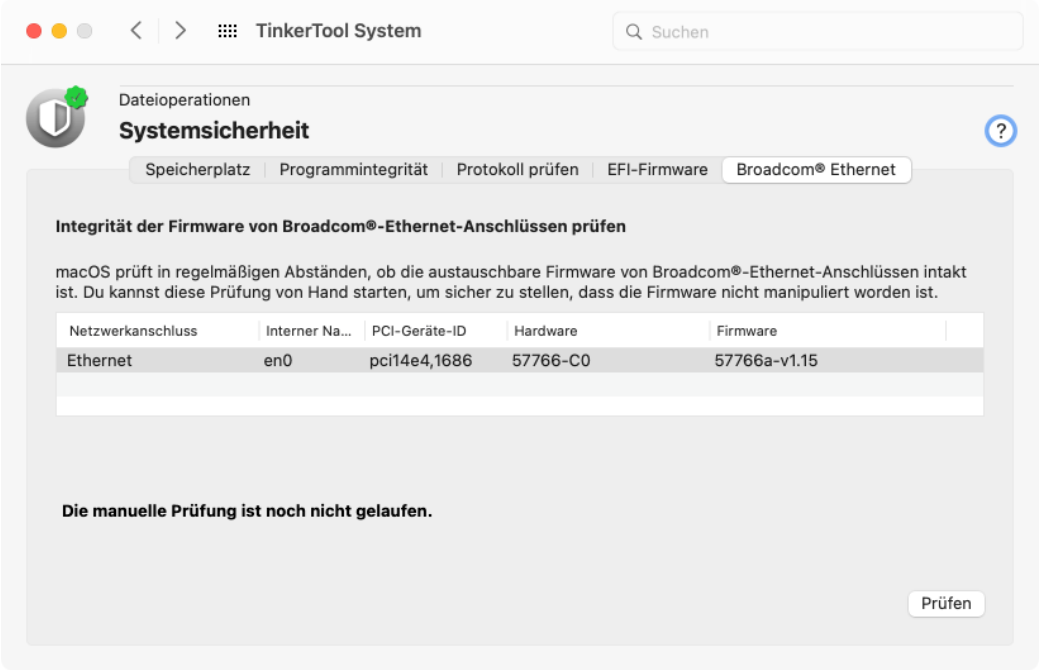

Abbildung 3.32: Eine Integritätsprüfung ist auch für Ethernet-Firmware von Broadcom möglich

TinkerTool System kann überprüfen, ob ein oder mehrere Ethernet-Anschlüsse von Broadcom in Ihren Mac eingebaut, bzw. extern angeschlossen sind. Falls ja, kann auch deren Firmware sofort auf mögliche Manipulationen getestet werden:

1. Öffnen Sie den Karteireiter **Broadcom® Ethernet** auf der Einstellungskarte **Systemsicherheit**.
2. Kontrollieren Sie in der angezeigten Tabelle, ob entsprechende Ethernet-Anschlüsse in Ihrem Computer vorhanden sind. Falls ja, drücken Sie den Knopf **Prüfen**.

Das Ergebnis der Prüfung wird nach ein paar Sekunden angezeigt. Falls mehrere Anschlüsse vorhanden sind, lässt sich jede Einheit im Bericht durch eine Nummer zuordnen, die *PCI-Geräte-ID*. Sie finden diese Nummer als hinteren Teil in der Spalte **PCI-Geräte-ID** in der Tabelle, so dass Sie den zugehörigen Netzwerkanschluss ablesen können.

> macOS überprüft zurzeit nur Ethernet-Baugruppen des Herstellers Broadcom. Ethernet-Anschlüsse anderer Hersteller werden nicht getestet, besitzen in der Regel aber auch keine angreifbare Firmware.

3.7 Die Einstellungskarte APFS

3.7.1 Überblick über APFS-Volumes

Wie bereits im vorigen Kapitel (Abschnitt 3.6 auf Seite 193) erläutert, verwendet Apples Dateisystem *APFS (Apple File System)* moderne Techniken zur Organisation von Speicherplatz, die auf den ersten Blick verwirrend sein können.
Der Karteireiter **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 **Objekttyp** 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 *kontingentierten Speicher*, ein Maximum an physischem Platz, der genutzt werden darf, selbst wenn mehr im Container zur Verfügung steht.

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.
Falls Sie mit mehreren Partitionen arbeiten oder mehrere Platten an Ihren Mac angeschlossen sind, ist der Platz in der Tabelle möglicherweise nicht ausreichend, um einen klaren

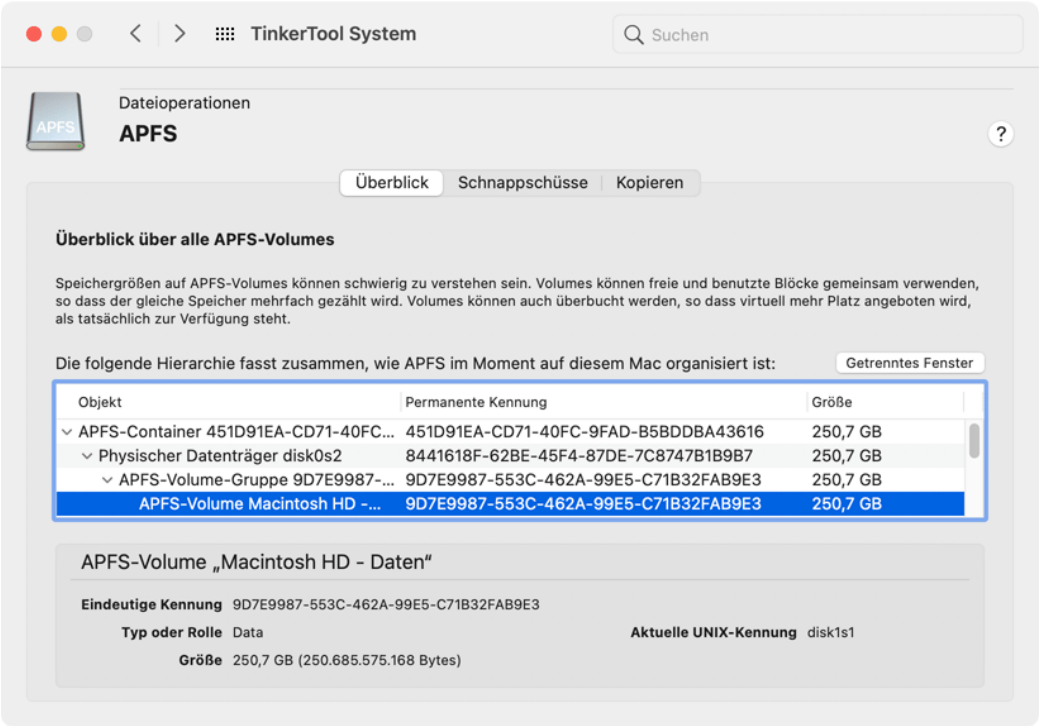

Abbildung 3.33: Der Zusammenhang der einzelnen APFS-Objekte lässt sich als Hierarchie darstellen

Überblick zu bekommen. Um in diesem Fall eine bessere Darstellung zu erreichen, drücken Sie den Knopf **Getrenntes Fenster**. Der APFS-Überblick wird danach in einem vergrößerbaren Fenster gezeigt, das auf den kompletten Bildschirm erweitert werden kann, falls nötig. Das Überblicksfenster geöffnet zu lassen kann besonders dann hilfreich sein, falls Sie mit kritischen APFS-Vorgängen arbeiten möchten, z.B. eine Platte auf eine andere zu kopieren (siehe unten).
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
- **User:** Privatordner der Benutzer
- **Recovery:** Minibetriebssystem zur Wiederherstellung
- **VM:** Auslagerungsspeicher als Teil des Virtuellen Speichermanagements
- **Preboot:** Komponenten für den Systemstart eines verschlüsselten Volumes (z.B. die Bedieneroberfläche von FileVault)

APFS-Überblick

Objekt	Permanente Kennung	Größe	APFS-Rolle	Unix-Gerät
APFS-Container „AppleAPFSMedia“	451D91EA-CD71-40FC-9FAD-B5BDDBA436...	250,7 GB		disk1
Physischer Datenträger „Untitle...	8441618F-62BE-45F4-87DE-7C8747B1B9B7	250,7 GB	Main	disk0s2
APFS-Volume-Gruppe „Macin...	9D7E9987-553C-462A-99E5-C71B32FAB9...	250,7 GB		disk1s5
APFS-Volume „Macintosh...	9D7E9987-553C-462A-99E5-C71B32FAB9...	250,7 GB	Data	disk1s1
APFS-Volume „Macintosh...	F2DEC970-E0A3-40F2-9405-4A7A10D6E375	250,7 GB	System	disk1s5
APFS-Schnappschuss „...	CA0C0759-9CE7-4EF5-B24D-F4915D9DA6...	250,7 GB	System (S...	disk1s5s1
APFS-Volume-Gruppe „Catali...	55963802-B0E8-4873-A7D8-04FE1268AEFE	250,7 GB		disk1s8
APFS-Volume „Catalina - D...	55963802-B0E8-4873-A7D8-04FE1268AEFE	250,7 GB	Data	disk1s7
APFS-Volume „Catalina“	C8B0BA3A-CDCD-41E3-8177-0C19C6ED4...	250,7 GB	System	disk1s8
APFS-Volume „Preboot“	0CDA081C-2F11-40EF-86B0-D37054C9E4...	250,7 GB	Preboot	disk1s2
APFS-Volume „Update“	2CBC1603-F4F3-41E3-8C31-E598BA42EB74	250,7 GB	Update	disk1s6
APFS-Volume „VM“	16C2CC66-3084-48C7-A90B-18D65CDDC...	250,7 GB	VM	disk1s4
APFS-Volume „Recovery“	34A8BB1F-1AC5-4B35-9CC1-6DD312BE37...	250,7 GB	Recovery	disk1s3
APFS-Container „AppleAPFSMedia“	F465B6BC-997D-40FE-90A5-A9A6D56672...	399,8 GB		disk3
Physischer Datenträger „disk im...	9BC2F38F-9863-49F4-A421-B2F0E8295D...	399,8 GB	Main	disk2s2
APFS-Volume „Backups von...	144FC1D6-5037-43A1-9519-F3D6DCCD00...	399,8 GB	Backup	disk3s1
APFS-Container „AppleAPFSMedia“	68519DED-DE1D-44D8-BC7C-B01D2BEA7...	79,8 GB		disk5
Physischer Datenträger „Untitle...	1505AC84-5B0D-428A-B532-6CB7750D9E...	79,8 GB	Main	disk4s2
APFS-Volume „Time Machine“	424AFB2B-6C45-47CA-940E-D7B2F37881...	79,8 GB	Backup	disk5s2

Abbildung 3.34: Die APFS-Tabelle kann in einem getrennten Fenster geöffnet werden um einen klareren Überblick zu erhalten.

- **Installer:** Vorübergehende Nutzung für Daten, die während der Installation des Betriebssystems benötigt werden
- **Data:** alle veränderlichen Daten von Benutzer und Betriebssystem
- **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
- **Prelogin:** ein Volume für das Minibetriebssystem, das von FileVault verwendet wird, um Benutzeranmeldungen zu ermöglichen, bevor das eigentliche (verschlüsselte) Betriebssystem gestartet wird
- **Reserved:** Für zukünftige Nutzungsarten reserviert.

3.7.2 Arbeiten mit APFS-Schnappschüssen

Sinn und Zweck von Schnappschüssen wurde bereits im Kapitel zur Karte Time Machine (Abschnitt 2.4 auf Seite 51) 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 Karteireiter **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.

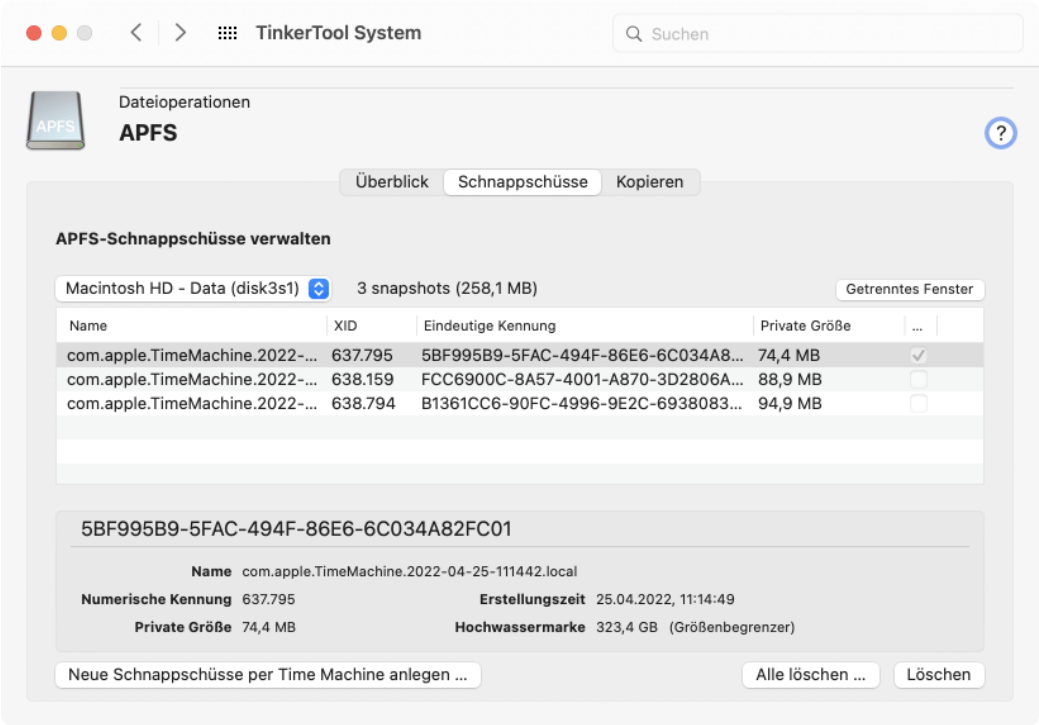

Abbildung 3.35: APFS-Schnappschüsse können eingesehen und gelöscht werden

Möchten Sie die aktuellen Schnappschüsse einsehen, die sich auf einem bestimmten APFS-Volume befinden, gehen Sie wie folgt vor:

1. Öffnen Sie den Karteireiter **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, 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 **Hochwassermarke** angegeben.
Aufgrund der festen Größe des Steuerungsfensters von TinkerTool System kann es manchmal schwer sein, alle Daten über Schnappschüsse ohne abgeschnittene Felder zu sehen. Wenn Sie den Knopf **Getrenntes Fenster** betätigen, kopiert TinkerTool System den Inhalt der Tabelle in ein getrenntes Fenster, das Sie auf beliebige Breite aufziehen können. Somit lassen sich alle Tabellenspalten ohne Einschränkungen sehen.
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.

3.7.3 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 Big Sur 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.

- 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.

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 Karteireiter **Kopieren** auf der Einstellungskarte **APFS**.

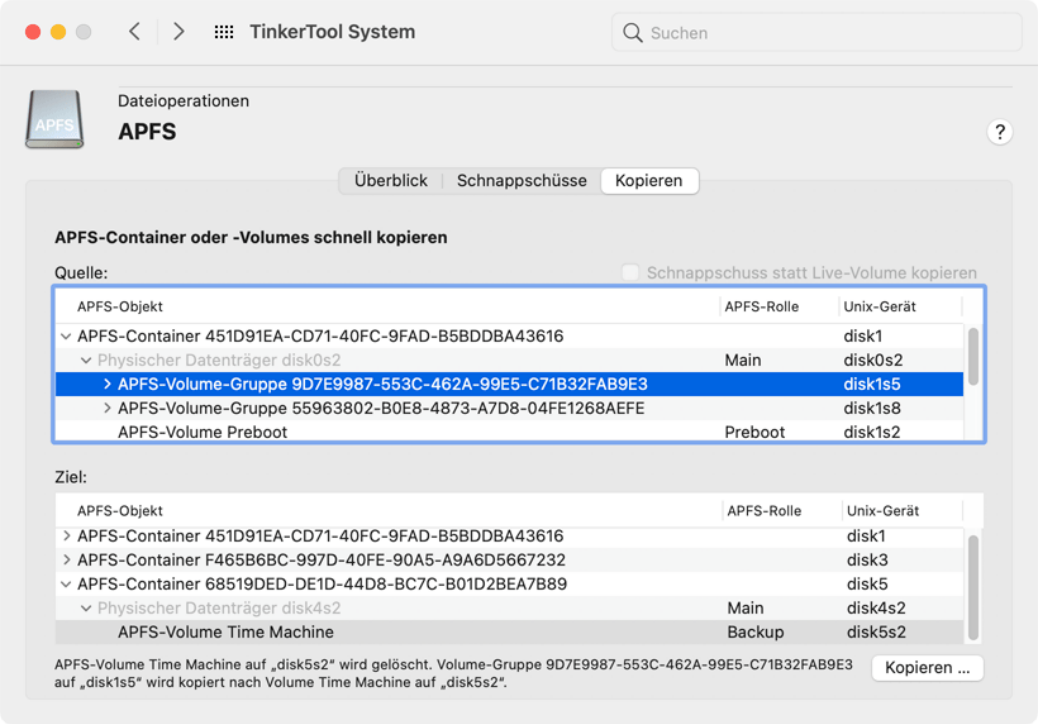

Abbildung 3.36: APFS-Objekte lassen sich besonders schnell kopieren

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 abzubrechen. 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 **Energie sparen** > **Wenn möglich, Ruhezustand für Festplatten aktivieren** im Programm **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 Karteireiter **Laufwerke** auf der Einstellungskarte **System**.

2. Ziehen Sie den Schieberegler **Ruhezustand der Festplatten aktivieren wenn unbenutzt 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.

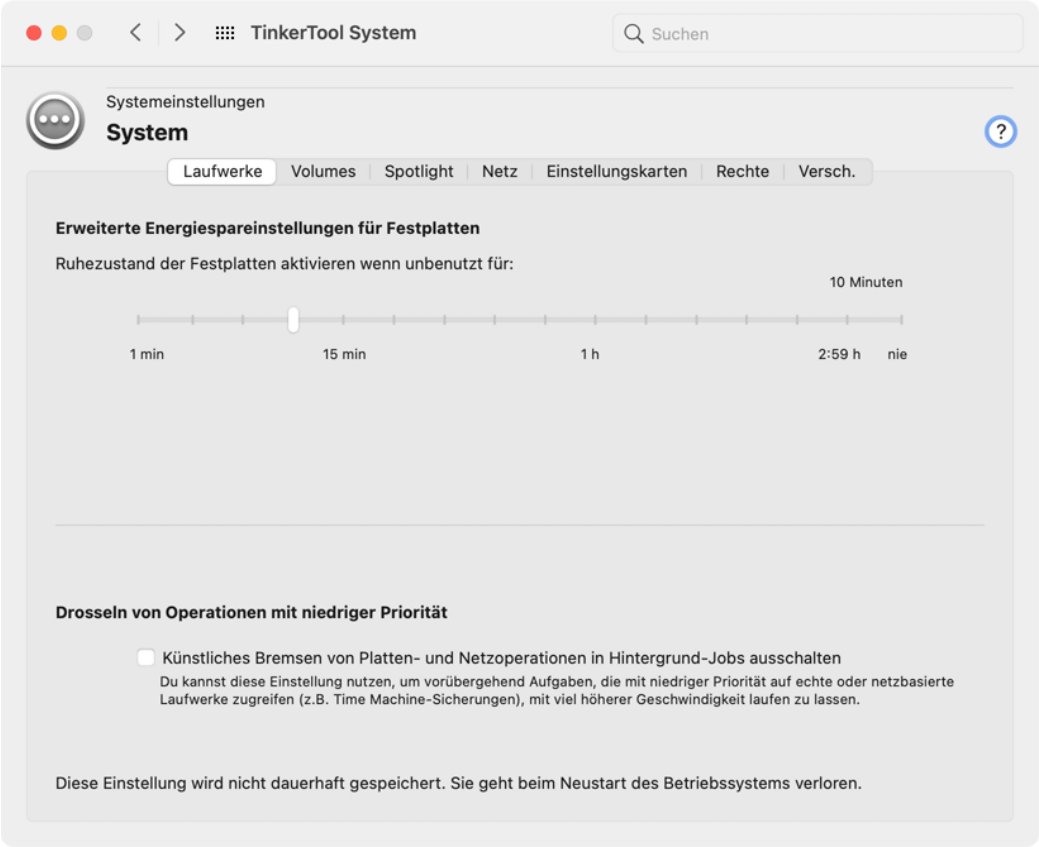

Abbildung 4.1: Laufwerke

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 Karteireiter **Laufwerke** auf der Einstellungskarte **System**.
2. Setzen Sie ein Häkchen bei **Künstliches Bremsen von Platten- und Netzoperationen in 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 Partitionen 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 Partitionen 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 Partitionen 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. jede Partition 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 jeder Partition 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 Dateisysteme wie ExFAT oder NTFS zu verarbeiten. Apples Nutzung von LIFS kann sich in jeder Version von macOS ändern.

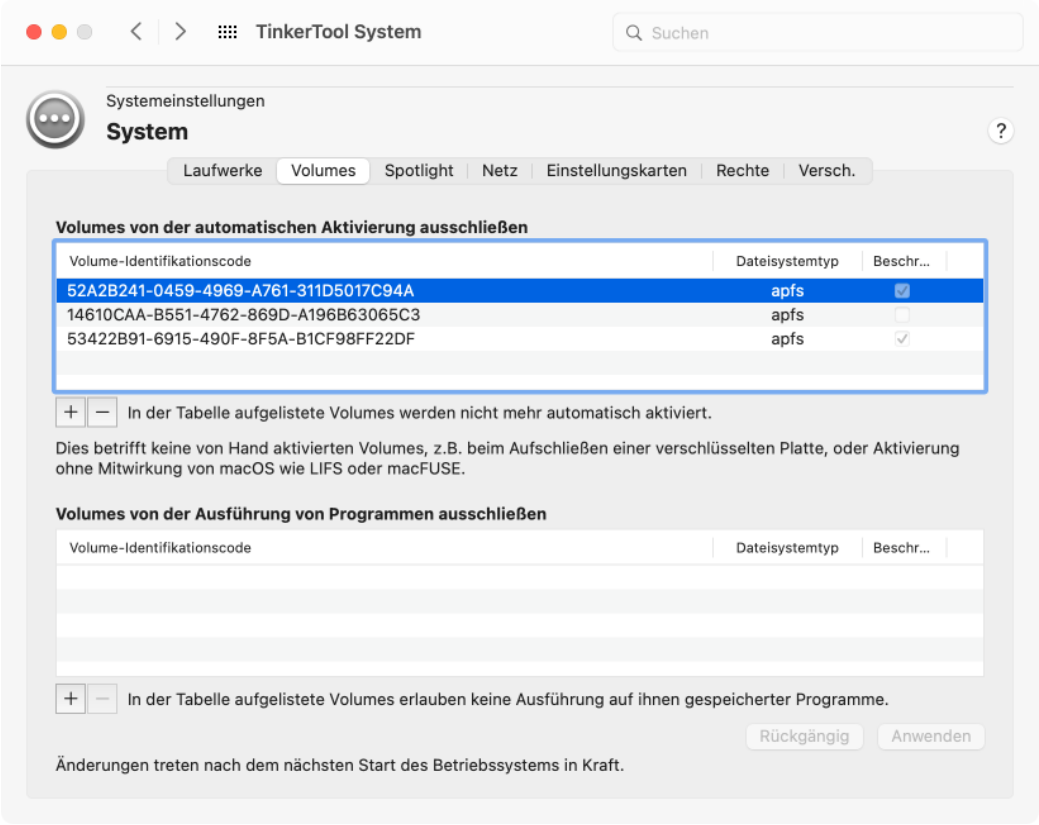

Abbildung 4.2: Volumes

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 Karteireiter **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 feinanpassen 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.

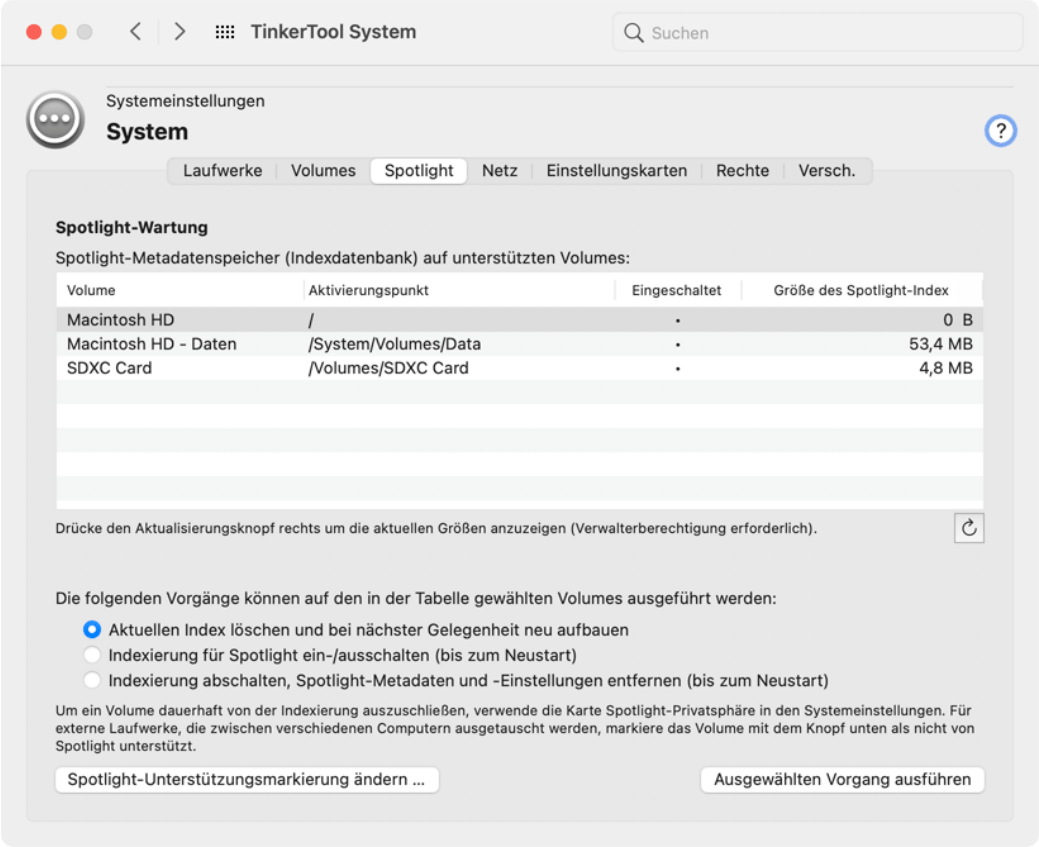

Abbildung 4.3: Spotlight

4.1.4 Spotlight-Indexdatenbanken

Wenn Spotlight aktiv ist, erzeugt es automatisch eine verstecke 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 *Metadatenspeicher* genannt.

Für jedes Volume erlaubt Ihnen TinkerTool System anzuzeigen, ob Spotlight auf diesem Volume aktiviert ist, und wie viel Plattenspeicherplatz im Moment für den Metadatenspeicher verbraucht wird. Diese Daten werden in der Tabelle **Spotlight-Metadatenspeicher** 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 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 oder mehrere Zeilen in der Tabelle ausgewählt haben, können Sie zwischen mehreren Operationen wählen, die durchgeführt werden können:

- Sie können den Metadatenspeicher auf den gewählten Volumes **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 den ausgewählten Volumes 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 Metadatenspeicher auf den gewählten Volumes **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 **Spotlight** > **Privatsphäre** in den **Systemeinstellungen** auf den betreffenden Volumes gesperrt haben, wird macOS seine Indexdienste beim nächsten Systemstart wieder aufnehmen.

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 Karteireiter **Spotlight** auf der Einstellungskarte **System**.
2. Klicken Sie den Knopf **Spotlight-Unterstützungsmarkierung ändern** … in der linken unteren Ecke des Fensters.
3. Kreuzen Sie den Punkt **Von allen Spotlight-Operationen ausgenommen** im Dialogfenster wie gewünscht für jedes der Volumes an, bzw. entfernen Sie die Häkchen.
4. Betätigen Sie den Knopf **OK** im Dialogfenster.

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 Karteireiter **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 Karteireiter **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.

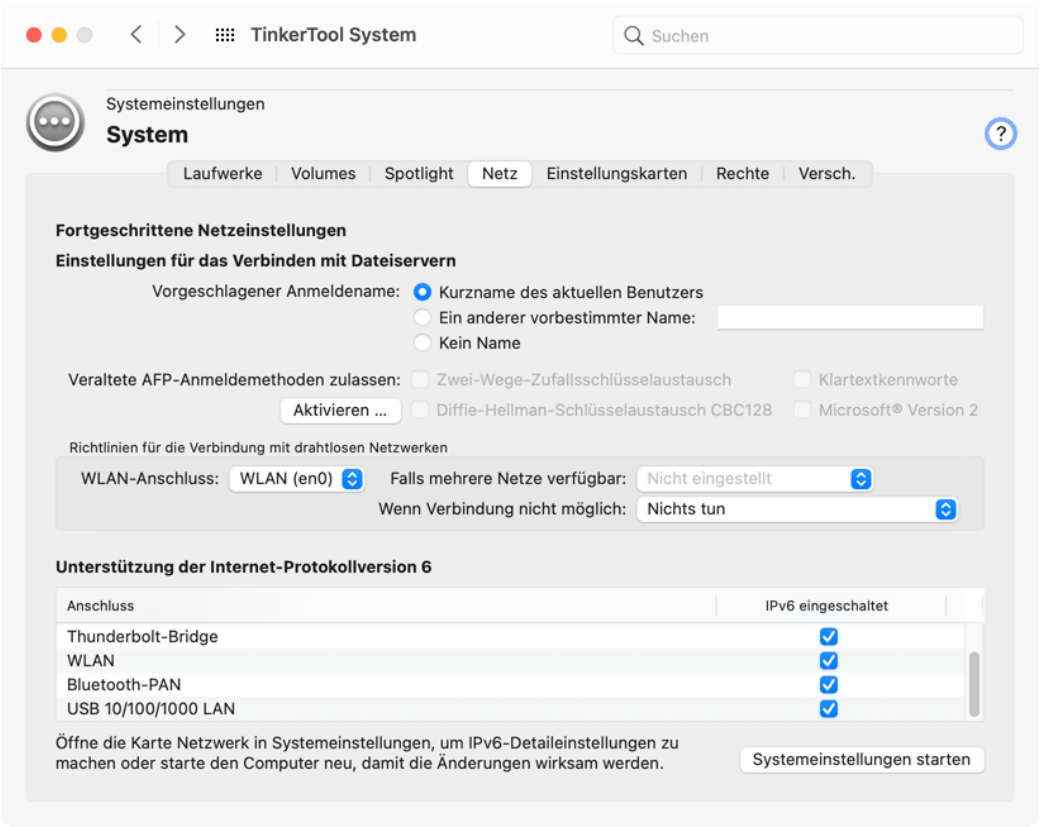

Abbildung 4.4: Netz

- **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 verfahren werden soll.
- **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. Falls Ihr Computer dazu eingerichtet ist, mehrere Sätze von Netzkonfigurationseinstellungen zu verwalten (was von macOS **Umgebung** genannt wird), stellen Sie zunächst sicher, dass die gewünschte Umgebung zurzeit aktiv ist, indem Sie diese mit dem Menüknopf auf der Karte **Netzwerk** von **Systemeinstellungen** auswählen. Falls Sie diese Funktion noch nie genutzt haben, ist die Umgebung standardmäßig auf **Automatisch** gesetzt.
2. Öffnen Sie den Karteireiter **Netz** auf der Einstellungskarte **System** in TinkerTool System.
3. Suchen Sie den Netzwerkanschluss, den Sie ändern möchten, in der Tabelle **Unterstützung der Internet-Protokollversion 6**.
4. 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 Einstellungskarten

Das Programm Systemeinstellungen ist dazu konstruiert, eine Plugin-Architektur zu unterstützen. Die unterschiedlichen Steuerbereiche, die *Einstellungskarten (Preference Panes)* genannt werden, werden automatisch ein- und ausgeschaltet, je nach dem, welchen Computertyp Sie verwenden. Zum Beispiel erscheint die Karte **Trackpad** nur auf Computern, die mit einem Trackpad ausgerüstet sind, die Karte **Ink** wird nur angezeigt, wenn ein Grafiktablett oder ein ähnliches Gerät mit Stiftunterstützung an den Computer angeschlossen ist.
Die Systemeinstellungen beinhalten eine zusätzliche Rubrik, die auswählbare Karten aufnimmt, die vom Benutzer installiert werden. Diese wird als fünfte Kategorie, in der untersten Zeile des Fensters angezeigt. TinkerTool System kann Ihnen dabei helfen, diesen Abschnitt zu verwalten: Es kann zusätzliche Einstellungskarten aktivieren, die Teil von macOS sind, aber fortgeschrittenen Benutzern vorbehalten sind und deshalb normalerweise verborgen bleiben. Es kann Ihnen auch dabei helfen, optionale Einstellungskarten zu entfernen, die Sie nicht mehr länger brauchen.
Die folgende zusätzliche Karte kann aktiviert werden:

- Eine Karte, um auf Einstellungen für das **macOS-Archivierungsprogramm** zuzugreifen. Es handelt sich hier um das Hilfsprogramm, das automatisch aktiv wird, wenn Sie archivierte oder komprimierte Dateien öffnen, z.B. ein ZIP-Archiv.

> Apple bietet zusätzliche Karten als Teil von macOS an. Deren Features können von der Systemversion abhängen und sich ohne Ankündigung ändern. Die optische Qualität der Karten hält sich möglicherweise nicht an die üblichen Design-Standards.

Um eine der versteckten Karten zu aktivieren, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Karteireiter **Einstellungskarten** auf der Einstellungskarte **System**.
2. Drücken Sie auf einen der Knöpfe **Aktivieren** ..., die neben den aufgeführten Einstellungskarten zu sehen sind.

Sie können Systemeinstellungen direkt von hier aus starten und die neuen Karten sofort nutzen. Drücken Sie dazu den Knopf **Systemeinstellungen starten**.

Optionale Einstellungskarten entfernen

Die im vorigen Abschnitt genannten Karten und die Karten anderer Anbieter, die im untersten Abschnitt von Systemeinstellungen erscheinen, können entfernt werden, wenn Sie diese nicht mehr länger brauchen. Es ist hierbei nicht erforderlich, dass Sie wissen müssen, wo die verschiedenen Anbieter diese Module installiert haben. Führen Sie die folgenden Schritte durch:

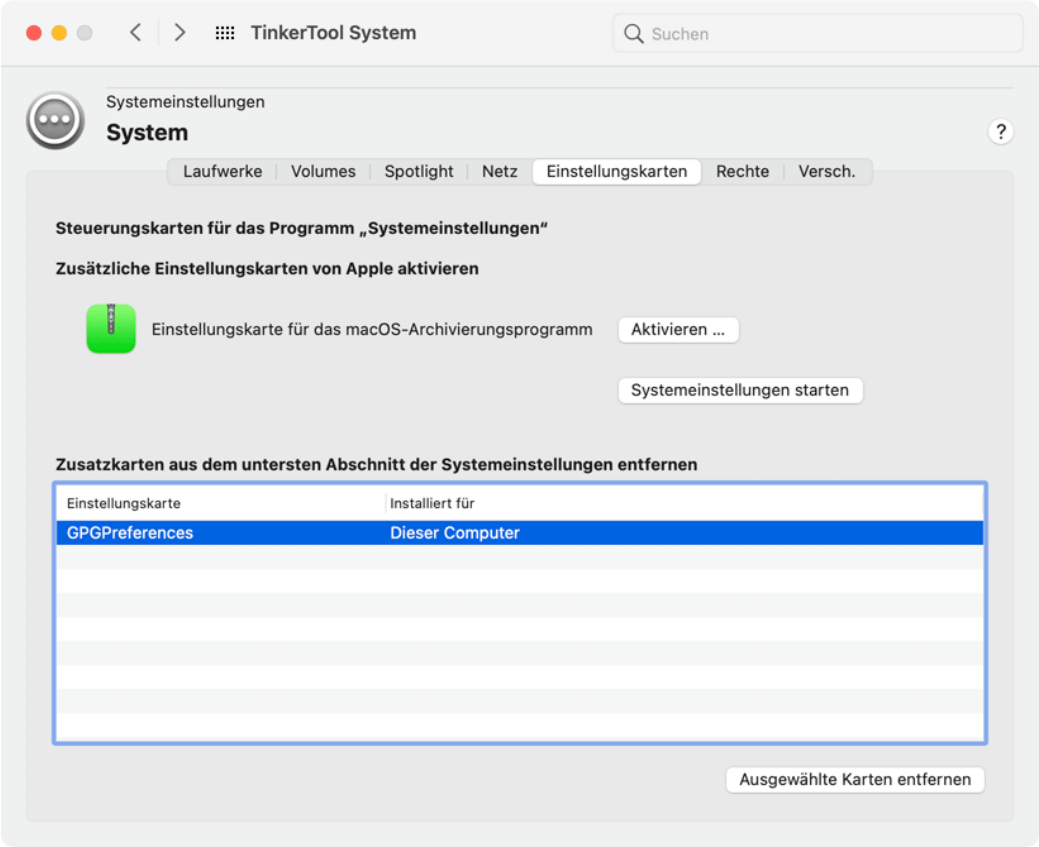

Abbildung 4.5: Einstellungskarten

1. Öffnen Sie den Karteireiter **Einstellungskarten** auf der Einstellungskarte **System**.
2. Wählen Sie einen oder mehrere Punkte in der Tabelle **Zusatzkarten aus dem untersten Abschnitt der Systemeinstellungen entfernen**.
3. Betätigen Sie den Knopf **Ausgewählte Karten entfernen**.

4.1.7 Zugriffsrechtsfilter für neue Dateisystemobjekte

Im Berechtigungssystem von macOS, das detailliert im Kapitel Die Einstellungskarte ACL-Berechtigung (Abschnitt 3.4 auf Seite 167) 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 laxe 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 167).
Standardmäßig verwendet macOS einen Berechtigungsfilter, der gemäß folgender Richtlinie voreingerichtet 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 Karteireiter **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.

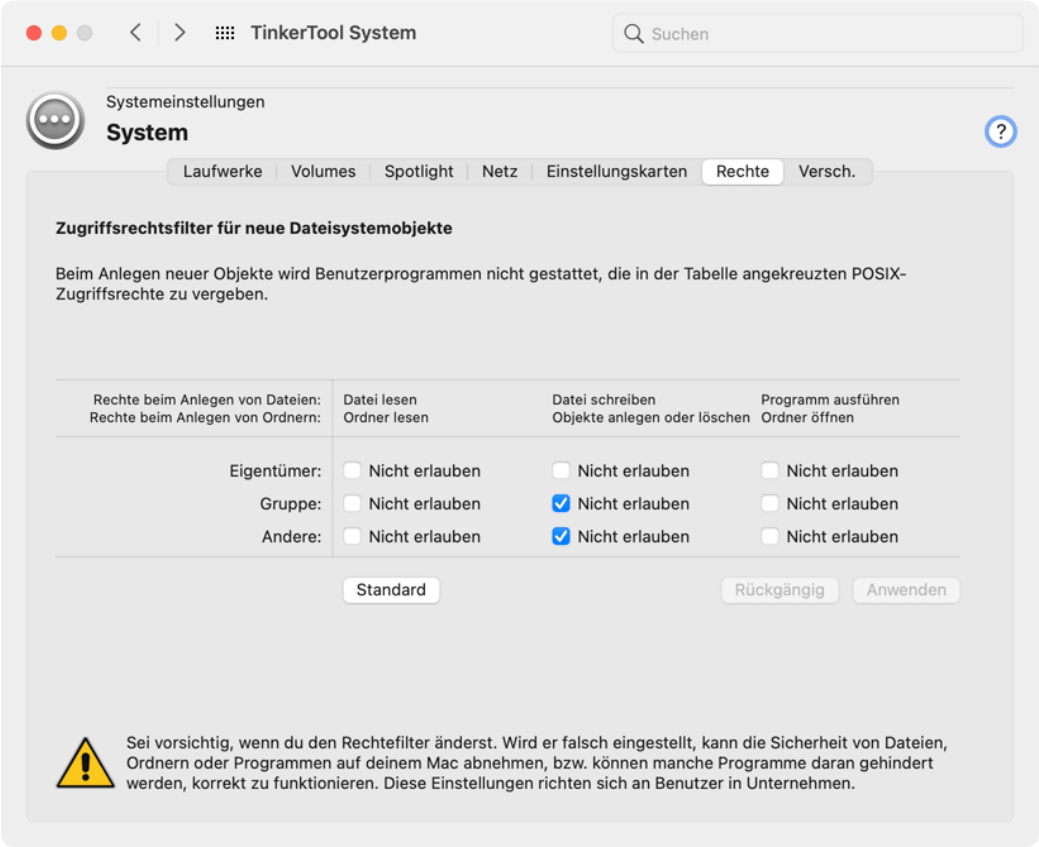

Abbildung 4.6: Zugriffsrechtsfilter

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 auf der linken Seite. 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.

4.1.8 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 Karteireiter **Versch.** 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 **Freigaben** 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 Karteireiter **Versch.** 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 2

Falls Sie die moderne Version von FileVault auf Ihrem Computer eingeschaltet haben (offiziell *FileVault 2* genannt), wird das komplette System-Volume mit einem sichern 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 einige Teile der unverschlüsselten Wiederherstellungspartition einen besonderen Anmeldeschirm (der dem Anmeldeschirm von macOS ähnelt). Benutzer müssen sich zuerst hier anmelden, wodurch für berechtigte Benutzer der geheime Entschlüsselungsschlüssel aufgeschlossen wird, mit dem danach die Betriebssystempartition 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 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 Karteireiter **Versch.** auf der Einstellungskarte **System**.

2. Klicken Sie auf den Punkt **Getrennte Anmeldung für Plattenentschlüsselung und erste Benutzersitzung**.

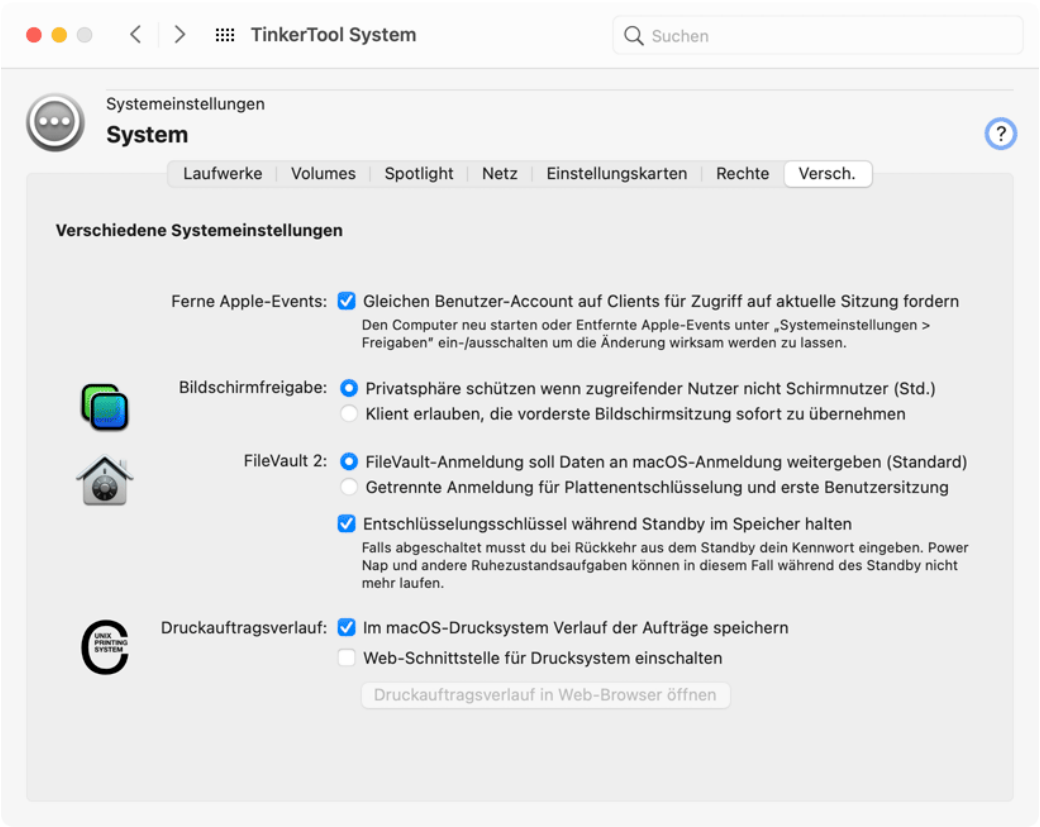

Abbildung 4.7: Verschiedenes

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 Karteireiter **Versch.** 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.

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.

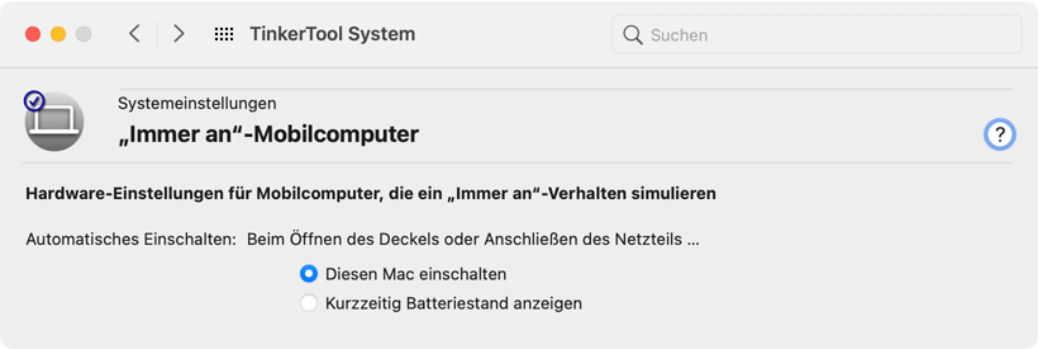

Abbildung 4.8: Einstellungen für die automatische Einschaltfunktion

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.

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

- 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 ein 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.

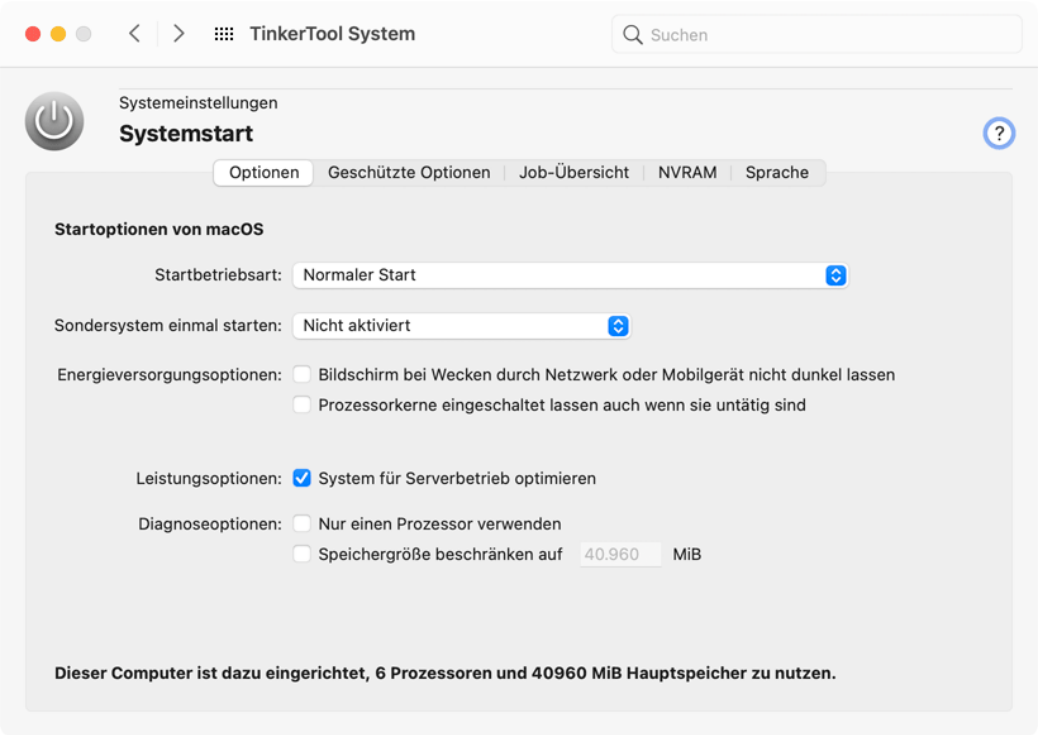

Abbildung 4.9: Optionen für den Systemstart

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 mit macOS Server optimieren**. Nach einem Neustart des Computers werden der Systemkern und einige Funktionen von macOS Server die neue Einstellung beachten.

> Apple kann die genaue Bedeutung dieser Einstellung jederzeit ohne vorherige Ankündigung ändern. Bei den neuesten Versionen von macOS kann es sinnvoll sein, diese Option einzuschalten, wenn Sie Server-Funktionen nutzen möchten, auch wenn macOS Server nicht installiert ist. Fast alle Server-Funktionen sind von der früheren Server-App in das Basisbetriebssystem gewandert.

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 Karteireiter **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 Karteireiter **Optionen** auf der Einstellungskarte **Systemstart**.
2. Betätigen Sie den Knopf **Bericht erstellen**.

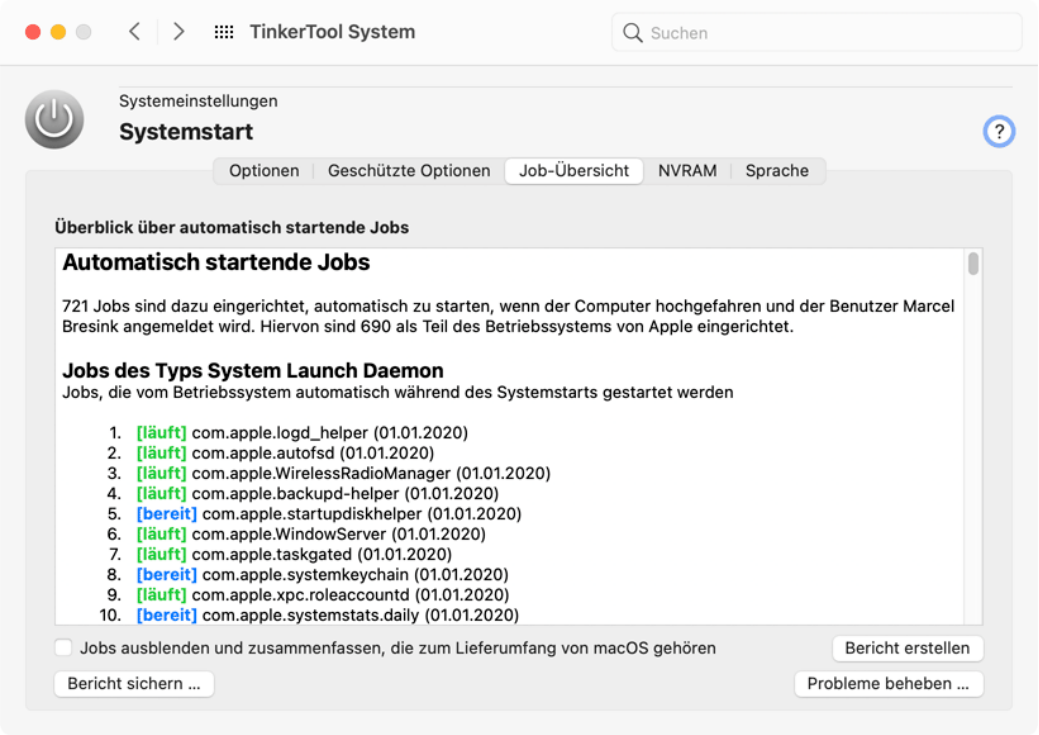

Abbildung 4.10: Übersicht über alle automatisch startenden Jobs

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 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 **Benutzer & Gruppen** 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** … in der unteren rechten Ecke 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 247).

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 Betriebssystem 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. Wenn der Mac beispielsweise von einem anderen Volume als dem unter der Systemeinstellung **Startvolume** festgelegten startet oder vor dem Starten des Mac vorübergehend ein Fragezeichen angezeigt wird, kann es erforderlich sein, das NVRAM zu löschen.
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 Karteireiter **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.

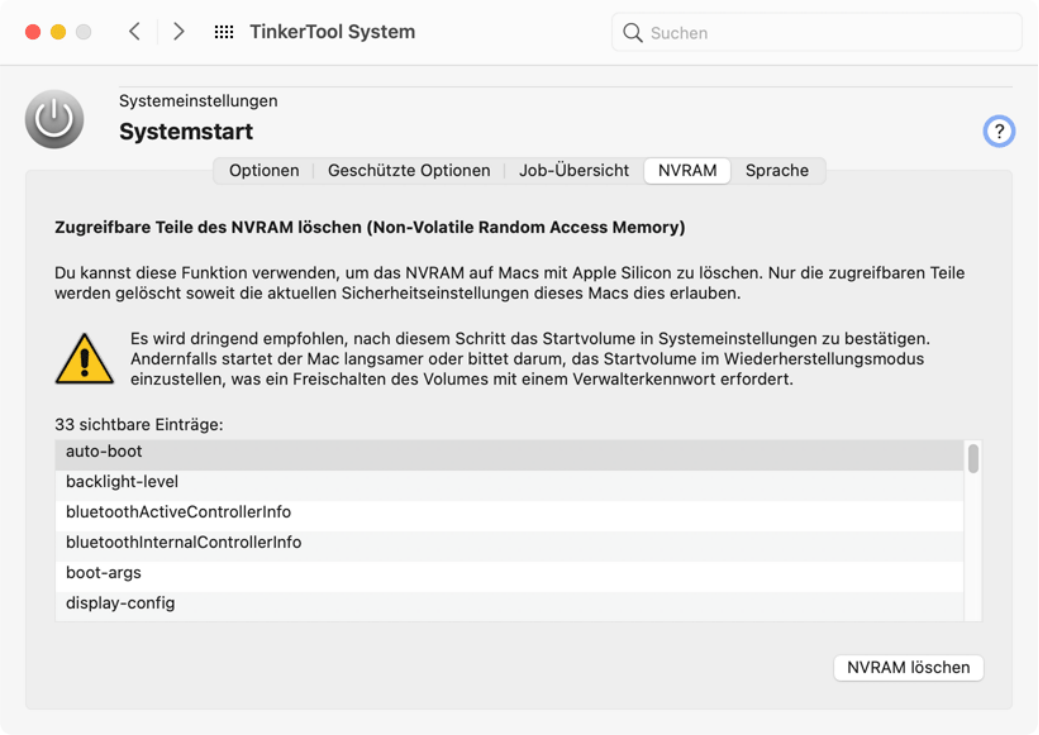

Abbildung 4.11: Löschen des NVRAM

Es wird dringend empfohlen, so schnell wie möglich nach dem Löschen die Systemeinstellung **Startvolume** wieder einzustellen. Ansonsten kann der nächste Start des Mac verzögert werden, oder macOS kann den Start abbrechen und stattdessen automatisch das Wiederherstellungsbetriebssystem laden, um die Einstellungen für das Startvolume dort überprüfen zu lassen. Hierbei kann sogar die (nicht korrekte) Warnmeldung angezeigt werden, dass das Betriebssystem neu installiert werden muss. Zum Einstellen des Startvolume im Wiederherstellungsbetriebssystem ist es notwendig, dieses Betriebssystem das verschlüsselte Startlaufwerk lesen zu lassen. Hierzu ist die Eingabe eines Administrator-Kennworts erforderlich.

Sie sollten diese aufwändige Prozedur vermeiden und das Startvolume sofort wieder einstellen, so lange der Computer noch nicht neu gestartet wurde. TinkerTool System wird Sie unmittelbar nach dem Löschen des NVRAM daran erinnern und kann **Systemeinstellungen** automatisch starten. Achten Sie darauf, dass auf der Karte **Startvolume** tatsächlich eine Bestätigungsmeldung nach dem Muster **Du hast macOS** *Versionsnummer* **auf dem Volume** *Volumename* **ausgewählt.** erscheint.

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 & Gruppen** > **Anmeldeoptionen** > **Automatische Anmeldung: 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
- **Liste von Benutzern, die diesen Computer verwenden dürfen**.

Falls die letztere Option gewählt wurde, können Sie noch genauer beeinflussen, welche Benutzer in die Liste aufgenommen werden sollen:

- **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.

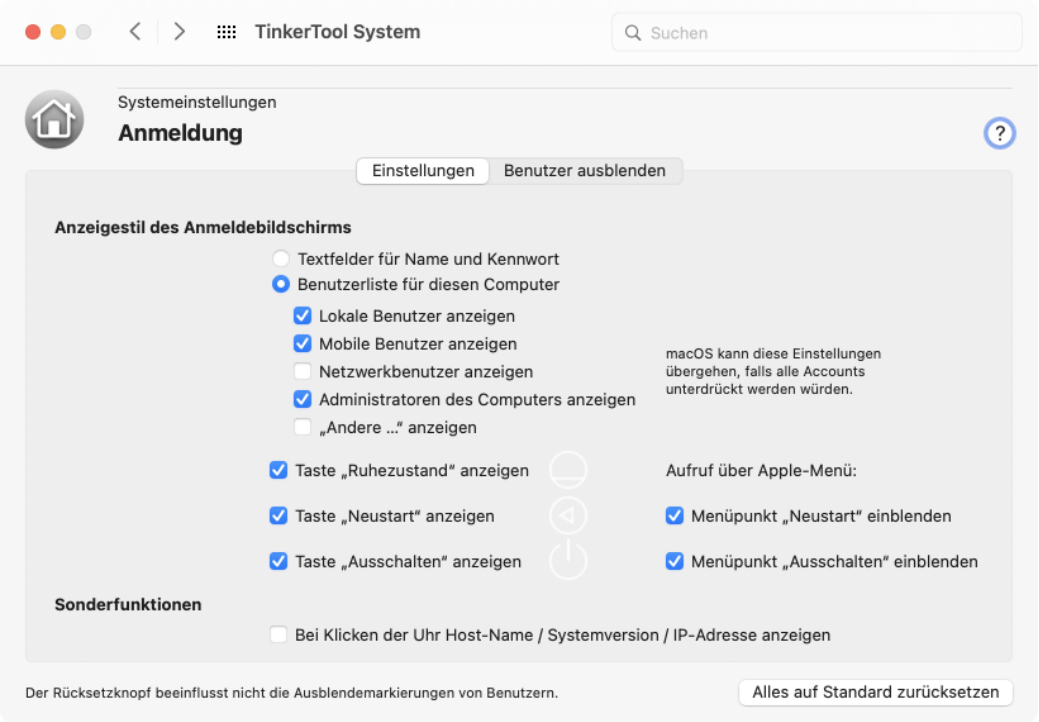

Abbildung 4.12: Einstellungen für den Anmeldeschirm

- **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 alleingestellte Dienstprogramm von TinkerTool System (Abschnitt 2.7 auf Seite 94) einsetzen, um den Anmeldeschirm auf Werkseinstellungen zurückzusetzen. Denken Sie daran, dass das Notfallprogramm im Voraus installiert werden muss, um verfügbar zu sein.

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 **Aufruf über Apple-Menü** verwenden. Alle Einstellungen sind unabhängig voneinander.
Standardmäßig zeigt der Anmeldeschirm neben den Eingabefeldern nur die aktuelle Zeit (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.
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.

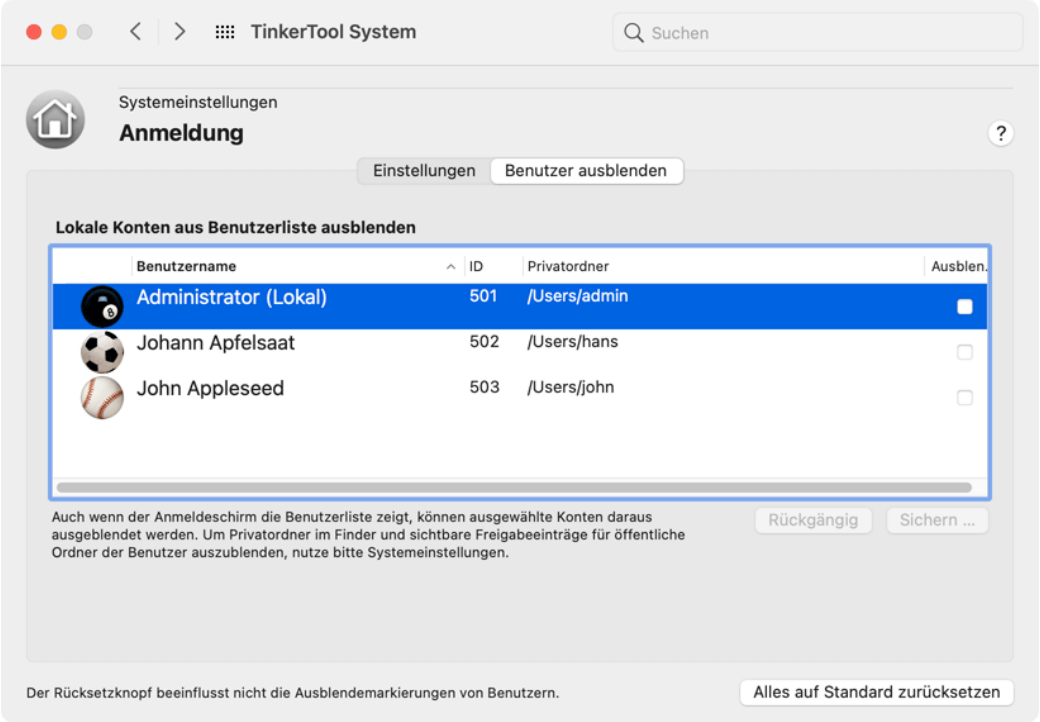

Abbildung 4.13: Accounts in der Benutzerliste der Anmeldung ausblenden

Die ausgeblendeten Benutzer-Accounts können immer noch indirekt sichtbar sein, z.B. über deren Privatordner im Ordner **Benutzer** (**/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 & 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** > **Freigaben** > **Dateifreigabe** und entfernen Sie alle Einträge in der Liste **Freigegebene 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 Programme 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** > **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.

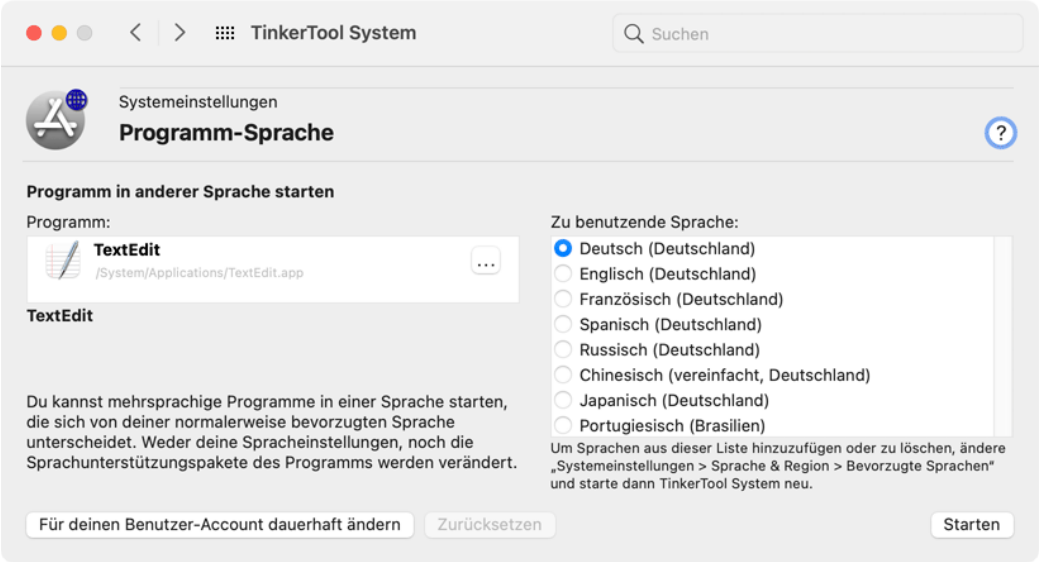

Abbildung 4.14: Programmsprache

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 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.

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 Programm 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, 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. über iCloud Drive, je nach Betriebssystemversion) und das
- Synchronisieren der Benutzerordner **Dokumente** und **Schreibtisch**

kann TinkerTool System die Dienste ausschalten und danach gegen Wiedereinschalten sperren. Für andere iCloud-Dienste kann TinkerTool System den Dienst *im derzeitigen Zustand* sperren, d.h. ist er gerade eingeschaltet, bleibt er eingeschaltet, ist er ausgeschaltet, bleibt er aus. Bevor Sie eine Sperre aktivieren, sollten Sie also prüfen, wie der derzeitige Zustand des jeweiligen Dienstes ist. Dies ist im Programm **Systemeinstellungen** unter **Apple-ID** > **iCloud** sichtbar. Sie können diese Einstellungskarte von TinkerTool System aus auch über den Knopf **Zustand in Systemeinstellungen zeigen** öffnen.

> 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.

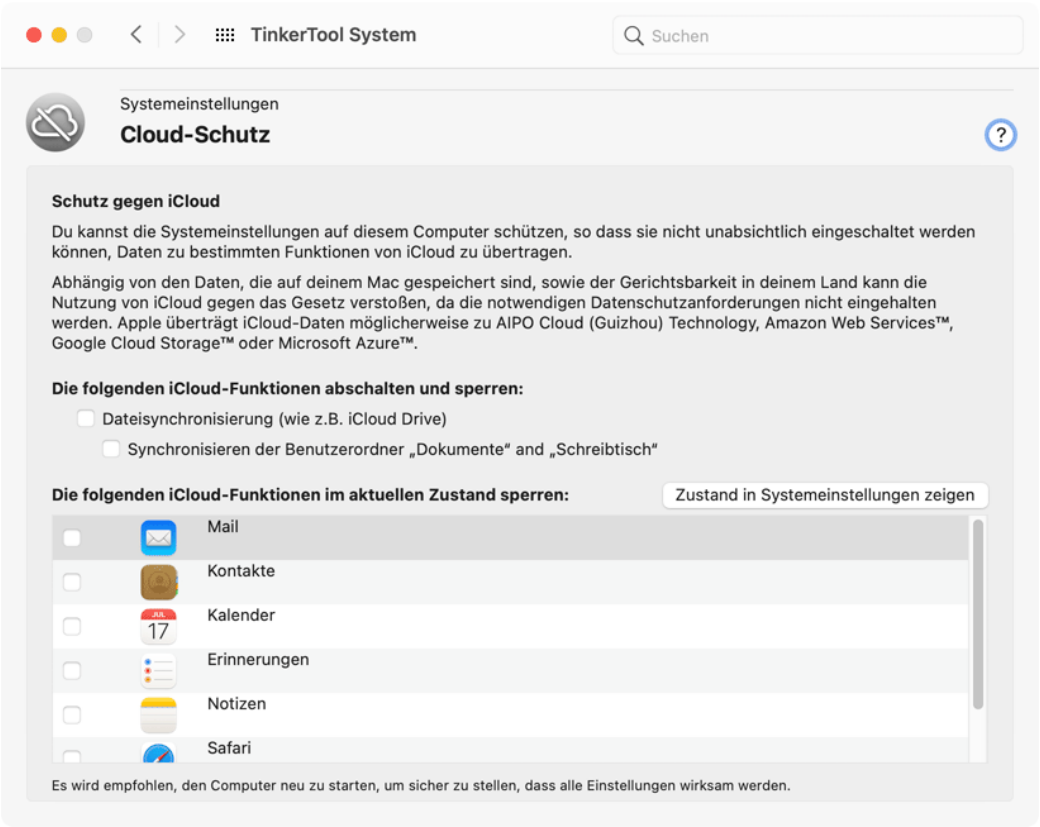

Abbildung 4.15: Cloud-Schutz

Um eine Sperre für einen iCloud-Dienst zu aktivieren oder zu entfernen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie die Einstellungskarte **Cloud-Schutz**.
2. Prüfen Sie über das Programm **Systemeinstellungen**, ob die jeweiligen iCloud-Dienste tatsächlich den gewünschten Zustand ein- oder ausgeschaltet aufweisen.
3. Sperren oder entsperren Sie den jeweiligen Dienst, indem Sie in TinkerTool System das jeweilige Häkchen setzen oder entfernen.

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 über TinkerTool System gleichzeitig deaktiviert und gesperrt worden, verschiebt macOS möglicherweise iCloud-Daten automatisch in einen Archivordner im Privatordner des jeweiligen Benutzers.

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 in der obersten Überschriftenzeile des Steuerungsfensters von TinkerTool System angegeben ist. Detaildaten über den ausgewählten Benutzer-Account können über den Karteireiter **Info** dieser Karte abgerufen werden.

5.1.1 Einstellungen („Präferenzen“)

Motivation

Macintosh-Software-Produkte werden normalerweise gemäß sehr hoher Standards für Bedienerfreundlichkeit 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 Namenserweiterung **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-Domänennamen (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-Domänennamen **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-Domänennamen 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 Karteireiter **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 **STOP**-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.

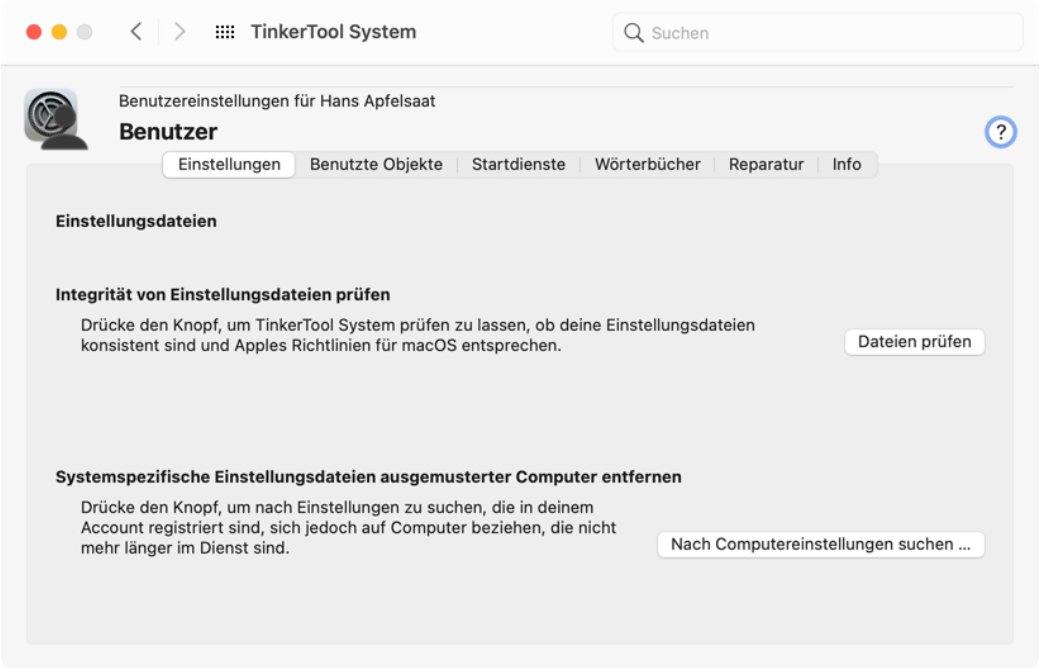

Abbildung 5.1: Einstellungen

- **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 alten Systemen war die primäre MAC-Adresse auf dem Typenschild des Computers aufgedruckt, üblicherweise begleitet von einem Strichcode, der die gleiche Information enthält. Die Adresse kann außerdem per Software abgerufen werden, indem Sie das Programm **Systeminformationen** aus dem Ordner **Dienstprogramme** starten. Sie finden die

Adresse, nachdem Sie die Informationskategorie **Netzwerk** auswählen, dann zur primären Netzwerkschnittstelle **(en0)** gehen und dort nach der Zeile **Ethernet** > **MAC-Adresse** schauen.
Bei modernen Versionen von macOS, die UUID-Codes verwenden, zeigt TinkerTool System die Identifikation unter **Info** > **Systeminformationen** > **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 Karteireiter **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 **STOP**-Knopf abbrechen. Ist das Durchsuchen der Einstellungen abgeschlossen, zeigt TinkerTool System einen Bericht an, der alle Dateien aufführt, 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:

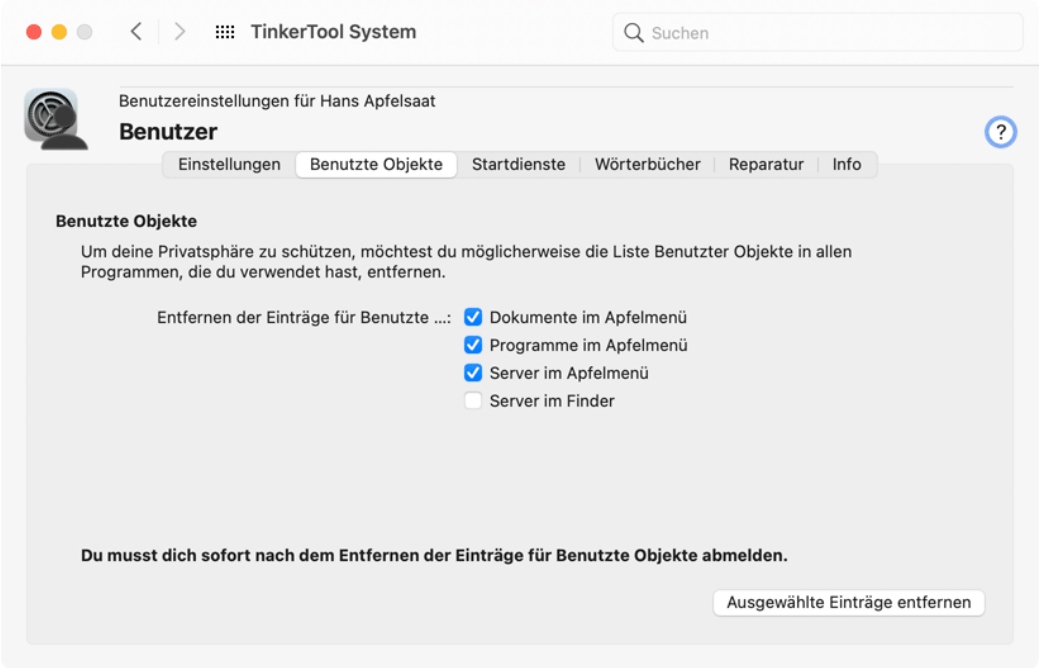

Abbildung 5.2: Benutzte Objekte

1. Öffnen Sie den Karteireiter **Benutzte Objekte** auf der Einstellungskarte **Privatsphäre**.
2. Wählen Sie jede Kategorie, für die die Einträge benutzter Objekte entfernt werden sollen.
3. Drücken Sie den Knopf **Ausgewählte Einträge entfernen**.

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.

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.

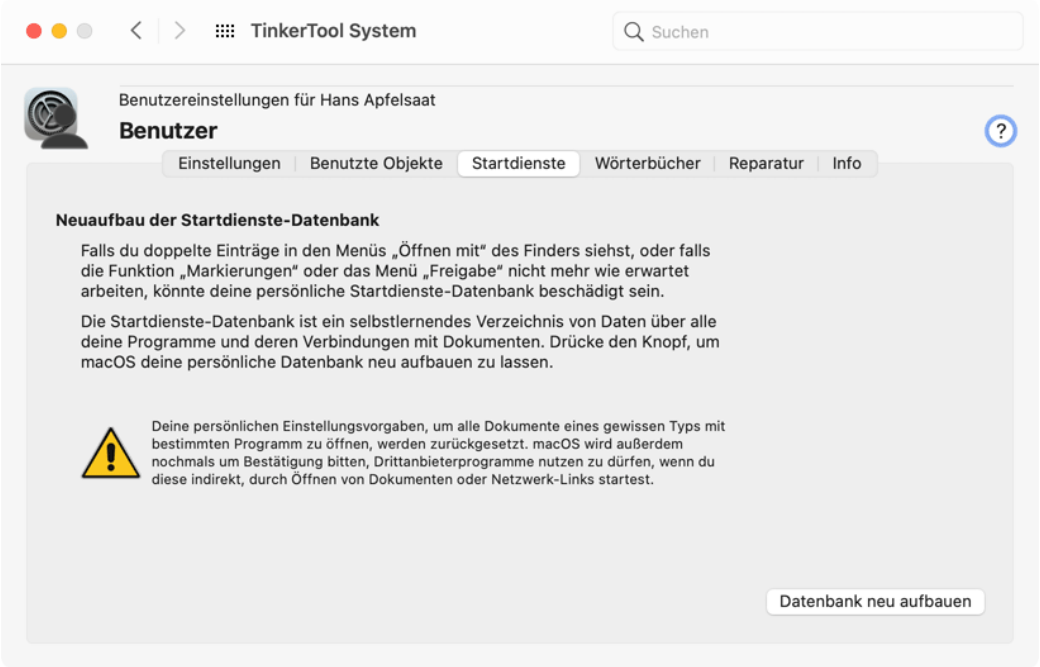

Abbildung 5.3: Startdienste

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 Karteireiter **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.

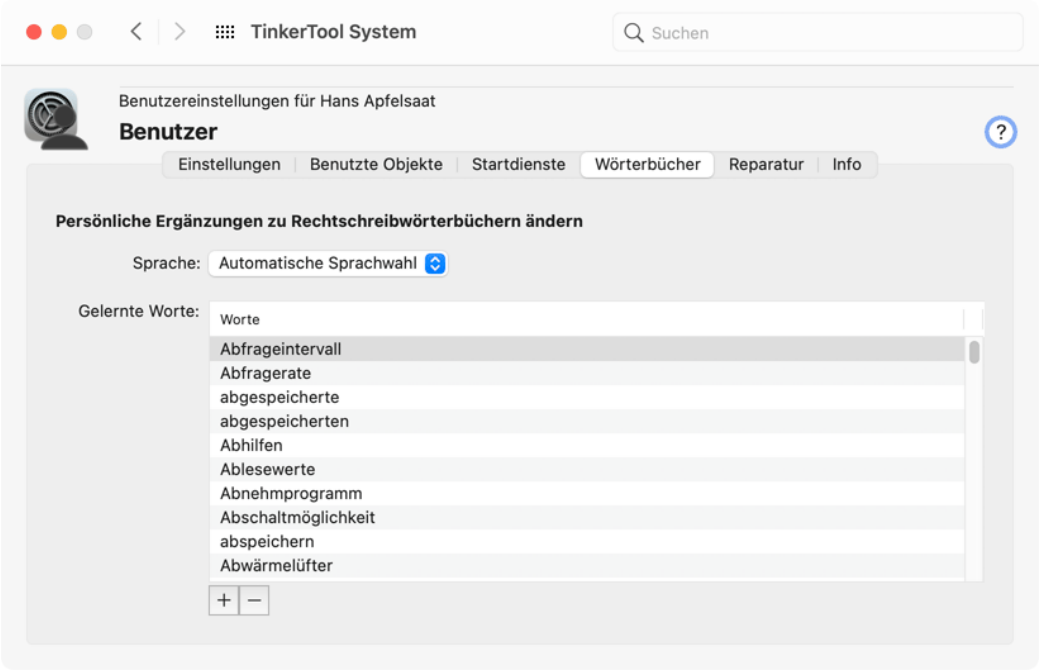

Abbildung 5.4: Rechtschreibwörterbücher

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 Karteireiter **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 selbständig und kontinuierlich alle auf dem Mac vorhandenen Programme mit grafischer Bedienerschnittstelle 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 Werkseinstellung 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 Karteireiter **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.

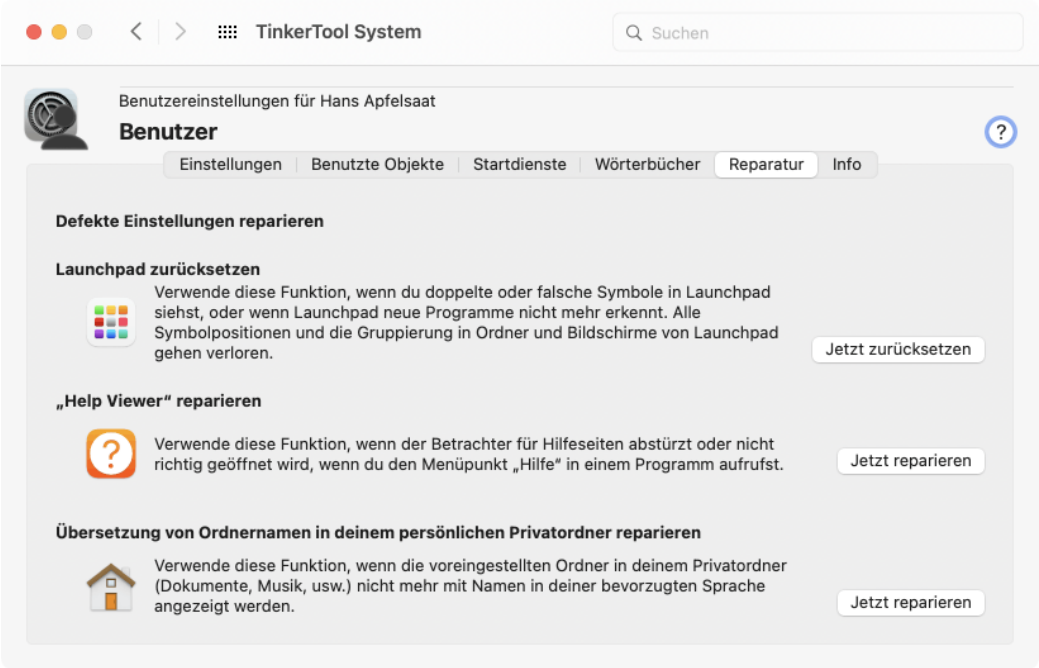

Abbildung 5.5: Reparaturfunktionen

- 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 Karteireiter **Reparatur** auf der Einstellungskarte **Benutzer**.
2. Betätigen Sie den Knopf **Jetzt reparieren** im Abschnitt **„Help Viewer" reparieren**.

Übersetzung von Ordnernamen 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 Karteireiter **Reparatur** auf der Einstellungskarte **Benutzer**.
2. Betätigen Sie den Knopf **Jetzt reparieren** im Abschnitt **Übersetzung von Ordnernamen in Ihrem persönlichen Privatordner reparieren**.

> Dies betrifft nur Ordner in Ihrem eigenen Privatordner, keine Systemordner oder Ordner anderer Benutzer-Accounts.

5.1.6 Info

Der Karteireiter **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. In Ergänzung zum vollen Benutzernamen, der bereits in der obersten Zeile des Fensters angezeigt wird, 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 oder durch das Umschalten auf die Darwin-Konsole (Abschnitt 4.4 auf Seite 238).
- 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 21) haben, können Sie mit den Einstellungskarten von TinkerTool direkt aus dem

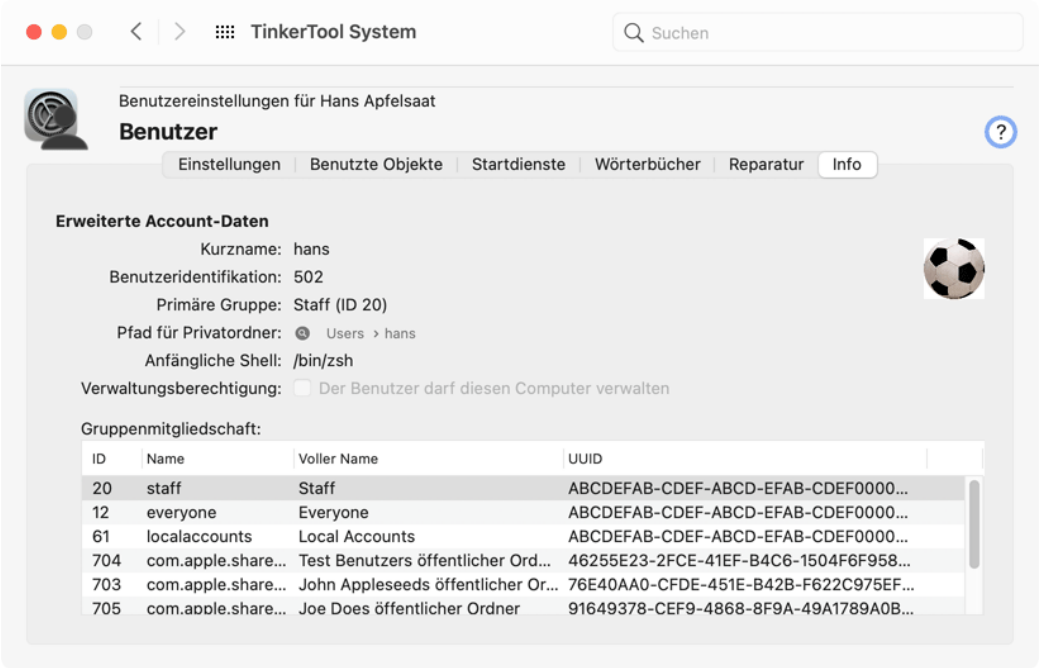

Abbildung 5.6: Info

System-Programm heraus arbeiten, so dass Sie nicht mehr beide Programme getrennt voneinander starten müssen, um Zugriff auf deren vollen Funktionsumfang zu haben. 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 für** … im Steuerungsfenster 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 2.7 auf Seite 94).

> 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 2.7 auf Seite 94) beschrieben sind.

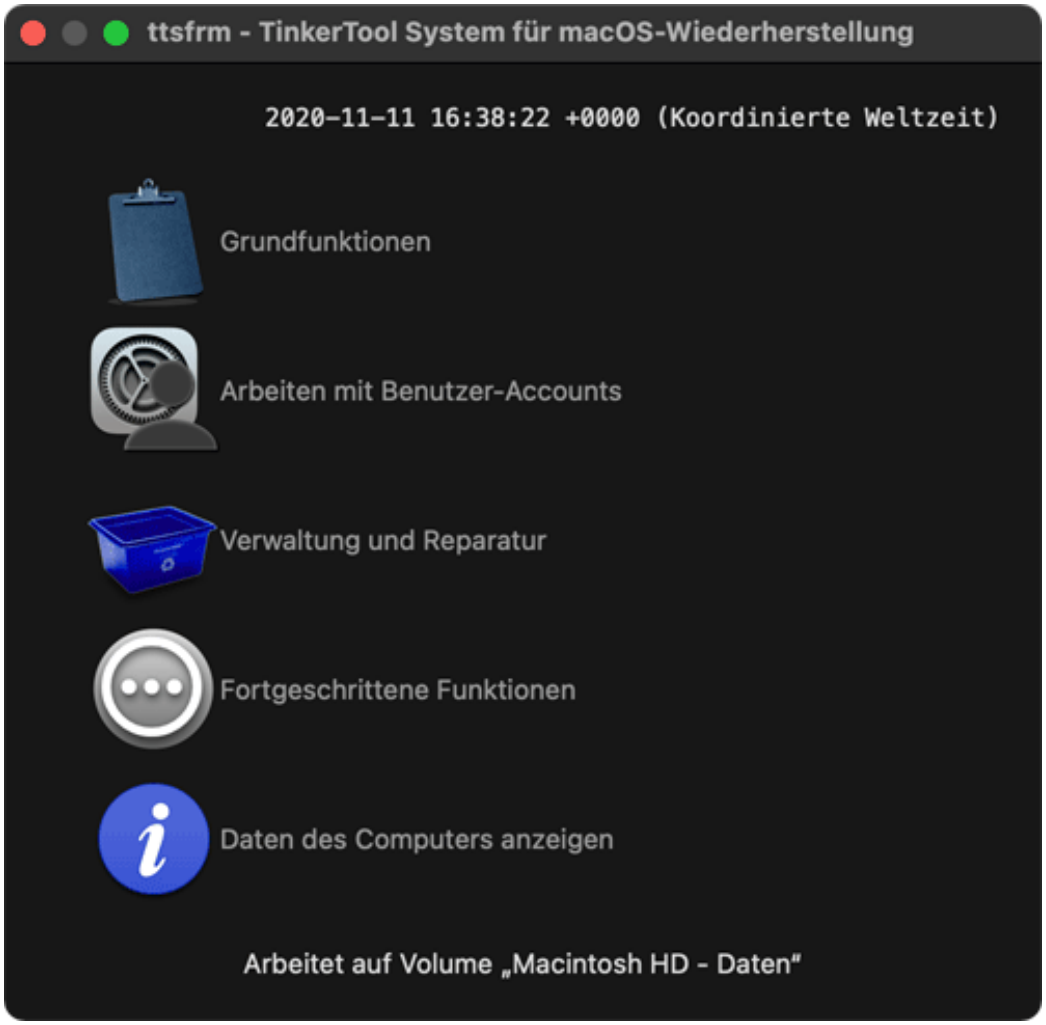

Abbildung 6.1: Das Hauptmenü von TinkerTool System für macOS-Wiederherstellung (ttsfrm)

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 261)
- Arbeiten mit Benutzer-Accounts (Abschnitt 6.3 auf Seite 262)
- Verwaltung und Reparatur (Abschnitt 6.4 auf Seite 265)
- Fortgeschrittene Funktionen (Abschnitt 6.5 auf Seite 270)
- Abrufen von Informationen (Abschnitt 6.6 auf Seite 271)

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.

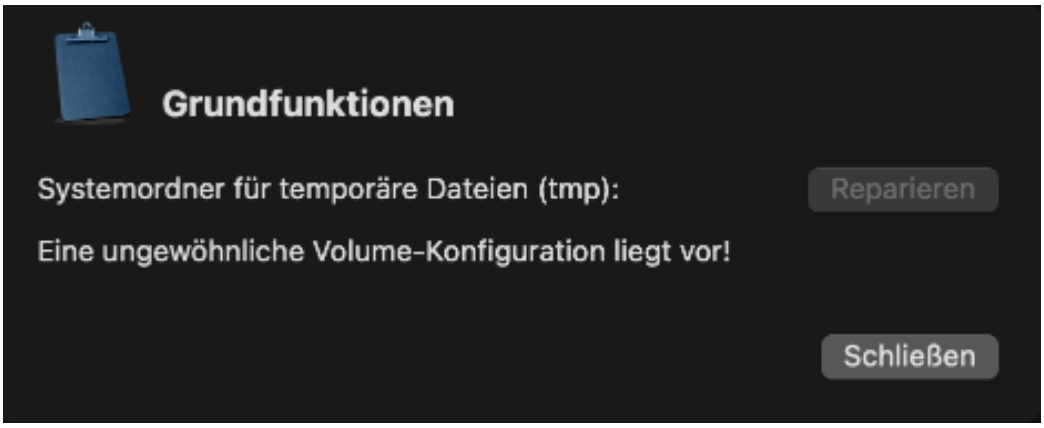

Abbildung 6.2: Grundfunktionen

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 **Benutzer**-Ordner *(/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 247)** > **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 27) 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.

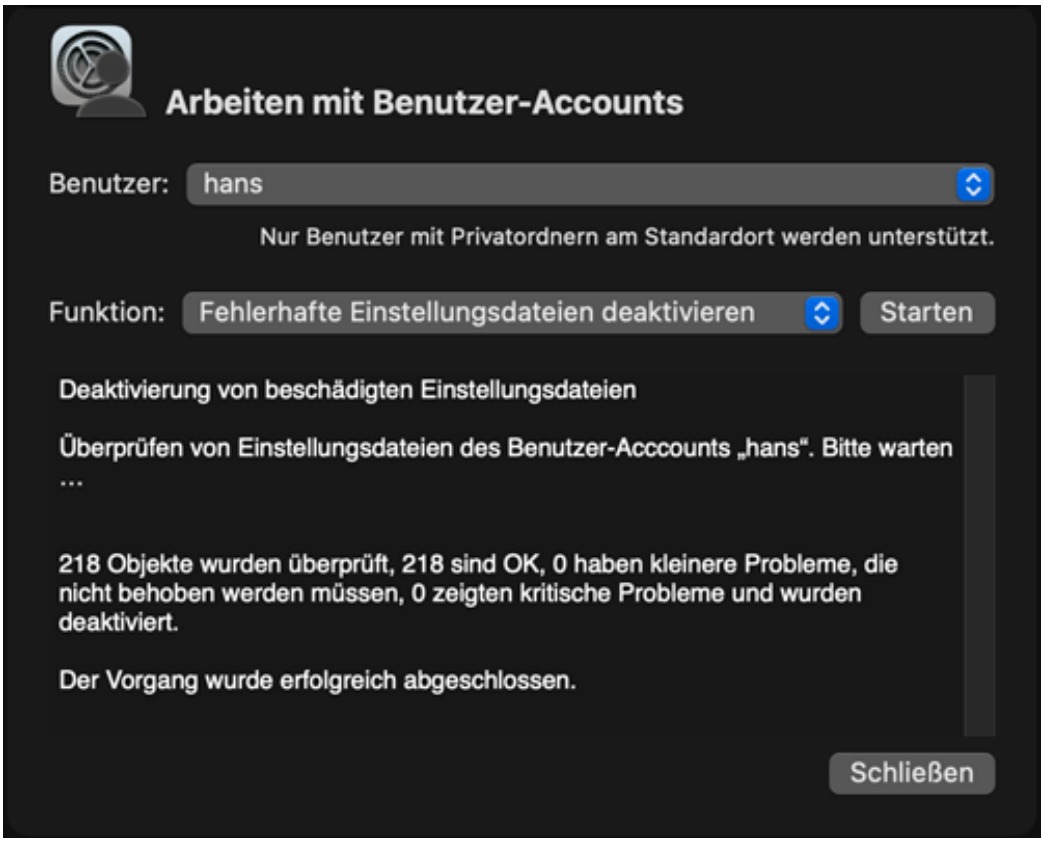

Abbildung 6.3: Arbeiten mit Benutzer-Accounts

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 247)** > **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**.

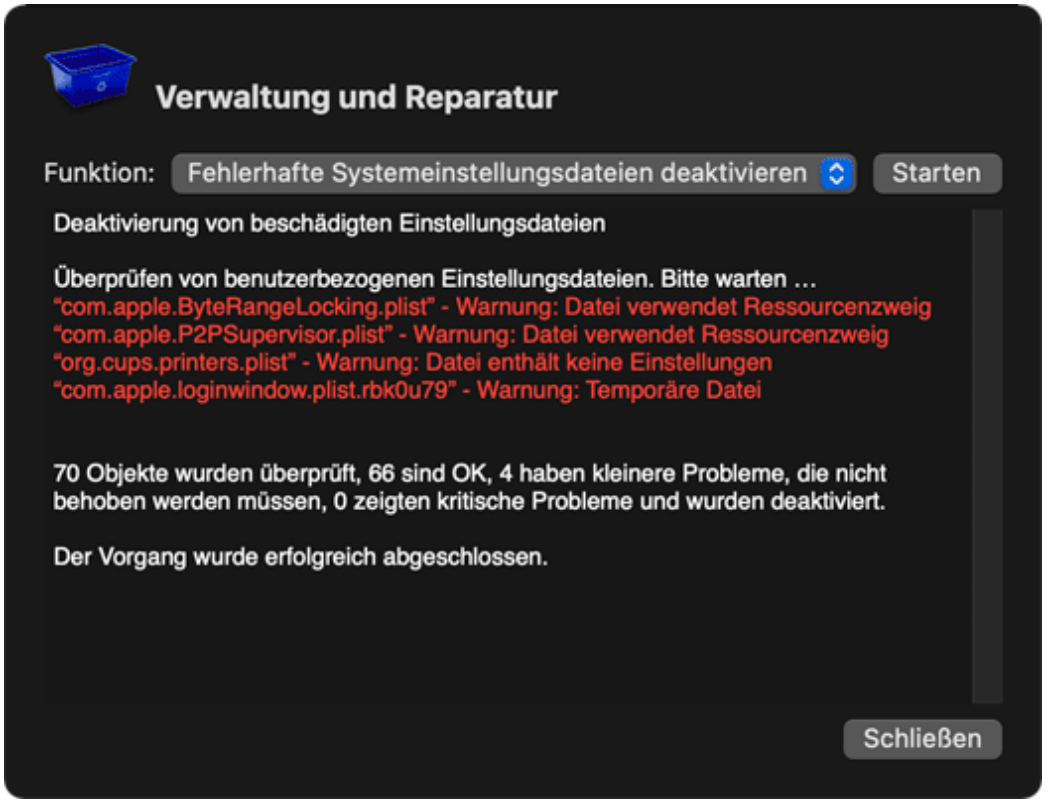

Abbildung 6.4: Verwaltung und Reparatur

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 27).

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 oder der Profilmanager von macOS Server 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 Werkseinstellung 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

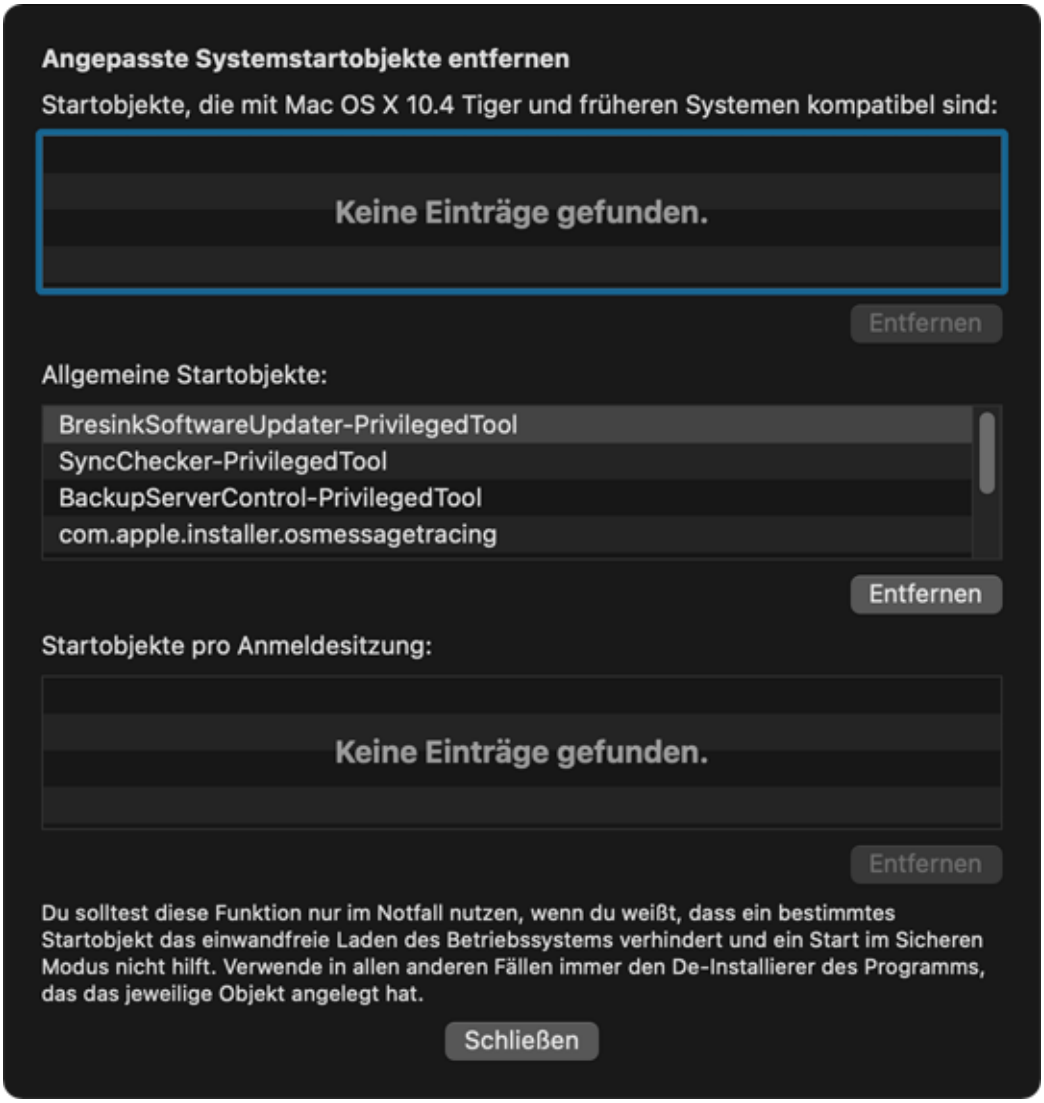

Abbildung 6.5: Angepasste Systemstartobjekte entfernen

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 & Gruppen** > **Anmeldeoptionen** 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 Einrichtungsassistent beim nächsten Start des Computer erneut laufen zu lassen, führen Sie die folgenden Schritte durch:

1. Klicken Sie im Hauptmenü auf **Fortgeschrittene Funktionen**.

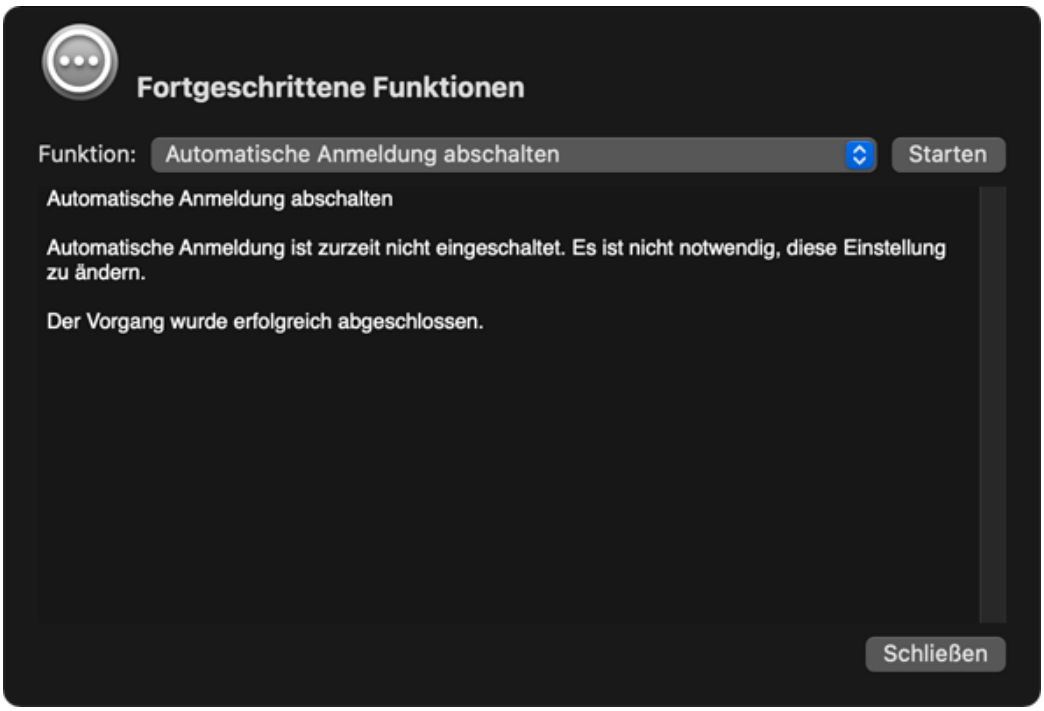

Abbildung 6.6: Fortgeschrittene Funktionen

2. Wählen Sie im Menüknopf **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**.
2. Stellen Sie sicher, dass der Karteireiter **Hardware-Überblick** ausgewählt ist.

Dies entspricht einer vereinfachten Version der Funktion **Info** > **Systeminformationen** in TinkerTool System.

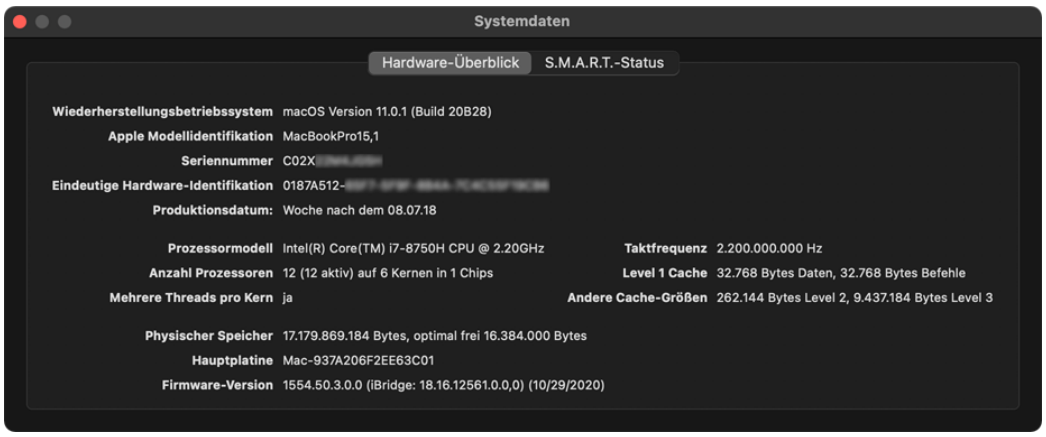

Abbildung 6.7: Hardware-Überblick

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.

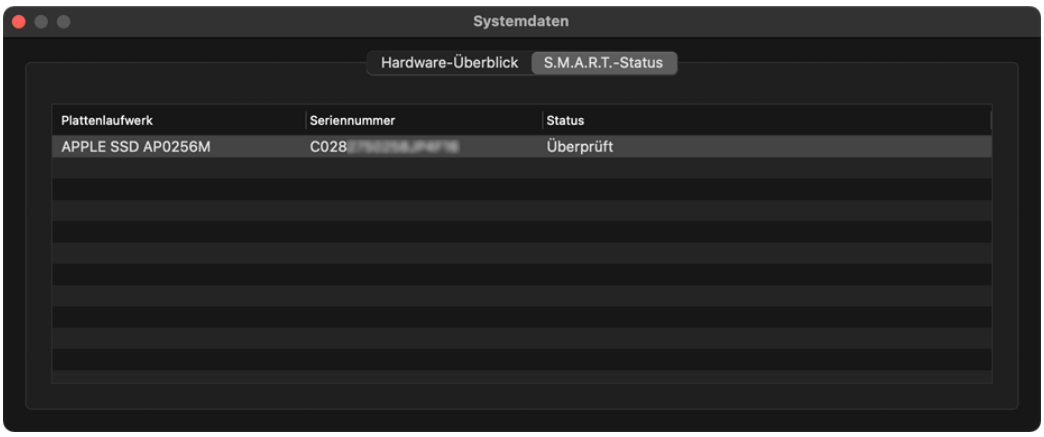

Abbildung 6.8: S.M.A.R.T.-Status

> 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 7 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 Werkseinstellungen

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 Registrierungsdatei, die einen Registrierungscode enthält, mit dem 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 Registrierungscodes

Die Bestellung von Registrierungscodes zu TinkerTool System 7 erfolgt über unseren Vertriebspartner. Sie kann per Internet, Post, Telefax oder Telefon erfolgen. Der Computer, auf dem das Programm eingesetzt wird, muss nicht notwendigerweise über eine Internet-Verbindung verfügen. Es ist lediglich erforderlich, dass Sie auf irgendeine Weise die E-Mail empfangen können, mit der der Registrierungscode ausgeliefert wird. Die Lieferung ist weltweit möglich. Die Zahlung kann in über 40 verschiedenen Währungen mit allen gängigen Zahlungsmitteln erfolgen.
Um genaue Details über die Abwicklung der Bestellung zu erfahren, verwenden Sie bitte die folgende Internet-Seite von TinkerTool System 7:
`https://www.bresink.com/osx/300863620-2/order-de.html`
Für erste schriftliche Informationen können Sie alternativ auch den Menüpunkt **Hilfe** > **Registrierungsschlüssel erwerben** ... im Programm aufrufen.

7.1.5 Registrieren per Datei oder per Texteingabe

Die Registrierungsdaten, die benötigt werden, um das Programm voll freizuschalten, können in zwei unterschiedlichen Formen an Sie ausgeliefert worden sein, entweder als Datei mit einem Eintrittskartensymbol, oder als lesbarer Text mit zwei Einträgen **Registrierungsname** und **Registrierungsschlüssel**. Auslieferung per Datei ist die bevorzugte Methode für alle neueren Bestellungen, da die Freischaltung dann mit einem simplen Doppelklick erledigt werden kann. Registrierung per lesbarem Text wird nur für sehr spezielle Lizenzsituationen verwendet.
Die notwendige Vorgehensweise zur Freischaltung unterscheidet sich, je nach dem welche Art von Registrierung Sie erhalten haben. Die beiden nachfolgenden Abschnitte beschreiben beide Vorgehensweisen zur Freischaltung im Detail. Nur eine der Vorgehensweisen gilt für Sie.

7.1.6 Freischalten der Software mit einer Registrierungsdatei

> Dieser Abschnitt beschreibt, wie Sie eine *Registrierungsdatei* verwenden, die Sie vom Software-Händler erhalten haben. Falls Sie ein Paar aus *Registrierungsname* und *Registrierungsschlüssel* direkt von Marcel Bresink Software-Systeme per E-Mail erhalten haben, überspringen Sie bitte diesen Abschnitt und schauen Sie weiter unten nach „Freischalten der Software mit einer Registrierungs-Mail“.

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 heruntergeladen 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 für diesen Zweck reserviert ist.
Falls Sie mehrere Lizenzen für das gleiche Programm bestellt hatten, wird jede Registrierung durch eine getrennte Datei dargestellt. Der Händler hat diese für das Herunterladen 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 **Software-Produktregistrierung 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.

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 Registrierungs-Mail

> Dieser Abschnitt beschreibt, wie Sie eine *Registrierungsnachricht* nutzen, die Sie per E-Mail direkt von Marcel Bresink Software-Systeme erhalten haben und die ein Paar aus *Registrierungsname* und *Registrierungsschlüssel* enthält. Falls Sie stattdessen eine *Registrierungsdatei* vom Software-Händler erhalten haben, lesen Sie bitte den vorigen Abschnitt „Freischalten der Software mit einer Registrierungsdatei".

Bitte beachten Sie, dass der Registrierungscode, den Sie per E-Mail erhalten haben, einen Wert darstellt und an einem sicheren Ort archiviert werden sollte, zum Beispiel als Ausdruck auf Papier. Der Code besteht aus zwei Teilen, dem *Registrierungsnamen* und dem *Registrierungsschlüssel*.

7.1.8 Eingeben einer per Mail zugesandten Registrierung von Hand

Gehen Sie wie folgt vor, um das Programm zur vollständigen Nutzung freizuschalten, wenn Sie Registrierungsname und Registrierungsschlüssel per E-Mail erhalten haben, und Sie diese beiden Angaben manuell übertragen müssen:

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 7 freischalten** ... auswählen.) Es erscheint das Fenster **Software-Produktregistrierung und Aktivierung**.

2. Drücken Sie den Knopf **Ich habe nur Registrierungsname und Registrierungsschlüssel**. 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** (⌘ + C) und **Bearbeiten** > **Einsetzen** (⌘ + V) 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 **Software-Produktregistrierung 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 der E-Mail, die Ihnen zugesandt wurde.

7.1.9 Eingeben 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 7 zu wechseln. In diesem besonderen Fall müssen zwei Registrierungen eingegeben werden, 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.

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, die Sie per E-Mail erhalten haben (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* 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 im vorigen Abschnitt erläutert, müssen Sie das Programm erneut registrieren, wenn Sie auf einen neuen Computer umziehen. Dies erfordert üblicherweise, dass Sie Ihre Registrierungsdatei erneut bereitstellen, und im Falle eines Upgrades auch eine zweite Registrierungsdatei (oder 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 Lizenzen 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).
Standort- und globale Lizenzen, die vor Juni 2016 ausgeliefert wurden, waren automatisch mit einer Art Abonnement-Dienst verbunden, der Administratoren die Möglichkeit gab, auf spezielle Versionen der Software zuzugreifen, die mit eingebetteten Volumenlizenzen ausgestattet waren. Diese kundenangepassten Software-Versionen konnten innerhalb der Organisation frei kopiert werden und waren „vorregistriert“, so dass der Wartungsaufwand zum Verwalten der Registrierungen auf ein Minimum reduziert war. Dieses Abonnement-Prinzip wurde im Juni 2016 eingestellt.
Seit diesem Datum ist die Verteilung von kundenangepassten Software-Versionen durch eine neue Methode abgelöst worden, die genauso einfach arbeitet:

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.

7.1.14 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.

7.1.15 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 > 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

Die Datenschutzfunktion von macOS, die TinkerTool System vollen Plattenzugriff genehmigt, kann scheitern wenn Sie mehrere Exemplare 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 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 **Sicherheit > Datenschutz > Festplattenvollzugriff**, melden Sie sich als Administrator an und entfernen Sie alle Einträge für TinkerTool System und TinkerToolSystem-PrivilegedTool, 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.

Privilegierte Vorgänge können nach einem Downgrade des Programms fehlschlagen: Die Sicherheitsfunktion von TinkerTool System arbeitet möglicherweise nicht mehr so wie erwartet, falls Sie ein Exemplar des Programms genutzt haben und später ein Exemplar mit einer kleineren Versionsnummer einsetzen. In diesem Fall werden Vorgänge, die von einem Systemverwalter autorisiert werden müssen, eventuell nicht mehr funktionieren. Stattdessen erhalten Sie eine Fehlermeldung, dass ein „Vertrauensproblem“ (bzw. „trust failure“) aufgetreten ist.
Abhilfe: Wir raten dringend davon ab, irgendeine Form von Downgrade (Wechsel auf eine ältere Version) durchzuführen. Falls die Verwendung einer früheren Version aus irgendeinem Grund nicht vermieden werden kann, müssen Sie sicherstellen, dass die Version der Sicherheitskomponente, die im Moment in macOS läuft, mit der Version übereinstimmt, die mit dem Exemplar von TinkerTool System ausgeliefert wurde, mit dem Sie arbeiten möchten. Führen Sie die folgenden Schritte durch:

1. Rufen Sie im laufenden Exemplar den Menüpunkt **Zurücksetzen** > **Sicherheitskomponente entfernen**... auf.

2. Folgen Sie den Anweisungen des Programms. Das Programm beendet sich selbst im letzten Schritt des Vorgangs.

3. Starten Sie die Version von TinkerTool System, die Sie nutzen möchten.

7.3 Versionshistorie

7.3.1 Release 7.99 (Build 241001)

- Kleinere Änderungen hinzugefügt, um die Unterstützung von macOS 12.7.4 und höher zu verbessern.
- Routine-Aktualisierungen in Metadaten und Dokumentation.

7.3.2 Release 7.98 (Build 240214)

Dies ist eine routinemäßige Aktualisierung, die kleinere Probleme behebt.

- Es wird ein Problem behoben, bei dem TinkerTool System for Recovery Mode (ttsfrm) eine irreführende Anleitung auf Macs mit Apple-Chips anzeigen konnte, wenn es außerhalb eines Wiederherstellungsbetriebssystems gestartet wurde.
- Es wird eine mögliche Race Condition vermieden, die dazu führen konnte, dass die Funktion zum Entfernen der Sicherheitskomponente möglicherweise ausfallen konnte.

7.3.3 Release 7.97 (Build 230822)

- Aufgrund von Architekturänderungen in neueren Macintosh-Modellen und macOS-Versionen musste die Funktion zum Abschalten des Systemintegritätsschutz 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.

7.3.4 Release 7.96 (Build 230605)

Dies ist ein Wartungs-Update, das ein Kompatibilitätsproblem mit bestimmten Versionen von macOS behebt, bei denen das Löschen eines Time Machine-Schnappschuss immer mit Fehlercode 2 abgewiesen wurde, falls das Sicherungsziel ein APFS-Volume war.

7.3.5 Release 7.95 (Build 230414)

- Neue Funktion hinzugefügt um die Build-Nummern verfügbarer macOS-Versionen anzugeben, wenn die Liste der von Apple zum Download angebotenen Installationsprogramme dargestellt wird. Diese Funktion ist nur in macOS 12 verfügbar, nicht in macOS 11.
- 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, 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.

7.3.6 Release 7.94 (Build 230207)

- Interne Änderungen für Funktionen mit Internet-Zugriff, was die Kompatibilität mit Firewalls von Drittanbietern verbessert.
- Diese Version behebt ein Problem, bei dem verschiedene Stufen von Betriebssystemkompatibilitätswarnungen sich gegenseitig in verwirrender Weise überschreiben konnten.

7.3.7 Release 7.93 (Build 221205)

- Diese Version behebt ein Problem, bei dem die allgemeine Reset-Funktion möglicherweise für die Karte Cloud-Schutz nicht wie erwartet funktioniert hat.

7.3.8 Release 7.92 (Build 221026)

- Bessere Bedienerführung hinzugefügt wenn das Programm mit macOS 13 Ventura eingesetzt wird.

7.3.9 Release 7.91 (Build 221012)

- Die Fehlerbehandlung für Ethernet-Firmware-Prüfungen (auf Intel-Macs) wurde überarbeitet, um in bestimmten Situationen klarere Meldungen zu liefern.
- Diese Version behebt ein Problem, bei dem der Zeitassistent für den Zugriff auf vereinheitlichte Protokolle unter bestimmten Umständen die letzte Aufwachzeit statt die Systemstartzeit einstellen konnte.

7.3.10 Release 7.9 (Build 220913)

Dies ist ein Wartungs-Build, das ein Kompatibilitätsproblem mit neueren Versionen von macOS Monterey behebt. Die Funktion zum Entfernen alter Versionen des privilegierten Hilfsprogramms zeigt nun auf den betroffenen Systemen die korrekte Statusinformation statt „unbekannt“.

7.3.11 Release 7.9 (Build 220809)

- Das Notfallwerkzeug (TinkerTool System for Recovery Mode) kann nun auch auf Macs mit Apple Silicon genutzt werden, falls macOS 12.5 oder höher installiert ist.
- Die Bedienerschnittstelle zur Startanleitung des Notfallwerkzeugs wurde überarbeitet.
- Es wurde ein Problem behoben, bei dem die Anzahl der Prozessor-Cluster bei bestimmten Apple-Chips nicht korrekt angegeben wurde.

7.3.12 Release 7.89 (Build 220711)

- Neue Einstellungen hinzugefügt, um die Menüpunkte für Neustart und Ausschalten aus dem Apfelmenü zu entfernen. Diese Vorgaben sind Teil der Einstellungen für den Anmeldebildschirm.

- Neue Funktionen hinzugefügt, um mit abgespeicherten Sätzen von Rechten zu arbeiten, wenn Berechtigungen über die Karte ACL-Rechte verändert werden. Benutzer können nun Berechtigungseinstellungen für Dateien und Ordner vordefinieren und diese später auf anderen Dateisystemobjekten mit wenigen Mausklicks wieder anwenden. Komplexe Konfigurationen mit einer hohen Zahl detaillierter Zugriffssteuerungseinträge lassen sich nun auf dem gleichen Computer einfach übertragen.

- Die Bedienerschnittstelle, um Ausschlusseinstellungen für Volumes nach Betriebssystem-Updates auf sekundären Volumes automatisch zu aktualisieren, wurde weiter optimiert.

7.3.13 Release 7.88 (Build 220614)

- Vorläufige Unterstützung für zukünftige Versionen von macOS hinzugefügt.

- Neue Funktion hinzugefügt um ein bekanntes Problem mit der Softwareupdate-Funktion von macOS Big Sur zu beheben. Es ist jetzt möglich, Apples Softwareaktualisierung in Fällen zurückzusetzen, in denen die Bedienerschnittstelle der Systemeinstellungen einen endlosen Wartezustand anzeigt wenn der Benutzer nach den neuesten Sicherheits-Updates sucht.

- Neue Funktion hinzugefügt um Volume-Ausschlusstabellen automatisch aktualisieren zu können, wenn ein Volume einer sekundären Installation von macOS gelistet war, aber ein Update dieses Betriebssystems das vorherige System-Volume durch ein neues ersetzt hat. Nach Bedienerbestätigung werden aktualisierte Volume-Identifikatoren hinzugefügt und die alten entfernt.

- Neue Benutzereinstellung für das Umschalten zwischen Einstellungskarten über Pfeiltasten oder -knöpfe hinzugefügt. Benutzer von TinkerTool System können nun entscheiden, ob die Pfeile zwischen benachbarten Karten navigieren (bisheriges Verhalten) oder innerhalb der Auswahlhistorie (entsprechend dem Verhalten von Systemeinstellungen).

- Die Karte zur Unterstützung zusätzlicher Hardware-Einstellungen von portablen Macs mit „Immer an“-Architektur kann nun auch für die achte und neunte Generation Intel-basierter MacBook Air-Modelle verwendet werden.

- Es wurde ein Problem bei der Auswahl von Einstellungskarten behoben, wenn per Menü in der gleichen Laufzeitsitzung navigiert wurde, in der TinkerTool eingebettet wurde.

- Es wurde ein Problem mit dem Layout eingebetteter TinkerTool-Karten, bzw. beim Umschalten zwischen Karten sehr unterschiedlicher Höhe behoben.

7.3.14 Release 7.87 (Build 220509)

- Neue Funktion hinzugefügt, um Daten aus einem lokalen oder fernen Verzeichnisdienst zu exportieren, der an einem Mac gebunden ist. Dies kann zum Beispiel nützlich sein, um Benutzer-Accounts aus der aufgegebenen macOS-Server-Software in andere Betriebssystem zu übertragen. Die neue Funktion ist auf der Karte Wartung zu finden.

- Neue Funktion zur einfachen Inspektion des Systemprotokolls hinzugefügt, um eine verdächtige Anzahl von Anmeldeversuchen am Konsolbildschirm, oder allgemeine

Autorisierungsfehler von Benutzern zu erkennen. Die neue Funktion kann auf der Karte Systemsicherheit gefunden werden.

- Neue Funktion hinzugefügt, um die genaue Konfiguration von Prozessoren mit Apple-Chips zu bestimmen. Die Anzahl der Effizienz-, Hochleistungs- und GPU-Kerne, sowie die Anzahl der Prozessor-Cluster kann ausgelesen werden.
- Neue Funktion hinzugefügt, um Kopien von APFS-Schnappschussübersichten in externen Fenstern anzuzeigen. Die Fenster lassen sich in der Größe verändern, so dass der vollständige Datensatz ohne abgeschnittene Tabellenspalten dargestellt werden kann.
- Neue Funktion hinzugefügt, um das Launchpad für den aktuellen Benutzer-Account auf Werkseinstellungen zurückzusetzen.
- Der Punkt zum Reparieren des Programms Systemeinstellungen wird in aktuellen Versionen von macOS nicht mehr benötigt und wurde entfernt.
- Die meisten Teile der Karte Netzwerk behalten nun ihre früheren Inhalte bei wenn das Programm erneut gestartet wird.
- Die Bedienerschnittstelle für die Trim-Funktionsübersicht bei AHCI-basierten SSDs wurde aktualisiert.
- Die Eingabe eines Textfilters beim Arbeiten mit Ergebnissen einer Protokolldatenbankabfrage erfordert nicht mehr das Betätigen der Eingabetaste.
- Es wurde ein Problem behoben, bei dem die Funktion zur Suche mit Schlüsselworten für Ergebnisse auf der Karte Wartung nicht immer korrekt gearbeitet hat.
- Es wurde ein Problem behoben, bei dem ein Textfilter unerwartet wiederverwendet werden konnte, wenn eine neue Anfrage an die Protokolldatenbank gestellt wurde.
- Es wurde ein Problem behoben, bei dem das Programm unerwartet beendet werden konnte, wenn die Kommunikation mit einem externen privilegierten Dienstprogramm abgebrochen wurde, während dieses Daten gesendet hat.

7.3.15 Release 7.86 (Build 220317)

- Neue Abhilfe für macOS Monterey hinzugefügt, wenn die Autorisierung privilegierter Vorgänge aufgrund von undokumentierten „ACM Policy“-Fehlern fehlschlägt.
- Das Programm kann nun die private Größe (Speicherplatzverbrauch) von einzelnen APFS-Schnappschüssen anzeigen.
- Die Bedienerschnittstelle zum Auflisten von APFS-Schnappschüssen wurde neu gestaltet.
- Das Programm kann nun interne Abstürze von Time Machine-Komponenten erkennen. Dies hilft bei der Diagnose von Systeminstallationen, bei denen Time Machine nicht zuverlässig genug arbeitet, um Wartungsaufgaben ausführen zu können.
- Die Bedienerführung für den Test des Netzantwortverhaltens wurde für Fälle verbessert, in denen der Benutzer eine Schnittstelle ausgewählt hat, die nicht ans Internet geleitet wird.
- Das Programm kann nun automatische Neuregistrierung anbieten, wenn es auf einen neuen Computer migriert wurde.

7.3.16 Release 7.85 (Build 220214)

- Neue Funktion hinzugefügt, um Dateisystemrechte im Privatordner eines lokalen Benutzers auf Standardwerte zurückzustellen. Dies schließt eine „Testlauf“-Möglichkeit mit ein, die eine vorläufige Prüfung erlaubt.
- Neuer Knopf „Im Finder zeigen“ für unlesbare Objekte hinzugefügt, die bei der Prüfung von Pfadlängen tief verschachtelter Ordner gefunden wurden.
- Es wurde eine zusätzliche Warnung beim Ändern von Vererbungseinstellungen von Zugriffssteuerungseinträgen hinzugefügt, wenn eine Kombination von Optionen zwar gültig, aber wirkungslos ist.
- Es wurde eine neue Option für das Abrufen von Standardsystemprotokollen hinzugefügt, die sich auf Ereignisse des Typs „Not-Aus“ beziehen.
- Es wurde eine neue Option für das Abrufen von Standardsystemprotokollen hinzugefügt, die sich auf Programmabstürze beziehen, die macOS im iPhone-IPS-Format aufgezeichnet hat.
- Viele Systemprotokolle werden jetzt automatisch neu aufbereitet und leicht lesbar gemacht, falls macOS diese im JSON-Format statt als reinen Text gespeichert hat.
- Neue Funktion hinzugefügt, um bestimmte Systemprotokolle im Programm Konsole zu öffnen, für Fälle, in denen macOS eine undokumentierte Aufbereitung vornimmt, um das rohe Protokoll in interpretierten Text zu übersetzen.
- Um Geschwindigkeitsprobleme mit der grafischen Oberfläche von macOS zu vermeiden, wenn Ergebnisse mit mehr als einer halben Million Einträge verarbeitet werden, wurde die Funktion zum Neusortieren von Spalten in der Ergebnistabelle der Time Machine-Vergleichsfunktion entfernt.
- Die Ergebnisse eines Time Machine-Schnappschussvergleichs können nun als zusätzliche Textdatei exportiert werden.
- Es wurde ein Problem behoben, bei dem das Exportieren einer Liste verwaister Dateien unter bestimmten Umständen fehlschlagen konnte.

7.3.17 Release 7.8 (Build 220112)

- Neue Funktion hinzugefügt, um neue Protokolltypen aus macOS auszulesen, die Diagnoseberichte über anwendungsinterne Vorfälle enthalten.
- Neuer Assistent zur Einstellung des Zeitintervalls wurde zur Bedienerschnittstelle hinzugefügt, die moderne macOS-Protokolle ausliest.
- Neue Filterfunktion hinzugefügt, die es erlaubt, Zeilen im generierten Text moderner macOS-Protokolle im Nachhinein auszublenden. Der Benutzer kann sich auf Meldungen konzentrieren, die ein bestimmtes Schlüsselwort enthalten.
- Neues Tab zum Produktdaten-Informationsfenster für einige Systeme mit Apple-Chips hinzugefügt, um technische Daten über das interne Netzteil anzeigen zu lassen. Diese Funktion ist nur auf bestimmten Macintosh-Baureihen verfügbar.

- Die Funktion zum Anlegen von macOS-Installationsmedien informiert nun den Benutzer im Detail, falls das Anlegen aufgrund einer Einschränkung eines bestimmten Installers fehlgeschlagen ist, wenn der Installer diesen Vorgang absichtlich in einer Überkreuz-Architektursituation blockiert (z.B. wenn ein Nur-Intel-Installer auf einem Mac mit Apple Chips erzeugt werden soll).
- Die Vorauswahl von zu löschenden Objekten ist nun für alle Arten von Software konsistenter, wenn der Deinstallationsassistent für Programme genutzt wird.

7.3.18 Release 7.71 (Build 211122)

- Neue Funktion hinzugefügt, um den eingebauten Internet-Geschwindigkeitstest von macOS Monterey laufen zu lassen (nur macOS 12 oder höher).
- Die Behandlung des Herstellungsdatums wurde für Apple-Geräte, die nach August 2021 gefertigt wurden, aktualisiert.
- Volle Unterstützung für Lüftertests bei Modellen des MacBook Pro 2021 wurde hinzugefügt. Diese behebt mögliche Probleme, bei denen das Programm die Durchführung des Tests verweigern konnte, wenn das System zu kalt war.

7.3.19 Release 7.7 (Build 211021)

- Volle Unterstützung für macOS 12 Monterey hinzugefügt.
- Neue Funktion auf der Karte System hinzugefügt, um zu steuern, wie macOS sich mit WLAN-Netzen verbindet wenn mehrere Netze verfügbar sind, oder die Verbindung mit dem ausgewählten Netz fehlgeschlagen ist.
- Die Live-Statusanzeige beim Abrufen von Protokolldaten von macOS wurde verbessert.
- Es wurde ein Problem mit der deutschen Bedienerschnittstelle der Karte Info behoben, das dazu führen konnte, dass einige Dialoge unerwartet auf englisch angezeigt wurden.

7.3.20 Release 7.6 (Build 210927)

- Diese Version fügt viele interne Änderungen hinzu, um die Kompatibilität mit zukünftigen Versionen von macOS sicher zu stellen.
- Eine Suchoption wurde zur Funktion zum Abrufen von Systemprotokollen hinzugefügt.
- Eine Suchfunktion ist nun auch für viele andere Berichtsanzeigen im Programm verwendbar.
- Alle Funktionen mit Druckausgabe vermeiden es jetzt, einen schwarzen Hintergrund zu drucken, selbst wenn der Benutzer ein dunkles Systemerscheinungsbild ausgewählt hat.
- Die Funktion zum Löschen der Partitionstabelle eines benutzten Plattenlaufwerks bietet es jetzt an, alle betroffenen Volumes zu deaktivieren statt sie auszuwerfen, was angemessener ist.

- Die Funktion, um nach langen Dateisystempfaden zu suchen, verhindert nun während der Arbeit das Einschalten des Ruhezustands.
- TinkerTool System für den Wiederherstellungsmodus (ttsfrm) akzeptiert jetzt mehr laufende Hintergrundprozesse, was Probleme mit der Erkennung des Wiederherstellungssystems behebt.
- Es wurde ein Problem behoben, bei dem die Darstellung von datenschutzrelevanten Einträgen im Systemprotokoll nicht mit der Beschreibung im Referenzhandbuch übereingestimmt hat.

7.3.21 Release 7.5 (Build 210824)

- Neue Diagnosefunktion hinzugefügt, um Bildschirme auf tote oder hängende Pixel zu testen. Die Funktion kann auch bei der Reinigung des Display-Glases helfen oder bei der Untersuchung von Staubproblemen.
- Neue Einstellungskarte hinzugefügt, um bestimmte iCloud-Dienste für alle Benutzer zu sperren. Hierdurch kann der jeweilige Dienst nicht mehr unabsichtlich eingeschaltet werden.
- Die Funktion zum Abrufen von Protokollen aus dem macOS-Protokollsubsystem verwendet nun farbige Hintergründe, um Nachrichten verschiedener Wichtigkeitsstufen klarer voneinander abgrenzen zu können.
- Die Bedienerschnittstelle der Funktion zur Suche nach Dateisystempfaden, die eine vom Benutzer vorgegebene Länge überschreiten, wurde überarbeitet. Es ist nicht mehr notwendig, die Eingabetaste zu drücken, nachdem der Grenzwert eingegeben wurde und der letzte verwendete Wert wird vom Programm behalten. Das Ergebnisfenster des Schnelltests kann jetzt die vollständigen Pfade anzeigen und im Finder aufdecken.
- Die Bedienerschnittstelle für alle Funktionen zum Erben einer fremden Time Machine-Sicherung wurde überarbeitet.
- In nicht englischen Versionen von TinkerTool System verwenden Programm und Dokumentation jetzt die korrekte Terminologie für Macs mit Apple-Chips.
- Es wurde ein Problem behoben, aus dem sich eine unerwartete Beendigung des Programms nach dem Ausdünnen, Löschen oder Anlegen eines Time Machine-Schnappschusses ergeben konnte.

7.3.22 Release 7.41 (Build 210721)

- Änderungen für bevorstehende Versionen von macOS hinzugefügt.
- Neue Funktion hinzugefügt, um alle Volumes einer physischen Platte automatisch auszuwerfen, bevor die Funktion zum Löschen aller Partitionierungsdaten verwendet wird.
- Die Funktion zum Herunterladen von macOS-Installationsprogrammen von Apple öffnet nun automatisch den Programme-Ordner nachdem der Vorgang abgeschlossen ist.
- Die Bedienerschnittstelle, um Volumes von automatischen Aktivierungsvorgängen auszuschließen, wurde überarbeitet.

- Es wurde ein Problem behoben, bei dem der Stopp-Knopf möglicherweise nicht funktioniert hat, wenn versucht wurde, eine privilegierte Funktion abzubrechen, die bereits eine längere Zeit gelaufen war.

7.3.23 Release 7.4 (Build 210621)

- Vorläufige Unterstützung für zukünftige Versionen von macOS wurde hinzugefügt.
- Neue Funktion hinzugefügt, um neue Absturzberichte für den „Immer an"-Teil von Macintosh-Modellen mit Apple-Chip im Bereich Standardprotokolle der Info-Karte abrufen zu können.
- Neue Funktion zu den Programmsicherheitsprüfungen hinzugefügt, um anzuzeigen, ob Software-Produkte die gehärtete Laufzeitumgebung verwenden.
- Unterstützung hinzugefügt, um Installationsmedien für zukünftige Versionen von macOS erstellen zu können.
- Die Kategorien Medien & Apple Music, HomeKit und Bluetooth wurden der Funktion zum Zurücksetzen der Datenschutzeinstellungen für Programme hinzugefügt.
- Die Funktion zum Zurücksetzen der Spracheinstellungen für einen Benutzer-Account wird mit aktuellen Versionen von macOS nicht mehr benötigt und wurde entfernt.
- Es wurde ein Problem behoben, bei dem die Web-Schnittstelle des CUPS-Druckersubsystems nicht mit dem entsprechenden Knopf auf der System-Karte geöffnet werden konnte.
- Es wurde ein Problem behoben, bei dem das Erzwingen eines erneuten Laufs des Einrichtungsassistenten über das Notfallwerkzeug im Wiederherstellungsmodus mit bestimmten Versionen von macOS nicht möglich war.
- Die APFS-Funktion zum Arbeiten mit Schnappschüssen nimmt aktivierte Schnappschüsse selbst nicht mehr in das Menü möglicher APFS-Quell-Volumes auf.

7.3.24 Release 7.3 (Build 210518)

- Unterstützung für macOS 11.4 wurde hinzugefügt.
- Das Klonen des Betriebssystems wird jetzt wieder unterstützt, falls macOS 11.4 oder höher zum Einsatz kommt. Bitte ziehen Sie das Referenzhandbuch hinzu, um mehr über momentane Einschränkungen zu erfahren.
- Es wurden Fehlerumgehungen für mehrere Defekte in macOS 11.3 oder höher hinzugefügt, bei denen das Erstellen von Installationsmedien mit bestimmten Installationsprogrammen von macOS 11 nicht möglich war.
- Die Richtlinien für das Format möglicher Zielplatten beim Erstellen von Installationsmedien wurden geändert, um das Verhalten von Apples neuesten Installationsprogrammen zu berücksichtigen.
- Die Fehlerbehandlung beim Erstellen von Installationsmedien wurde erweitert, um dem Benutzer den genauen Grund anzuzeigen, weshalb ein Vorgang fehlgeschlagen ist.
- Es wurde ein Problem behoben, beim dem eine reparierte Kopie des defekten Installationsprogramms für macOS 10.12.6 Sierra nicht als gültig zum Anlegen von Installationsmedien akzeptiert wurde.

- Es wurde ein Problem behoben, bei dem das Bereinigen des Staging-Bereichs für Kernel-Erweiterungen mit der Meldung „ungültiges Argument“ zurückgewiesen wurde.

7.3.25 Release 7.21 (Build 210504)

- Unterstützung für macOS 11.3.1 wurde hinzugefügt. Wir raten nun dringend davon ab, macOS 11.3(.0) zu verwenden.
- Es wurde eine Fehlerumgehung für ein Problem hinzugefügt, bei dem ein Defekt in macOS 11.3 dazu führt, dass viele Apple-Installationsprogramme von der Funktion zum Erstellen von Installationsmedien als ungültig eingestuft werden.
- Es wurde ein Problem behoben, bei dem ein Gesundheitsbericht für Apple-Flash-Speicher Nullwerte für einige ältere Apple-SSD-Modelle anzeigen konnte. Das Programm stellt jetzt klarer heraus, dass der volle Bericht nur in Konfigurationen zur Verfügung steht, die die NVMe-Norm einhalten.
- Es wurde ein Problem behoben, bei dem die Anzeige Schutz auf der Karte Info nach dem Upgrade auf macOS 11.3 leer sein konnte.
- Es wurde ein Problem behoben, bei die Ergebnistabelle einer Massensicherheitsprüfung von Programmen nicht nach den Detailspalten sortiert werden konnte.

7.3.26 Release 7.2 (Build 210414)

- Unterstützung für macOS 11.3 hinzugefügt.
- Neue Funktion zur Diagnose hinzugefügt, um den Gesundheitsstatus von originalen Apple-SSDs oder Apple-Flash-Speicher anzuzeigen. Dies schließt die geschätzte verbrauchte Lebensdauer mit ein.
- Neue Funktion hinzugefügt, um ein Problem mit dem App Store-Programm zu beheben, wenn Benutzer fehlerhafte Update-Benachrichtigungen für Apps erhalten, die bereits aktualisiert wurden.
- Neue Funktion hinzugefügt, um die Liste von macOS-Installations-Apps anzuzeigen, die Apple zum direkten Download bereitstellt. Benutzer können nun einfach einen Installer auswählen und herunterladen.
- Neue Funktion hinzugefügt, um ISO-Disk-Images aus einer macOS-Installations-App zu erzeugen. Ein ISO-Plattenabbild kann verwendet werden, um OS X oder macOS in Virtuellen Maschinen zu installieren.
- Neue Funktion hinzugefügt, um die defekte Oktober–2019-Ausgabe der macOS-Installations-App für macOS 10.12.6 zu reparieren. Nach der Reparatur akzeptiert TinkerTool System die App als Quelle, um Installationsmedien für macOS Sierra anzulegen.
- Neue Funktion hinzugefügt, um Programme mit besonderen Optionen zu starten, beispielsweise mit ausgeblendeten Fenstern, ohne Eintrag für Benutzte Objekte, oder in mehreren Exemplaren.
- Neue Funktion für Macs mit Apple-Chip hinzugefügt, um die zugänglichen Teile des NVRAM zu löschen (für Intel-basierte Macs nicht notwendig).

- Neue Funktion für Benutzer von Upgrade-Lizenzen hinzugefügt: Ein Administrator, der das Programm über eine Upgrade-Registrierungsdatei aktiviert hat, kann jetzt ein „Ein-Schritt-Ticket“ anlegen, das die Information über die Upgrade-Lizenz und die Lizenz über ein vorausgesetztes früheres Produkt in eine einzelne Datei kombiniert. Diese Datei kann verwendet werden, um das Programm in einem einzelnen Schritt neu zu registrieren, ohne dass die Upgrade-Berechtigung noch einmal bewiesen werden muss, z.B. beim Umstieg auf einen neuen Computer.
- Die Time Machine-Teile des Programms wurden komplett neu geschrieben. Das Programm verwendet nun unterschiedliche Karten beim Betrieb von Time Machine im macOS 10-Modus (HFS-Ziel), bzw. macOS 11-Modus (APFS-Ziel). Die Unterstützung von netzbasierten Zielen wurde reaktiviert.
- Die Time Machine-Vergleichsfunktion ist von der Diagnose-Karte zur Time Machine-Karte gewandert.
- Das Programm verwendet detailliertere Fehlermeldungen wenn das Entfernen eines fehlerhaften Start-Jobs aus irgendeinem Grund fehlschlägt.
- Das Programm verwendet detailliertere Fehlermeldungen wenn ein Drittanbieterprogramm die Sicherheitsumgebung von TinkerTool System deaktiviert hat.
- Das Programm wurde robuster gegen Fehler in Drittanbieterprogrammen gemacht, die dazu führen können, dass die Sicherheitskomponente von TinkerTool System fälschlicherweise als Adware eingestuft wird.
- Es wurde eine Umgehung für einen Fehler in macOS Big Sur hinzugefügt, bei dem die Kommunikation mit externen Programmen fehlschlagen konnte, wenn diese in schneller Abfolge gestartet wurden.
- Es wurde ein Problem behoben, bei denen Kandidaten für Software-Komponenten, die im Deinstallationsassistenten zur Löschung anstehen, mit einer Typinformation in der falschen Landessprache angezeigt wurden.
- Es wurde ein Problem behoben, bei dem das Einstellen der Startsprache mit der Meldung „Datei existiert nicht“ auf bestimmten Systemkonfigurationen fehlgeschlagen ist.
- Die Benutzerführung für den Testmodus verwendet in der englischen Bedieneroberfläche bessere Formulierungen.

7.3.27 Release 7.12 (Build 210208)

- Neue Funktion hinzugefügt, um Benutzer-Accounts zu reparieren, die von einem Defekt in macOS 11.2 betroffen sind, der verursacht, dass alle Bedienungselemente für die Verbindung zu Netzwerk-Computern ausfallen. TinkerTool System kann aktive lokale Benutzer-Accounts überprüfen und reparieren, bei denen der Netzwerk-Ordner des Finders, Anmeldedialoge für Server, AirDrop, Handoff und Instant Hotspot fehlen.
- Neue interne Funktion hinzugefügt, die es normalen Benutzern erlaubt, Zugriffssteuerungslisten auf Dateisystemobjekte, die ihnen gehören, zu prüfen, entfernen und wiedereinzusetzen. Dies macht es möglich, dass nicht-administrative Nutzer die Möglichkeit wiedererlangen, ihre persönlichen Caches zu deaktivieren, reaktivieren oder zu löschen, falls die Cache-Ordner Apples empfohlene Standardberechtigungseinstellungen verwenden.

- TinkerTool System verlässt sich nicht mehr auf Time Machine selbst um zu prüfen, ob Time Machine auf ein netzbasiertes Sicherungsziel eingestellt ist. Da aktuelle Versionen von macOS 11 zu unzuverlässig sind, um Wartungsfunktionen von Time Machine auf Netzwerk-Servern auszuführen, schaltet TinkerTool System jetzt alle seine diesbezüglichen Time Machine-Funktionen ab, wenn eine solche Konfiguration erkannt wird.
- Die Detailanzeige für die aktuelle Einstellung des Systemintegritätsschutzes wurde für die neuesten Versionen von macOS aktualisiert.
- Die Benutzerführung zur Änderung der Auswahl zu reparierender Start-Jobs während der Reparaturvorgang bereits läuft, wurde verbessert.

7.3.28 Release 7.11 (Build 210114)

- Aufgrund von größeren Performance-Problemen und kritischen Fehlern in Apples Time Machine-Schnittstelle für Drittanbieterprogramme wurde die Unterstützung für alle Funktionen, die netzbasierte Datensicherungen verwalten, abgeschaltet. (Plattenbasierte Sicherungen sind hiervon nicht betroffen.) Es ist geplant, die Funktionen wieder zu reaktivieren, sobald diese macOS-Komponente in zukünftigen Versionen des Betriebssystems korrekt arbeitet.
- Die Kommunikation mit langsamen Bestandteilen von macOS im Hintergrund konnte manchmal fälschlich als „Hängen“ des Programms fehlinterpretiert werden. Um dies zu vermeiden, sind viele Elemente der Bedienerschnittstelle zur Steuerung von Funktionen in Time Machine, Spotlight und CUPS auf asynchrones Verhalten umgestellt worden. TinkerTool System wartet nicht mehr auf sofortige Antwort von macOS, sondern deaktiviert vorübergehend die betroffenen Steuerungselemente, bis die zugehörigen Vorgänge abgeschlossen sind.
- Die Liste der bekannten Defekte in den Startprogrammen von macOS 11.1 wurde aktualisiert.
- Diese Version behebt ein Problem beim Erstellen von Installationsmedien, bei dem Installer-Apps von macOS 11 als ungültig angezeigt werden konnten, falls eine solche App in der gleichen Anmeldesitzung des Benutzers gestartet und beendet wurde.

7.3.29 Release 7.1 (Build 201214)

- Die Funktion zum Deaktivieren der persönlichen Standard-Caches eines Benutzers wurde wiedereingesetzt.
- Neue geänderte Funktion hinzugefügt, um systemweite Caches zu bereinigen.
- Die Funktion zum Bereinigen der persönlichen Hochgeschwindigkeits-Caches eines Benutzers wurde wiedereingesetzt.
- Die Funktion zum Bereinigen der Caches des Betriebssystems wurde wiedereingesetzt.
- Die Funktion, um ungültige Schlüsselbunde von Xcode zu entfernen, kann nun zusätzlich auch Import-Einträge in Ergänzung zu der bereits vorhandenen Funktion für Export-Einträge behandeln.
- Unterstützung für die 4. Generation des System Management Controller wurde hinzugefügt, der in den neuesten Mac-Modellen zum Einsatz kommt.

- Beim Macs mit Apple-Chip werden nun mehr Detaildaten auf der Systeminformationsseite der Karte Info angezeigt.
- Es wurde ein neues Informationsdialogfenster hinzugefügt, das für Macs mit Apple-Chip interne Produktdaten auflistet.
- Die Schnellhilfefunktion wurde komplett mit aktualisierten Links auf neue Webseiten von Apple überarbeitet, die zusätzliche Informationen über Support- oder Wartungsthemen bieten.
- Die Benutzerführung wurde in den Fällen geändert, in denen Benutzer versuchen, das System-Volume zu klonen, was von macOS 11 nicht unterstützt wird.
- Die Kommunikation mit externen Programmen wurde optimiert, insbesondere bezüglich möglicher Fehlersituationen, was andernfalls zu Speicherlecks, Erschöpfen der zulässigen Menge offener Dateien oder unerwarteter Programmbeendigung führen konnte.
- Es wurde ein Problem mit der Karte „Immer an"-Mobilcomputer behoben, die fälschlicherweise auch für bestimmte Mac-Baureihen eingeblendet werden konnte, die technisch nicht in der Lage sind, diese Funktion zu unterstützen.
- Die Funktion zum Einstellen des Software-Aktualisierungsservers musste entfernt werden, da Apple den Einsatz von Servern von Drittanbietern nicht mehr erlaubt.

7.3.30 Release 7.01 (Build 201119)

- Unterstützung für zukünftige Versionen von macOS wurde hinzugefügt.
- Es wurde ein Problem bei Macs mit Apple-Chip behoben, bei dem statt der Herstellungswoche das Systeminstallationsdatum angezeigt wurde.
- Es wurde ein mögliches Layout-Problem in der Tabelle der IPv6-Adressen auf der Netzwerkinfokarte behoben, bei dem die Adressen abhängig von der Breite anderer Werte abgeschnitten werden konnten.
- Es wurde ein Problem behoben, bei dem das Programm möglicherweise auf die Webseite von Version 6 statt 7 verwiesen hat.

7.3.31 Release 7.0 (Build 201111)

- Volle Unterstützung für macOS 11.0 Big Sur hinzugefügt. macOS 11 ist die Mindestvoraussetzung zur Nutzung von TinkerTool System 7.
- Neue Funktion hinzugefügt, um ungültige Schlüsselbundeinträge von Xcode des Typs „accountsKeychainExport" entfernen zu können.
- Neue Funktion zur Anzeige von Apple-Bestellnummer und Gehäusemodellnummer für Macs mit Apple-Prozessor
- Das in Big Sur weggefallene Netzwerkdienstprogramm wird durch eine neue Karte in TinkerTool System zurückgebracht, wobei modernere Funktionen unterstützt werden:
  - Neue Funktion zur Anzeige der Netzwerkschnittstellen, -Adressen und -Statistik hinzugefügt.

  - Neue Funktion zur Anzeige der Routing-Tabelle, Protokollstatistik, Multicast-Daten und Socket-Verbindungen hinzugefügt.
  - Neue Funktion zur Ping-Diagnose für IPv4 und IPv6 hinzugefügt.
  - Neue Funktion zum Ermitteln von Adressen oder Host-Namen für IPv4 und IPv6 hinzugefügt.
  - Neue Funktion zur Wegverfolgung von Datenpaketen (traceroute) hinzugefügt.
  - Neue Funktion zur Abfrage von Whois-Datenbanken hinzugefügt.
  - Neue Funktion zur Abfrage des „Finger"-Auskunftsdienstes für Netzwerkbenutzer (RFC 1288) hinzugefügt.
  - Neue Funktion zum Scannen von offenen IPv4-Ports hinzugefügt.

- VoiceOver wird jetzt auch im Notfallwerkzeug ttsfrm voll unterstützt.
- Die Anzeige des S.M.A.R.T.-Status in ttsfrm wird jetzt auch für SSDs mit NVMe-Verbindung unterstützt.
- Bei der Testfunktion für Lüfter wird die Anzeige der Drehzahl jetzt auch auf denjenigen Mac-Modellen gerundet, bei denen Apple die Rotation mit Nachkommastellen misst.
- Hunderte kleine Änderungen und Anpassungen für macOS 11.
- Die folgenden Funktionen wurden entfernt, da sie in macOS Big Sur nicht mehr enthalten sind, keinen Sinn mehr ergeben oder durch neue macOS-Funktionen ersetzt wurden: Wiederholen der Systemoptimierung, Deaktivieren von Caches während das System läuft, Wiederaufbau des Treiber-Caches, Wiederaufbau des XPC-Caches, Größenänderung von DMG-Image-Dateien, Anzeige der Sperrliste für Kernel-Treiber, automatisches Vorschlagen von Komponenten beim Entfernen von Software, Abschalten der automatischen Aktivierung von Platten außerhalb von Benutzersitzungen, Option zur Unterstützung von Captive-Netzen, zusätzliche Anzeige von HiDPI-Auflösungen, Abschalten der Options-ROM-Sicherheitsfunktion für den Startup Manager, Ausschalten der Unterstützung von 32-Bit-Software, Steuern des Bildschirmschoners für den Anmeldeschirm.

7.3.32 Release 6.93 (Build 201007)

- Die Sicherheitsfunktion, die kritische Dateien schützt, wurde modernisiert, um Änderungen in neuen Versionen von macOS zu berücksichtigen.
- Es wurde ein Workaround und Dokumentation bezüglich Defekten in macOS hinzugefügt, die dazu führen können, dass Time Machine-Wartungsfunktionen fehlschlagen, falls die Datensicherungen netzbasiert sind.
- Es wurde eine Funktion hinzugefügt, um kaputte Versionen des Installationsprogramms für macOS Sierra zu erkennen, die nicht in der Lage sind, Installationsmedien zu erzeugen. Apple hat alle Zusicherungen offiziell zurückgezogen, dass die Installer-App für Sierra 10.12.6 hierzu in der Lage wäre und TinkerTool System wurde dementsprechend angepasst.
- Es wurde ein Problem behoben, bei dem die Karte APFS nicht gezeigt oder nicht richtig aktualisiert wird, wenn eine Platte angeschlossen wird, die Volumes mit zukünftigen APFS-Funktionen enthält, die vom laufenden Betriebssystem als ungültig angesehen werden.

- Es wurde ein Problem behoben, bei dem unter macOS Mojave Punkte in der Tabelle der Datenschutzeinstellungen für Programme möglicherweise nicht in die bevorzugte Sprache des Benutzers übersetzt wurden.

7.3.33 Release 6.92 (Build 200910)

- Diese Version fügt Unterstützung für eine SIP-geschützte Startoption hinzu, die steuert, auf welche Weise eine nicht-maskierbare Unterbrechung (NMI) ausgelöst werden kann. Die Einstellungen und deren Beschreibung bezüglich Start des macOS Remote-Kernel-Debuggers werden nun klarer dargestellt.

- Die Startoption zur Steuerung, wie Kernel-Panic-Nachrichten dargestellt werden sollen, wurde entfernt, weil die zugrundeliegende Funktion in modernen Versionen von macOS nicht mehr vorhanden ist.

- Es wurde ein Problem behoben, bei dem netzbasierte Sicherungen von Time Machine bei Verwendung von macOS Catalina nicht für die Neuzuordnung eines Volumes ausgewählt werden konnten.

- Es wurde ein Paketierproblem behoben, das dazu führen konnte, dass die Schnellhilfeseite für die Funktion ACL-ID-Finder nicht angezeigt wurde.

- Der „Build 200813-Hotfix“ ist enthalten, der kleinere Probleme mit der Bedienerschnittstelle für Produktaktivierung für Version 6.91 behoben hat. Dies betrifft die Beibehaltung der Position des Registrierungsfensters, das Doppelklicken von Registrierungsdateien und die Verarbeitung manuell eingegebener Voraussetzungsdaten für Upgrade-Lizenzen.

7.3.34 Release 6.91 (Build 200804)

- Vorläufige Unterstützung der Erstellung von Installationsmedien für und mit macOS 11 hinzugefügt.

- Unterstützung für die Erkennung neuer Funktionen in zukünftigen APFS-Implementationen hinzugefügt.

- In bestimmten Situationen erfolgt die Kommunikation mit Time Machine jetzt im Hintergrund, so dass die Bedienerschnittstelle auch mit langsamen Time Machine-Geräten schneller reagiert.

- Die Barrierefreiheit wurde durch mehr als 800 Änderungen in der Bedienerschnittstelle weiter optimiert, insbesondere für Benutzer von VoiceOver.

- Die Anleitung für das Notfallwerkzeug wurde überarbeitet, um die neuesten Versionen des macOS-Wiederherstellungsbetriebssystems zu berücksichtigen.

- Teile der Bedienerschnittstelle zur Produktaktivierung und Registrierungsmanagement wurden neu gestaltet.

7.3.35 Release 6.9 (Build 200702)

Diese Version fügt vorläufige Unterstützung für zukünftige Betriebssysteme hinzu.

7.3.36 Release 6.89 (Build 200527)

- Diese Version fügt Unterstützung für macOS 10.14.6 Build 18G5033 (Security Update 2020–003) hinzu: Da Apple absichtlich die Betriebssystemfunktion zum Ignorieren des macOS Catalina-Updates in macOS Mojave sabotiert hat, wurden die diesbezüglichen Einstellmöglichkeiten entfernt.
- Es wurde ein Hinweis hinzugefügt, der das Entfernen der Systemeinstellung zum Ignorieren des Catalina-Updates vorschlägt, nachdem ein Upgrade auf macOS Catalina installiert wurde.
- Es wurde eine Abhilfe für Layout-Probleme in einigen Statusanzeigen für physische Festplatten hinzugefügt, falls mit speziellen Drittanbieterlaufwerken gearbeitet wird, die außergewöhnlich lange Seriennummern mit mehr als 80 Stellen bereitstellen.
- Es wurde eine Abhilfe für ein Problem in der macOS-Bedienerschnittstelle zur Authentifizierung von Benutzern hinzugefügt, für Fälle, in denen das System nur die undokumentierte Fehlermeldung „ACMContextVerifyPolicyEx“ angezeigt hat.

7.3.37 Release 6.88 (Build 200427)

Diese Version behebt ein Kompatibilitätsproblem zwischen der Starteinstellung „Sondersystem einmal starten: Wiederherstellungssystem“ und bestimmten Firmware- oder Wiederherstellungs-OS-Versionen: Bei manchen Systemen konnte diese Einmaleinstellung permanent wirksam bleiben bis das Parameter-RAM zurückgesetzt wurde. Falls Sie diese Option der Starteinstellung nicht nutzen, benötigen Sie diese Aktualisierung nicht.

7.3.38 Release 6.87 (Build 200422)

- Neue Funktion hinzugefügt, um die Staging-Ablage zu bereinigen, die macOS nutzt, um Kernel-Erweiterungen zu sammeln, die auf Genehmigung oder Ablehnung des Benutzers warten. Dieses Feature ist auf dem Karteireiter zum Bereinigen des Treiber-Caches verfügbar.
- Neue Funktion hinzugefügt, um die geschützte Systemkernoption zu ändern, die die prozessorassistierte Unterstützung für Virtuelle Maschinen abschaltet. Dies kann dabei helfen, Abstürze von macOS Catalina beim Kopieren großer Datenmengen zu vermeiden.
- Das Startlimit für unbegrenzten Produkttest ohne Lizenz wurde um eins erhöht, da macOS das Programm möglicherweise neu startet, um seine Sicherheitseinstellungen zu aktualisieren. Sechs (6) Startvorgänge werden nun pro Computer erlaubt.
- Das Programm akzeptiert jetzt, dass der Benutzer ein angepasstes Symbol definiert.
- Protokolldateien für Abstürze des Betriebssystems (Kernel Panics) werden nun in besser lesbarer Form dargestellt, wenn macOS diese mit eingebetteten Berichten in JSON-Formaten versehen hat.
- Es wurde ein Problem bei den Berichten zu Time Machine-Speicherstatistiken behoben, bei denen Zeilen vertauscht sein konnten und die Zusammenfassung gefehlt hat.
- Es wurde ein Problem behoben, bei dem die Zusammenfassung des Speicherplatzgewinns möglicherweise mit falschen Zahlen angegeben wurde, nachdem Time Machine-Schnappschüsse gelöscht wurden.

- Es wurde ein Problem behoben, bei dem die Anzeige der gespeicherten Systemeinstellung für die Behandlung von Trim-Befehlen bei AHCI-Drittanbieter-SSDs mit bestimmten Systemversionen falsch sein konnte, während die Darstellung der Live-Vorgaben für jedes Laufwerk richtig war.

7.3.39 Release 6.86 (Build 200323)

- Unterstützung für macOS Catalina 10.15.4 und höher wurde hinzugefügt. Beachten Sie, dass frühere Fassungen von TinkerTool System nicht mit dieser Betriebssystemversion kompatibel sind.

- Es wurde ein getrenntes, beliebig vergrößerbares APFS-Überblicksfenster hinzugefügt. Dies ist hilfreich, wenn komplexe APFS-Vorgänge durchgeführt werden, die mehrere Partitionen oder Platten betreffen.

- Der Funktion zum Speicherplatzüberblick wurden Prozentwerte hinzugefügt.

- Es wurde neue Fehlerumgehungen hinzugefügt, die weiterbestehende Defekte in macOS betreffen, bei denen das System möglicherweise Einstellungs- und Resume-Daten verliert wenn sich der Benutzer zu schnell abmeldet. Die Dialoge, die anzeigen, dass sich der Benutzer zum Fortsetzen eines anstehenden Wartungsvorgangs abmelden muss, wurden neu gestaltet.

7.3.40 Release 6.85 (Build 200218)

- Neue Funktion hinzugefügt, um den klassischen Startton auf ausgewählten Macintosh-Modellen, die nach Sommer 2016 veröffentlicht wurden, einzuschalten.

- Neue Startoption hinzugefügt, um spezielle Wartungssysteme für den nächsten Neustart auszuwählen. Das Wiederherstellungssystem, Internet-Wiederherstellung, Apple Diagnose und Apple Diagnose per Internet sind verfügbar.

- Neue Option hinzugefügt, um verfügbare „Signpost“-Daten für Software-Entwickler hinzuzufügen wenn Protokolldaten aus dem Betriebssystem abgerufen werden.

- Die Systemstart-Karte wurde neu designt, um weniger Platz auf kleinen Bildschirmen zu benötigen.

- Die Info-Karte wurde neu designt, um weniger Platz auf kleinen Bildschirmen zu benötigen.

- Interne Diagnosefunktionen wurden optimiert.

- Die Kommunikation mit der privilegierten Komponente unterstützt neue Funktionen, um sicher zu stellen, dass Daten auch in kritischen Situationen in der korrekten Reihenfolge verarbeitet werden, z.B. bei hoher Systemlast oder stark parallelisierten Vorgängen.

- Es wurde ein Problem behoben, bei dem einige Zeilen von Protokollberichten teilweise beschädigt oder in falscher Reihenfolge angezeigt werden konnten.

7.3.41 Release 6.84 (Build 200117)

- Die Bedienerschnittstelle für die Darstellung der Hierarchie von APFS-Objekten wurde verbessert.
- Die Datenschutzwarnung, die angezeigt wird, wenn der Benutzer noch nicht sein Einverständnis für Festplattenvollzugriff des Programms erteilt hat, wird nun stärker hervorgehoben.
- Fehlermeldungen und Fehlerbehandlung wurden optimiert, um besser zwischen den Ursachen für Zugriffsprobleme unterscheiden zu können, die vom Systemintegritätsschutz, Datenschutzgenehmigung, Benutzerrechten oder anderen Gründen ausgelöst werden.
- Diese Version fügt eine Umgehung einer Mehrdeutigkeit hinzu, die eine fehlerhafte Anzeige des Produktionsdatums von Macintosh-Baureihen verursachen konnte, bei denen es eine aktuelle Betriebssystemunterstützung von mehr als 10 Jahren gibt.
- Diese Version behebt ein Problem, bei dem macOS sich geweigert hat, eine APFS-Volume-Gruppe zu kopieren, wenn diese Teil eines Containers mit mehreren Volume-Gruppen war.
- Es wurde ein Problem behoben, bei dem das Zurücksetzen von Datenschutzeinstellungen bei bestimmten Versionen von macOS Catalina nicht für alle Kategorien durchführbar war.
- Das Programm fügt nun eine besondere Benutzerführung hinzu, wenn eine Datenschutzkategorie zurückgesetzt wird, die Einfluss auf das Programm selbst hat.

7.3.42 Release 6.83 (Build 191211)

- Neue Funktion hinzugefügt, um einen Überblick über alle Details der aktuellen APFS-Konfiguration zu bekommen, wobei das Verhältnis zwischen Containern, physischen Datenträgern, Volume-Gruppen und Volumes dargestellt wird.
- Neue Funktion hinzugefügt, um die vollständige Liste aller APFS-Schnappschüsse auf einem Volume anzuzeigen.
- Neue Funktion hinzugefügt, um einige oder alle APFS-Schnappschüsse von einem Volume zu entfernen.
- Neue Funktion hinzugefügt, um APFS-Container, -Volume-Gruppen, -Volumes oder -Schnappschüsse durch schnelle Replikation zu kopieren. (Nur verfügbar mit macOS 10.15 Catalina oder höher.)
- Neue Funktion hinzugefügt, um Time Maschine-Schnappschüsse sicher aus einer aktiven Datensicherung zu entfernen.
- Neue Funktion hinzugefügt, um Time Machine-Schnappschüsse, Datensicherungssätze oder alle Time Machine-Daten von lokalen Festplatten zu entfernen.
- Neue Bedienerschnittstelle hinzugefügt, um ausstehende Datenschutzgenehmigungen einzublenden. Wenn nötig wird auf eine fehlende Genehmigung direkt sichtbar in der Symbolleiste des Steuerungsfensters hingewiesen. Das vermeidet, dass das Programm einen möglicherweise fehlschlagenden Vorgang erst versuchen muss, bevor es dem Benutzer einen möglichen Konflikt mit Sicherheitsrichtlinien anzeigen kann.

- Neue Funktion hinzugefügt, um einen optionalen Textbericht zu erstellen, wenn verwaiste Objekte auf einem Volume gefunden wurden.
- Die Funktionen, um Volumes von der automatischen Aktivierung oder von der Programmausführung auszuschließen, unterstützen nun auch unsichtbare, aber aktivierte Volumes nicht laufender Catalina-Installationen. Dies ist für Nutzer hilfreich, die mehrere Exemplare von macOS Catalina installiert haben. (Nur notwendig für macOS 10.15 oder höher.)
- Die Einstellungskarte Info unterstützt nun das Abrufen von Details über den Apple T2-Prozessor in Ergänzung zum originalen iBridge-System. Die Bedienerschnittstelle wurde entsprechend überarbeitet.
- Das Ausdrucken der Anleitung zum Aufrufen des Notfallwerkzeugs im Wiederherstellungsbetrieb passt nun automatisch die Größe der Ausgabe an die Papiergröße des Druckers an, um sicherzustellen, dass die Anleitung gut lesbar und nicht abgeschnitten ist.
- Die Bedienerführung zum Ändern von Dateiberechtigungen wurde für diejenigen Fälle neu entworfen, in denen das Betriebssystem Berechtigungen nicht voll unterstützen kann.
- Das Programm fügt nun Warnungen über mögliche APFS-Bugs hinzu, die das Behandeln automatischer Vererbung von ACL-Rechten betreffen.

7.3.43 Release 6.82 (Build 191114)

- Die Prüfung auf langsamen Systemstart aufgrund gelöschter NVRAM-Einstellungen wurde geändert um Fehlalarme auf bestimmten Mac Pro-Modellen zu vermeiden.
- Die Prüfung auf korrekte Kommunikation mit der Sicherheitskomponente wurde geändert um Fehlalarme zu vermeiden, wenn das Programm in extremen Überlastsituationen gestartet wurde.
- Es wurde eine Abhilfe für ein Problem mit macOS 10.15.1 hinzugefügt, das dazu führen konnte, dass die Warnung über eine fehlende benutzerbezogene Zustimmung zum Festplattenvollzugriff unter bestimmten Bedingungen nicht eingeblendet wurde.
- Es wurde eine Abhilfe für ein Problem hinzugefügt, das dazu führen konnte, dass Volumes im Format HFS+ für bestimmte Funktionen der Einstellungskarte System nicht angeboten wurden.
- Die Bedeutung der „Dark Wake“-Startoption wird in der Bedienerschnittstelle und im Referenzhandbuch klargestellt.

7.3.44 Release 6.81 (Build 191030)

- Unterstützung für macOS 10.15.1 hinzugefügt.
- Neue Funktion hinzugefügt, um den Bericht über Start-Jobs in eine RTF-Textdatei zu speichern.
- Neue Funktion hinzugefügt, um ausgewählte macOS-Installations-Apps, die von Apple bereitgestellt werden, ohne Verwendung des App Store herunterzuladen (nur macOS Catalina).

- Neue Funktion hinzugefügt, um Update-Benachrichtigungen bezüglich macOS Catalina zu unterdrücken und die zugehörige Erinnerungsmarkierung im Dock zu entfernen (nur macOS Mojave).
- Neue Funktion hinzugefügt, um die Benutzer-Account-Sicherheitsvorgaben für Ferne Apple-Events umzustellen (nur macOS Catalina).
- Die Funktion, um den Treiber-Cache (Kernel Extensions) zu löschen und aufzufrischen, wurde für macOS Catalina wieder freigeschaltet.
- Die Funktion, um macOS-Installationsmedien anzulegen, verwendet aktualisiertes Wissen und überarbeitete Sicherheitsvorgaben bezüglich der Größenanforderungen an Ziel-Volumes.
- Diese Version erkennt zusätzliche Situationen in der Betriebsumgebung, die dazu führen können, dass die Kommunikation mit Systemdiensten fehlschlägt. Der Benutzer wird über solche Probleme automatisch informiert.
- Die Funktion, um nach Softwarekomponenten bestimmten Typs als Vorbereitung für den Deinstallationsassistenten zu suchen, ist für macOS Catalina nicht mehr verfügbar, da sie in modernen Systemversionen nicht mehr sinnvoll ist.

7.3.45 Release 6.8 (Build 191009)

- Diese Version fügt volle Unterstützung für macOS 10.15 Catalina hinzu.
- Neue Funktion hinzugefügt, um den Beglaubigungszustand („Notarisierung“) für Programme oder Disk Images anzuzeigen (nur macOS Catalina).
- Die Referenzhandbücher wurden mit Informationen aktualisiert, die während des bestehenden Nachrichtenembargos für macOS Catalina nicht veröffentlicht werden durften.
- Der Testbetrieb (Evaluationsmodus im Angebot „Erst testen, dann kaufen“) ist nun für macOS Catalina freigeschaltet.
- Es wurde ein Problem behoben, bei dem die Liste der Start-Jobs in der Kategorie Benutzerdienst-Anmeldeobjekt ungenau sein konnte, wobei Einträge aufgeführt wurden, die bereits deaktiviert waren.
- Es wurde ein Problem behoben, bei dem der Datenteil des Catalina-System-Volumes für bestimmte Wartungsaufgaben nicht angeboten wurde.

7.3.46 Release 6.7 (Build 190916)

- Neue Funktion hinzugefügt um Disk Images (DMG-Dateien) in der Größe zu ändern, wobei die Fehler des Festplattendienstprogramms vermieden werden.
- Weitere Unterstützung für zukünftige Versionen von macOS wurde hinzugefügt.
- Die selbständige Version von TinkerTool System (tts im Einbenutzerbetrieb) wurde komplett neu geschrieben. Das neue „TinkerTool System für macOS-Wiederherstellung“ (ttsfrm) ersetzt das frühere Notfallwerkzeug. Dies führt zu folgenden Vorteilen:
  - Kompatibilität mit aktuellen und zukünftigen Versionen von macOS wird verbessert, da der Einbenutzerbetrieb (Single User Mode) von Apple nicht mehr offiziell unterstützt wird.

  - Bei Macs mit T2-Sicherheitschip ist es nicht mehr notwendig, die Sicherheitseinstellungen zu ändern.
  - Probleme mit der Tastaturentprellung auf bestimmten Mac-Modellen werden vermieden.
  - Apples Einbenutzer-Terminal wird vermieden, so dass die Lesbarkeit auf Systemen mit Retina-Bildschirm wieder voll gewährleistet ist.
  - Das Notfallwerkzeug kann jetzt den vollen Zeichenvorrat und eine grafische Oberfläche nutzen.
  - Getrennte, proaktive Installationsschritte für das Notfallwerkzeug sind nicht mehr notwendig.

- Eine grafische Bedieneroberfläche zum Aus- oder Einschalten des Systemintegritätsschutzes wurde dem Notfallwerkzeug hinzugefügt. Die folgenden Funktionen sind im Wiederherstellungsbetrieb von macOS nicht mehr sinnvoll und wurden entfernt: Dateisystemprüfung für das System-Volume, Löschen von Input-Managern, Neuaufbau von XPC-Caches, Selbstentfernung.
- Die Funktion zum Erstellen von macOS-Installationsmedien akzeptiert nun Ziel-Volumes mit etwas weniger als 8 GB Speicherplatz. Dies berücksichtigt, dass Apples Installationsprogramm sich an Volumes (nicht Platten) orientiert, deren formatierte Kapazität spürbar geringer sein kann, als die des physischen Speichermediums.

7.3.47 Release 6.6 (Build 190812)

- Viele interne Änderungen zur Unterstützung zukünftiger Betriebssystemversionen.
- Neue Funktion „ID-Finder“ für Benutzer- und Gruppen-Accounts hinzugefügt. Nach der Eingabe von entweder Account-Name, vollem Namen, POSIX-Bezeichner oder UUID findet das Programm die jeweils fehlenden drei anderen Punkte.
- Neuen Protokolltyp hinzugefügt, um das macOS-Protokoll für Plattenschreibvorgänge abzurufen.
- Neuen Protokolltyp hinzugefügt, um das macOS-Protokoll für Datenübertragungen der Differential Privacy-Funktion abzurufen.
- Neuen Protokolltyp hinzugefügt, um das macOS-Protokoll für iCloud-Dienste abzurufen.
- Neuen Protokolltyp hinzugefügt, um das macOS-Protokoll für Vorfälle mit dem Basisbandprozessor abzurufen.
- Neuen Protokolltyp hinzugefügt, um das macOS-Protokoll für Telefonieüberwachung abzurufen.
- Neuen Protokolltyp hinzugefügt, um das macOS-Protokoll für Vertrauensprüfungen abzurufen.
- Neuen Protokolltyp hinzugefügt, um das macOS-Protokoll für iPhone-Softwareaktualisierungen abzurufen.
- Neuen Protokolltyp hinzugefügt, um das macOS-Protokoll für iPad-Softwareaktualisierungen abzurufen.
- Neuen Protokolltyp hinzugefügt, um das macOS-Protokoll für proaktive Ereignisse abzurufen.
- Die Bedienerschnittstelle für Lizenzregistrierung wurde überarbeitet.

7.3.48 Release 6.51 (Build 190625)

- Dieses Update ist notwendig, um die Kompatibilität mit neuen Versionen von TinkerTool zu erhalten (Version 7.4 oder höher).
- Weitere Unterstützung für zukünftige Versionen von macOS wurde hinzugefügt.
- Bessere Bedienerführung der Funktion, ungeeignete Update-Benachrichtigungen zu entfernen, für Benutzer, die einen angepassten Update-Server eingestellt haben.
- Es wurde ein Problem behoben, bei dem das Programm hängen konnte, wenn es begonnen hat, Live-Ausgaben externer Dienstprogramme anzuzeigen, die ohne privilegierte Rechte gestartet wurden.

7.3.49 Release 6.5 (Build 190611)

- Es wurde größere Änderungen der Architektur durchgeführt, die es möglich machen, lange laufende Vorgänge abzubrechen.
- Neue Betriebssystemeinstellung für den vollen Schutz gegen „ZombieLoad“-Angriffe hinzugefügt. Diese Einstellung kann nur geändert werden während der Systemintegritätsschutz abgeschaltet ist.
- Betriebssystemeinstellung hinzugefügt um die Unterstützung des Assistenten für Captive Networks (automatische Konfiguration des Zugangs zu „Hotspots“) ausschalten zu können.
- Neue Funktion hinzugefügt, um eine bestimmte Beschädigung des Papierkorbs automatisch reparieren zu lassen, die von Drittanbieterprogrammen ausgelöst wird. Diese Funktion hat keine permanente Bedienerschnittstelle, sondern wird bei Bedarf während des Programmstarts aktiviert falls nötig.
- Die Systemeinstellung zum Optimieren der Betriebsparameter für die Nutzung als Server-Computer kann nun auch aktiviert werden, wenn macOS Server nicht installiert ist.
- Es wurde ein seltenes Problem behoben, bei dem der Autostart-Zustand von Drittanbieterdiensten nicht korrekt ermittelt werden konnten, falls das betroffene ausführbare Programm ungewöhnliche Berechtigungseinstellungen hatte.
- Es wurde ein Problem behoben, bei dem neue Systemdienste, die kürzlich zu macOS Mojave hinzugefügt wurden, nicht als von Apple bereitgestellte Komponenten angezeigt wurden.
- Vorläufige Unterstützung für zukünftige Versionen von macOS wurde hinzugefügt.

7.3.50 Release 6.4 (Build 190508)

- Neue Funktion hinzugefügt, um „Im-Finder-zeigen“-Knöpfe bei Objekten vorzusehen, die in der Vorschauliste gezeigt werden, wenn Dateien als Teil einer Bereinigungsfunktion gelöscht werden.
- Neue Funktion hinzugefügt, um eine Dateisystemhierarchie gegen ein vom Benutzer angegebenes Limit für die Länge absoluter oder relativer Pfade zu prüfen.

- Neue Warnfunktion zur ACL-Karte hinzugefügt, die den Benutzer darauf aufmerksam macht, falls ein ausgewähltes Dateisystem keine ACL-Berechtigungen unterstützt oder nur virtuelle Berechtigungseinstellungen erlaubt. Ein neues Informationsfenster bietet Unterstützung für unerfahrene Benutzer.
- Beim Propagieren von Berechtigungen auf eine große Orderhierarchie wurde für bestimmte Anwendungsfälle der temporäre Speicherplatzverbrauch stark reduziert.
- Es wurde ein Problem behoben, bei dem bestimmte Regionaleinstellungen des Benutzer-Accounts dazu führen konnten, dass eine Anforderung zur automatischen Freigabe von APFS-Time Machine-Schnappschüssen über eine angegebene Größe keine bemerkbare Wirkung hatten.

7.3.51 Release 6.3 (Build 190327)

- Neue Funktion hinzugefügt um alle lokalen Time Machine-APFS-Schnappschüsse sofort von einem ausgewählten Volume zu entfernen.
- Neue Einstellung hinzugefügt, um zu steuern, ob FileVault den Entschlüsselungsschlüssel für die Systemplatte aus dem Speicher entfernen soll, sobald das System in den Standby-Modus wechselt.
- Neue Funktion hinzugefügt, um beim Abspeichern einer geänderten Automount-Konfiguration alle Volumes auszuwerfen, die dazu eingestellt wurden, nicht mehr automatisch von macOS aktiviert zu werden.
- Neue Funktion hinzugefügt, um auf Wunsch das Programm sich selbst in den Programme-Ordner des Systems kopieren zu lassen, wenn es von seiner virtuellen Vertriebsplatte gestartet wurde.
- Die internen Diagnosefunktionen wurden komplett neu geschrieben, um auch in Fällen betriebsbereit zu bleiben, in denen die Protokollfunktionen des Betriebssystems nicht genutzt werden können.
- Das Programm wurde gegen unseriöse „Cleaner“-Software robust gemacht, die die Startkonfiguration des Betriebssystems beschädigt.
- Bessere Fehlermeldungen in Fällen, in denen Benutzer das Programm nicht registrieren können weil sie versehentlich eine falsche Lizenzdatei durch Ziehen installieren.

7.3.52 Release 6.2 (Build 190212)

- Neue Diagnosefunktion hinzugefügt um die Anmeldezeitstatistik abzurufen, die vom Betriebssystem geführt wird. Die Gesamtanmeldezeit pro Benutzer oder die Nutzungszeit pro Tag kann geprüft werden.
- Es wurde eine Fehlerumgehung für einen Defekt in macOS Mojave hinzugefügt, der das Betriebssystem für 7 Minuten stoppen kann, falls ein Programm das Betriebssystem nach der vollständigen Liste von Gruppen-Accounts in einer Konfiguration mit einem Netzwerkverzeichnisdienst fragt. Alle Benutzer- und Gruppendialogfenster zeigen nur noch gecachete Accounts. Die vollständige Liste der Accounts kann bei Bedarf über einen extra Knopf in den Dialogfenstern abgerufen werden.
- Die Benutzerführung für die Auswahl von Ziel-Volumes wurde beim Anlegen von macOS-Installationsmedien verbessert.

- Es wurde ein seltenes Problem behoben, bei dem das Programm die Nachricht „Systemaufruf wurde unterbrochen“ statt der richtigen Fehlermeldung angezeigt hat, wenn versucht wurde, bestimmte Dateien zu löschen, die durch den Systemintegritätsschutz abgeschirmt sind.

7.3.53 Release 6.1 (Build 190121)

- Neue Option für die Funktion zum Übertragen von Berechtigungseinstellungen hinzugefügt, die die Vererbung von Zugriffssteuerungslisten (ACLs) präzise simulieren kann, statt diese bedingungslos zu kopieren. Dies entspricht dem Verhalten alter Versionen von macOS Server. Die Option, das Einschalten der Vererbungsmarkierung zu erzwingen, wurde entfernt.
- Neue Option für die Funktion zum Übertragen von Berechtigungseinstellungen hinzugefügt, um alle geschützten Dateien währen des Vorgangs zu ignorieren. Dies entspricht dem Verhalten alter Versionen von macOS Server.
- Neue Funktion zur Speicherplatzübersicht für Volumes hinzugefügt, die alle Systemdienste auflistet, die zurzeit für die Freigabe löschbaren Speichers angemeldet sind.
- Neue Funktion hinzugefügt, um einen Textbericht aus den Ergebnissen einer Massenintegritätsprüfung von Programmen zu erstellen. Der Bericht kann gedruckt oder in eine RTF-Datei exportiert werden.
- Neue Funktion zur Überprüfung von absoluten Pfadlängen tief verschachtelter Ordner hinzugefügt, die nicht nur existierende Objekte testet, sondern die zusätzlich potenzielle Pfade überprüft, die entstehen würden, wenn die getesteten Dateien auf gerade angeschlossene Volumes kopiert würden.
- Neue Benutzereinstellung hinzugefügt, um das Programm dazu zu zwingen, Apples Identitätsauswahldialog statt TinkerTool Systems eigener Fenster zur Auswahl von Benutzer- und Gruppen-Accounts zu verwenden. Dies ist weniger komfortabler und bietet keine systemeigenen Accounts an, kann aber genutzt werden, um einen Fehler im Verzeichnisdiensteklient von macOS Mojave zu umgehen, der das System für mehrere Minuten blockieren kann, falls ein oder mehr externe Verzeichnisdienst-Server konfiguriert sind und eine Bedienerschnittstelle zur Auswahl eines Accounts geöffnet wird.
- Sowohl das Hauptprogramm als auch das selbständige Notfallwerkzeug können nun die neue Option des Systemintegritätsschutzes zum Übergehen der Sicherheitsstrategie ausführbarer Programme anzeigen, falls diese in einer angepassten Konfiguration aktiv ist.
- Die Tastatursteuerung des selbständigen Notfallwerkzeugs wurde noch einmal optimiert.
- Das Volume für Auslagerungsspeicher (VM) wird in bestimmten Funktionen nicht mehr als mögliches Ziel für Operationen angeboten, um Verwirrung zu vermeiden.
- Ein Layout-Problem in der Pfadpräsentation für den obersten Ordner im Ergebnisfenster für überlange Pfade wurde behoben. Dies vermeidet, dass der Dialog breiter als der Bildschirm werden kann.
- Defekte symbolische Links führen nicht mehr zu einem Abbrechen eines Übertragungsvorgangs auf der ACL-Karte, falls die Option zum Übertragen von Zugriffssteuerungslisten eingeschaltet ist.

- Unterstützungscode für alte Betriebssysteme wurde aus der Karte „Fehler“ entfernt.

7.3.54 Release 6.02 (Build 181122)

- Neue Funktion zur Karte Info hinzugefügt, um anzuzeigen, ob ein Mac die Apple-iBridge-Technik verwendet, was Apple-T2-Prozessoren mit einschließt. Ein Detailfenster zeigt zusätzliche Daten über dessen Konfiguration.
- Kleine Änderungen in der nicht-englischsprachigen Bedieneroberfläche in Fällen, bei denen Apple die Übersetzung bestimmter Begriffe ab macOS 10.14.1 verändert hat.
- Die Karte für das Notfallwerkzeug wurde neu gestaltet und zeigt einen Hinweis an, falls ein Mac eine extrem kleine Schriftart im Einbenutzermodus verwendet.
- Links zu Apple-Dokumentation in Verbindung mit der Schnellhilfefunktion wurden aktualisiert, bzw. entfernt, falls Apple bestimmte Informationen nicht mehr veröffentlicht.
- Es wurde eine Fehlerumgehung für die Tastatursteuerung des Einbenutzermodus hinzugefügt, die das Selbständige Hilfsprogramm betreffen konnte. Abhängig von Tastaturmodell und Betriebssystemversion konnte es in einigen Fällen passieren, dass ein einzelner Tastendruck als mehrfache Tastenereignisse fehlinterpretiert werden konnten.
- Die irreführende Beschriftung der Funktion zur Abschaltung von Dark Wake in macOS wurde klarer gestaltet.
- Es wurde ein Kompatibilitätsproblem mit der automatischen Neustartfunktion behoben, das auftreten konnte, wenn das Programm umbenannt wurde.
- Interne technische Aktualisierung für Änderungen in der Netzwerkinfrastruktur, die die Funktion zum Testbetrieb (Evaluation) betrifft.
- Das Programm zeigt nun konkretere Fehlermeldungen an, wenn die Lizenzierung aufgrund einer falsch konfigurierten Netzwerk-Firewall fehlschlägt.
- Das Distributionspaket verwendet nun die neuesten Gatekeeper-Sicherheitsfunktionen.

7.3.55 Release 6.01 (Build 181002)

Dies ist ein Wartungs-Update, das kleinere Probleme behebt.

- Unterstützung für zukünftige Versionen von macOS Mojave wurde hinzugefügt.
- Es wurde eine Fehlerumgehung für ein Deklarationsproblem in den neuesten Versionen des macOS Mojave-Installationsprogramms hinzugefügt, das dazu führen konnte, dass der Installer nicht als gültig für das Erzeugen von Installationsmedien anerkannt wurde.
- Einige Änderungen und Optimierungen in der Benutzerführung beim Arbeiten mit Start-Jobs, Einstellungen des Anmeldeschirms und Lizenzregistrierung.
- Es wurde ein Problem behoben, bei dem ein privater Software-Update-Server nicht genutzt werden konnte, wenn macOS die Verwendung von HTTPS mit TLS und erweiterter Validierung erzwungen hat.

- Es wurde ein Problem behoben, bei dem das Programm auf Systemen, die von OS X 10.10 Yosemite aktualisiert wurden, nicht erkennen konnte, ob voller Festplattenzugriff bereits genehmigt war.
- Es wurde ein Problem behoben, bei dem die Bedienerschnittstelle für bestimmte Time-Machine-Funktionen möglicherweise nicht aktiv wurde, wenn die Datensicherung auf einem Netzwerk-Server gespeichert war.

7.3.56 Release 6.0 (Build 180918)

- Volle Unterstützung für macOS 10.14 Mojave hinzugefügt.
- Neuen Protokolltyp für langsames Programmantwortverhalten zur Funktion hinzugefügt, mit klassischen Systemprotokollen zu arbeiten.
- Neuen Protokolltyp für langsames Herunterfahren des Computers zur Funktion hinzugefügt, mit klassischen Systemprotokollen zu arbeiten.
- Andere neue Protokolltypen wurden in die entsprechende Kategorie im Protokollübersichtsmenü hinzugefügt.
- Hunderte andere kleine Änderungen und Anpassungen für macOS Mojave.
- Die folgenden Funktionen wurden entfernt, da sie in macOS Mojave nicht mehr enthalten sind, keinen Sinn mehr ergeben oder durch neue macOS-Funktionen ersetzt wurden: Entfernen von Sprachunterstützungspaketen, Überprüfen von Anmeldeobjekten, erzwungenes Leeren des Papierkorbs, Reparieren von Safari-Schriftproblemen, Reparieren von App Store-Lizenzen, Einschalten der Unterstützung externer Accounts im Anmeldeschirm, Abschalten der Unterstützung von Konsolanmeldung im Textmodus, vorübergehendes Entfernen von Auslagerungsdateien.
- Die folgenden Funktionen sind an neue Orte umgezogen: Entfernen Benutzter Objekte (Benutzer-Karte), Zurücksetzen der Datenschutzeinstellungen (Programme-Karte).

TinkerTool System 6 ist der Beginn einer neuen Produktlinie. Der obenstehende Abschnitt listet Änderungen in Bezug auf TinkerTool System 5, Version 5.96 auf. Für weitere Informationen über die Versionshistorie von TinkerTool System 5 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 6 umgestiegen sind

Falls Sie ein Upgrade von macOS 10.14 Mojave oder macOS 10.15 Catalina auf macOS 11 Big Sur oder höher vorgenommen haben und nach fehlenden Funktionen in TinkerTool System 7 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.
Alle Punkte, die hier nicht aufgeführt sind, haben ihren Platz und Namen beibehalten.

A.2 Sollte ich regelmäßige Wartungsarbeiten durchführen?

Die kurze Antwortet 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.

Tabelle A.1: Vergleich der Orte der verschiedenen Funktionen

Früherer Platz	Aktueller Status
Wartung > Systemoptimierung	*entfernt*, da in macOS 11 überflüssig
Caches > Treiber-Cache > Start-Cache bereinigen	*entfernt*, da in macOS 11 überflüssig
Caches > Treiber-Cache > Staging-Bereich bereinigen	Caches > Treiber-Staging
Caches > XPC-Cache	*entfernt*, da in macOS 11 überflüssig
Fehler > Image-Dateien	*entfernt*, da Fehler von Apple in macOS 11 behoben
Diagnose > Time Machine	Time Machine [X] > Vergleich
Info > Sperrliste Treiber	*entfernt*, da in macOS 11 überflüssig
Programme > Deinstallationsassistent > Suche nach Komponenten	*in modernen macOS-Versionen nicht mehr sinnvoll*
System > Laufwerke > Automatisches Aktivieren externer Laufwerke	*entfernt*, da seit macOS 10.15 Standard
System > Netz > Unterstützung für Captive-Netze	Systemeinstellungen > Netzwerk > WLAN > Zum Beitreten zu einem persönlichen Hotspot fragen
System > Bildschirm	*entfernt*, da ab macOS 10.15 überflüssig
System > Versch. > Auf privaten Softwareaktualisierungsserver zugreifen	*entfernt*, da von Apple nicht mehr erlaubt
Systemstart > Optionen > Klassischen Startton einschalten	Systemeinstellungen > Ton > Beim Starten Ton abspielen
Systemstart > Optionen > Startup Manager-Sicherheit	*entfernt*, da bei modernen Macs überflüssig
Systemstart > Geschützte Optionen > Unterstützung für gesamte 32-Bit-Software abschalten	*entfernt*, da ab macOS 10.15 Standard
Anmeldung > Bildschirmschoner	*entfernt*, da von Apple ab macOS 10.15 weggelassen
Benutzer > Sprache	*entfernt*, da in macOS 11 überflüssig

> 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 Betriebssystem 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 Karteireiter **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 27).

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 Karteireiter **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 167).

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 Karteireiter **Reparatur**.
3. Drücken Sie auf den Knopf **Jetzt reparieren** in der Rubrik **„Help Viewer“ reparieren**.

Weitere Informationen: Die Einstellungskarte Benutzer (Abschnitt 5 auf Seite 247).

A.6 Freischalten des Programms

Wenn Sie TinkerTool System 6 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 **Software-Produktregistrierung und Aktivierung** erscheint.
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. Bestätigen Sie Ihr Einverständnis, dass das Programm eine Internet-Verbindung herstellen darf.
5. 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 275)

Index

/Local/Default, 25
/tmp, 261
5k, 116

A
Abhilfe, 282
Ablaufverfolgung, 123
Abmeldung, 29
abschalten, 211
Abschottung, 73
absoluter Pfad, 137
Absturz, 73
Absturzbericht, 118, 146
Access Control Entry, 170
Access Control List, 167, 170
Account, 240
Account-Name, 186
accountsKeychain, 68
ACE, 170
ACL, 167, 170
ACL entfernen, 179
Active Directory, 25
Adams, Carlisle, 218
Ad-Hoc-Signatur, 167
Administrator, 3, 4, 122, 270
Adobe® Flash®, 114
adressierbarer Speicher, 109
Advanced Host Controller Interface, 83
Änderungsrate, 41
AFP, 173
Agent, 233
AHCI, 83
AirDrop, 69
aktivieren, 279
Aktivitätsbezeichner, 124
Aktualisierung, 16, 17, 280
Alias, 129, 152
Amazon, 244
Analyse, 143
analysieren, 135
Anbieterkennung, 109
Anbieterkennzeichnung, 111
Andere, 168
Andere (Benutzer), 239
anhängen, 171
anlegen, 171
Anleitung drucken, 95
Anmeldebildschirm, 267
Anmeldeobjekt, 159, 234
Anmeldeverfahren, 218
Anmeldezeit, 90
Antwortverhalten, 106
Anwendungs-Sandbox, 163
Apfelmenü, 240, 251
APFS, 36, 173, 196, 203
APFS-Container, 196, 203
APFS-Rolle, 204
APFS-Schnappschuss, 45, 60
APFS-Volume, 203
APFS-Volumegruppe, 203
App Nap, 116
App Store, 64, 65, 114, 116, 215
Apple Diagnose, 230
Apple File System , 36, 203
Apple Filing Protocol, 173
Apple GPU-Kern, 109
Apple T2, 112
Apple-Chip, 94, 109, 201, 229
Apple-Chip-Problem, 120
AppleDouble, 77, 144
Apple-Menü, 240
Apple-Modellidentifikation, 109
AppleShare, 173
App-Regeln, 165
App-Software, 165
App-Updates, 64
Arbeitsumfang, 75
Archiv, 146
Archivierungsprogramm, 221
Archivordner, 251
ASCII, 133
ATA8-ACS2, 82
Attribut, 132, 144, 170
aufheben, 132
auflösen, 152
Auftragsverarbeitungsvertrag, 244

Aufzeichnungsformat, 80
Aufzeichnungsschicht, 80
Ausfall, 272
ausführbare Datei, 168
ausführen, 168, 213
Auslagerung, 76
Auslagerungsspeicher, 73, 76
ausmustern, 250
ausschalten, 240
Auswahlknopf, 12
auswerfen, 80, 155
auswerten, 74
Automation, 20
automatische Aktivierung, 31
automatische Anmeldung, 270
Automatische Benachrichtigung, 16
automatische Softwareaktualisierung, 3
automatische Sprachwahl, 255
Autopilot, 309
Autoradio, 153
Autorisierung aufheben, 6
Azure Active Directory, 25

B
Balken, 8
Baseband-Verarbeitung, 121
Bedrohung, 114
Befugnis, 163
Beglaubigung, 166
bekannter Fehler, 282
Benutzer ausblenden, 240
Benutzer-Account, 149, 257, 262
Benutzerdienst-Anmeldeobjekt, 234
Benutzereinstellung, 247
Benutzerfoto, 257
Benutzergruppe, 257
Benutzerliste, 238
Benutzername, 257
Benutzerordner, 184
Benutzerordner, gemeinsamer, 27
Benutzersitzung, 225, 238
benutztes Objekt, 251
Berechtigung, 167, 223
bereinigen, 143
Bereinigung, 197
Bericht, 12, 14, 118, 143, 159
Bestätigen, 14
Bestätigung, 143
bestellen, 277
Bestellnummer, 109
Beta-Programm, 65
Betriebssystem, 3
Betriebssystemversion, 113
bevorzugte Sprache, 241
Bildpunkt, 92
Bildschirm, 92
Bildschirmfreigabe, 226
Block, 74
Blu-Ray Disc, 80
böswillige Software, 114
Bookmark, 130
Bridge-Chip, 273
BridgeOS, 88, 112, 201
Broadcom, 202
Buchführung, 90
Build-Nummer, 113
Byte, 133

C
CA, 166
Cache, 23, 27, 262, 265
Cache-Bereinigung, 28
Cache-Größe, 109
Cache-Speicher, 76
CBC128, 218
CD, 80
Certificate Authority, 166
CIFS, 173
Cipher Block Chain, 218
Codesigning, 163, 193
Common Unix Printing System, 228
Computer, 109
Computereinstellung, 251
computerweit, 157
CPU, 232
Creator Code, 132
CSR, 17
csrutil, 19
CUPS, 228
Customer System Restriction, 17

D
Daemon, 233
dark wake, 231
Darstellung, 8
Darstellungseinstellung, 144
Darwin, 113, 257
Datei, 11
Dateiname, 137
Dateinamenserweiterung, 135
Dateiserver, 174, 217
Dateisystem, 11, 77, 144
Dateizweig, 141
Datenbank, 123

Datenschutz, 19, 162
Datenzweig, 141
deaktivieren, 249, 262
Defragmentieren, 309
Deinstallationsassistent, 157
deinstallieren, 157
Demomodus, 16, 275
Demonstrationsfenster, 276
Desktop Services Store, 144
Dialogfenster, 12
Dienste-Menü, 253
Dienstleistungsmarken, ii
Dienstprogramme, 250
Differential Privacy, 121
Diffie-Hellman, 218
digitales Siegel, 165
Directory, 135
Disk Image, 165
Diskmedien, 80
Display, 92
DMG, 165
DNS, 101
DNS-Auflöser, 24
DNS-Name, 248
Dock, 270
Dockmenü, 11
Domain Name Service, 101
Download, 163, 165
drahtlos, 218
Drahtlos-Diagnose, 121
Drosseln, 211
Druckauftrag, 228
drucken, 114, 159
Druckverlauf, 228
dsimport, 26
.DS_Store, 144
dtrace, 18
durcheinandergewürfelter Text, 32
Durchmesser, 80
durchqueren, 168, 170
DVD, 80
DVD+R, 82
DVD-ROM, 82

E
Effizienzkern, 109
EFI, 199
eigene Berechtigung, 176
Eigenschaftsliste, 247
Eigentümer, 149, 168, 171
Ein-/Ausgabe, 211
ein-/ausschalten, 217
Einbenutzerbetrieb, 97
eingeschränkt, 18
Einheit (für Speichergröße), 195
Einheiten, 15
Einrichtungsassistent, 270
Einschalttaste, 229
Ein-Schritt-Upgrade-Ticket, 280
Einstellungen, 13, 155
Einstellungsdatei, 262, 265
Einstellungsdomäne, 247
Einstellungskarte, 1, 8, 21, 221
Einstellungssystem, 247
empfohlener freier Speicher, 76
emulieren, 144
Energiesparen, 211
entfernbare Platte, 153
entfernen, 14
entfernen (Registrierung), 280
Erkennungsmerkmal, 114
erlauben, 170
erst prüfen, dann kaufen, 275
erteilen, 168
erweiterte Attribute, 77
Erweitertes Attribut, 141
erweitertes Attribut, 170
Erweiterung, 12
Erweiterungssteckplatz, 111
Erzeugercode, 132
Ethernet, 202
everyone, 168
ExFAT, 174, 214
expliziter Eintrag, 172
externes Laufwerk, 273

F
Familiennummer, 109
Farbetikett, 141
Farbfeld, 109
FAT, 77, 141, 174
FAT32, 174
Fenster, herausgleitendes, 12
Fernseher, 153
fester Link, 129
Festplatte, 211, 272
Festplattendienstprogramm, 71, 189, 196
Festplattenvollzugriff, 20
File-Server, 77, 238, 250
FileVault, 198, 226, 238
Finder, 77, 129, 135, 137, 144, 149, 153, 174, 196, 223, 249, 251–253, 256, 257, 270
Finder Kopieren, 79
Finger-Protokoll, 104

FireWire, 273
Firma, 223
Firmlink, 203
Firmware, 80, 111, 112, 199, 229
firmware, 113
Flash-Speicher, 82, 83
Fokusring, 10
fork, 141
Format, 77, 80
Fragezeichen, 11
Framework, 79
freier Speicher, 76
Freigabe & Zugriffsrechte, 174
Freigabestatus, 113
freischalten, 279
Freispeichergröße, 109
FTP, 174
Funktionsbereich, 8
Fusion Drive, 85, 204

G
Gatekeeper, 135, 164
Gebläse, 88
GECOS, 187
geerbter Eintrag, 172
Gegenanzeige, 11
gehärtete Laufzeit, 163
Gehäuse, 111
Gehäusefarbe, 109
Gehäusemodell, 109
gelerntes Wort, 254
gelockt, 131
gemanagte Einstellungen, 267
gemeinsam verwendeter Speicher, 76
Gerät, 149
Geräteverwaltung, 122
Geschwindigkeitstest, 106
Gesundheit (Flash-Speicher), 85
geteilt (Benutzerordner), 27
gleichzeitiger Lauf, 242
globale Lizenz, 281
Google, 244
Grafikchip, 76
Grammatik, 254
grüner Pfeil, 30
Grundfunktionen, 261
Gruppe, 257
Gruppeneigentümer, 168
Gültigkeitsprüfung, 8
GUID, 181
Guizhou, 244

H
hängendes Pixel, 92
Handoff, 69
Hardware, 271
Hardware-Identifikation, 109
Hauptfenster, 8
Hauptplatine, 111
Hauptspeicher, 73
Help Viewer, 255
Hersteller, 80
heruntergeladen, 165
herunterladen, 17, 277
Hexadezimalziffer, 133
HFS, 77, 132
HFS+, 36, 173
HiDPI, 116
Hierarchie, 248
Hilfefenster, 11
Hilfeknopf, 2
Hilfsprogramm, 3
Hintergrund, 7
Hintergrunddienst, 230
Hintergrundprogramm, 211, 225
Hitze, 231
Hochgeschwindigkeits-Cache, 29
Hochwassermarke, 207
Höchstleistungskern, 109
Hohe Auflösung, 116
Host-Name, 240
HTML, 114
https, 275
Hypervisor, 192

I
iCloud, 121, 244
Icon-Caches, 32
Identifikationsnummer, 257
IEEE 1003, 168
immer an, 228
INACTIVE-plist, 250
Info, 109, 257
Inhalt, 135
inkrementelle Sicherung, 35
inspizieren, 80
Installationsmedium, 189
Installationsprogramm, 136, 160
Installer, 189
Instant Hotspot, 69
Integrität, 248
intelligente Deaktivierung, 29
interner Cache, 29
Internet, 11, 17, 134, 277

Internet-Adresse, 165
Internet-Plugin, 114
Internet-Protokollversion 6, 220
Internet-Verbindung, 107
iOS-Stil, 120
iPad-Aktualisierung, 121
IP-Adresse, 240
iPhone-Aktualisierung, 121
iPod, 148
IPv6, 220
ISO-Datei, 192
iTunes, 27

J
Java™, 114
Jeder, 168
Jobstatus, 234

K
kanonische Sortierung, 178
Karte, 13
Karteireiter, 10
Kategoriebezeichner, 124
Kennwort, 238, 251
Kern, 231
Kern (Prozessor), 109
Kernel, 73
Kernel Panic, 120
Kernel-Erweiterung, 230
Kibi, 15
Klartextübertragung, 218
Klon, 207
Kollision, 99
komprimiert, 146, 221
komprimierter Auslagerungsspeicher, 76
komprimierter Speicher, 74
Konsole, 123, 198
Kontexthilfe, 11
Kopiervorgang, 79
kritischer Vorgang, 14
Kühlung, 88
Kurzname, 186, 218, 257

L
langsames Antwortverhalten, 121
langsames Herunterfahren, 121
Launchpad, 155, 255
LDAPv3, 25
Leistung, 73, 232
lesen, 168
LIFS, 214
Link, 11, 129
Linux, 153
Liste für sichere Downloads, 114
Live File Provider File System, 214
Lizenz, 277
locate, 26
Lock, 131
löschbarer Speicher, 196
löschen, 171, 250
Löschen (Platte), 71
löschen (Schnappschüsse), 62
löschen (Sicherungsdaten), 48
Löschung, 137, 143
Löschungsstärke, 158
Logic Board, 111
lokaler Benutzer, 238
lokaler Schnappschuss, 45, 60
Lüfter, 88

M
Mac App Store, 64
Mac OS, 129, 152, 153, 248
Mac OS Extended, 36
Mac OS X 10.1, *siehe* Mac OS X Puma
Mac OS X 10.4, *siehe* Mac OS X Tiger
Mac OS X Puma, 256
Mac OS X Tiger, 268
MAC-Adresse, 98, 250
macFUSE, 214
Macintosh, 111
Macintosh File System in User Space, 214
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 Big Sur, 2, 3, 35
macOS Catalina, 2
macOS Mojave, 2, 19
macOS Monterey, 2, 3, 64
macOS Server, 24, 232
macOS Sierra, 167, 192
macOS Ventura, 2
macOS-Wiederherstellung, 259
Malware, 114
Malware-Schutz, 114
Managementeinträge, 111
Marketing-Name, 109
Markierung, 217
Markierungen (Markup), 252
mbsalicreq-Datei, 282
mbsetupuser, 92
mbsreg-Datei, 278
MDM server, 122

Medium Access Control, 98
mehrsprachig, 241, 255
Memory Management Unit, 73
Metadaten, 136
Metadatenspeicher, 216
Microsoft Azure, 244
Migrationsassistent, 268, 280
Mitgliedschaft, 257
MMU, 73
Mobilcomputer, 238
Mobile Device Management, 122
mobiler Benutzer, 238
Mobilgerät, 148
Modellbezeichnung, 109
Modellnummer (Prozessor), 109
Monitor, 92
MS-DOS, 141, 144
Multicast, 100

N
named fork, 141
NAS, 35
NetBoot, 188
Netz, 218
Netzbenutzer, 238
Netzqualität, 106
Netzteil, 113
netzweit, 158
Netzwerk Bedienelemente, 69
Netzwerkdienstprogramm, 98
Neulauf, 270
Neustart, 240
Neuzuweisung, 37, 53
NFS, 79
NFSv2, 174
NFSv3, 174
NFSv4, 173
niedrige Auflösung, 118
Notarisierung, 166
Not-Aus, 120
Notfallwerkzeug, 94
NTFS, 174, 214
nur hinzufügen, 170
Nutzungsdauer, 90
Nutzungserlaubnis, 277
NVMe, 83, 85, 273
NVRAM, 18, 236

O
öffentlicher Ordner, 170
Öffnen mit, 252
Öffnen-Dialog, 12
Open Directory, 122, 240
Open Directory Server, 24
Operationen (ACL), 178
optische Disk, 80
optisches Laufwerk, 80
Ordner, 11, 135, 171
Ordnerebene, 172
Ordnerhierarchie, 137
Ortsangabe, 11

P
Paket, 135
Paketinhalt, 136
Paketverfolgung, 103
Papierkorb, 136, 153, 159, 251
Parameter-RAM, 236
Partei, 168
Partition, 71, 77
Partitionierung, 196
PC, 111
PCI-Geräte-ID, 202
persönlicher Cache, 29
Pfad, 11, 137, 257
Pfeilknöpfe, 8
Pfeilnavigation, 14
physischer Datenträger, 203
Ping, 100
Pixel, 92
Platte, 77, 153
Plattenabbild, 165
Plattenplatz, 216
Plattenschreibaktivität, 121
Plattenspeicher, 15
plist, 247
Ports, 106
Portscan, 106
POSIX, 137, 187, 223
POSIX.1e, 167
POSIX-Berechtigung, 167, 172
post mortem, 155
Primärgruppe, 257
Priorität, 211
Prioritätsliste, 241
Privatgröße (APFS), 207
Privatordner, 149, 184, 238, 250, 256, 257
Privatsphäre, 124
PrivilegedHelperTools, 7
PrivilegedTool, 7
privilegierter Vorgang, 3
proaktives Ereignis, 122
Problem, 282
Produktionswoche, 109

Profilmanager, 267
Programmabsturzbericht, 118
Programmaktivität, 120
Programme-Ordner, 253
Programmsprache, 242, 243
Programmstillstandsbericht, 120
Programmvorfall, 122
Property List, 247
Protokoll, 118
Protokoll (Time Machine), 49
Protokollarchiv, 125
Protokolldatei, 146
Protokollierung, 123
Prozess, 73, 76
Prozessor, 109, 271
Prozessoraktivität, 120
Prozessor-Cluster, 109
Prozessorkern, 231
Prozessormodell, 109
Punkt-Unterstrich, 144

Q
Quarantäne, 134, 144, 163

R
RAM, 73, 109, 232
Random Access Memory, 73, 109
Recht, 167, 170
Rechte reparieren, 184
Rechte zurückstellen, 184
Rechtetrennung, 4
Rechtschreibprüfung, 254
Recovery Mode, 95
Registrierung, 16
Registrierungsbescheinigung, 279
Registrierungscode, 277
Registrierungsdatei, 277
Registrierungsname, 279
Registrierungsschlüssel, 279
relativer Pfad, 138
reparieren, 255
Replizieren (APFS), 207
reservierter Speicher, 76
resident, 169
resource fork, 141
Ressourcenzweig, 141, 144
restricted, 18
Retina, 116
Review Team, 165
RFC 952, 101
RFC 2307, 25
Richtlinie, 218
root, 92
root-Benutzer, 18
rootless, 17
Rotationsgeschwindigkeit, 80
rückgängigmachen, 16
Ruhezustand, 240
Ruhezustandszeitgeber, 211
runden, 15

S
sandbox-geschützt, 19
SATA, 273
SATA-Bus, 83
Schalter, 111
Schicht, 80
Schlosssymbol, 131
Schlüsselbund, 68
Schnappschuss, 196
Schrägstrich, 12
schreiben, 168
Schreibschutz, 136
Schrift-Cache, 31
Schriftregistrierungsserver, 31
Schriftsammlung, 32
Schriftzeichen, 31
Schubfach, 80
Schule, 223
Schutz, 114, 131
Schutzmechanismus, 14
Seeding Program, 113
Seite, 74
Self Monitoring, Analysis, and Reporting Technology, 272
Sensoren, 111
Seriennummer, 109
Server, 158
Serverbetrieb, 232
Server-Protokolle, 122
Services für Macintosh, 218
Session, 80
set group identification, 169
set user identification, 169
Setup Assistant, 270
SGID, 169
Shell, 257
shoebox app, 158
sicherer Modus, 230
Sicherheit, 3, 14, 19, 134, 169, 253
Sicherheitseinschätzung, 164
Sicherheitskomponente, 4, 7
Sicherheitsprüfung, 8
Sicherheitsstandard, 17

Sicherheits-Updates, 114, 116
sichtbar, 143
Sichtbarkeit, 132, 144
Signatur, 114
Signatur (Prozessor), 109
Simultanes Multithreading, 109
Sitzung, 80
S.M.A.R.T., 272
Smart Queue Management, 107
SMB, 79, 173
SMBIOS, 112
SMC, 88, 111
SoC, 112
Socket, 100
Sockets, 106
Softwareaktualisierung, 16, 17
Software-Entwickler, 232
Software-Produktregistrierung und Aktivierung, 278, 279
softwareupdate (Befehl), 64
Softwareupdate (Karte), 64
Solid-State-Laufwerk, 82
Speicher, 73, 109, 271
Speicher, löschbarer, 197
Speicherabzug, 155
Speichergröße, 15, 232
Speicherkapazität, 80
Speichermanagementeinheit, 73
Speicherplatz, 195
Speicherraum, 73
Speichersteckplatz, 111
Speicherverbrauch, 41, 120
spezielles Recht, 167
Spindelmotor, 211
Spotlight, 20, 26, 136, 153, 215
Spotlight-Kommentar, 141
Spotlight-Unterstützungsmarkierung, 217
Sprache, 241
SQM, 107
SSD, 82
SSD-Verschlüsselung, 112
Staging, 33
Standard, 16, 238
Standardeinstellungen, 16
Standortlizenz, 281
Start (von Programmen), 160
Startdienste, 253
Startobjekt, 268
Startvolume, 237
Startzeit, 114
Statistik, 73, 90
Statistik (Time Machine), 39
Status, 26
Steckbrücke, 111
Steckverbinder, 111
Stepping, 109
Steuerung, 10
Steuerungsfenster, 8
Steuerungskarte, 8
sticky, 169, 181
Stiftsymbol, 176
Stillstandsbericht, 120
Strichcode, 250
Subsystembezeichner, 124
Suche, 215
sudo, 4
SUID, 169, 181
Support-Richtlinie, 2
Symbol, 8, 12, 252
Symbol-Caches, 32
symbolischer Link, 77, 129, 179
Symbolleiste, 8
Synchronisation, 250
System Integrity Protection, 17
System Management BIOS, 112
System Management Controller, 88, 111
System on a chip, 112
Systemabsturz, 120
Systemanforderungen, 3
Systemdaten, 109
Systemeinstellungen, 4, 8, 64, 114, 116, 149, 211, 217, 221, 238, 242, 257, 258
Systemgerät, 111
Systeminformationen, 109, 250, 251
Systemintegritätsschutz, 17, 29, 34, 113
Systemkern, 113, 155, 230
Systemplatine, 111
Systemprotokoll, 118
Systemstart, 229
Systemverwalter, 3, 15, 122, 239
systemweiter Cache, 29

T

T2-Prozessor, 88
Tab, 10
Tag, 141
Taktfrequenz, 109
Tastatur, 10
Tastatursteuerung, 10
Tavares, Stafford, 218
Technische Hinweise, 282
Teilen, 253
Telefax, 277
Telefon, 277

Telefonieüberwachung, 121
Temporärordner, 261
Terminal, 257
Terminplan, 309
Test, 79
Testmodus, 16, 275
TextEdit, 114
Throttling, 211
Thunderbolt, 273
Ticket für Testmodus, 275
Time Capsule, 35
Time Machine, 35, 80, 141, 215
Time Machine X, 36
Time Machine-Dateifreigabe, 35
Time-Sharing, 90
TinkerTool, 3, 21, 134, 144, 257
TinkerTool 8, 22
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 Release 2, 2
Toneffekt, 79
totes Pixel, 92
Touch Bar, 6, 10
Touch ID, 6, 229
TouchID, 112
Traceroute, 103
Transportplatte, 155
Treiber, 230
Trennung, Benutzerrechte, 4
Trim-Befehl, 82
trimforce, 83
ttsfrm, 95
Typcode, 132, 144
Typenschild, 250
Typmarkierung, 135

U

Überbuchung, 196
Überprovisionierung, 85
überprüft, 272
Überprüfung (Time Machine), 41, 55
Übersetzung, 256
Übersicht, 8
übertragen (Rechte), 179
Übertragungsprotokoll, 77
UFS, 174
umgekehrte Reihenfolge, 248
Umschalttaste, 230
umsortieren (ACL), 178
Unicode, 138
Universal Unique Identifier, 213, 250
universeller einzigartiger Bezeichner, 213
UNIX, 167, 173
Unix, 25, 90
UNIX-Pfad, 11
unknown, 168
unsichtbar, 132
untätig, 231
Unterordner, 171
Update, 280
Uptime, 114
URL, 165
USB, 273
USB-Flash-Laufwerk, 189
UTF-8, 138
UUID, 187, 213, 250

V

vererben, 170
Vererbung, 171
verfügbarer Speicher, 196
Vergrößerungsglas, 249, 257
Version, 240
versteckt, 132, 143, 153
Verteilaktion, 113
Vertrauen, 134
Vertrauensprüfung, 121
vertraulich, 122, 169, 216
Vertrieb, 277
verwaist, 146, 149
Verwalter, 239, 270, 275
Verwalterautorisierung, 15
verweigern, 168, 170
verwerfen, 30
Verzeichnis, 24
Verzeichnisdienst, 23, 188, 238
Verzeichnisdienstserver, 15, 178
Verzeichnisknoten, 24
VFAT, 174
Virenscanner, 114
Virtuelle Maschine, 192
virtueller Speicher, 73
voller Name, 187
Vollzugriff, 178
Volume, 214
Volume (Time Machine), 39, 53
Volumenlizenz, 281
Vordefinieren von Rechten, 180
Vorschaubild, 141

W

Währung, 277
Warenzeichen, ii
Wartung, 23
Web-Browser, 114, 228
Web-Cache, 28
WebDAV, 174
Web-Schnittstelle, 228
Web-Seite, 17
Werkseinstellung, 16, 276
whois, 103
wiederherstellen, 30
Wiederherstellungs-Betriebssystem, 95
Wiederherstellungspunkt, 45, 60
Wiederherstellungssystem, 18, 45, 60, 230
Wiederherstellungs-Volume, 188
Windows, 153, 173
wirksames Zugriffsrecht, 181
WLAN-Schnittstelle, 218
Wörterbuch, 254
wortreich, 230

X

Xcode, 68
XID, 207
XProtect, 114, 191

Z

Zahlung, 277
Zeichen, 31
Zeitassistent, 127
ZFS, 174
Ziehen, 12
Ziehen und Ablegen, 155
ZIP-Archiv, 221
Zip-Registrierungsdatei, 278
Zugriffsrecht, 167, 171, 174, 180
Zugriffsrechtsfilter, 223
Zugriffssteuerungseintrag, 170
Zugriffssteuerungsliste, 167, 170
zurücknehmen (Registrierung), 280
zurücksetzen, 16
zurückstellen, 16
Zwangslöschung, 136
Zweig, benannter, 141
Zwei-Wege-Zufallsschlüssel, 218