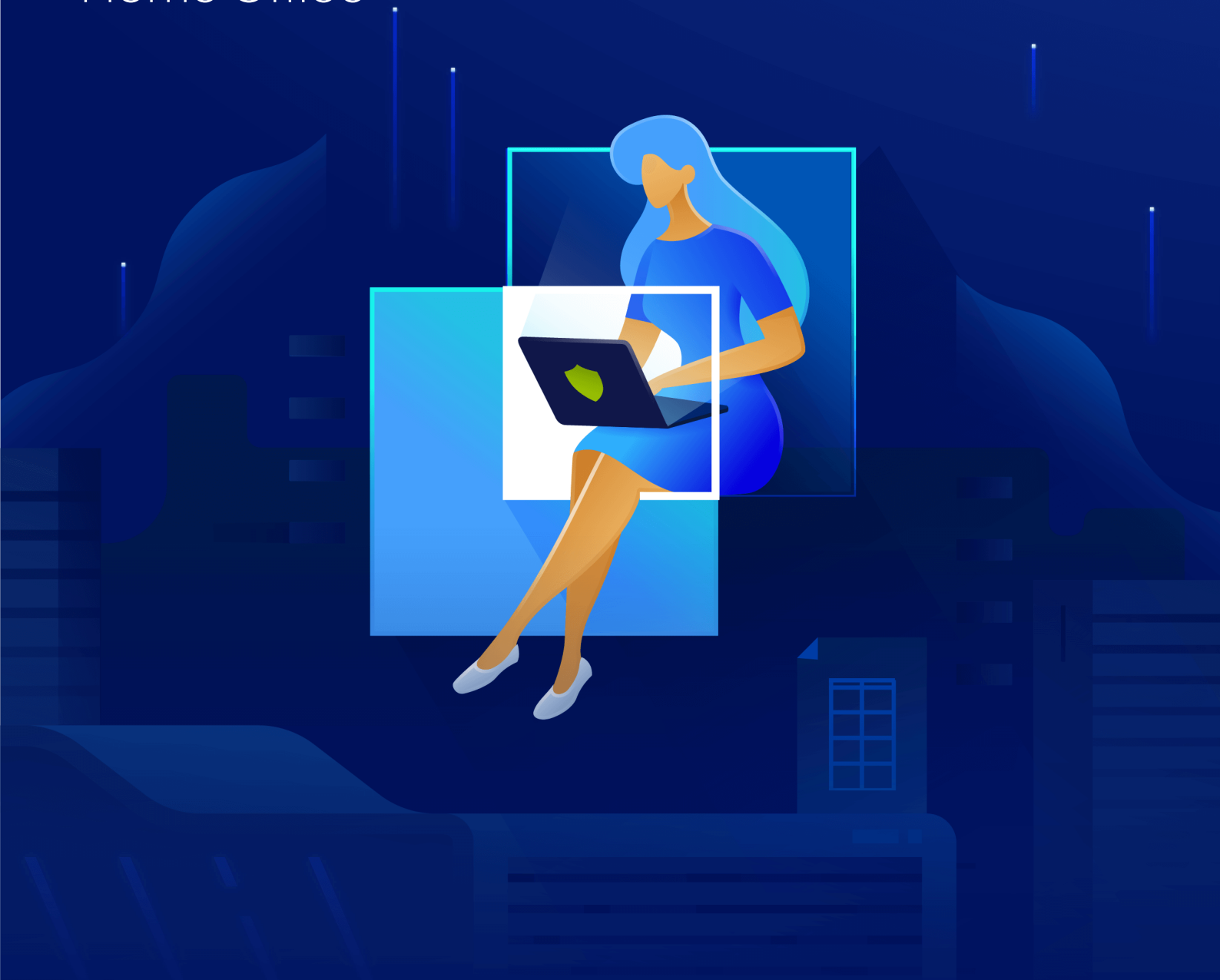
Acronis

acronis.com

# Acronis Cyber Protect

## Home Office



Benutzeranleitung

REVISION: 21.06.2023

# Inhaltsverzeichnis

**Einführung** ..... **10**
Was ist Acronis Cyber Protect Home Office? ..... 10
Backups, die in Acronis True Image (2020 oder 2021) oder Acronis Cyber Protect Home Office erstellt wurden ..... 10
Backup-Schemata ..... 11
Backups im TIBX-Format bereinigen ..... 11
Die manuelle Bereinigung von lokalen Backups erfolgt nach folgendem Schema: ..... 11
Welches Backup behält das TIB-Format? ..... 11
Systemanforderungen und unterstützte Medien ..... 12
Minimale Systemanforderungen ..... 12
Unterstützte Betriebssysteme ..... 12
Unterstützte Dateisysteme ..... 13
Unterstützte Typen von Internetverbindungen ..... 14
Unterstützte Speichermedien ..... 15
Acronis Cyber Protect Home Office installieren und deinstallieren ..... 15
Acronis Cyber Protect Home Office aktivieren ..... 18
Das Problem 'Zu viele Aktivierungen' ..... 18
Ihre Abonnementlizenzen manuell verwalten ..... 18
Informationen zur Testversion ..... 19
Allgemeine Beschränkungen ..... 19
Synchronisierung ..... 19
Acronis Cloud ..... 19
Die Vollversion kaufen ..... 19
Upgrade von Acronis Cyber Protect Home Office ..... 20
Integrierte Kaufmöglichkeit ..... 21
Technischer Support ..... 21
**Erste Schritte** ..... **22**
Sprache für die Benutzeroberfläche ..... 22
Ihr System schützen ..... 22
Backup Ihres Computers ..... 22
Ein Acronis Boot-Medium erstellen ..... 24
Alle Daten auf Ihrem PC sichern ..... 25
Ein Acronis Survival Kit erstellen ..... 27
Backups Ihrer Dateien ..... 29
Ein Laufwerk klonen ..... 31

Warum benötige ich das? 31
Bevor Sie beginnen 31
Ein Laufwerk klonen 32
Ihren Computer wiederherstellen 33
Acronis Konto 35
Erste Schritte mit der Acronis Cloud 36
Remote-Storage 36
Webapplikation 36
So gewährleisten wir die Sicherheit Ihrer Daten 37
Abonnementinformationen 37
**Grundlegende Konzepte 38**
Unterschied zwischen dateibasierten Backups und Images von Laufwerken/Volumes 40
Vollständige, inkrementelle und differentielle Backups 41
Vollständige Methode 41
Inkrementelle Methode 42
Differentielle Methode 43
Changed Block Tracker (CBT) 44
So entscheiden Sie, wo Sie Ihre Backups speichern 45
Ein neues Laufwerk zur Nutzung für Backups vorbereiten 46
FTP-Verbindung 47
Authentifizierungseinstellungen 48
Acronis Nonstop Backup 48
Beschränkungen für Nonstop Backup 49
Und so funktioniert es 49
Aufbewahrungsregeln 49
Acronis Nonstop Backup Storage 50
Nonstop Backup – Häufig gestellte Fragen (FAQs) 51
Benennung von Backup-Dateien 52
Die Namenskonvention für Backup-Dateien, die mit Acronis True Image (2020 oder 2021) oder Acronis Cyber Protect Home Office erstellt wurden 52
Die Namenskonvention für Backup-Dateien, die mit einer Acronis True Image-Version vor 2020 erstellt wurden 53
Integration in Windows 53
Assistenten 55
FAQ über Backup, Recovery und Klonen 56
**Daten werden per Backup gesichert 58**
Backups von Laufwerken und Volumes 58

Backup von Dateien und Ordnern ..... 60
Mobilgeräte per Backup sichern ..... 62
Acronis Mobile ..... 63
Lokaler Zielort für Backups von Mobilgeräten ..... 64
Microsoft 365-Daten per Backup sichern ..... 64
Warum sollten Sie Microsoft 365-Daten per Backup sichern? ..... 64
Microsoft 365-Daten per Backup sichern ..... 65
Backup-Optionen ..... 65
Planung ..... 66
Backup-Schemata ..... 69
Benachrichtigungen für Backup-Aktionen ..... 77
Elemente vom Backup ausschließen ..... 79
Modus zur Image-Erstellung ..... 81
Backup-Schutz ..... 81
Online Backups schützen ..... 83
Befehle vor bzw. nach dem Backup ..... 83
Backup-Aufteilung ..... 84
Optionen für Backup-Validierung ..... 85
Backup-Reservekopie ..... 86
Einstellungen für Wechselmedien ..... 86
Fehlerbehandlung ..... 88
Dateisicherheitseinstellungen für Backups ..... 89
Computer herunterfahren ..... 90
Die Performance von Backup-Aktionen ..... 91
Ein Datacenter für Backups auswählen ..... 93
Energieeinstellungen für Notebooks und Tablets ..... 93
WLAN-Verbindungen für Backups in die Acronis Cloud ..... 94
Aktionen mit Backups ..... 95
Das Menü 'Backup-Aktionen' ..... 95
Backup-Aktivität und -Statistiken ..... 97
Backups in der Liste sortieren ..... 99
Backups in die Acronis Cloud replizieren ..... 100
Backups validieren ..... 101
Backups an verschiedene Plätze ..... 101
Ein vorhandenes Backup der Liste hinzufügen ..... 102
Notarized Backup ..... 103
Backups, Backup-Versionen und Replikate bereinigen ..... 108

Speicherplatz in der Acronis Cloud bereinigen ... 111
Daten aus der Acronis Cloud entfernen ... 111
**Daten wiederherstellen ... 114**
Laufwerke und Volumes wiederherstellen ... 114
Ihr System nach einem Absturz wiederherstellen ... 114
Volumes und Laufwerke wiederherstellen ... 127
Recovery von Laufwerken und Volumes vom Typ 'Dynamisch' oder 'GPT' ... 141
Boot-Reihenfolge im BIOS oder UEFI-BIOS arrangieren ... 144
Laufwerk-Recovery aus der Cloud ... 146
Dateien und Ordner wiederherstellen ... 151
Backup-Inhalte durchsuchen ... 153
Microsoft 365-Daten wiederherstellen ... 154
Welche Elemente können wiederhergestellt werden? ... 154
Microsoft 365-Daten wiederherstellen ... 155
Recovery-Optionen ... 156
Recovery-Modus 'Laufwerk' ... 156
Vor-/Nach-Befehle für Wiederherstellung ... 156
Optionen für Validierung ... 157
Computer-Neustart ... 157
Optionen für Datei-Recovery ... 158
Optionen für das Überschreiben von Dateien ... 158
Die Performance von Recovery-Aktionen ... 159
Benachrichtigungen für Recovery-Aktionen ... 159
**Daten archivieren ... 162**
Was tut die Datenarchivierungsfunktion? ... 162
Was wird von Archiven ausgeschlossen? ... 163
Cloud-Archivierung vs. Online Backup ... 163
Archivierung Ihrer Daten ... 164
Datenarchivierungsoptionen ... 165
Zugriff auf Ihre archivierten Dateien ... 166
**Daten freigeben ... 167**
**Die Daten der ganzen Familie sichern ... 168**
Was bedeutet 'Data Protection für die ganze Familie'? ... 168
Im Online Dashboard ein neues Gerät hinzufügen ... 168
Daten aus der Ferne sichern (Remote-Backup) ... 169
Daten über das Online Dashboard wiederherstellen ... 170
E-Mail-Benachrichtigungen ... 171

**Schutz** ... **173**
Das Protection Dashboard ... 173
Active Protection ... 174
Anti-Ransomware Protection ... 174
Echtzeitschutz ... 175
Webfilter ... 176
Active Protection konfigurieren ... 177
Antivirus-Scans ... 179
Antivirus-Scans konfigurieren ... 180
Schwachstellenbewertung ... 181
Erkannte Probleme verwalten ... 182
In Quarantäne befindliche Dateien verwalten ... 183
Schutz-Ausschlüsse konfigurieren ... 184
Schutz für Videokonferenz-Applikationen ... 185
Schutz-Updates herunterladen ... 185
**Daten synchronisieren** ... **187**
Über die Synchronisierungsfunktion (Sync) ... 187
Was Sie synchronisieren können und was nicht ... 187
Storage-Typen ... 187
Datentypen ... 188
Synchronisierungssymbole ... 188
Der Infobereich ... 188
Windows Explorer ... 189
Eine Synchronisierung erstellen ... 189
Versionen von synchronisierten Dateien ... 190
Wiederherstellen einer vorherigen Dateiversion ... 190
So stellen Sie eine gelöschte Datei wieder her ... 191
Eine Synchronisierung löschen ... 191
**Laufwerk klonen und Migration** ... **192**
Das Werkzeug 'Laufwerk klonen' ... 192
'Laufwerk klonen'-Assistent ... 193
Manuelle Partitionierung ... 194
Elemente vom Klonen ausschließen ... 196
Migrationsmethode ... 198
Migration Ihres Systems von einer Festplatte auf SSD ... 204
SSD-Größe ... 204
Die Wahl der Migrationsmethode ... 204

Was Sie tun können, wenn Acronis Cyber Protect Home Office Ihre SSD nicht erkennt ..... 204
Migration auf eine SSD mit der 'Backup und Recovery'-Methode ..... 206
**Extras** ..... **208**
Acronis Cloud Backup Download ..... 208
Acronis Media Builder ..... 210
Ein Acronis Boot-Medium erstellen ..... 211
Startparameter für das Acronis Boot-Medium ..... 213
Treiber zu einem vorhandenen .wim-Image hinzufügen ..... 215
Eine .iso-Datei von einer .wim-Datei erstellen ..... 216
So stellen Sie sicher, dass Ihr Boot-Medium bei Bedarf auch funktioniert ..... 217
Auswahl des Grafikkartenmodus beim Starten des Boot-Mediums ..... 221
Acronis Startup Recovery Manager ..... 223
Zusätzliche Informationen ..... 224
Try&Decide ..... 225
Szenarien, bei denen Try&Decide helfen kann ..... 225
Die Vorgehensweise von Try&Decide nach einem Computer-Neustart ..... 226
Einschränkungen bei Verwendung von Try&Decide ..... 227
Try&Decide verwenden ..... 228
Try&Decide-Optionen und -Benachrichtigungen ..... 229
Try&Decide: Typische Einsatzfälle ..... 230
Acronis Secure Zone ..... 232
Bereinigung der Acronis Secure Zone ..... 232
Eine Acronis Secure Zone erstellen und verwalten ..... 233
Der Speicherort für die Acronis Secure Zone ..... 233
Die Größe der Acronis Secure Zone ..... 234
Schutz für Acronis Secure Zone ..... 236
Die Acronis Secure Zone entfernen ..... 237
Ein neues Laufwerk hinzufügen ..... 237
Ein Laufwerk auswählen ..... 237
Wahl der Initialisierungsmethode ..... 238
Neue Volumes erstellen ..... 239
Werkzeuge für Sicherheit und zum Schutz Ihrer Privatsphäre ..... 242
Acronis DriveCleanser ..... 242
Systembereinigung ..... 249
Ein Backup-Image mounten ..... 257
So können Sie ein Image mounten ..... 257
Ein gemountetes Image trennen ..... 258

Mit .vhd(x)-Dateien arbeiten ... 259
So können Sie .vhd(x)-Dateien verwenden ... 259
Beschränkungen und zusätzliche Informationen ... 259
Ein Acronis Backup konvertieren ... 259
Backup-Einstellungen importieren und exportieren ... 260
Acronis Universal Restore ... 261
Welches Problem wird dabei gelöst? ... 262
Wie wird es verwendet? ... 262
Ein Acronis Universal Boot-Medium erstellen ... 262
Acronis Universal Restore verwenden ... 265
**Problembehebung (Troubleshooting)** ... **267**
Lösungen für die häufigsten Probleme ... 267
Acronis System Report ... 267
Acronis Smart Error Reporting ... 269
Wenn Sie eine Internetverbindung haben ... 269
Wenn Sie keine Internetverbindung haben ... 269
Feedback an Acronis senden ... 270
So sammeln Sie Speicherabbilder (Crash Dumps) ... 272
Acronis Programm zur Kundenzufriedenheit (CEP) ... 272
**Glossar** ... **274**
**Index** ... **280**

# Urheberrechtserklärung



# Von Acronis patentierte Technologien

Die in diesem Produkt verwendeten Technologien werden durch einzelne oder mehrere U.S.-Patentnummern abgedeckt und geschützt: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234 sowie weitere, schwebende Patentanmeldungen.

# Einführung

## Was ist Acronis Cyber Protect Home Office?

Acronis Cyber Protect Home Office ist eine umfassende Cyber Protection-Lösung, die die Sicherheit aller Informationen auf Ihrem Computer gewährleistet. Sie können damit Ihre Dokumente, Fotos, E-Mails, einzelne Volumes oder auch komplette Laufwerke (das Betriebssystem, alle Anwendungen, Einstellungen und Daten eingeschlossen) per Backup sichern. Einer der Hauptvorteile sind die Data Protection- und Sicherheitsfunktionen.

Backups versetzen Sie in die Lage, Ihr Computersystem im Notfall (einem 'Desaster') wiederherstellen zu können – beispielsweise, wenn Daten verloren gingen, wichtige Dateien bzw. Ordner versehentlich gelöscht wurden oder ein komplettes Laufwerk ausgefallen ist.

Online Backups ermöglichen Ihnen, Ihre Dateien und Laufwerke in der Acronis Cloud zu sichern. Ihre Daten sind damit sogar dann geschützt, wenn Ihr Computer verloren gehen, gestohlen oder zerstört werden sollte. Ihre Daten können bei Bedarf auf einem neuen Gerät vollständig wiederhergestellt werden.

**Kernfunktionen:**

- Laufwerk-Backup zu einem lokalen Storage und in die Acronis Cloud
- Datei-Backup zu einem lokalen Storage und in die Acronis Cloud
- Antivirus & Antimalware Protection
- Acronis Boot-Medium
- Klonen von Festplattenlaufwerken
- Archivierung von Daten
- Data Protection für die ganze Familie
- Dateisynchronisierung
- Extrafunktionen (Tools) für den Bereich 'Sicherheit' und 'Schutz der Privatsphäre'

**Hinweis**
Backups in die Acronis Cloud können nicht mit dem Acronis Startup Recovery Manager oder einem Acronis Boot-Medium erstellt werden.

Erfahren Sie, wie Sie Ihren Computer schützen können: "Ihr System schützen".

## Backups, die in Acronis True Image (2020 oder 2021) oder Acronis Cyber Protect Home Office erstellt wurden

Mit Acronis True Image 2020 wurde das neue Backup-Format 'TIBX' eingeführt, welches zuverlässiger und komfortabler ist. Das TIBX-Format wird für Laufwerk-Backups verwendet, die

einen Netzwerk-Storage oder interne bzw. externe Laufwerke als Backup-Ziel verwenden.

Weitere Informationen zur Benennung von Backup-Dateien finden Sie im Abschnitt '"Benennung von Backup-Dateien" (S. 52)'.

## Backup-Schemata

Bei der Erstellung von Backups im TIBX-Format werden alle Backup-Schemata unterstützt. Anders als beim TIB-Format, bei dem jede Backup-Version als separate Datei gespeichert wurde, werden beim TIBX-Format nur die vollständigen und differentielle Backup-Versionen als separate Dateien gespeichert. Die Inkrementellen Backup-Versionen werden dagegen automatisch in ihr jeweiliges Basis-Backups (vollständig oder differentiell) eingebunden.

## Backups im TIBX-Format bereinigen

Wenn Sie nicht mehr benötigte Backup-Versionen bereinigen wollen, können Sie dafür automatische oder manuelle Bereinigungsmethoden verwenden.

Egal ob Sie eine automatische oder manuelle Bereinigungen konfigurieren: nach der Bereinigung können einige Hilfsdateien im Storage übrigbleiben. Diese Dateien werden von Windows möglicherweise größer angezeigt, als sie es tatsächlich sind. Sie können die physische Größe der Datei überprüfen, wenn Sie sich deren Dateieigenschaften von Windows anzeigen lassen.

**Hinweis**
Sie sollten keine dieser Dateien manuell löschen!

## Die manuelle Bereinigung von lokalen Backups erfolgt nach folgendem Schema:

- Vollständige Backups können nur mit ihren abhängigen Versionen zusammen gelöscht werden.
- Differentielle Backup-Versionen können unabhängig von anderen Backup-Versionen gelöscht werden.
- Inkrementelle Backups:
  - Wenn es sich um die letzte Backup-Kette handelt, kann jedes inkrementelle Backup gelöscht werden, um Speicherplatz freizugeben.
  - Wenn es sich nicht um die letzte Backup-Kette handelt, kann eine inkrementelle Backup-Version nur zusammen mit den anderen inkrementellen Versionen derselben Kette gelöscht werden.

## Welches Backup behält das TIB-Format?

Folgende Backups verwenden weiterhin das TIB-Format:

- Backups auf Dateiebene
- Nonstop Backups

- Beglaubigte Backups (Notarized Backups)
- Backups, die CDs/DVDs/Blu-rays, einen FTP-Server oder die Acronis Secure Zone als Backup-Ziel verwenden

Informationen zur unterschiedlichen Benennung von .tibx- und .tib-Archiven fnden Sie im Abschnitt 'Benennung von Backup-Dateien'.

Weitere Informationen zur Bereinigung finden Sie im Abschnitt 'Backups, Backup-Versionen und Replikate bereinigen'.

# Systemanforderungen und unterstützte Medien

## Minimale Systemanforderungen

Acronis Cyber Protect Home Office erfordert mindestens folgende Hardware:

- Einen Prozessor vom Typ Intel CORE 2 Duo (2GHz) oder vergleichbares
  Die CPU muss den SSE-Befehlssatz unterstützen.
- 2 GB RAM
- 7 GB freier Speicherplatz auf dem Systemlaufwerk
- Ein CD-RW-/DVD-RW-Laufwerk oder USB-Stick zur Erstellung eines Boot-Mediums
  - Der erforderliche freie Speicherplatz für die verwendete Linux-Version beträgt ca. 660 MB.
  - Der erforderliche freie Speicherplatz für die verwendete Windows-Version beträgt ca. 700 MB.
- Eine Bildschirmauflösung von 1024 x 768
- Maus oder anderes Zeigegerät (empfohlen)

**Warnung!**
Erfolgreiche Backups und Wiederherstellungen für Installationen auf virtuellen Maschinen werden nicht garantiert.

## Andere Anforderungen

- Für die Produktaktivierung, zum Herunterladen von Schutz-Updates und für alle Funktionen, die auf der Acronis Cloud basieren, wird eine Internetverbindung benötigt.Sollte Ihr Computer keine Internetverbindung haben, können Sie das Produkt dennoch aktivieren – und zwar über einen anderen Computer, der über eine Internetverbindung verfügt. Weitere Informationen finden Sie im Abschnitt 'Acronis Cyber Protect Home Office aktivieren'.
- Sie benötigen administrative Berechtigungen, um Acronis Cyber Protect Home Office ausführen zu können.

## Unterstützte Betriebssysteme

Acronis Cyber Protect Home Office wurde auf folgenden Betriebssystemen getestet:

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1 (alle Editionen)
- Windows Home Server 2011

**Hinweis**

- Beta-Versionen werden nicht unterstützt. Siehe: https://kb.acronis.com/de/content/60589.
- Windows Embedded, die Windows IoT-Editionen, Windows 10 LTSB, Windows 10 LTSC und Windows 10 im S-Modus werden nicht unterstützt.
- Um Acronis Cyber Protect Home Office unter Windows 7, Windows 8 und Windows 8.1 verwenden zu können, benötigen Sie folgende Sicherheitsupdates von Microsoft: KB4474419 und KB4490628. Siehe: https://kb.acronis.com/de/content/69302.

Acronis Cyber Protect Home Office ermöglicht die Erstellung einer bootfähigen CD-R/DVD-R oder eines bootfähigen USB-Sticks, mit der/dem Sie Backups und Wiederherstellungen von Laufwerken bzw. Volumes auf Computern mit Intel-/AMD-basierten Betriebssystemen (einschließlich Linux®) durchführen können.

Eine korrekte Funktion der Software auf anderen Windows-Betriebssystemen ist möglich, wird jedoch nicht garantiert.

**Warnung!**

Eine erfolgreiche Wiederherstellung wird nur für die unterstützten Betriebssysteme garantiert. Andere Betriebssysteme können mithilfe eines 'Sektor-für-Sektor'-Backups gesichert werden. Nach einer Wiederherstellung kann es jedoch sein, dass das entsprechende System nicht mehr bootfähig ist.

## Unterstützte Dateisysteme

- NTFS
- Ext2/Ext3/Ext4
- ReiserFS(3)[1]
- Linux SWAP[2]

[1]Bei diesen Dateisystemen werden nur Backup-/Recovery-Aktionen von/mit kompletten Laufwerke bzw. Volumes unterstützt.
[2]Bei diesen Dateisystemen werden nur Backup-/Recovery-Aktionen von/mit kompletten Laufwerke bzw. Volumes unterstützt.

- HFS+/HFSX[1]
- FAT16/32/exFAT[2]

Wenn ein Dateisystem nicht unterstützt wird oder beschädigt ist, kann Acronis Cyber Protect Home Office dessen Daten dennoch mithilfe eines 'Sektor-für-Sektor'-Backups sichern.

## Unterstützte Typen von Internetverbindungen

Die nachfolgende Tabelle zeigt, welchen Möglichkeiten zur Internetverbindung von den Produktfunktionen unterstützt werden.

| | **Typ der Internetverbindung** | | | | |
|---|---|---|---|---|---|
| | Acronis Konsole unter Windows | | Acronis Boot-Medium | | |
| | Jede unter Windows verfügbare Verbindung | Proxy-Server | Ethernet-Netzwerkkabel | WLAN | Proxy-Server |
| Backups auf Laufwerk- und Dateiebene in die Acronis Cloud | + | - | - | - | - |
| Recovery auf Laufwerkebene aus der Acronis Cloud | + | - | + | + | - |
| Recovery auf Dateiebene aus der Acronis Cloud | + | - | - | - | - |
| Datensynchronisierung | + | - | - | - | - |
| Produktaktivierung | + | - * | - | - | - |
| Produkt-Update | + | - * * | - | - | - |

* - Sie können das Produkt mit einem Aktivierungscode aktivieren. Weitere Details finden Sie im Abschnitt '**Aktivierung von einem anderen Computer aus**' des Kapitels 'Acronis Cyber Protect Home Office aktivieren'.

* * - Laden Sie zum Update des Produkts die neuere Produktversion von der Acronis Website herunter und installieren Sie diese Version über die bereits vorhandene.

[1]Die Aktionen 'Laufwerk wiederherstellen', 'Volume wiederherstellen' und 'Laufwerk klonen' werden nur ohne Größenanpassungen unterstützt.
[2]Die Aktionen 'Laufwerk wiederherstellen', 'Volume wiederherstellen' und 'Laufwerk klonen' werden nur ohne Größenanpassungen unterstützt.

## Unterstützte Speichermedien

- Festplattenlaufwerke (HDDs)
- SSD-Laufwerke (Solid State Drives)
- Per Netzwerk angebundene Speichergeräte (NAS)
- FTP-Server

**Hinweis**
Der entsprechende FTP-Server muss für die Dateiübertragung den 'Passiven Modus' zulassen. Wenn Sie mit Acronis Cyber Protect Home Office ein Backup direkt zu einem FTP-Server (als Ziel) erstellen, wird das Backup in Dateien mit einer maximalen Größe von 2 GB aufgeteilt.

- CD-R/RW, DVD-R/RW, DVD+R (einschließlich Double-Layer DVD+R), DVD+RW, DVD-RAM, BD-R, BD-RE
- Über USB 1.1 / 2.0 / 3.0, USB-C, eSATA, FireWire (IEEE-1394), SCSI und PC-Card angeschlossene Speichergeräte

### Limitierungen bei Aktionen mit dynamischen Datenträgern

- Das Erstellen einer Acronis Secure Zone auf dynamischen Datenträgern wird nicht unterstützt.
- Die Wiederherstellung eines dynamischen Volumes als dynamisches Volume und bei gleichzeitiger manueller Größenanpassung wird nicht unterstützt.
- Try&Decide® kann nicht verwendet werden, um dynamische Datenträger zu schützen.
- Die Aktion 'Laufwerk klonen' wird nicht für dynamische Datenträger unterstützt.

Die Firewall-Einstellungen des Quellcomputers sollten die Ports 20 und 21 geöffnet haben (für TCP- und UDP-Protokolle). Der Windows-Dienst **Routing und RAS** sollte deaktiviert sein.

# Acronis Cyber Protect Home Office installieren und deinstallieren

***So können Sie Acronis Cyber Protect Home Office installieren***

1. Laden Sie die Acronis Cyber Protect Home Office-Setup-Datei von der Acronis Website unter https://go.acronis.com/home-office herunter.
2. Starten Sie die Setup-Datei.
   Vor dem eigentlichen Start der Installation wird Acronis Cyber Protect Home Office prüfen, ob ein neueres Build übers Internet verfügbar ist. Wenn ja, wird diese neuere Version zur Installation angeboten.
3. Wählen Sie den Installationsmodus:

- Klicken Sie auf **Installieren**, wenn Sie die Standardinstallation starten wollen.
- Klicken Sie auf **Benutzerdefinierte Installation**, um die erforderlichen Komponenten auszuwählen.
  - **Backup und zentrale Schutzkomponenten (Core Protection).**. Diese Komponente ist essenziell für:
    - "Daten werden per Backup gesichert" (S. 58)
    - "Daten wiederherstellen" (S. 114)
    - "Schwachstellenbewertung" (S. 181)
    - "Daten archivieren" (S. 162)
    - "Daten freigeben" (S. 167)
    - "Daten synchronisieren" (S. 187)
    - "Laufwerk klonen und Migration" (S. 192)
    - "Extras" (S. 208)
  - **Antiransomware Protection, Cryptomining-Erkennung und Schutz für Videokonferenzen.**. Weitere Informationen dazu finden Sie im Abschnitt '"Active Protection" (S. 174)'.
  - **Echtzeitschutz, Antivirus-Scans und Webfilterung.**. Weitere Informationen dazu finden Sie in den Abschnitten '"Active Protection" (S. 174)' und '"Antivirus-Scans" (S. 179)'.
  - **Try&Decide-Tool**. Wenn Sie die Funktion Speicher-Integrität" von Windows verwenden, sollten Sie diese Komponente nicht installieren, um Kompatibilitätsprobleme zu vermeiden. Weitere Informationen dazu finden Sie im Abschnitt '"Try&Decide" (S. 225)'.

  Acronis Cyber Protect Home Office wird auf Ihrem System-Volume installiert (üblicherweise das Volume mit dem Laufwerksbuchstaben C:).
4. Klicken Sie nach Abschluss der Installation auf **Anwendung starten**.
5. Lesen und akzeptieren Sie die Bedingungen der Lizenzvereinbarung für Acronis Cyber Protect Home Office und Bonjour.

   Die Bonjour-Software wird auf Ihrem Computer installiert, um eine erweiterte Unterstützung für NAS-Geräte bereitzustellen. Sie können die Software bei Bedarf jederzeit wieder deinstallieren.

   Sie können außerdem zustimmen, dass Sie am 'Acronis Programm zur Kundenzufriedenheit (CEP)' teilnehmen wollen. Sie können diese Einstellung jederzeit ändern.
6. Sie können im Fenster **Aktivierung** eine der folgenden Aktionen ausführen:
   - Wenn Sie Acronis Cyber Protect Home Office aktivieren wollen, geben Sie Ihre Seriennummer ein und klicken Sie dann auf **Aktivieren**. Das Produkt wird automatisch aktiviert.
   - Wenn Sie sich an Ihrem Acronis Konto anmelden wollen, klicken Sie auf **Anmelden**. Weitere Informationen finden Sie im Abschnitt 'Acronis Konto'.
   - Wenn Sie die Testversion verwenden wollen, klicken Sie auf **Testversion starten**.

***Eine fehlerhafte Installation von Acronis Cyber Protect Home Office reparieren***

Wenn Acronis Cyber Protect Home Office nicht mehr läuft oder Fehler verursacht, sind möglicherweise Teile des Programms beschädigt. Um dieses Problem zu beheben, müssen Sie zuerst das Programm wiederherstellen. Starten Sie dazu erneut den Installer von Acronis Cyber Protect Home Office. Das Installationsprogramm wird Acronis Cyber Protect Home Office automatisch erkennen und Ihnen anbieten, das Programm zu ändern oder zu entfernen.

***So können Sie Komponenten von Acronis Cyber Protect Home Office hinzufügen oder entfernen***

- Falls Sie Windows 11 verwenden, klicken Sie auf **Start** –> **Einstellungen** –> **Apps** –> **Acronis Cyber Protect Home Office** –> **Ändern**.
- Falls Sie Windows 10 verwenden, klicken Sie auf **Start** –> **Einstellungen** –> **Apps** –> **Acronis Cyber Protect Home Office** –> **Ändern**.
- Falls Sie Windows 8 verwenden, klicken Sie auf das Symbol **Einstellungen** und wählen Sie dann die Befehlsfolge **Systemsteuerung** –> **Programm deinstallieren oder ändern** –> **Acronis Cyber Protect Home Office** –> **Ändern**.
- Falls Sie Windows 7 verwenden, wählen Sie die Befehlskette **Start** –> **Systemsteuerung** –> **Programme und Funktionen –> Programm deinstallieren oder ändern** –> **Acronis Cyber Protect Home Office** –> **Ändern**.

Klicken Sie im Installer auf **Ändern**. Aktivieren oder deaktivieren Sie dann nach Bedarf die Kontrollkästchen der gewünschten Komponenten. Sie müssen Ihren Computer anschließend vermutlich neu starten, damit der Task abgeschlossen werden kann.

***So können Sie Acronis Cyber Protect Home Office vollständig deinstallieren***

- Falls Sie Windows 11 verwenden, klicken Sie auf **Start** –> **Einstellungen** –> **Apps** –> **Acronis Cyber Protect Home Office** –> **Deinstallieren**.
- Falls Sie Windows 10 verwenden, klicken Sie auf **Start** –> **Einstellungen** –> **Apps** –> **Acronis Cyber Protect Home Office** –> **Deinstallieren**.
- Falls Sie Windows 8 verwenden, klicken Sie auf das Symbol **Einstellungen** und wählen Sie dann die Befehlsfolge **Systemsteuerung** –> **Programm deinstallieren** –> **Acronis Cyber Protect Home Office** –> **Deinstalllieren**.
- Falls Sie Windows 7 verwenden, wählen Sie die Befehlskette **Start** –> **Systemsteuerung** –> **Programme und Funktionen –> Programm deinstallieren** –> **Acronis Cyber Protect Home Office** –> **Deinstallieren**.

Folgen Sie anschließend den Anweisungen auf dem Bildschirm. Sie müssen den Computer abschließend neu starten, damit der Task fertiggestellt werden kann.

**Hinweis**

Falls Sie die "Acronis Secure Zone" (S. 232) oder "Acronis Nonstop Backup" (S. 48) verwendet haben, dann bestimmen Sie in dem nun angezeigten Fenster, was mit der Zone und den Nonstop Backup Storages passieren soll.

# Acronis Cyber Protect Home Office aktivieren

Um Acronis Cyber Protect Home Office nutzen zu können, müssen Sie dieses über das Internet aktivieren. Ohne Aktivierung können Sie das Produkt für 30 Tage mit vollem Funktionsumfang nutzen. Wenn Sie es innerhalb dieses Zeitraums nicht aktivieren, steht Ihnen anschließend nur noch die Programmfunktion 'Recovery' (Wiederherstellung) zur Verfügung. Wenn Ihr Computer zum ersten Mal mit dem Internet verbunden wird und Sie sich mit Ihrem Anmeldenamen und Kennwort an Acronis Cyber Protect Home Office anmelden, wird das Produkt automatisch aktiviert.

## Das Problem 'Zu viele Aktivierungen'

Mögliche Gründe für das 'Zu viele Aktivierungen'-Problem

- **Sie haben die maximale Anzahl der Computer, auf denen Acronis Cyber Protect Home Office installiert ist, überschritten.**

  Beispielsweise, weil Sie eine Lizenz oder eine Seriennummer für nur einen Computer haben und versuchen, Acronis Cyber Protect Home Office auf einem zweiten Computer zu installieren.

  **Lösungen:**

  - Geben Sie eine neue Seriennummer ein. Sollten Sie noch keine haben, dann können Sie diese über den integrierten Acronis Store oder über die Acronis Website erwerben.
  - Verschieben Sie die Lizenz von Ihrem anderen Computer, auf dem das Produkt bereits aktiviert ist, auf bzw. zu Ihrem neuen Computer. Wählen Sie dazu denjenigen Computer aus, von dem aus Sie die Lizenz verschieben wollen. Beachten Sie, dass Acronis Cyber Protect Home Office auf diesem Computer deaktiviert wird.
- **Sie installieren Windows neu oder ändern die Hardware Ihres Computers.**

  Sie führen beispielsweise bei Ihrem Computer ein Upgrade Ihres Mainboards oder Prozessors durch. Die Aktivierung ging verloren, weil Acronis Cyber Protect Home Office Ihren Computer als neu betrachtet.

  **Lösung:**

  Um Acronis Cyber Protect Home Office auf Ihrem Computer erneut aktivieren zu können, wählen Sie denselben Computer aus der Liste über seinen alten (bisherigen) Namen aus.

## Ihre Abonnementlizenzen manuell verwalten

Wenn Sie eine abonnementbasierte Version von Acronis Cyber Protect Home Office verwenden, können Sie die entsprechende(n) Lizenz(en) manuell auf der Acronis Website verwalten. Sie können Folgendes tun:

- Lizenzen zwischen Ihren Computer verschieben
- Lizenzen zwischen Ihren Konten übertragen
- Eine Lizenz von einem Computer entfernen

- Produktaktivierungskonflikte lösen (inkl. dem Problem 'Zu viele Aktivierungen')
- Neue Lizenzen kaufen

***So können Sie Lizenzen verwalten***

1. Gehen Sie zu 'https://account.acronis.com/' und melden Sie sich an Ihrem Acronis Konto an.
2. Suchen Sie im Bereich '**Produkte**' den Eintrag für 'Acronis Cyber Protect Home Office' und klicken Sie dann auf **Verwalten**.

# Informationen zur Testversion

## Allgemeine Beschränkungen

Sie können mit der Testversion von Acronis Cyber Protect Home Office nur während des 30-tägigen Testzeitraums arbeiten. Dabei gibt es folgende Einschränkungen:

- Das Klonen von Laufwerken ist deaktiviert.
- Beim Starten mit einem Acronis Boot-Medium ist nur die Aktion 'Recovery' (Wiederherstellung) verfügbar.

## Synchronisierung

Die Möglichkeit zur Datensynchronisierung ist ohne Einschränkung verfügbar, aber nach Ablauf des Testzeitraums gilt:

- Ihr Computer wird von allen Synchronisierungen (Syncs) ausgeschlossen. Wenn Sie die Vollversion von Acronis Cyber Protect Home Office aktiviert, können Sie sich mit den verwendeten Synchronisierungen wieder verbinden.
- Alle Versionen der synchronisierten Dateien werden aus der Acronis Cloud dauerhaft gelöscht.

## Acronis Cloud

Für den Testzeitraum stehen Ihnen 1000 GB Cloud-Speicherplatz zur Verfügung. Sie können diesen Speicherplatz verwenden, um Ihre Online Backups, Archive und synchronisierten Dateiversionen zu speichern. Nach Ablauf des Testzeitraums funktioniert die Acronis Cloud noch für 30 Tage im Modus 'Nur Recovery'. Nach Ablauf dieses Zeitraums können Sie den Acronis Cloud Service nicht mehr verwenden und Ihre Daten werden komplett aus der Cloud gelöscht.

## Die Vollversion kaufen

Sie können die Vollversion auf der Acronis Website erwerben oder die integrierte Kauffunktion verwenden. Weitere Informationen finden Sie im Abschnitt 'Upgrade von Acronis Cyber Protect Home Office'.

# Upgrade von Acronis Cyber Protect Home Office

Wenn die Acronis Website ein Update für Acronis Cyber Protect Home Office bereitstellt, können Sie dieses herunterladen. Wenn Sie Acronis True Image (2017 oder höher) bereits installiert haben, wird die neue Version ein direktes Update durchführen. In diesem Fall ist es also nicht notwendig, die ältere Version zu entfernen und erst dann die neue Version zu installieren. Wenn die von Ihnen aktuell verwendete Version jedoch älter (als die genannten Versionen) ist, empfehlen wir Ihnen, Ihre vorliegende Version zuerst zu entfernen, bevor Sie die neue aufspielen.

Backups, die Sie mit einer früheren Version von Acronis Cyber Protect Home Office erstellt haben, sind vollständig mit neueren bzw. dieser aktuellen Produktversionen kompatibel. Nach Beendigung des Upgrade-Prozesses werden Ihre gesamten Backups automatisch in die Backup-Liste der neuen Programmversion aufgenommen.

Backups, die mit einer neueren Programmversion erstellt werden, können zu früheren (älteren) Versionen inkompatibel sein. Wenn Sie Acronis Cyber Protect Home Office auf eine frühere Version zurücksetzen, müssen Sie dann vermutlich auch Ihre Backups mit der älteren Version neu erstellen. Wir empfehlen daher dringend, dass Sie nach jedem Upgrade von Acronis Cyber Protect Home Office auch ein neues Boot-Medium erstellen.

***So können Sie die Vollversion erwerben***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Konto** und dann auf **Vollversion kaufen**. Die integrierte Kaufmöglichkeit (Store) wird geöffnet.
3. Wählen Sie die Lizenz, die Sie erwerben möchten, und klicken Sie dann auf **Jetzt kaufen**.
4. Geben Sie Ihre Zahlungsinformationen an.

***So können Sie Acronis Cyber Protect Home Office aktualisieren***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Konto**.
   Falls eine neue Version verfügbar ist, wird Ihnen neben der aktuellen Build-Nummer eine entsprechende Meldung angezeigt.
3. Klicken Sie auf **Herunterladen und installieren**.

   **Hinweis**
   Stellen Sie vor dem Download sicher, dass Ihre Firewall den Download-Vorgang nicht blockieren wird.

4. Klicken Sie nach dem Download der neuen Version auf **Jetzt installieren**.

Wenn Sie die automatische Prüfung auf Updates nutzen wollen, gehen Sie zur Registerkarte **Einstellungen** und aktivieren Sie dort das Kontrollkästchen **Beim Start automatisch auf Updates prüfen**.

## Integrierte Kaufmöglichkeit

Acronis Cyber Protect Home Office stellt Ihnen einen integrierten Shop in Form einer 'In-App'-Kaufmöglichkeit zur Verfügung. Über diesen Shop können Sie:

- Die Vollversion von Acronis Cyber Protect Home Office kaufen.
- Ein Acronis Cyber Protect Home Office-Abonnement kaufen.
- Mehr Speicherplatz in der Acronis Cloud kaufen.

Sie können auf den In-App-Shop zugreifen, wenn Sie in der Registerkarte **Konto** auf **Acronis Store** klicken. Dort wird Ihnen der In-App-Shop mit allen verfügbaren Kaufoptionen angezeigt.

# Technischer Support

Falls Sie Unterstützung für Acronis Cyber Protect Home Office brauchen, gehen Sie zu https://www.acronis.com/support/.

# Erste Schritte

## Sprache für die Benutzeroberfläche

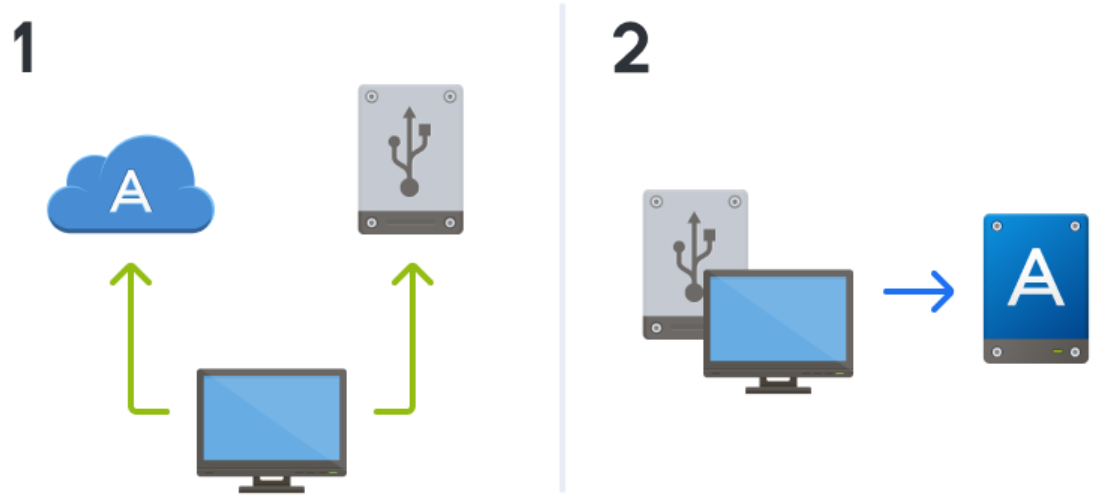
Legen Sie direkt zu Beginn Ihre bevorzugte Sprache für die Benutzeroberfläche von Acronis Cyber Protect Home Office fest. Standardmäßig ist diejenige Sprache vorausgewählt, die in Ihrem Windows-Betriebssystem als Anzeigesprache festgelegt ist.

***So können Sie die Sprache der Benutzeroberfläche ändern:***

1. Acronis Cyber Protect Home Office starten.
2. Wählen Sie im Programmbereich **Einstellungen** die von Ihnen bevorzugte Sprache aus der angezeigten Liste aus.

## Ihr System schützen

1. Sichern Sie Ihren Computer per Backup.
2. Erstellen Sie ein Acronis Boot-Medium.




Wir empfehlen Ihnen, das Boot-Medium zu testen (wie im Abschnitt 'So stellen Sie sicher, dass Ihr Boot-Medium bei Bedarf auch funktioniert' beschrieben).

### Backup Ihres Computers

***Wann sollte ich meinen Computer per Backup sichern?***

Erstellen Sie eine neue Backup-Version nach jedem signifikanten 'Ereignis', das in Ihrem System aufgetreten ist.

Beispiele für solche Ereignisse sind:

- Sie haben einen neuen Computer gekauft.
- Sie haben Windows auf Ihrem Computer neu installiert.
- Sie haben die Systemeinstellungen (beispielsweise für Zeit, Datum, Sprache) geändert und alle notwendigen Programme auf Ihrem neuen Computer installiert.
- Wichtige System-Updates.

**Hinweis**
Um sicherzustellen, dass Sie ein Laufwerk in einem fehlerfreien Zustand sichern, ist es empfehlenswert, dieses vor dem Backup auf Viren zu überprüfen. Verwenden Sie dafür ein entsprechendes Antivirus-Programm. Beachten Sie, dass diese Aktion eine beträchtliche Zeit benötigen kann.

***Wie erstelle ich ein Backup meines Computers?***

Es stehen zwei Optionen zur Verfügung, wenn Sie Ihr System schützen wollen:

- **Ein 'Backup des kompletten PCs' (empfohlen)**
  Hierbei sichert Acronis Cyber Protect Home Office alle vorhandenen internen Festplattenlaufwerke im sogenannten Laufwerk-Modus. Dieses Backup enthält dann das Betriebssystem, alle installierten Programme, alle Systemeinstellungen und all Ihre persönlichen Daten (Fotos, Musikdateien und Dokumente eingeschlossen). Weitere Informationen finden Sie im Abschnitt 'Alle Daten auf Ihrem PC sichern'.
- **Ein 'Backup des System-Laufwerks'**
  Sie können bei dieser Backup-Art zudem wählen, ob nur das System-Volume oder das komplette System-Laufwerk gesichert werden soll. Weitere Informationen finden Sie im Abschnitt 'Backup von Laufwerken und Volumes'.

Wir empfehlen nicht, dass Sie für die Sicherung Ihres System vorrangig das Nonstop Backup verwenden. Denn diese Technologie ist primär für den Schutz von häufig geänderten Dateien ausgelegt. Um die Sicherheit Ihres Systems zu gewährleisten, sollten Sie stattdessen eine der anderen Planungsvarianten verwenden. Beispiele finden Sie im Abschnitt '"Beispiele für benutzerdefinierte Schemata" (S. 74)'. Weitere Informationen über die Nonstop Backup-Funktion finden Sie im Abschnitt '"Acronis Nonstop Backup" (S. 48)'.

***So können Sie Ihre Computer per Backup sichern***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Backup**.
   Falls dies Ihr erstes Backup ist, wird Ihnen der Bildschirm zur Backup-Konfiguration angezeigt. Falls Sie bereits einige Backups in der Backup-Liste haben, klicken Sie auf **Backup hinzufügen**.
3. Klicken Sie auf das Symbol **Backup-Quelle** und wählen Sie **Kompletter PC**.
   Falls Sie nur Ihr System-Laufwerk sichern wollen, klicken Sie auf **Laufwerke und Volumes**. Wählen Sie anschließend Ihr System-Volume (hat normalerweise den Laufwerksbuchstaben C:) sowie das Volume 'System-reserviert' aus (sofern vorhanden).

4. Klicken Sie auf das Symbol für **Backup-Ziel** und wählen Sie den Speicherplatz für das Backup (vergleiche die unteren Empfehlungen).
5. Klicken Sie auf **Backup jetzt**.

Daraufhin wird in der Backup-Liste eine neue Backup-Box angezeigt. Wenn Sie später eine neue Version dieses Backups erstellen wollen, wählen Sie einfach die entsprechende Backup-Box in der Liste aus und klicken Sie auf **Backup jetzt**.

***Wo sollte ich meine Laufwerk-Backups speichern?***

- **Gut** – Ihre normale interne Festplatte.
- **Besser** – Die Acronis Secure Zone. Dabei handelt es sich um ein spezielles, geschütztes Volume auf einem Ihrer lokalen Festplattenlaufwerke, welches besonders auf die Speicherung von Backups ausgelegt ist.
- **Die Beste** – Die Acronis Cloud oder eine externe Festplatte.

Weitere Informationen finden Sie im Abschnitt 'So entscheiden Sie, wo Sie Ihre Backups speichern'.

***Wie viele Backup-Versionen benötige ich?***

Sie benötigen in den meisten Fällen 2-3 (maximal 4-6) Backup-Versionen Ihres kompletten PCs (bzw. seiner Inhalte) oder des System-Laufwerks (siehe weiter oben zu Informationen darüber, wann Backups erstellt werden sollten). Sie können die Anzahl der Backup-Versionen mithilfe automatischer Bereinigungsregeln steuern. Weitere Informationen finden Sie im Abschnitt 'Benutzerdefinierte Schemata'.

Beachten Sie, dass die erste Backup-Version (die Voll-Backup-Version) die wichtigste ist. Diese ist auch die größte, weil Sie alle auf dem Laufwerk gespeicherten Daten enthält. Nachfolgende Backup-Versionen (die inkrementellen und differentiellen Backup-Versionen) können zudem nach bestimmten Schemata organisiert sein. Diese Versionen enthalten nur Daten, die geändert wurden. Dies ist der Grund, warum sie von der Voll-Backup-Version abhängig sind – und folglich die Voll-Backup-Version so wichtig ist.

Ein Laufwerk-Backup wird standardmäßig mit dem Schema 'Inkrementell' erstellt. In den meisten Fällen ist dieses Schema optimal.

**Hinweis**
Für erfahrene Benutzer: es ist eine gute Idee, 2-3 Voll-Backup-Versionen zu erstellen und diese auf unterschiedlichen Speichergeräten zu hinterlegen. Diese Methode ist sehr zuverlässig.

## Ein Acronis Boot-Medium erstellen

Ein Acronis Boot-Medium ist eine CD, eine DVD, ein USB-Stick oder ein anderes Wechselmedium, von dem Sie Acronis Cyber Protect Home Office ausführen können, wenn Windows selbst nicht mehr starten kann. Sie können einen solchen Datenträger durch Verwendung des Acronis Media Builder bootfähig machen.

***So können Sie ein Acronis Boot-Medium erstellen***

1. Legen Sie eine beschreibbare CD/DVD ein oder schließen Sie ein bootfähiges USB-Laufwerk (ein USB-Stick oder eine externe HDD/SSD) an.
2. Acronis Cyber Protect Home Office starten.
3. Klicken Sie in der Seitenleiste auf **Extras** und dann auf **Rescue Media Builder**.
4. Wählen Sie im ersten Schritt den Eintrag **Einfach**.
5. Wählen Sie das Gerät, das zum Erstellen des Boot-Mediums verwendet werden soll.
6. Klicken Sie auf **Fertigstellen**.

***So können Sie ein Acronis Boot-Medium verwenden***

Verwenden Sie das Acronis Boot-Medium, um Ihren Computer wiederherzustellen, wenn Windows nicht mehr startfähig ist.

1. Verbinden Sie das Boot-Medium mit Ihrem Computer (legen Sie die CD bzw. DVD ein oder schließen Sie das USB-Laufwerk an).
2. Konfigurieren Sie die Boot-Reihenfolge in Ihrem BIOS so, dass das Gerät/Laufwerk Ihres Acronis Boot-Mediums das primäre Boot-Gerät ist.
   Weitere Informationen finden Sie im Abschnitt 'Boot-Reihenfolge im BIOS arrangieren'.
3. Starten Sie Ihren Computer mit dem Boot-Medium – und wählen Sie dann den Eintrag **Acronis Cyber Protect Home Office**.
   Sobald Acronis Cyber Protect Home Office gestartet wurde, können Sie es verwenden, um Ihren Computer wiederherzustellen.

Ausführlichere Informationen finden Sie im Abschnitt 'Acronis Media Builder'.

# Alle Daten auf Ihrem PC sichern

***Was ist das Backup eines kompletten PCs?***

Ein Backup des kompletten PCs ist die einfachste Möglichkeit, alle Inhalte Ihres Computers zu sichern. Wir empfehlen die Verwendung dieser Option, wenn Sie sich nicht sicher sind, welche Ihrer Daten per Backup geschützt werden müssen. Falls Sie lediglich Ihr System-Volume sichern wollen, dann informieren Sie sich im Abschnitt 'Backup von Laufwerken und Volumes'.

Wenn Sie den Backup-Typ 'Kompletter PC' auswählen, sichert Acronis Cyber Protect Home Office alle vorhandenen internen Festplattenlaufwerke im sogenannten Laufwerk-Modus. Dieses Backup enthält dann das Betriebssystem, alle installierten Programme, alle Systemeinstellungen und all Ihre persönlichen Daten (Fotos, Musikdateien und Dokumente eingeschlossen).

Die Wiederherstellung von einem solchen Backup des kompletten PCs ist ebenfalls eine vereinfachte Prozedur. Sie müssen lediglich das Datum auswählen, auf das hin Ihre Daten zurückgesetzt werden. Acronis Cyber Protect Home Office stellt alle Daten aus dem Backup an den jeweiligen ursprünglichen Speicherorten wieder her. Beachten Sie, dass Sie weder bestimmte Laufwerke bzw. Volumes wiederherstellen noch das vorgegebene Wiederherstellungsziel ändern können. Falls Sie diese Beschränkungen vermeiden wollen, empfehlen wir, dass Sie Ihre Daten mit

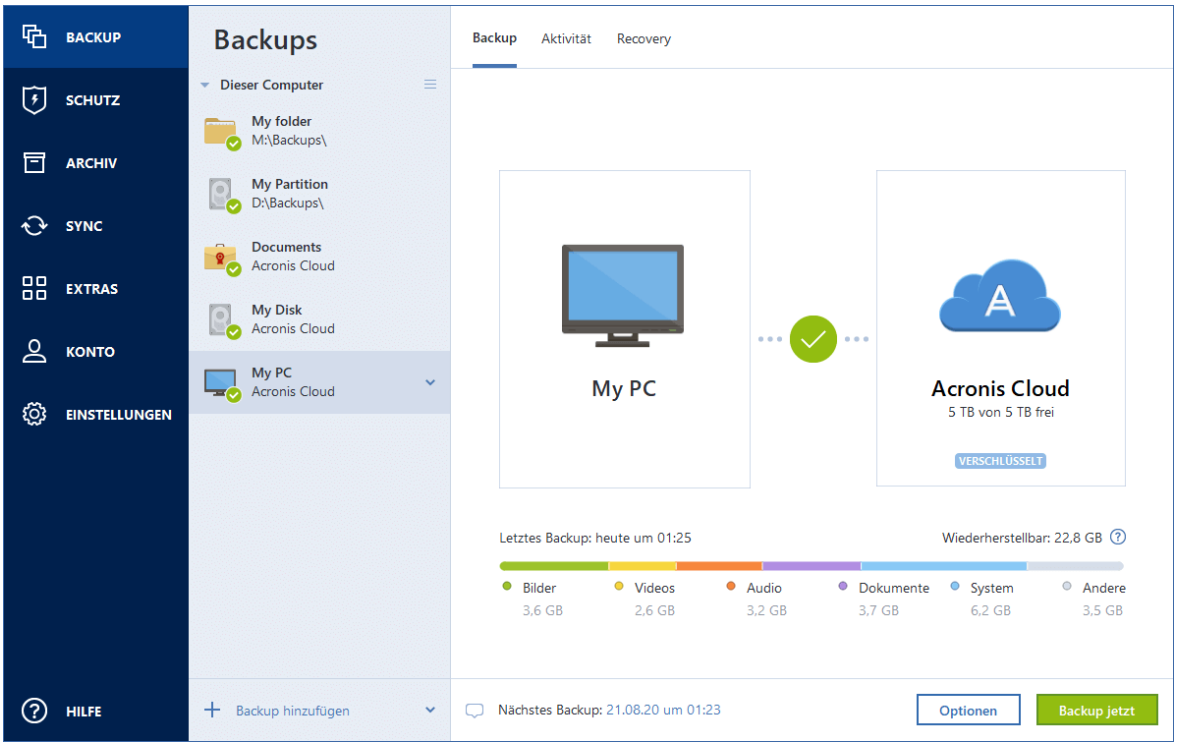
einer gewöhnlichen Laufwerk-Backup-Methode sichern. Weitere Informationen finden Sie im Abschnitt 'Backup von Laufwerken und Volumes'.

Sie können außerdem auch einzelne Dateien und Ordner aus einem 'Backup des kompletten PCs' wiederherstellen. Weitere Informationen finden Sie im Abschnitt 'Backup von Dateien und Ordnern'.

Falls ein Backup des kompletten PCs dynamische Datenträger enthält, stellen Sie Ihre Daten im Volume-Modus wieder her. Das bedeutet, dass Sie die wiederherzustellenden Volumes auswählen und das Recovery-Ziel ändern können. Weitere Details finden Sie unter "Recovery von Laufwerken und Volumes vom Typ 'Dynamisch' oder 'GPT'".

***So können Sie ein Backup des kompletten PCs erstellen***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Backup**.
3. Klicken Sie im unteren Bereich der Backup-Liste auf das Plus-Zeichen (+).
4. Klicken Sie auf das Symbol **Backup-Quelle** und wählen Sie **Kompletter PC**.
5. Klicken Sie auf das Symbol für '**Backup-Ziel**' und wählen Sie dann einen Zielort für das Backup. Wir empfehlen, dass Sie als Backup-Ziel für Ihren Computer entweder die Acronis Cloud, einen lokalen Storage oder einen Netzwerk-Storage verwenden. Weitere Informationen finden Sie im Abschnitt 'So entscheiden Sie, wo Sie Ihre Backups speichern'.




6. [Optionaler Schritt] Klicken Sie auf **Optionen**, um die Einstellungen des betreffenden Backups zu konfigurieren. Zu weiteren Informationen siehe Backup-Optionen.
7. Klicken Sie auf **Backup jetzt**.

**Hinweis**
Wenn Sie Ihre Daten in die Acronis Cloud sichern, kann die Fertigstellung des ersten Backups eine längere Zeit in Anspruch nehmen. Spätere Backup-Prozesse werden voraussichtlich schneller ablaufen, da via Internet nur Änderungen an den Dateien gesichert werden.

Zusätzlich können Sie sich englischsprachige Video-Anleitungen unter folgender Adresse anschauen: https://goo.gl/KjW5sM.

**Siehe auch**: Der Unterschied zwischen dem Backup und Klonen eines Laufwerks

# Ein Acronis Survival Kit erstellen

Um Ihren Computer bei einem Ausfall zuverlässig wiederherstellen zu können, benötigen Sie zwei wichtige Komponenten – ein Backup Ihres Systemlaufwerks und ein Acronis Boot-Medium (auch Notfallmedium genannt). Meistens liegen diese Komponenten getrennt vor – beispielsweise, weil das System-Backup auf einem externen Laufwerk oder in der Acronis Cloud Cloud vorliegt und ein kleiner USB-Stick als Boot-Medium dient. Ein Acronis Survival Kit kombiniert diese beiden Komponenten, sodass Sie ein einziges Gerät erhalten, welches alles enthält, was Sie zur Wiederherstellung Ihres Computers bei einem Ausfall benötigen. Es handelt sich um ein externes Speicherlaufwerk, welches die Dateien eines Acronis Boot-Medium sowie ein Backup Ihres System-Volumes, Ihres kompletten Computers oder eines anderen Laufwerks enthält. Darüber hinaus kann das Backup Ihrer Daten wie ein normales Backup verwendet werden: es kann alle Daten enthalten, die Sie sichern wollen, und Sie können zudem eine Planung einrichten, um es wie ein normales Backup zu aktualisieren. Da das externe Laufwerk nicht exklusiv vom Acronis Survival Kit belegt wird (denn dessen Boot-Medium benötigt nur ca. 2 GB Speicherplatz), kann der verbleibende Speicherplatz für weitere Daten genutzt werden. Dazu gehört natürlich zuerst einmal das Backup des System-Volumes bzw. des kompletten PCs, welches ein fester Bestandteil des Acronis Survival Kits ist. Darüber hinaus können Sie aber auch noch beliebige andere Daten oder Backups mit auf dem Laufwerk speichern – beispielsweise persönliche Dokumente, Fotos oder was auch immer. Sie sollten jedoch auf einem externen Laufwerk immer nur je ein Acronis Survival Kit speichern.

Egal, wie viele Backups letztendlich auf diesem externen Laufwerk gespeichert sind: für die Wiederherstellung eines Computers ist jeweils nur ein Acronis Survival Kit erforderlich. Dessen integrierte Boot-Medium-Komponente funktioniert mit jedem System-Backup (egal ob ein Backup der System-Partition oder ein Backup des kompletten PCs), solange dieses Backup nur für denselben Computer oder einen Computer mit gleicher Hardware-Konfiguration erstellt wurde.

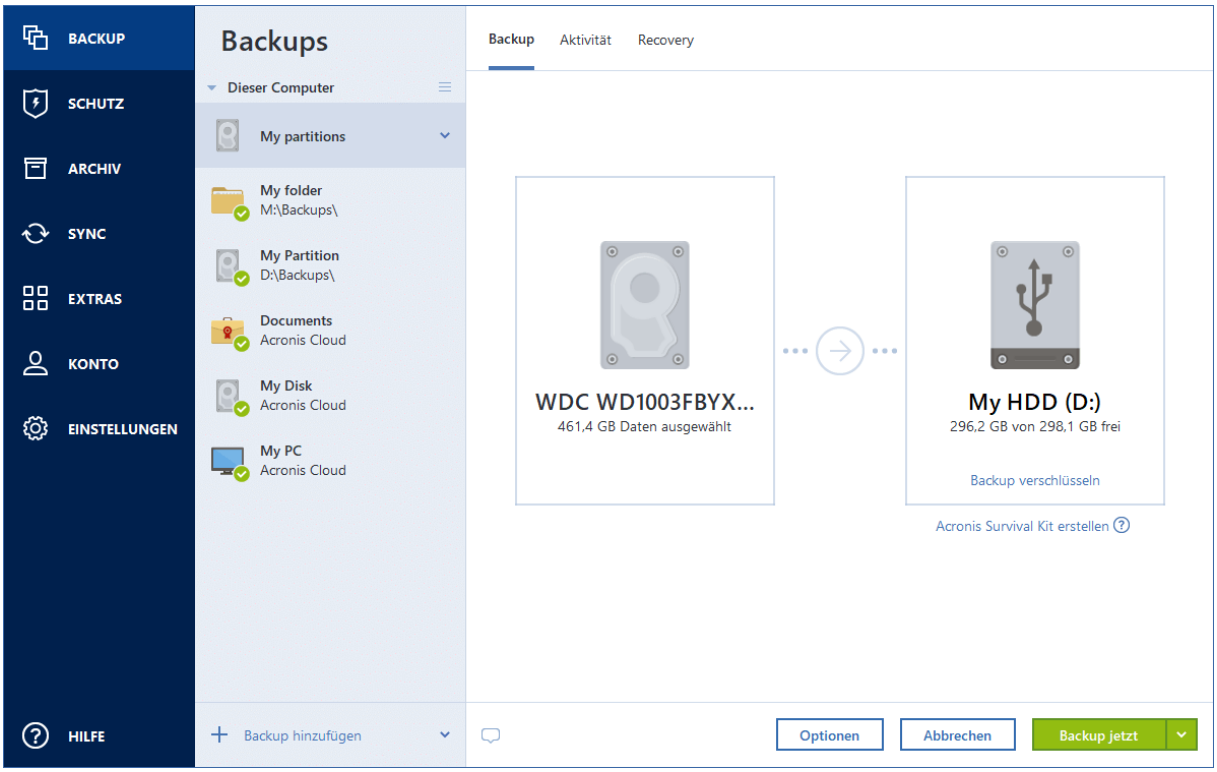
Sie können folgende Geräte als Acronis Survival Kit verwenden:

- **ein externes Festplattenlaufwerk**
  Es sollte größer als 32 GB sein und NTFS, FAT32 oder exFAT als Dateisystem verwenden. Wenn das Laufwerk ein anderes Dateisystem hat, wird Ihnen Acronis Cyber Protect Home Office vorschlagen, das Laufwerk zu formatieren.
- **einen USB-Stick (Flash-Speicher-Laufwerk)**

Es sollte sich um ein Flash-Laufwerk handeln, welches das Partitionierungsschema 'MBR' verwendet und mindestens 32 GB Speicherplatz hat. Wenn Sie ein Flash-Speicher-Laufwerk vom Typ 'GPT' einsetzen, wird Ihnen Acronis Cyber Protect Home Office vorschlagen, das Partitionierungsschema zu 'MBR' zu konvertieren. Beachten Sie, dass Flash-Speicher-Laufwerke für diesen Einsatzzweck nur für Windows 10 (Build 1703 und höher) und für Windows 11 unterstützt werden.

***So können Sie ein Acronis Survival Kit erstellen***

Wenn Sie ein Backup Ihres System-Volumes, Ihres kompletten Computers oder ein anderes Laufwerk-Backup konfigurieren und dabei ein externes Festplattenlaufwerk als Ziel auswählen, wird Ihnen Acronis Cyber Protect Home Office vorschlagen, auf diesem externen Laufwerk ein Acronis Survival Kit zu erstellen.




1. Klicken Sie auf **Backup jetzt** oder **Acronis Survival Kit erstellen**.
2. Klicken Sie im dann geöffneten Fenster auf **Erstellen**.

   Acronis Cyber Protect Home Office erstellt ein kleines Volume (Partition) auf dem ausgewählten Laufwerk und speichert in diesem Volume die Boot-Dateien. Um das Volume erstellen zu können, muss eines der bereits vorhandenen Volumes verkleinert werden. Wenn es sich nicht um ein GPT-Laufwerk handelt und es sich bei dem vorhandenen Dateisystem nicht um NTFS, FAT32 oder exFAT handelt, wird Ihnen Acronis Cyber Protect Home Office vorschlagen, das Laufwerk zu formatieren. Beachten Sie dabei, dass durch das Formatieren des Laufwerks auch alle darauf gespeicherten Daten gelöscht werden.
3. Wenn die Boot-Dateien erfolgreich auf das Laufwerk geschrieben wurden, ist das Volume zu einem Acronis Boot-Medium geworden, welches Sie zur Wiederherstellung Ihres Computers

verwenden können. Um die Erstellung des Acronis Survival Kits abzuschließen, müssen Sie noch ein Backup Ihres System-Volumes, Ihres kompletten Computers oder ein anderes Laufwerk-Backup auf dem externen Laufwerk speichern. Klicken Sie dazu auf **Backup jetzt**. Sie können diesen Schritt überspringen, müssen dann aber daran denken, noch später ein entsprechendes Backup auf dem Laufwerk zu speichern. Weitere Informationen finden Sie im Abschnitt 'Backup von Laufwerken und Volumes'.

Wenn Ihr Acronis Survival Kit fertiggestellt ist, können Sie es zur Wiederherstellung Ihres Computers verwenden. Weitere Details finden Sie im Abschnitt 'Ein System auf demselben Laufwerk wiederherstellen'.

Jedes Mal, wenn Sie ein Backup konfigurieren, welches ein externes Laufwerk mit einem Survival Kit als Ziel verwenden soll, wird Acronis Cyber Protect Home Office die Version des Survival Kits überprüfen. Wenn es eine neuere Version des Survival Kits gibt, schlägt Acronis Cyber Protect Home Office vor, das Survival Kit auf Ihrem externen Gerät zu aktualisieren.

# Backups Ihrer Dateien

Um bestimmte Dateien wie Dokumente, Fotos, Musik- und Videodateien zu schützen, ist es nicht notwendig, das komplette Volume (welches die Dateien enthält) zu sichern. Sie können bestimmte Dateien und Ordner per Backup sichern und diese auf folgenden Storage-Typen speichern:

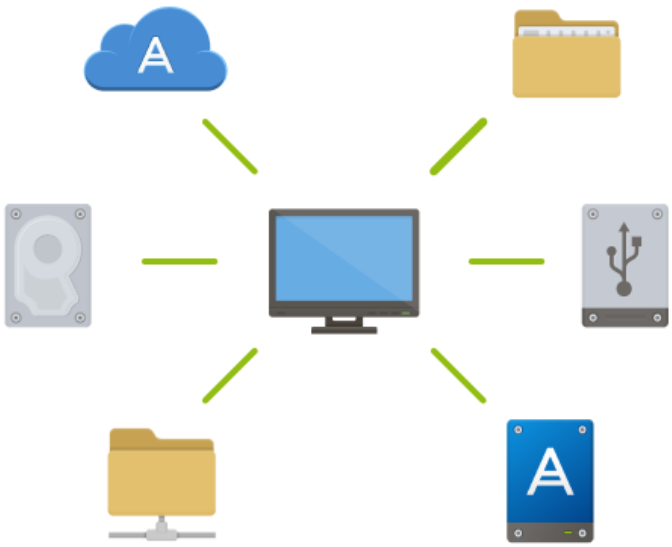
- **Lokaler oder Netzwerk-Storage**

  Diese Option ist schnell und einfach. Verwenden Sie diese Option, um Dateien zu schützen, die selten geändert werden.
- **Acronis Cloud**

  Diese Option ist besonders zuverlässig. Verwenden Sie diesen, um wichtige Dateien zu schützen – und Dateien, die Sie für andere Geräte oder Personen freigeben wollen.

  Wenn Sie die Acronis Cloud verwenden wollen, müssen Sie ein Acronis Konto und ein Abonnement für den Acronis Cloud Service haben.

  Ausführlichere Informationen finden Sie im Abschnitt '"Abonnementinformationen" (S. 37)'.



***So können Sie Backups von Dateien und Ordnern erstellen***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Backup**.
3. Klicken Sie auf das Symbol **Backup-Quelle** und wählen Sie **Dateien und Ordner**.
4. Aktivieren Sie im geöffneten Fenster die Kontrollkästchen, die neben den zu sichernden Dateien und Ordnern liegen, und klicken Sie dann auf **OK**.
5. Klicken Sie auf das Symbol für **Backup-Ziel** und wählen Sie dann einen Zielort für das Backup:
   - **Acronis Cloud** – Melden Sie sich an Ihrem Konto an und klicken Sie dann auf **OK**.
   - **Ihr externes Laufwerk** – Falls ein externes Laufwerk an Ihrem Computer angeschlossen ist, können Sie dieses aus der Liste auswählen.
   - **NAS** – Wählen Sie ein NAS-Gerät aus der Liste der gefundenen NAS-Geräte. Falls Sie nur ein (1) NAS-Gerät haben, wird Acronis Cyber Protect Home Office vorschlagen, dieses als Standardziel für Backups zu verwenden.
   - **Durchsuchen** – Wählen Sie einen Zielordner aus dem Verzeichnisbaum.
6. Klicken Sie auf **Backup jetzt**.

Weitere Informationen finden Sie im Abschnitt 'Backup von Dateien und Ordnern'.

Zusätzlich können Sie sich englischsprachige Video-Anleitungen unter folgender Adresse anschauen: https://goo.gl/i4J1AN.

# Ein Laufwerk klonen

## Warum benötige ich das?

Wenn Sie erkennen, dass der freie Speicherplatz eines Festplattenlaufwerks für Ihre Daten nicht mehr ausreicht, möchten Sie möglicherweise ein neues, größeres Laufwerk kaufen und Ihre kompletten Daten auf dieses übertragen. Eine gewöhnliche Kopier-Aktion bewirkt nicht, dass Ihr neues Laufwerk mit dem alten identisch ist. Wenn Sie beispielsweise den Windows Datei-Explorer öffnen würden, um alle Dateien und Ordner auf das neue Laufwerk zu kopieren, würde Windows von dem neuen Laufwerk nicht starten können. Das Werkzeug 'Laufwerk klonen' ermöglicht Ihnen, all Ihre Daten zu duplizieren und Windows auf dem neuen Laufwerk bootfähig zu machen.

## Bevor Sie beginnen

Wir empfehlen, dass Sie das (neue) Ziellaufwerk dort installieren (einbauen), wo Sie es später verwenden wollen. Das Quelllaufwerk sollten Sie dagegen möglichst an einem anderen Ort einbauen (beispielsweise in ein externes USB-Gehäuse). Diese ist besonders bei Notebooks wichtig.

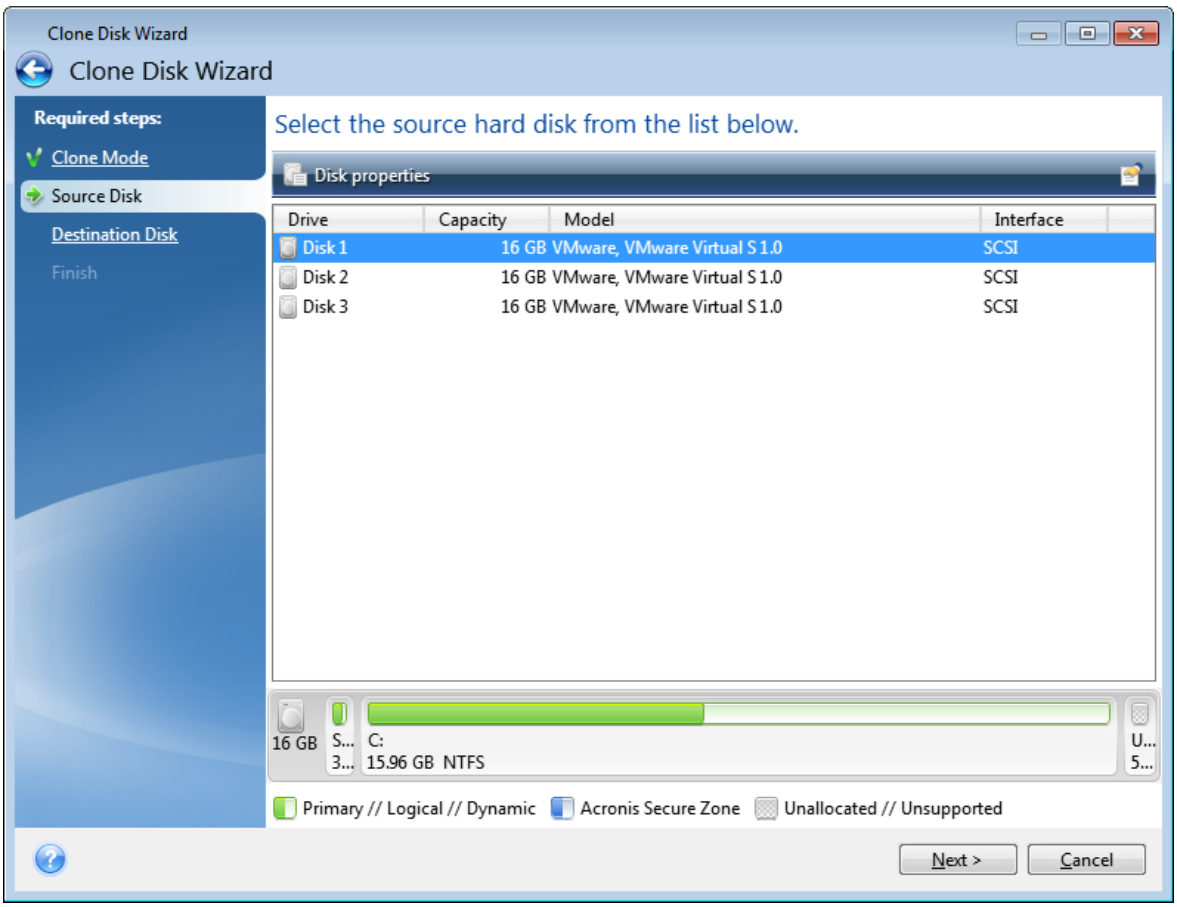
**Hinweis**
Es wird empfohlen, dass das alte und neue Laufwerk im selben 'Controller-Modus' (beispielsweise 'IDE' oder 'AHCI') arbeiten. Anderenfalls wird Ihr Computer möglicherweise nicht von dem neuen Laufwerk booten können.

## Ein Laufwerk klonen

1. Klicken Sie in der Seitenleiste auf **Extras** und dann auf **Laufwerk klonen**.
2. Wir empfehlen, dass Sie im Schritt **Modus für das Klonen** die Option **Automatisch** als Übertragungsmodus auswählen. Damit werden die Volumes so in der Größe angepasst, dass sie auf Ihr neues Laufwerk passen. Der Modus **Manuell** bietet dagegen eine höhere Flexibilität. Weitere Details zum manuellen Modus werden Ihnen im 'Laufwerk klonen'-Assistent angezeigt.

   **Hinweis**
   Wenn das Programm zwei Laufwerke findet, eins partitioniert (also mit Volumes) und das andere nicht, erkennt es automatisch das partitionierte Laufwerk als Quelle und das unpartitionierte Laufwerk als Ziel. In diesem Fall werden die nächsten Schritte übersprungen und Sie gelangen zum Fenster 'Zusammenfassung' der Aktion 'Klonen'.

3. Wählen Sie im Schritt **Quelllaufwerk** dasjenige Laufwerk aus, das Sie klonen wollen.




4. Wählen Sie im Schritt **Ziellaufwerk** dasjenige Laufwerk aus, das als Ziel für die zu klonenden Daten dienen soll.

**Hinweis**
Wenn ein vorhandenes Laufwerk unpartitioniert ist, erkennt das Programm dieses automatisch als Ziellaufwerk und überspringt den nächsten Schritt.

5. Stellen Sie im Schritt **Abschluss** sicher, dass die konfigurierten Einstellungen Ihren Vorstellungen entsprechen – und klicken Sie dann auf **Fertigstellen**.

Acronis Cyber Protect Home Office fährt in der Standardeinstellung den Computer nach Abschluss des Klon-Vorgangs herunter. Dies ermöglicht Ihnen, eines der Laufwerke zu entfernen. Bei alten IDE-Festplatten können Sie außerdem die Position der Master-/Slave-Jumper verändern.

Zusätzlich können Sie sich englischsprachige Video-Anleitungen unter folgender Adresse anschauen: https://goo.gl/bjWRLL.

# Ihren Computer wiederherstellen

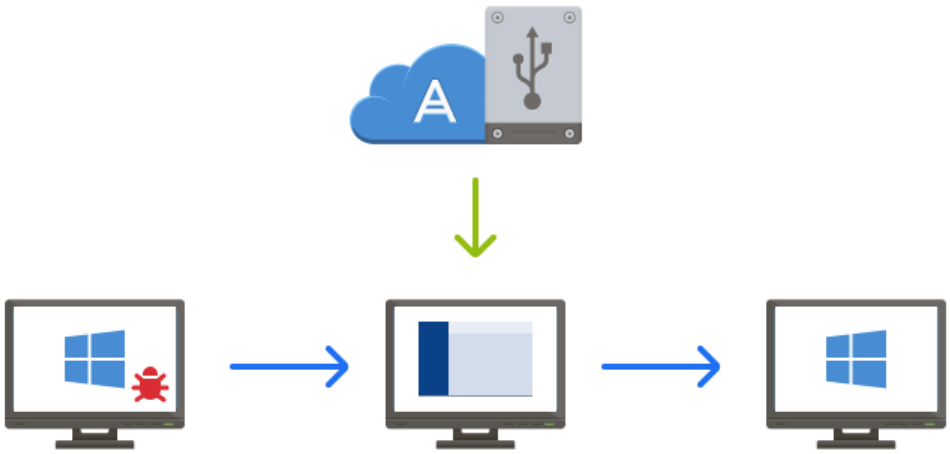
Die Wiederherstellung eines Systemlaufwerks ist eine wichtige Aktion. Wir empfehlen daher, dass Sie vor Beginn der Aktion die ausführlichen Beschreibungen folgender Hilfethemen lesen:

- Versuche zur Bestimmung der Absturzursache
- Wiederherstellung vorbereiten
- Ein System auf demselben Laufwerk wiederherstellen

Betrachten wir zwei unterschiedliche Fälle:

1. Windows funktioniert fehlerhaft, aber Sie können Acronis Cyber Protect Home Office noch starten.
2. Windows kann nicht mehr starten (Sie sehen beispielsweise beim Einschalten Ihres Computer eine ungewöhnliche Bildschirmanzeige).

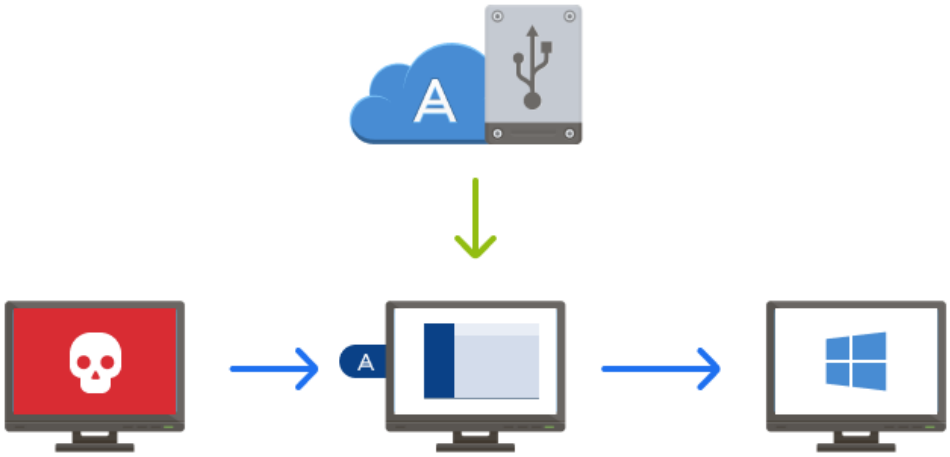
***Fall 1: Wie wird der Computer wiederhergestellt, falls Windows fehlerhaft funktioniert?***



1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Backup**.
3. Wählen Sie das Backup, welches Ihr Systemlaufwerk enthält, aus der Backup-Liste aus. Das Backup kann lokal, im Netzwerk oder in der Acronis Cloud gespeichert sein.
4. Klicken Sie im rechten Fensterbereich auf **Recovery**.
5. Klicken Sie je nach Backup-Typ entweder auf **PC wiederherstellen** oder **Laufwerke wiederherstellen**.
6. Wählen Sie im geöffneten Fenster die gewünschte Backup-Version (der Datenzustand an einem bestimmten Zeitpunkt).
7. Wählen Sie als Quelle für die Wiederherstellung das System-Volume und (sofern vorhanden) das Volume 'System-reserviert'.
8. Klicken Sie auf **Recovery jetzt**.

**Hinweis**
Acronis Cyber Protect Home Office muss Ihr System neu starten, um die Aktion abschließen zu können.

***Fall 2: Wie wird der Computer wiederhergestellt, falls Windows nicht mehr starten kann?***



1. Verbinden Sie ein Acronis Boot-Medium mit Ihrem Computer und starten Sie von diesem die spezielle autonome Notfallversion von Acronis Cyber Protect Home Office.
   Genauere Informationen finden Sie unter Schritt 2: 'Ein Acronis Boot-Medium erstellen' und 'Boot-Reihenfolge im BIOS arrangieren'.
2. Wählen Sie auf der Willkommensseite das Element **Laufwerke** (unterhalb des Elements **Recovery**).
3. Wählen Sie das Systemlaufwerk-Backup, welches für die Wiederherstellung verwendet werden soll. Klicken Sie mit der rechten Maustaste auf das Backup und wählen Sie **Recovery**.

Sollte das Backup nicht angezeigt werden, dann klicken Sie auf **Durchsuchen** und geben Sie den Pfad zum Backup manuell ein. Sie können sich im selben Fenster auch mit der Acronis Cloud verbinden und ein Online Backup auswählen. Weitere Details finden Sie im Abschnitt 'Ihr System aus der Acronis Cloud wiederherstellen'.

4. Wählen Sie im Schritt **Recovery-Methode** den Befehl **Recovery kompletter Laufwerke und Volumes**.
5. Wählen Sie in der Anzeige **Recovery-Quelle** die Systempartition aus (üblicherweise C). Beachten Sie, dass Sie das System-Volume von anderen Volumes anhand der Kennungen (Flags) 'Pri.' und 'Akt.' unterscheiden können. Wählen Sie auch das Volume 'System-reserviert' aus, sofern es vorhanden ist.
6. Sie können alle Einstellungen der Volumes (Partitionen) unverändert übernehmen und dann auf **Abschluss** klicken.
7. Überprüfen Sie die Zusammenfassung der Aktionen und klicken Sie dann auf **Fertigstellen**.
8. Beenden Sie nach Abschluss der Aktion die autonome Notfallversion von Acronis Cyber Protect Home Office, entnehmen Sie das Boot-Medium (sofern vorhanden) und booten Sie das eben wiederhergestellte System-Volume. Wenn Sie sich vergewissert haben, dass Sie Windows zu dem von Ihnen gewünschten Stadium wiederhergestellt haben, können Sie die ursprüngliche Boot-Reihenfolge im BIOS wieder einrichten.

# Acronis Konto

Sie benötigen ein Acronis Konto, um folgende Aktionen durchführen zu können:

- Ein Acronis Produkt zu registrieren.
- Backups in die Acronis Cloud zu erstellen.
- Ihre Daten zu synchronisieren.
- Ihre Daten zu archivieren.

***So können Sie ein Acronis Konto erstellen***

1. Klicken Sie in der Seitenleiste auf **Konto** und dann auf **Anmelden oder ein Konto erstellen**.
2. Klicken Sie auf **Ein Konto erstellen**.
3. Füllen Sie das Registrierungsformular aus. Geben Sie die erforderlichen Daten ein, akzeptieren Sie die Nutzungsbedingungen und melden Sie sich optional an, wenn Sie gelegentlich News und Werbeangebote erhalten wollen.

   **Hinweis**
   Damit Ihre persönlichen Daten geschützt sind, sollten Sie ein sicheres Kennwort für Ihre Online Backups festlegen; sorgen Sie dafür, dass es nicht in falsche Hände gerät und ändern Sie es von Zeit zu Zeit.

4. Klicken Sie auf **Konto erstellen**.

5. Es wird eine E-Mail-Nachricht wird an die von Ihnen spezifizierte Adresse gesendet. Öffnen Sie diese Nachricht und bestätigen Sie Ihren Wunsch, ein Konto zu erstellen.

***So können Sie sich mit Ihrem Acronis Konto anmelden***

1. Klicken Sie in der Seitenleiste auf **Konto** und dann auf **Anmelden oder ein Konto erstellen**.
2. Geben Sie Ihre Registrierungsdaten (E-Mail-Adresse und Kennwort) ein und klicken Sie dann auf **Anmelden**.

***So können Sie sich von Ihrem Acronis Konto abmelden:***

1. Klicken Sie in der Seitenleiste auf **Konto**.
2. Klicken Sie auf Ihre E-Mail-Adresse und wählen Sie dann den Befehl **Abmelden**.

# Erste Schritte mit der Acronis Cloud

**Hinweis**
Acronis Cloud ist möglicherweise in Ihrer Region nicht verfügbar. Für weitere Informationen klicken Sie hier: https://kb.acronis.com/content/4541

## Remote-Storage

Die Acronis Cloud ist ein geschützter Remote-Storage (entferntes Speichersystem), den Sie zur Sicherung folgender Daten verwenden können:

- Backups Ihrer Dateien und Ordner
- Backups Ihrer Volumes (Partitionen) und Laufwerke
- Versionen Ihrer synchronisierten Dateien und Ordner

Da die Dateien auf einem Remote-Storage vorliegen, sind diese selbst dann noch geschützt, wenn Ihr Computer gestohlen wurde oder Ihr Haus niederbrennen sollte. Sie können Ihre Dateien und sogar die kompletten Inhalte Ihres Computers wiederherstellen, falls es zu einem Desaster oder einer Datenbeschädigung kommen sollte.

Sie können mit einem Konto die Daten mehrerer Computer und all Ihrer Mobilgeräte (die mit den Betriebssystemen iOS oder Android laufen) sichern.

Um die Acronis Cloud verwenden zu können, benötigen Sie ein Abonnement für den entsprechenden Service. Weitere Informationen finden Sie im Abschnitt 'Abonnementinformationen'.

## Webapplikation

Die Acronis Cloud ist zudem eine Webapplikation, die es Ihnen ermöglicht, in der Acronis Cloud gespeicherte Daten wiederherzustellen und zu verwalten. Um mit der Anwendung zu arbeiten, können Sie einen beliebigen Computer verwenden, der mit dem Internet verbunden ist.

Wenn Sie auf die Applikation zugreifen wollen, können Sie zu https://www.acronis.com/my/online-backup/webrestore/ gehen und Sie sich dann an Ihrem Acronis Konto anmelden.

## So gewährleisten wir die Sicherheit Ihrer Daten

Wenn Sie die Acronis Cloud als Storage verwenden, wollen Sie sicher gewährleisten, dass Ihre persönlichen Dateien nicht in falsche Hände geraten können. Das kann insbesondere für die Daten auf Ihrem Mobilgerät gelten, da all Ihre Daten über das Internet übertragen werden.

Seien Sie versichert, dass all Ihre Daten geschützt sind. Zuerst einmal verwenden wir für die Datenübertragung im Internet und LAN entsprechende Verschlüsselungsprotokolle (SSL, TLS). Um auf die Daten zugreifen zu können, müssen Sie sich an Ihrem Konto unter Angabe Ihrer E-Mail-Adresse und einem Kennwort anmelden. Zweitens können Sie festlegen, dass die Sicherung Ihrer Daten nur über eine geschützte WLAN-Verbindung erfolgen soll. Dadurch können Sie gewährleisten, dass die Daten bei der Übertragung in die Acronis Cloud komplett geschützt sind. Wählen Sie die gewünschten sicheren **WLAN-Verbindungen für Backup** in den **Einstellungen**.

## Abonnementinformationen

Einige Funktionen von Acronis Cyber Protect Home Office (wie Online Backup, Cloud-Archivierung und Cloud-Synchronisierung) verwenden die Acronis Cloud und benötigen daher ein Abonnement für den Acronis Cloud Storage. Wenn Sie ein entsprechendes Abonnement testen oder erwerben wollen, starten Sie Acronis Cyber Protect Home Office, wechseln Sie zur Registerkarte **Konto** und wählen Sie dort, ob Sie ein Testabonnement starten oder ein vollständiges Abonnement kaufen wollen.

**Hinweis**
Acronis Cloud unterliegt unserer Richtlinie zur fairen Nutzung (Fair Usage Policy). Weitere Informationen finden Sie unter https://kb.acronis.com/ati/fairusage.

***Testversion***

Wenn Sie die Testversion des Produktes aktivieren, wird Ihrem Konto automatisch ein kostenloses Acronis Cloud-Abonnement inkl. 1000 GB Cloud-Speicherplatz für die Dauer Ihres Acronis Cyber Protect Home Office-Testzeitraums zugewiesen. Details finden Sie unter 'Informationen zur Testversion'.

***Vollversion:***

Sie können das vollständige Acronis Cloud-Abonnement entwedert im Bereich **Konto** Ihrer Acronis Cyber Protect Home Office-Version erwerben – oder über die Acronis Website. Weitere Informationen finden Sie im Abschnitt 'Upgrade von Acronis Cyber Protect Home Office'.

# Grundlegende Konzepte

Dieser Abschnitt bietet allgemeine Informationen zu den grundlegenden Konzepten, die Ihnen helfen sollen zu verstehen, wie das Programm funktioniert.

***Backup und Recovery***

Der Begriff **Backup** bezieht sich auf die Erstellung von Daten-Kopien, damit diese zusätzlichen Kopien dazu verwendet werden können, diese Daten nach einem Datenverlust **wiederherzustellen**.

Backups haben in erster Linie zwei Funktionen:

- Um ein Betriebssystem wiederherzustellen, wenn es beschädigt ist oder nicht mehr starten kann (auch 'Disaster Recovery' genannt). Weitere Details zum Schutz Ihres Computers vor einem Desaster finden Sie im Abschnitt 'Ihr System schützen'.
- Um bestimmte Dateien und Ordner wiederherzustellen, nachdem diese versehentlich gelöscht oder beschädigt wurden.

Acronis Cyber Protect Home Office ist für beide Funktionen geeignet; es erstellt sowohl Images von Laufwerken (oder Volumes) als auch Backups auf Dateiebene.

Recovery-Methoden:

- Ein **Vollständiges Recovery** kann zum ursprünglichen oder einem neuen Speicherort durchgeführt werden.

  Wird der ursprüngliche Speicherort ausgewählt, so werden die Daten an diesem Speicherort durch die Daten aus dem Backup vollständig überschrieben. Wird ein neuer Speicherort ausgewählt, so werden die Daten aus dem Backup einfach nur zu diesem neuen Speicherort kopiert.
- Ein **Inkrementelles Recovery** kann nur zum ursprünglichen Speicherort und nur aus einem Cloud Backup durchgeführt werden. Bevor die Wiederherstellung startet, werden die Dateien am ursprünglichen Speicherort mit den Dateien im Backup anhand von Dateiattributen (wie Dateigröße und letztes Änderungsdatum) verglichen. Dateien, die nicht übereinstimmen, werden als 'wiederherzustellen' gekennzeichnet, während die übrigen Dateien bei der Wiederherstellung übersprungen werden. Anders als bei der vollständigen Wiederherstellung stellt Acronis Cyber Protect Home Office dabei nur Dateien wieder her, die seit dem Backup verändert wurden. Mit dieser Methode lässt sich bei Wiederherstellungen aus der Acronis Cloud die Wiederherstellungszeit und über das Internet übertragene Datenmenge deutlich reduzieren.

***Backup-Versionen***

Eine Backup-Version besteht aus einer oder mehrere Dateien, die als Ergebnis einer Backup-Aktion erstellt werden. Die Anzahl der erstellten Versionen entspricht der Häufigkeit, mit der das Backup ausgeführt wurde. Eine Version repräsentiert daher jeweils einen Zeitpunkt, auf den ein System oder Daten zurückgesetzt werden können – und zwar durch Wiederherstellung aus einem Backup.

Backup-Versionen entsprechen vollständigen, inkrementellen und differentiellen Backups – siehe 'Vollständige, inkrementelle und differentielle Backups'.

Backup-Versionen sind ähnlich zu Dateiversionen. Das Konzept der Dateiversionen dürfte Anwendern von Windows bekannt sein, da es hier eine Funktion namens 'Vorherige Dateiversionen' gibt (auch 'Vorgängerversionen' genannt). Diese Funktion ermöglicht Ihnen, eine Datei in dem Zustand wiederherzustellen, in der sie zu einem bestimmten Zeitpunkt und Datum vorlag. Eine Backup-Version erlaubt Ihnen die Wiederherstellung Ihrer Daten auf vergleichbare Art.

***Laufwerk klonen***

Diese Aktion kopiert den gesamten Inhalt eines Laufwerks auf ein anderes. Das kann beispielsweise notwendig werden, wenn Sie Ihr Betriebssystem (inkl. Anwendungen und Daten) auf ein neues Laufwerk mit größerer Kapazität klonen wollen. Sie können dies auf zwei Arten tun:

- Verwenden Sie das Werkzeug 'Laufwerk klonen'.
- Erstellen Sie ein Backup Ihres alten Laufwerks und stellen Sie dieses dann auf dem neuen Laufwerk wieder her.

***Format der Backup-Datei***

Acronis Cyber Protect Home Office speichert Backup-Daten im proprietären TIBX-Format unter Verwendung einer Kompression. Daten aus .tibx-Backup-Dateien können nur mit Acronis Cyber Protect Home Office unter Windows oder in einer Wiederherstellungsumgebung (also mit einem Boot-Medium) wiederhergestellt werden.

Acronis Nonstop Backup verwendet einen speziellen, versteckten Storage für Daten und Metadaten. Die gesicherten Daten werden komprimiert und in Dateien von ungefähr 1 GByte aufgeteilt. Diese Dateien haben zudem ein proprietäres Format; die in ihnen enthaltenen Daten können nur mithilfe von Acronis Cyber Protect Home Office wiederhergestellt werden.

***Backup-Validierung***

Mit der Funktion 'Backup-Validierung' können Sie prüfen, ob Ihre Daten zu einem späteren Zeitpunkt wiederhergestellt werden können. Das Programm fügt allen gesicherten Datenblöcken Prüfsummen hinzu. Während einer Backup-Validierung öffnet Acronis Cyber Protect Home Office die Backup-Datei, berechnet die Prüfsumme neu und vergleicht die ermittelten mit den gespeicherten Werten. Stimmen alle verglichenen Werte überein, dann ist die Backup-Datei nicht beschädigt.

***Planung***

Damit Ihre Backups auch wirklich hilfreich sind, sollten diese so aktuell wie möglich sein. Planen Sie Ihre Backups, um diese automatisch und regelmäßig ausführen zu können.

***Backups löschen***

Wenn Sie nicht mehr benötigte Backup-Versionen löschen wollen, empfehlen wir Ihnen dringend, dies nur mit den von Acronis Cyber Protect Home Office dafür bereitgestellten Werkzeugen durchzuführen.Weitere Details finden Sie im Abschnitt 'Backups und Backup-Versionen löschen'.

Acronis Cyber Protect Home Office speichert Informationen über Backups in einer Datenbank für Metadaten-Informationen. Wenn Sie nicht mehr benötigte Backup-Dateien daher einfach in einem Windows-Dateimanager (wie dem Windows Explorer) löschen, werden die Metadaten-Informationen dieser Backups nicht auch aus der Datenbank entfernt. Das führt zu Fehlern, wenn das Programm versucht, Aktionen mit nicht mehr existierenden Backups auszuführen.

# Unterschied zwischen dateibasierten Backups und Images von Laufwerken/Volumes

Wenn Sie Dateien und Ordner sichern, werden nur diese Dateien und ihr Verzeichnisbaum komprimiert und gespeichert.

Die Backups von Laufwerken/Volumes (Partitionen) unterscheiden sich von Datei-/Ordner-Backups. Acronis Cyber Protect Home Office speichert einen exakten Snapshot (Schnappschuss) des Laufwerks bzw. Volumes. Dieses Verfahren wird 'Erstellen eines Disk-Images' oder 'Erstellen eines Laufwerk-Backups' genannt. Das resultierende Backup wird üblicherweise als 'Laufwerk-/Volume-Image' oder 'Laufwerk-/Volume-Backup' bezeichnet.

***Welche Daten sind in einem Laufwerk-/Volume-Backup enthalten?***

Ein Laufwerk-/Volume-Backup enthält alle auf dem entsprechenden Laufwerk bzw. Volume gespeicherten Daten:

1. Die Spur Null (Track Zero) des Festplattenlaufwerks mit dem Master Boot Record (MBR, gilt nur für Backups von MBR-Laufwerken).
2. Ein oder mehrere Volumes (Partitionen). Dazu gehören auch folgende Elemente:
   a. Boot-Code.
   b. Dateisystem-Metadaten (inkl. Dienstdateien), die FAT (File Allocation Table, Dateizuordnungstabelle) und der Boot-Record (Startdatensatz) eines Volumes.
   c. Dateisystemdaten, einschließlich des Betriebssystems (mit Systemdateien, Registry, Treiber), der Benutzerdaten und Software-Anwendungen.
3. Das Volume 'System-reserviert' (sofern vorhanden).
4. EFI-System-Volume (sofern vorhanden) (gilt nur für Backups von GPT-Laufwerken).

***Welche Daten werden von Laufwerk-Backups ausgeschlossen?***

Um die Größe des Images zu reduzieren und seine Erstellung zu beschleunigen, speichert Acronis Cyber Protect Home Office standardmäßig nur solche Festplattensektoren, die auch Daten enthalten.

Folgende Dateien werden von Acronis Cyber Protect Home Office von einem Laufwerk-Backup ausgeschlossen:

- pagefile.sys
- hiberfil.sys (eine Datei, die den Inhalt des Hauptspeichers bewahrt, wenn der Computer in den Ruhezustand wechselt)

Sie können diese Standardmethode ändern, indem Sie den Sektor-für-Sektor-Modus einschalten. In diesem Fall kopiert Acronis Cyber Protect Home Office alle Festplattensektoren – also nicht nur solche, die auch Daten enthalten.

Wenn Sie Ihr System-Volume/-Laufwerk in die Acronis Cloud Cloud sichern, werden dabei folgende Daten von Acronis Cyber Protect Home Office ausgeschlossen:

- Der Ordner 'Temp', der folgenden üblichen Speicherort hat:
  - C:\Windows\Temp\
  - C:\Benutzer\<Benutzername>\AppData\Local\Temp
- Der Ordner 'System Volume Information' (der übliche Speicherort ist 'C:\System Volume Information\')
- Der 'Papierkorb'
- Die temporären Daten des Webbrowsers:
  - Die temporären Internetdateien
  - Cookies
  - Verlauf
  - Cache
- .tib- und .tibx-Dateien
- .tmp-Dateien
- Dateien mit der Erweiterung .~

# Vollständige, inkrementelle und differentielle Backups

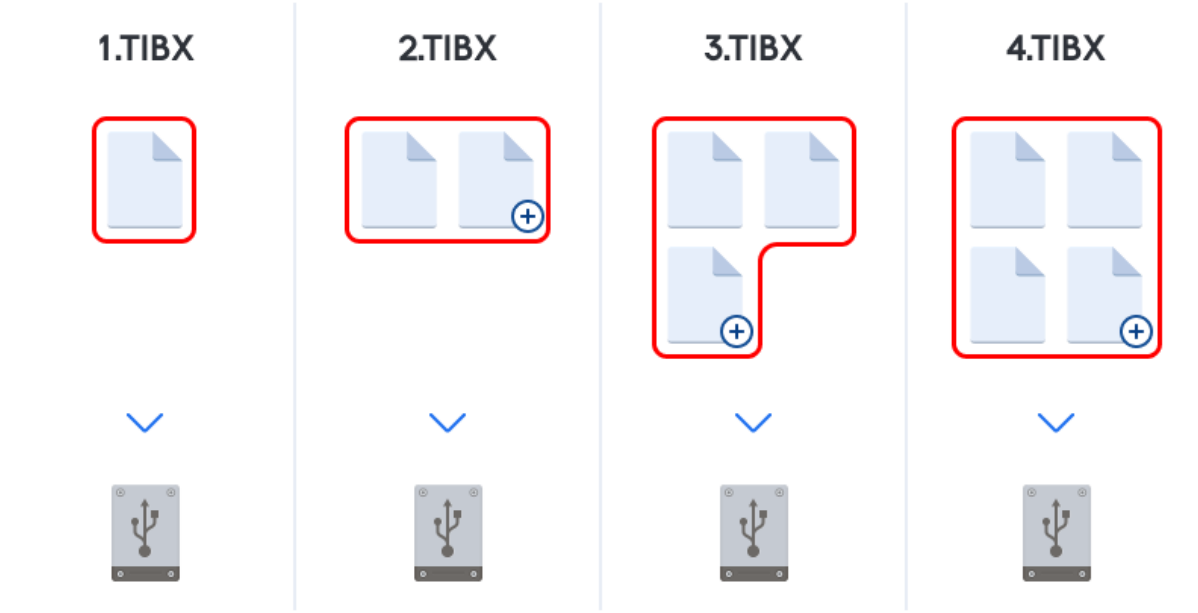
Acronis Cyber Protect Home Office bietet drei Backup-Methoden: vollständig, inkrementell und differentiell.

## Vollständige Methode

Das Ergebnis einer Backup-Aktion mit der Methode 'Voll-Backup' (auch als Voll-Backup-Version bezeichnet) enthält alle Daten zum Zeitpunkt der Backup-Erstellung.

**Beispiel:** Sie schreiben täglich eine Seite an einem Dokument und sichern dieses mit der vollständigen Methode. Acronis Cyber Protect Home Office speichert bei jeder Backup-Ausführung das vollständige Dokument.

1.tibx, 2.tibx, 3.tibx, 4.tibx – Dateien der Voll-Backup-Versionen.




**Zusätzliche Informationen**

Eine Voll-Backup-Version bildet die Basis für nachfolgende inkrementelle und differentielle Backups. Es kann auch als unabhängiges Backup verwendet werden. Ein autonomes Voll-Backup kann die richtige Wahl sein, wenn Sie Ihr System häufig in seinen ursprünglichen Zustand zurücksetzen müssen oder wenn Sie nicht mehrere Backup-Versionen verwalten wollen.

**Recovery:** Im oberen Beispiel benötigen Sie zur Wiederherstellung der kompletten Arbeit von Datei 4.tibx nur eine Backup-Version – nämlich 4.tib.

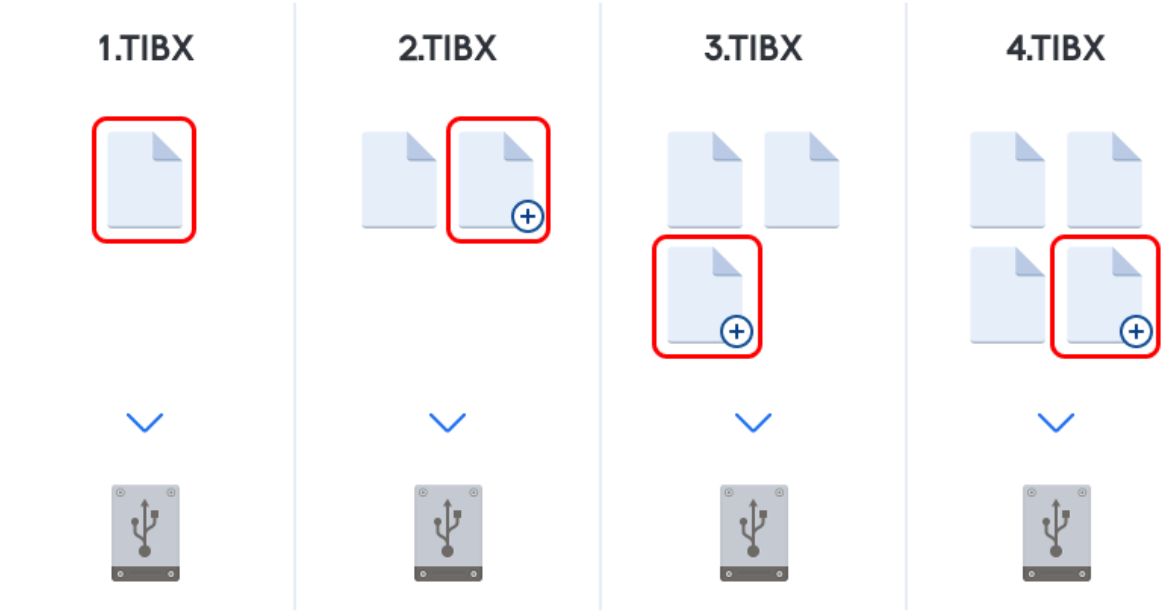
## Inkrementelle Methode

Das Ergebnis einer Backup-Aktion mit der Methode 'inkrementell' (auch als inkrementelle Backup-Version bezeichnet) enthält nur solche Dateien, die seit dem letzten Backup geändert wurden.

**Beispiel:** Sie schreiben täglich eine Seite an einem Dokument und sichern dieses mit der inkrementellen Methode. Acronis Cyber Protect Home Office speichert mit jeder Ausführung des Backups die jeweils neue Seite.

**Hinweis:** Die erste von Ihnen erstellte Backup-Version verwendet immer die vollständige Methode.

- 1.tibx – Datei der Voll-Backup-Version.
- 2.tibx, 3.tibx, 4.tibx – Dateien der inkrementellen Backup-Versionen.




**Zusätzliche Informationen**

Die inkrementelle Methode ist am nützlichsten, wenn Sie Backup-Versionen in hoher Frequenz benötigen oder um verschiedene Wiederherstellungspunkte zu erzeugen. Inkrementelle Backup-Versionen sind deutlich kleiner als vollständige oder differentielle Versionen. Auf der anderen Seite muss das Programm bei der Wiederherstellung inkrementeller Versionen einen größeren Aufwand betreiben.

**Recovery:** Im oberen Beispiel benötigen Sie zur Wiederherstellung der kompletten Arbeit von Datei 4.tibx alle Backup-Version – also 1.tibx, 2.tibx, 3.tibx und 4.tibx. Sollten Sie daher eine inkrementelle Backup-Version verlieren oder sollte diese beschädigt werden, dann werden alle nachfolgenden inkrementellen Versionen ebenfalls unbrauchbar.

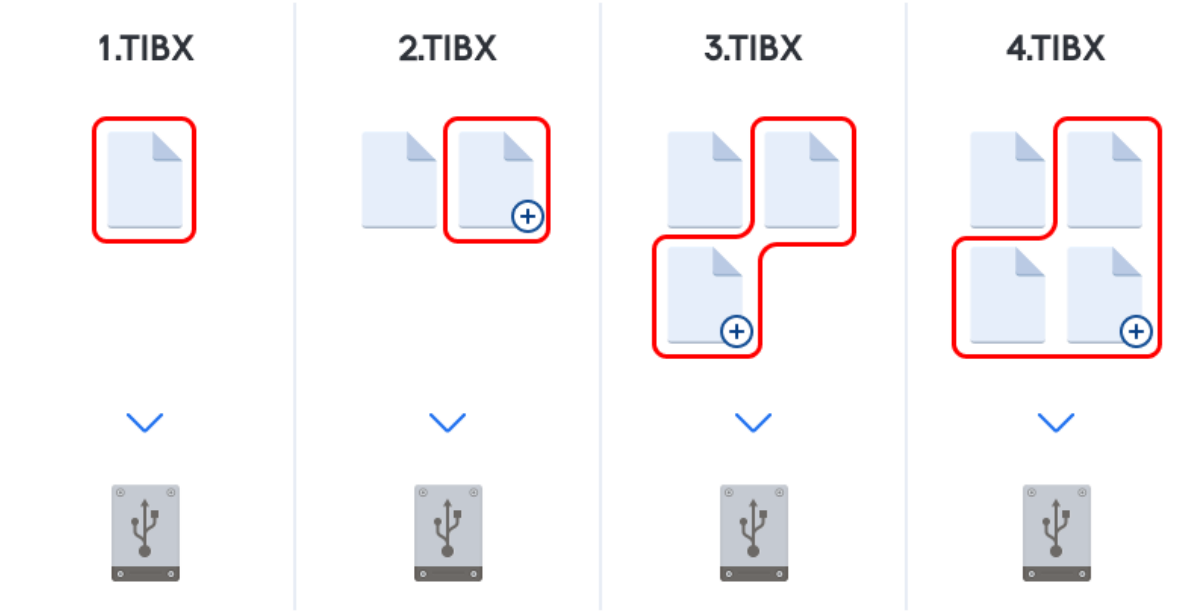
## Differentielle Methode

Das Ergebnis einer Backup-Aktion mit der Methode 'differentiell' (auch als differentielle Backup-Version bezeichnet) enthält nur solche Dateien, die seit dem letzten Voll-Backup geändert wurden.

**Beispiel:** Sie schreiben täglich eine Seite an einem Dokument und sichern dieses mit der differentiellen Methode. Acronis Cyber Protect Home Office speichert das komplette Dokument – mit Ausnahme der ersten Seite, die in der Voll-Backup-Version gespeichert wurde.

**Hinweis:** Die erste von Ihnen erstellte Backup-Version verwendet immer die vollständige Methode.

- 1.tibx – Datei der Voll-Backup-Version.
- 2.tibx, 3.tibx, 4.tibx – Dateien der differentiellen Backup-Versionen.




**Zusätzliche Informationen**

Die differentielle Methode bietet einen Mittelweg zu den beiden ersten Ansätzen. Es benötigt weniger Zeit und Speicherplatz als ein vollständiges Backup, aber mehr als ein inkrementelles. Zur Datenwiederherstellung von einer differentiellen Backup-Version benötigt Acronis Cyber Protect Home Office nur die jeweilige differentielle Version und die letzte vollständige Version. Die Wiederherstellung von einer differentiellen Version ist (im Vergleich zu einer inkrementellen) daher einfacher und zuverlässiger.

**Recovery:** Im oberen Beispiel benötigen Sie zur Wiederherstellung der kompletten Arbeit von Datei 4.tibx zwei Backup-Version – nämlich 1.tibx und 4.tibx.

Sie müssen normalerweise ein benutzerdefiniertes Backup-Schema konfigurieren, um eine gewünschte Backup-Methode zu wählen. Zu weiteren Informationen siehe Benutzerdefinierte Schemata.

**Hinweis**
Wenn ein inkrementelles oder differentielles Backup erstellt wird, nachdem ein Laufwerk defragmentiert wurde, dann kann seine Dateigröße ungewöhnlich stark ansteigen. Der Grund liegt darin, dass das Defragmentierungsprogramm zu viele Sektoren auf der Platte verändert hat und die Backups reflektieren diese Veränderungen. Sie sollten daher nach einer Defragmentierung erneut ein Voll-Backup erstellen.

## Changed Block Tracker (CBT)

Die CBT-Technologie kann Backup-Prozesse beschleunigen, wenn lokale inkrementelle oder differentielle Backup-Versionen auf Laufwerksebene erstellt werden. Dabei werden entsprechende Laufwerke kontinuierlich auf Blockebene überwacht, ob vorhandene Dateninhalte geändert

wurden. Wenn dann ein Backup durchgeführt wird, können die zuvor bereits ermittelten Änderungen direkt im Backup gespeichert werden.

# So entscheiden Sie, wo Sie Ihre Backups speichern

Acronis Cyber Protect Home Office unterstützt eine Vielzahl von Speichergeräten. Weitere Informationen dazu finden Sie hier: "Unterstützte Speichermedien" (S. 15).

Die nachfolgende Tabelle zeigt, welche Backup-Ziele Sie für Ihre Daten verwenden können.

| | **HDD*** | **SSD*** | **USB-Stick** | **Acronis Cloud** | **Datei-Server, NAS oder NDAS** | **Netzwerkfreigabe** | **SMB** | **FTP** | **DVD** | **Speicherkarte** |
|---|---|---|---|---|---|---|---|---|---|---|
| MBR-Volumes oder komplette Laufwerke (HDD, SSD) | + | + | + | + | + | + | + | + | + | + |
| GPT-/dynamische Volumes oder Laufwerke | + | + | + | + | + | + | + | + | + | + |
| Dateien und Ordner | + | + | + | + | + | + | + | + | + | + |

*intern oder extern.

Obwohl die Erstellung von Backups auf Ihr lokales Festplattenlaufwerk die einfachste Möglichkeit ist, empfehlen wir dennoch, dass Sie Ihre Backups extern ('off-site') speichern, um die Sicherheit Ihrer Daten zu erhöhen.

**Empfohlene Speichermedien/-Systeme:**

1. **Acronis Cloud**
2. **Externes Laufwerk**
   Wenn Sie eine externe USB-Festplatte mit Ihrem Desktop-PC verwenden wollen, empfehlen wir, das Laufwerk mit einem kurzen Kabel an einem der Anschlüsse auf der Computerrückseite zu verbinden.
3. **Heim-Datei-Server, NAS oder NDAS**

Überprüfen Sie, ob Acronis Cyber Protect Home Office den ausgewählten Backup Storage sowohl unter Windows wie auch beim Booten mit einem Boot-Medium erkennen kann.

Um Zugriff auf ein NDAS-Speichergerät zu erhalten, müssen Sie in den meisten Fällen eine NDAS-Geräte-ID (20 Zeichen) und einen Schreibschlüssel (fünf Zeichen) angeben. Mit dem Schreibschlüssel können Sie ein NDAS-fähiges Speichergerät auch im Schreibmodus verwenden (z.B. zum Speichern von Backups). Normalerweise befindet sich die Geräte-ID und der Schreibschlüssel auf einem Aufkleber, der am Boden des NDAS-Gerätes oder irgendwo bei der Verpackung bzw. den Unterlagen angebracht ist. Sollte bei Ihnen ein solcher Sticker fehlen, müssen Sie den Hersteller des NDAS-Gerätes kontaktieren, um die entsprechenden Informationen zu erhalten.

4. **Netzwerkfreigabe**

   Siehe auch: Authentifizierungseinstellungen.
5. **FTP-Server**

   Siehe auch: FTP-Verbindung.
6. **Optische Datenträger (CD, DVD, BD)**

   Leere optische Datenträger wie DVD-R/DVD+R sind preiswert und verursachen geringe Backup-Kosten; allerdings ist ihr Einsatz die langsamste Lösung.

   Da es meist notwendig ist, für das Erstellen von Backups auf DVDs mehrere optische Speichermedien zu nutzen, raten wir davon ab, wenn die für die Sicherung erforderliche Anzahl drei übersteigt. Gibt es keine Alternative zu einer Sicherung auf DVD, dann ist es ratsam, die Inhalte aller entsprechenden DVDs vor einer Wiederherstellung in einen Ordner auf einer Festplatte (oder einem ähnlichen Laufwerk) zu kopieren – und die Recovery-Aktion dann von dort aus zu starten.

## Ein neues Laufwerk zur Nutzung für Backups vorbereiten

Es kann vorkommen, dass Acronis Cyber Protect Home Office ein neues internes oder externes Festplattenlaufwerk nicht direkt erkennt. Verwenden Sie in einem solchen Fall das entsprechende Laufwerksverwaltungsprogramm des Betriebssystems, um den Laufwerksstatus auf **Online** zu setzen und das Laufwerk zu initialisieren.

***So können Sie den Laufwerksstatus auf 'online' ändern***

1. Öffnen Sie die **Datenträgerverwaltung**. Verwenden Sie dafür diese Befehlsfolge: **Systemsteuerung** –> **System und Sicherheit** –> **Verwaltung**, **Computerverwaltung** und dann **Datenträgerverwaltung**.
2. Suchen Sie das Laufwerk, welches als '**Offline**' gekennzeichet ist. Klicken Sie mit der rechten Maustaste auf die Datenbank und wählen Sie **Online**.
3. Der Laufwerkstatus wird auf **Online** geändert. Danach können Sie das Laufwerk initialisieren.

***So können Sie ein Laufwerk initialisieren:***

1. Öffnen Sie die **Datenträgerverwaltung**. Verwenden Sie dafür diese Befehlsfolge: **Systemsteuerung** –> **System und Sicherheit** –> **Verwaltung**, **Computerverwaltung** und dann

**Datenträgerverwaltung**.

2. Suchen Sie das Laufwerk, welches als '**Nicht initialisiert**' gekennzeichet ist. Klicken Sie mit der rechten Maustaste auf das betreffende Laufwerk und wählen Sie den Befehl **Datenträger initialisieren**.
3. Bestimmen Sie den Partitionsstil des Laufwerks – MBR oder GPT – und klicken Sie dann auf **OK**.
4. [Optionaler Schritt] Wenn Sie auf dem Laufwerk ein Volume (Partition) erstellen wollen, klicken Sie auf **Neues einfaches Volume**. Folgen Sie anschließend den Anweisungen des entsprechenden Assistenten, um das neue Volume zu konfigurieren. Um weitere Volumes zu erstellen, wiederholen Sie diese Aktion.

## FTP-Verbindung

Acronis Cyber Protect Home Office bietet die Möglichkeit, Backups auf FTP-Servern zu speichern.

Klicken Sie auf **FTP-Verbindung**, um bei Wahl des Backup Storages einen FTP-Server als Ziel anzugeben und stellen Sie Folgendes im geöffneten Fenster zur Verfügung:

- Den Pfad zum FTP-Server, beispielsweise: *mein.server.de*
- Port
- Benutzername
- Kennwort

Klicken Sie zur Überprüfung Ihrer Einstellungen auf die Schaltfläche **Verbindung testen**. Der Computer wird daraufhin versuchen, eine Verbindung zum angegebenen FTP-Server aufzubauen. Klicken Sie, wenn die Testverbindung erfolgreich war, auf die Schaltfläche **Verbinden**, um die FTP-Verbindung zu speichern.

Die erstellte FTP-Verbindung erscheint dann im Verzeichnisbaum. Wählen Sie die Verbindung und durchsuchen Sie den gewünschten Backup-Storage.

**Hinweis**
Durch das einfache Öffnen des Stammverzeichnisses eines FTP-Servers gelangen Sie nicht automatisch zu Ihrem Home-Verzeichnis.

**Hinweis**
Um Daten direkt von einem FTP-Server wiederherstellen zu können, darf das Backup nur aus Dateien bestehen, die nicht größer als 2 GB sind.

**Hinweis**
Acronis Cyber Protect Home Office teilt ein Backup daher in Dateien mit einer Größe von 2 GB auf, wenn Sie direkte Backups zu einem FTP-Server durchführen. Sollten Sie das Backup auf eine Festplatte erstellen, um dieses Backup später dann auf einen FTP-Server zu übertragen, dann sollten Sie das Backup in Dateien von je maximal 2 GB aufteilen, indem Sie die entsprechende Dateigröße in den Backup-Optionen einstellen.

**Hinweis**
Der entsprechende FTP-Server muss für die Dateiübertragung den 'Passiven Modus' zulassen.

**Hinweis**
In den Firewall-Einstellungen des Quellcomputers müssen die Ports 20 und 21 freigegeben sein (für TCP- und UDP-Protokolle), damit die Übertragung funktionieren kann. Der Windows-Dienst **Routing und RAS** sollte deaktiviert sein.

## Authentifizierungseinstellungen

Wenn Sie sich mit einem Computer im Netzwerk oder einem NAS-Gerät verbinden, müssen Sie normalerweise Anmeldedaten spezifizieren, um auf den entsprechenden Netzwerk-Speicherort zugreifen zu können. Dies ist beispielsweise möglich, wenn Sie einen Backup Storage auswählen. Das Fenster **Authentifizierungseinstellungen** öffnet sich automatisch, wenn Sie den Namen eines Rechners im Netzwerk auswählen.

Spezifizieren Sie bei Bedarf den Benutzernamen und das Kennwort und klicken Sie dann auf **Verbindung testen**. Klicken Sie auf **Verbinden**, falls der Test erfolgreich war.

### Problembehebung (Troubleshooting)

Wenn Sie eine Netzwerkfreigabe als Backup-Storage verwenden wollen, sollten Sie überprüfen, dass mindestens eine der nachfolgenden Bedingungen erfüllt ist:

- Das Windows-Konto verfügt über ein Kennwort auf dem Computer, auf dem sich der freigegebene Ordner befindet.
- Die Funktion 'Kennwortgeschütztes Freigeben' ist in Windows ausgeschaltet.
  Unter Windows 7 können Sie diese Einstellung beispielsweise hier finden: **Systemsteuerung** –> **Netzwerk und Internet** –> **Netzwerk- und Freigabecenter** –> **Erweiterte Freigabeeinstellungen** –> Kennwortgeschütztes Freigeben ausschalten.

Ansonsten werden Sie auf den freigegebenen Ordner nicht zugreifen können.

# Acronis Nonstop Backup

Acronis Nonstop Backup ermöglicht einen einfachen Schutz Ihrer Laufwerke und Dateien. Sie können komplette Laufwerke, einzelne Dateien und verschiedene Versionen von diesen wiederherstellen.

Acronis Nonstop Backup ist in erster Linie dazu gedacht, Ihre Daten (Dateien, Ordner, Kontakte usw.) kontinuierlich zu schützen, Sie können es aber auch zum Schutz kompletter Volumes verwenden. Falls Sie ein komplettes Volume zum Schutz ausgewählt haben, können Sie später unter Verwendung einer Recovery-Aktion für Images das Volume auch im Ganzen wiederherstellen.

Wir raten davon ab, das Nonstop Backup als vorrangiges Mittel zu verwenden, um damit Ihr System zu sichern (statt einem normalen Backup). Um die Sicherheit Ihres Systems zu gewährleisten, sollten

Sie stattdessen eine der anderen Planungsvarianten verwenden. Entsprechende Beispiele und ausführliche Informationen finden Sie im Abschnitt 'Beispiele für benutzerdefinierte Schemata'.

## Beschränkungen für Nonstop Backup

- Sie können nur ein Nonstop Backup erstellen.
- Die Acronis Cloud kann nicht als Speicherziel für ein Nonstop Backup auf Laufwerksebene verwendet werden.
- Windows-Bibliotheken (Dokumente, Musik etc.) können nur mit einem Nonstop Backup auf Laufwerksebene geschützt werden.
- Daten auf externen Festplatten können per Nonstop Backup nicht gesichert werden.
- Nonstop Backup und Try&Decide können nicht gleichzeitig arbeiten.

## Und so funktioniert es

Nachdem Sie Acronis Nonstop Backup gestartet haben, führt das Programm ein anfängliches Voll-Backup der für die Sicherung ausgewählten Daten aus. Acronis Nonstop Backup wird die zu schützenden Dateien dann kontinuierlich überwachen (inkl. Dateien, die in Anwendungen geöffnet sind). Sobald eine Änderung an den Dateien erkannt wird, werden die entsprechenden Daten gesichert. Das kürzeste Intervall zwischen zwei inkrementellen Backup-Aktionen beträgt fünf Minuten. Damit können Sie Ihr System zu einem bestimmten Zeitpunkt hin (in der Vergangenheit) wiederherzustellen bzw. auf diesen zurückzusetzen.

Acronis Nonstop Backup überwacht nur Änderungen an Dateien auf dem Laufwerk und nicht von Daten im Hauptspeicher. Falls Sie beispielsweise mit Microsoft Word ein Dokument bearbeiten und dieses währenddessen nicht speichern, werden diese Änderungen (seit der letzten Speicherung) folglich nicht per Nonstop Backup erfasst.

Sie vermuten sicher, dass bei dieser Backup-Frequenz der Speicherplatz schnell erschöpft ist. Ihre Sorge ist unbegründet, da Acronis Cyber Protect Home Office nur sogenannte 'Deltas' sichert. Das bedeutet, dass nur die Unterschiede zwischen alten und neuen Versionen gesichert werden und nicht die geänderten Dateien als Ganzes. Wenn Sie z.B. Microsofts Outlook oder Windows Mail verwenden ist, ist die PST-Datei möglicherweise sehr groß. Außerdem wird sie mit jeder gesendeten oder empfangenen E-Mail geändert. Das Sichern der gesamten pst-Datei nach jeder Änderung wäre eine nicht akzeptierbare Speicherplatzverschwendung, also sichert Acronis Cyber Protect Home Office zusätzlich zur anfänglich gesicherten Datei nur geänderte Teile.

## Aufbewahrungsregeln

**Lokale Backups**

Acronis Nonstop Backup bewahrt alle gespeicherten Backups für die letzten 24 Stunden. Ältere Backups werden so konsolidiert, dass Nonstop Backup tägliche Backups für die letzten 30 Tage und wöchentliche Backups solange behält, bis der komplette Speicherplatz des Nonstop Backup-Datenspeichers belegt ist.

Die Konsolidierung wird täglich zwischen Mitternacht und 1 Uhr durchgeführt. Die erste Konsolidierung erfolgt, nachdem Nonstop Backup mindestens 24 Stunden gelaufen ist. Wenn Sie das Nonstop Backup z.B. um 10 Uhr am 12. Juli gestartet haben, findet die erste Konsolidierung zwischen 0 und 1 Uhr am 14. Juli statt. Danach konsolidiert das Programm die Daten jeden Tag zur selben Zeit. Ist der Computer im Zeitraum zwischen 0 Uhr und 1 Uhr ausgeschaltet, findet die Konsolidierung beim Einschalten des Computers statt. Wenn Sie Nonstop Backup für einige Zeit ausschalten, findet die Konsolidierung statt, nachdem Sie es wieder starten.

**Cloud Backups**

Acronis Cyber Protect Home Office bewahrt nur folgende Backup-Versionen auf:

- Alle Versionen der letzten Stunde
- Die ersten Versionen einer jeden Stunde der letzten 24 Stunden
- Die erste Version eines jeden Tages der letzten Woche
- Die erste Version einer jeden Woche des letzten Monats
- Die erste Version eines jeden Monats

Alle anderen Versionen werden automatisch gelöscht. Die Aufbewahrungsregeln sind voreingestellt und können nicht geändert werden.

## Acronis Nonstop Backup Storage

Ein Acronis Nonstop Backup Storage kann auf lokalen (internen oder externen) Laufwerken oder auch in der Acronis Cloud erstellt werden.

In den meisten Fällen dürfte ein externes Festplattenlaufwerk eine gute Wahl als Nonstop Backup Storage sein. Sie können externe Laufwerke mit folgenden Schnittstellen nutzen: USB (inklusive USB 3.0), eSATA, FireWire und SCSI.

Sie können auch einen NAS-Datenspeicher verwenden, allerdings mit der Einschränkung, dass er mit dem (von Windows und Samba verwendeten) SMB-Protokoll erreichbar sein muss. Es ist dabei unerheblich, ob die NAS-Freigabe, die als Datenspeicher verwendet werden soll, als lokales Laufwerk zugeordnet ist. Wenn für die Freigabe eine Anmeldung erforderlich ist, müssen Sie die entsprechenden Anmeldedaten (Benutzername, Kennwort) angeben. Weitere Informationen finden Sie im Abschnitt 'Authentifizierungseinstellungen'. Acronis Cyber Protect Home Office speichert die Anmeldedaten, damit für spätere Verbindungen zur Freigabe keine erneute Anmeldung erforderlich ist.

Wenn Sie kein externes Laufwerk oder NAS haben, kann auch ein internes Laufwerk (inklusive dynamischer Laufwerke) als Zielspeicherort für das Nonstop Backup verwendet werden. Beachten Sie, dass Sie kein Volume als Nonstop Backup Storage verwenden können, welches Sie von Nonstop Backup auch gleichzeitig schützen lassen. Sollte Ihr Computer nur ein Laufwerk mit nur einem einzigen Volume haben, dann können Sie die Acronis Nonstop Backup-Funktion dennoch nutzen, indem Sie eine Acronis Secure Zone erstellen und diese dann als Nonstop Backup Storage angeben.

Acronis Cyber Protect Home Office überprüft vor Erstellung eines Acronis Nonstop Backup Storages, ob der angegebenen Zielort auch genügend freien Speicherplatz hat. Dazu wird der Umfang der zu schützenden Daten mit 1,2 multipliziert und der so errechnete Wert mit dem verfügbaren Speicherplatz verglichen. Sofern der freie Speicherplatz des Zielorts diesen minimalen Größenanforderungen entspricht, kann er als Speicherziel zur Aufnahme der Nonstop Backup-Daten verwendet werden.

## Nonstop Backup – Häufig gestellte Fragen (FAQs)

**Warum pausiert Acronis Nonstop Backup von alleine?** – Das ist ein vorgesehenes Verhalten von Acronis Nonstop Backup. Wenn die Systemauslastung auf einen kritischen Wert steigt, erhält Acronis Nonstop Backup einen Überlastungsalarm von Windows und unterbricht seinen Prozess selbstständig. Dadurch soll Windows bei der Auslastung durch andere Anwendungen geholfen werden. Eine solche Überlastung kann durch die Ausführung Ressourcen-hungriger Anwendungen verursacht werden (beispielsweise ein systemweiter Scan durch eine Antivirus-Software).

Die Nonstop Backup-Aktion wird in so einem Fall automatisch unterbrochen und kann von Ihnen nicht wieder manuell gestartet werden. Acronis Nonstop Backup gibt dem System nach Aktivierung seines Pausenzustands eine Stunde Zeit, die Belastung zu verringern und versucht dann automatisch, sich neu zu starten.

Dabei hat Acronis Nonstop Backup einen automatischen 'Neustartzähler' von 6. Das bedeutet, dass Acronis Nonstop Backup nach dem ersten automatischen Neustartversuch noch fünfmal einen Versuch zum erneuten Starten durchführt – mit einem Zeitspanne von einer Stunde zwischen den Versuchen.

Ist auch der sechste Versuch nicht erfolgreich, wartet Acronis Nonstop Backup bis zum nächsten Kalendertag. Am nächsten Tag wird der automatische Neustartzähler auch wieder zurückgesetzt. Wenn nicht gestört, führt Acronis Nonstop Backup also sechs Neustartversuche pro Tag aus.

Sie können den Neustartzähler durch eine der folgenden Aktionen zurücksetzen lassen:

- Einen Neustart des Acronis Nonstop Backup Service;
- Einen Neustart des Computers.

Durch einen Neustart des Acronis Nonstop Backup Service wird nur der Neustartzähler auf 0 gesetzt. Sollte das System immer noch überlastet sein, wird Acronis Nonstop Backup wieder pausiert. Weitere Informationen zum Neustart des Acronis Nonstop Backup Service finden Sie unter 'https://kb.acronis.com/content/14708'.

Durch einen Neustart des Computers wird sowohl dessen Auslastung wie auch der Neustartzähler zurückgesetzt. Sollte das System danach erneut überlastet werden, pausiert auch Acronis Nonstop Backup wieder.

**Warum verursacht Acronis Nonstop Backup manchmal eine hohe CPU-Last?** – Dies ist das erwartete Verhalten von Acronis Nonstop Backup. Dies kann beispielsweise passieren, wenn Acronis Nonstop Backup nach einer Pause neu gestartet wurde und während dieser Pause eine beachtliche Menge zu schützender Daten verändert wurden.

Wenn Sie beispielsweise Acronis Nonstop Backup, welches Sie zum Schutz Ihres System-Volumes einsetzen, manuell pausieren – und dann ein neues Anwendungsprogramm installieren. Wenn Sie Acronis Nonstop Backup erneut starten, wird für einige Zeit eine CPU-Last erzeugt. Der Prozess (afcdpsrv.exe) geht danach aber wieder auf normal zurück.

Das passiert, weil Acronis Nonstop Backup die bisher gesicherten Daten gegen diejenigen überprüfen muss, die während der Pause verändert wurden. Wurde eine beträchtliche Datenmenge verändert, kann der Prozess für einige Zeit eine erhöhte CPU-Last bewirken. Acronis Nonstop Backup kehrt zu seiner normalen Aktivität zurück, sobald die Überprüfung durchgeführt wurde und alle veränderten Daten gesichert wurden.

**Kann ein Acronis Nonstop Backup Storage auf einem FAT32-Volume (Partition) eines lokalen Laufwerks liegen?** – Ja, es können FAT32- und NTFS-Volumes als Storage verwendet werden.

**Kann ein Acronis Nonstop Backup Storage auf einer Netzwerkfreigabe oder einem NAS-Gerät liegen?** – Ja, Acronis Nonstop Backup unterstützt Netzwerkfreigaben, Netzlaufwerke, NAS- und andere über das Netzwerk angeschlossene Geräte, mit einer Einschränkung – diese müssen das SMB-Protokoll verwenden.

# Benennung von Backup-Dateien

Der Name einer Backup-Datei hängt davon ab, mit welcher Version ein Backup erstellt wurde.

## Die Namenskonvention für Backup-Dateien, die mit Acronis True Image (2020 oder 2021) oder Acronis Cyber Protect Home Office erstellt wurden

Ein Backup-Dateiname besteht nur aus dem Backup-Namen und einem schrittweise steigenden Zähler. Der Name enthält keine weiteren Informationen (wie beispielsweise die Backup-Methode, die Nummer der Backup-Ketten, die Nummer der Backup-Version oder eine Volume-Nummer).

Ein Backup-Name kann folgendermaßen aussehen:

1. `meine_Dokumente.tibx`
2. `meine_Dokumente_0001.tibx`
3. `meine_Dokumente_0002.tibx`
4. `meine_Dokumente_0003.tibx`

Vollständige und differentielle Backups werden in separaten Dateien gespeichert und inkrementelle Backups werden automatisch zu Voll-Backups zusammengeführt.

Folgende Backups verwenden weiterhin das TIB-Format und die entsprechende Namenskonvention:

- Datei-Backups für alle Backup-Ziele mit Ausnahme der Acronis Cloud. Datei-Backups in die Acronis Cloud werden im .tibx-Format erstellt.
- Nonstop Backups

- Beglaubigte Backups (Notarized Backups)
- Backups, die CDs/DVDs/Blu-rays, einen FTP-Server oder die Secure Zone als Backup-Ziel verwenden

## Die Namenskonvention für Backup-Dateien, die mit einer Acronis True Image-Version vor 2020 erstellt wurden

Ein TIB-Backup-Dateiname hat folgende Attribute:

- Backup-Name
- Backup-Methode (full, inc, diff: vollständig/inkrementell/differentiell)
- Nummer der Backup-Kette[1], sofern angebracht (angegeben als b#)
- Nummer der Backup-Version[2] (angegeben als s#)
- Nummer des Volumes (angegeben als v#)
  Dieses Attribut ändert sich beispielsweise, wenn Sie ein Backup in mehrere Dateien aufteilen. Weitere Details finden Sie im Abschnitt 'Backup-Aufteilung'.

Ein Backup-Name kann daher folgendermaßen aussehen:

1. `my_documents_full_b1_s1_v1.tib`
2. `my_documents_full_b2_s1_v1.tib`
3. `my_documents_inc_b2_s2_v1.tib`
4. `my_documents_inc_b2_s3_v1.tib`

Sollten Sie ein neues Backup erstellen und es bereits eine Datei desselben Namens geben, dann löscht das Programm die alte Datei nicht, sondern es erweitert den neuen Dateinamen um das Suffix '-number' (beispielsweise `meine_Dokumente_ink_b2_s2_v1-2.tib`).

# Integration in Windows

Während der Installation integriert sich Acronis Cyber Protect Home Office noch stärker in Windows. Durch diese 'Verschmelzung' können Sie Ihren Computer noch besser nutzen.

Acronis Cyber Protect Home Office integriert folgende Komponenten:

---

[1]Sequenz von mindestens zwei Backup-Versionen, bestehend aus dem ersten Voll-Backup-Version sowie einer oder mehreren nachfolgenden inkrementellen oder differentiellen Backup-Versionen. Eine Backup-Versionskette setzt sich fort, bis die nächste Voll-Backup-Version erstellt wird (sofern überhaupt erstellt).
[2]Das Ergebnis einer einzelnen Backup-Aktion. Physisch handelt es sich um eine Datei oder eine Zusammenstellung von Dateien, die eine Kopie der gesicherten Daten zu einem spezifischen Zeitpunkt enthält. Backup-Versionen von Dateien, die von Acronis Cyber Protect Home Office erstellt werden, erhalten die Dateierweiterung '.tibx'. TIBX-Dateien, die sich aus einer Konsolidierung von Backup-Versionen ergeben, werden ebenfalls als Backup-Versionen bezeichnet.

- Acronis Elemente im **Start**-Menü von Windows
- Die Acronis Cyber Protect Home Office Schaltfläche in der Taskleiste
- Kontextmenübefehle

***Windows-Start-Menü***

Im **Start**-Menü werden Befehle, Tools und Werkzeuge von Acronis angezeigt. Dies ermöglicht Ihnen den Zugriff auf Acronis Cyber Protect Home Office-Funktionen, ohne dass Sie das Programm selbst starten müssen.

***Die Acronis Cyber Protect Home Office Schaltfläche in der Taskleiste***

Die Acronis Cyber Protect Home Office-Schaltfläche in der Windows-Taskleiste zeigt den Fortschritt und das Ergebnis von Acronis Cyber Protect Home Office-Aktionen an.


***Tray Notification Center***

Wenn Acronis Cyber Protect Home Office geöffnet ist, können Sie dort den Status einer jeden Aktion einsehen. Da einige Aktionen (wie Backups) jedoch eine längere Zeit dauern können, müssen Sie Acronis Cyber Protect Home Office nicht die ganze Zeit geöffnet halten, um über das Ergebnis der Aktion(en) informiert zu werden.

Das Tray Notification Center zeigt die neuesten Benachrichtigungen an einem Ort an, sodass Sie wichtige Statusmeldungen einsehen können, ohne Acronis Cyber Protect Home Office jedes Mal öffnen müssen, wenn Sie die Benachrichtigungen benötigen. Die folgenden Benachrichtigungen werden im Acronis Tray Notification Center angezeigt: Informationen über die Ergebnisse von Backup-Aktionen und andere wichtige Benachrichtigungen von Acronis Cyber Protect Home Office. Das Tray Notification Center wird minimiert angezeigt und ist unter Acronis Cyber Protect Home Office in der Info-Leiste verborgen.

***Kontextmenübefehle***

Um auf die Kontextmenübefehle zugreifen zu können, müssen Sie den Windows Explorer öffnen, mit der rechten Maustaste auf die ausgewählten Elemente/Dateien klicken, dann Acronis Cyber Protect Home Office auswählen und abschließend den gewünschten Befehl.

- Wenn Sie ein neues Datei-Backup erstellen wollen, wählen Sie den Befehl **Neues Datei-Backup**.
- Wenn Sie ein neues Laufwerk-Backup erstellen wollen, wählen Sie den Befehl **Neues Laufwerk-Backup**.
- Wenn Sie ein Laufwerk-Backup (.tibx-Datei) als virtuelles Laufwerk einbinden wollen, klicken Sie auf **Mounten**.
- Wenn Sie ein Backup (.tibx-Datei) überprüfen wollen, klicken Sie auf **Validieren**.

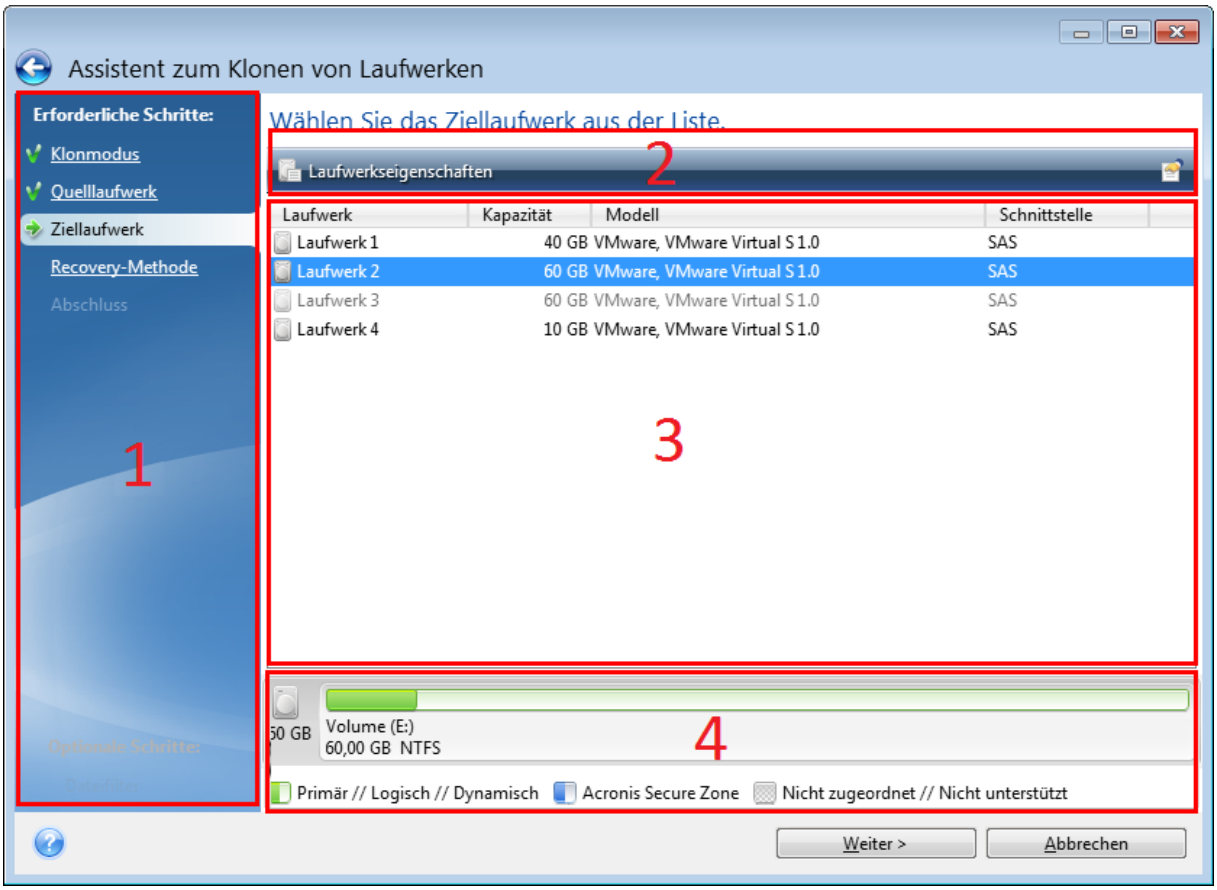
***Datei-Recovery über den Windows Explorer***

1. Klicken Sie im Windows Explorer doppelt auf die Backup-Datei (.tibx-Datei), welche die wiederherzustellenden Daten enthält.
2. Sie können die gewünschten Dateien/Ordner aus dem Backup (als würde es sich um ein herkömmliches Laufwerk handeln) per 'Kopieren und Einfügen' oder per 'Drag & Drop'-Aktion an einem beliebigen Zielort auf Ihrem Computer speichern.

# Assistenten

Wenn Sie die verfügbaren Funktionen von Acronis Cyber Protect Home Office verwenden, wird das Programm in vielen Fällen Assistenten einsetzen, um Sie durch die Aktion zu leiten.

Die untere Bildschirmabbildung zeigt ein Beispiel.




Das Fenster eines Assistenten besteht üblicherweise aus folgenden Bereichen:

1. Dies ist die Liste der Schritte, um die Aktion abzuschließen. Neben einem abgeschlossenen Schritt erscheint ein grünes Häkchen. Ein grüner Pfeil kennzeichnet den aktuellen Schritt. Nach Fertigstellung aller Schritte zeigt das Programm im Schritt **Abschluss** eine Zusammenfassung an. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertigstellen**, um die entsprechende Aktion zu starten.
2. Diese Symbolleiste enthält Schaltflächen, um die von Ihnen in 'Bereich 3' ausgewählten Objekte zu verwalten.

   Zum Beispiel:

-  **Details** – öffnet ein Fenster, welches ausführliche Informationen über das ausgewählte Backup anzeigt.
-  **Eigenschaften** – zeigt das Fenster 'Eigenschaften' zu dem ausgewählten Element an.
-  **Neues Volume erstellen** – öffnet ein Fenster, in dem Sie Einstellungen für ein neues Volume konfigurieren können.
-  **Spalten** – mit dieser Schaltfläche können Sie die anzuzeigenden Tabellenspalten und ihre Anordnung wählen.

3. Dies ist der Hauptbereich, in dem Sie Elemente auswählen und Einstellungen ändern.
4. In diesem Bereich werden zusätzliche Informationen zu dem von Ihnen in Bereich 3 gewählten Element angezeigt.

# FAQ über Backup, Recovery und Klonen

- **Ich habe ein System-Volume von 150 GB, der belegte Speicherplatz auf dem Volume beträgt aber nur 80 GB. Was wird von Acronis Cyber Protect Home Office in ein Backup aufgenommen?**– Standardmäßig kopiert Acronis Cyber Protect Home Office nur solche Festplattensektoren, die Daten enthalten; daher wird ein entsprechendes Backup nur 80 GB enthalten. Sie können außerdem den Sektor-für-Sektor-Modus wählen. Beachten Sie dabei aber, dass dieser Backup-Modus nur in speziellen Fällen erforderlich ist. Weitere Informationen finden Sie im Abschnitt 'Modus zur Image-Erstellung'. Bei Erstellung eines Sektor-für-Sektor-Backups kopiert das Programm benutzte und unbenutzte Festplattensektoren, weshalb die resultierende Backup-Datei üblicherweise wesentlich größer wird.
- **Wird das Backup meines Laufwerks auch alle Treiber, Dokumente, Bilder und ähnliche Daten enthalten?** – Ja, ein solches Backup wird sowohl alle Treiber, wie auch die Inhalte der persönlichen Benutzerordner (wie 'Eigene Dateien', 'Dokumente' und Unterordner) enthalten (sofern Sie die Standardspeicherorte für die persönlichen Benutzerordner nicht geändert haben). Sollten Sie in Ihrem PC nur ein einziges Festplattenlaufwerk haben, dann wird ein solches Backup das komplette Betriebssysteme, alle Anwendungen und Daten enthalten.
- **Ich habe ein altes Festplattenlaufwerk in meinem Notebook, das beinahe voll ist. Ich habe ein neues, größeres Festplattenlaufwerk erworben. Wie kann ich Windows, alle Programme und Daten auf das neue Laufwerk übertragen?** – Sie können entweder das alte Festplattenlaufwerk auf das neue klonen – oder ein Backup des alten Laufwerks erstellen und dieses Backup dann auf dem neuen Laufwerk wiederherstellen. Die optimale Methode hängt üblicherweise vom Partitionslayout Ihres alten Festplattenlaufwerks ab.
- **Ich möchte mein altes System-Festplattenlaufwerk auf eine SSD migrieren. Kann das mit Acronis Cyber Protect Home Office umgesetzt werden?**– Ja, Acronis Cyber Protect Home Office stellte eine entsprechende Funktion bereit. Eine ausführliche Erläuterung der Prozedur finden Sie unter 'Migration Ihres Systems von einer Festplatte auf SSD'.
- **Was ist der beste Weg, um das System auf ein neues Laufwerk zu migrieren: Klonen oder eine Kombination aus Backup und Recovery?** – Die 'Backup und Recovery'-Methode bietet mehr Flexibilität. Wir empfehlen aber auf jeden Fall, ein Backup von Ihrem alten

Festplattenlaufwerk zu erstellen, auch wenn Sie sich für das Klonen entscheiden. Das könnte die Rettung für Ihre Daten bedeuten, falls mit dem ursprünglichen Laufwerk beim Klonen etwas schief geht. Es gibt beispielsweise Fällen, in denen Anwender das falsche Laufwerk als Ziel gewählt haben und auf diese Weise ihr Systemlaufwerk ausgelöscht haben. Sie können zudem mehr als ein Backup erstellen, um so per Redundanz die Sicherheit zu erhöhen.

- **Was sollte ich per Backup sichern: ein Volume (entspricht einer Partition) oder das komplette Laufwerk?** – Es ist in den meisten Fällen besser, ein Backup des kompletten Laufwerks zu erstellen. Es gibt jedoch einige Fällen, in denen ein Volume-Backup ratsam ist. Nehmen wir als Beispiel an, Ihr Notebook verfügt über ein einzelnes Festplattenlaufwerk mit zwei Volumes (Partitionen): für das System (Laufwerksbuchstabe C) und für Ihre Daten (Laufwerksbuchstabe D). Das System-Volume speichert Ihre Arbeitsdokumente im persönlichen Benutzerordner **Dokumente** (samt Unterordner). Im Daten-Volume sind dagegen Ihre Videos, Bilder und Musikdateien gespeichert. Wenn Sie lediglich das System-Volume sichern wollen, müssen Sie nicht das komplette Laufwerk sichern. In diesem Fall reicht es aus, nur ein Backup von diesem Volume zu erstellen. Wenn Sie ausschließlich Ihre persönlichen Daten (ohne die Systemdateien) sichern wollen, brauchen Sie nur ein Datei-Backup zu erstellen. Sollte Ihr Backup-Storage (Speichergeräte und vergleichbare Lösungen) über ausreichend Platz verfügen, dann empfehlen wir, wenigstens ein komplettes Laufwerk-Backup zu erstellen.
- **Werden auch RAID-Volumes von Acronis Cyber Protect Home Office unterstützt?** – Acronis Cyber Protect Home Office unterstützt alle gängigen Arten von Hardware-RAID-Arrays. Eine Unterstützung für Software-RAID-Konfigurationen mit dynamischen Datenträgern wird ebenfalls bereitgestellt. Das Acronis Boot-Medium unterstützt die meisten gängigen Hardware-RAID-Controller. Sollte das standardmäßige Acronis Boot-Medium das RAID nicht als einzelnes Volume erkennen, dann verfügt das Medium nicht über die passenden Treiber. In diesem Fall können Sie einen WinPE-basiertes Medium erstellen und dort dann (im erweiterten Modus) die erforderlichen Treiber hinzufügen.

# Daten werden per Backup gesichert

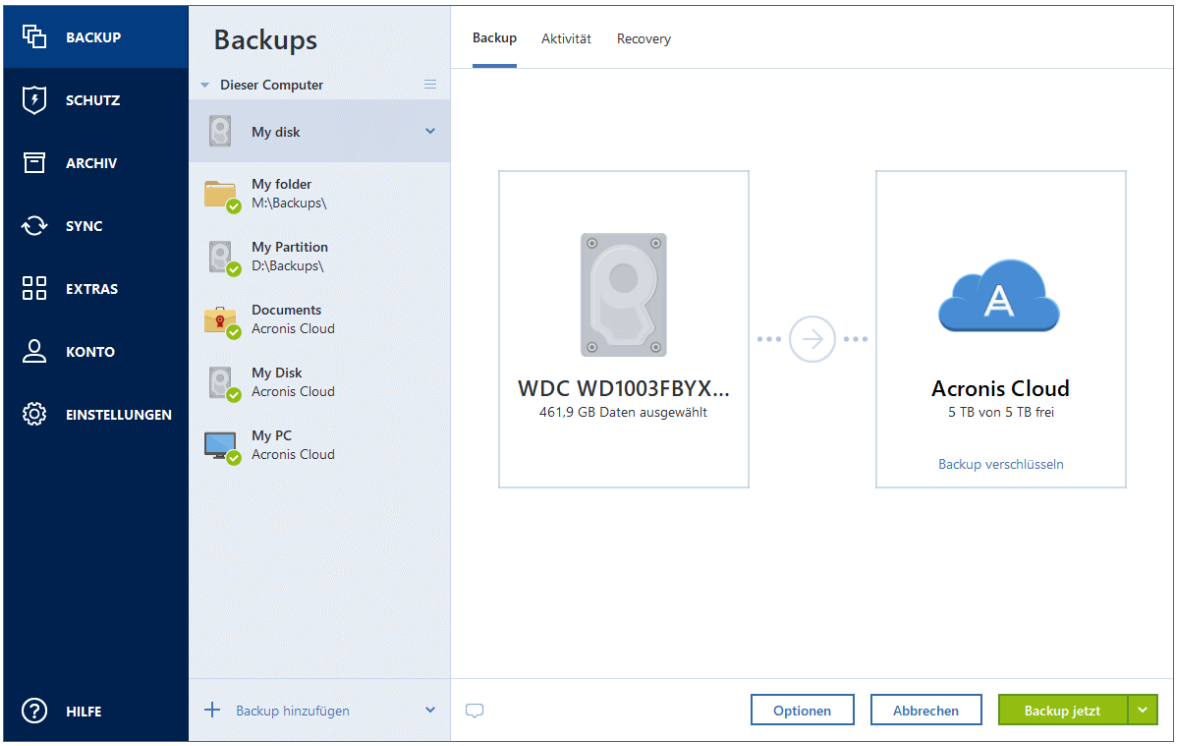
## Backups von Laufwerken und Volumes

Im Gegensatz zu Datei-Backups enthalten Laufwerk- und Volume-Backups alle auf dem entsprechenden Laufwerk bzw. Volume gespeicherten Daten. Dieser Backup-Typ wird üblicherweise verwendet, um von dem System-Volume oder dem kompletten System-Laufwerk eine exakte Kopie zu erstellen. Ein solches Backup ermöglicht die Wiederherstellung Ihres Computers, wenn Windows nicht mehr richtig arbeitet oder nicht mehr starten kann.

***So können Sie Backups von Laufwerken und Volumes erstellen***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Backup**.
3. Klicken Sie auf **Backup hinzufügen**.
4. [Optional] Um ein Backup umzubenennen, müssen Sie zuerst auf den Pfeil neben dem Backup-Namen und dann auf **Umbenennen** klicken. Geben Sie anschließend den gewünschten neuen Namen ein.
5. Klicken Sie auf den Bereich **Backup-Quelle** und wählen Sie **Laufwerke und Volumes**.
6. Aktivieren Sie im geöffneten Fenster die Kontrollkästchen, die neben den zu sichernden Volumes und Laufwerken liegen, und klicken Sie dann auf **OK**.
   Klicken Sie auf **Vollständige Volume-Liste**, damit Ihnen versteckte Volumes (Partitionen) angezeigt werden.

**Hinweis**
Zur Sicherung dynamischer Datenträger können Sie nur den Volume-Modus verwenden.




7. Klicken Sie auf den Bereich **Backup-Ziel** und wählen Sie dann einen Zielort für das Backup:
   - **Acronis Cloud** – Melden Sie sich an Ihrem Konto an und klicken Sie dann auf **OK**.
   - **Ihr externes Laufwerk** – Falls ein externes Laufwerk an Ihrem Computer angeschlossen ist, können Sie dieses aus der Liste auswählen.
   - **NAS** – Wählen Sie ein NAS-Gerät aus der Liste der gefundenen NAS-Geräte. Falls Sie nur ein (1) NAS-Gerät haben, wird Acronis Cyber Protect Home Office vorschlagen, dieses als Standardziel für Backups zu verwenden.
   - **Durchsuchen** – Wählen Sie einen Zielordner aus dem Verzeichnisbaum.

   **Hinweis**
   Vermeiden Sie es möglichst, die Backups Ihres System-Volumes auf dynamischen Datenträgern zu speichern, da das System-Volume unter einer Linux-basierten autonomen Notfallversion wiederhergestellt wird. Linux und Windows gehen aber auf unterschiedliche Art mit dynamischen Datenträgern um. Das kann bei einer Wiederherstellung wiederum zu Problemen führen.

8. [Optionaler Schritt] Klicken Sie auf **Optionen**, um die Einstellungen des betreffenden Backups zu konfigurieren. Zu weiteren Informationen siehe Backup-Optionen.
9. [Optionaler Schritt] Klicken Sie auf das Symbol **Kommentar hinzufügen** und geben Sie dann einen gewünschten Kommentar für die Backup-Version ein. Backup-Kommentare erleichtern Ihnen das Auffinden einer gewünschten Backup-Version, wenn Sie Ihre Daten zu einem späteren Zeitpunkt wiederherstellen wollen.
10. Gehen Sie folgendermaßen vor:

- Klicken Sie auf **Backup jetzt**, um das Backup umgehend auszuführen.
- Wenn Sie möchten, dass das Backup zu einem späteren Zeitpunkt oder nach Planung ausgeführt wird, dann klicken Sie auf den rechts neben der Schaltfläche **Backup jetzt** liegenden Pfeil und anschließend auf **Später**.

**Hinweis**
Wenn Sie Ihre Daten in die Acronis Cloud sichern, kann die Fertigstellung des ersten Backups eine längere Zeit in Anspruch nehmen. Spätere Backup-Prozesse werden voraussichtlich schneller ablaufen, da via Internet nur Änderungen an den Dateien gesichert werden.

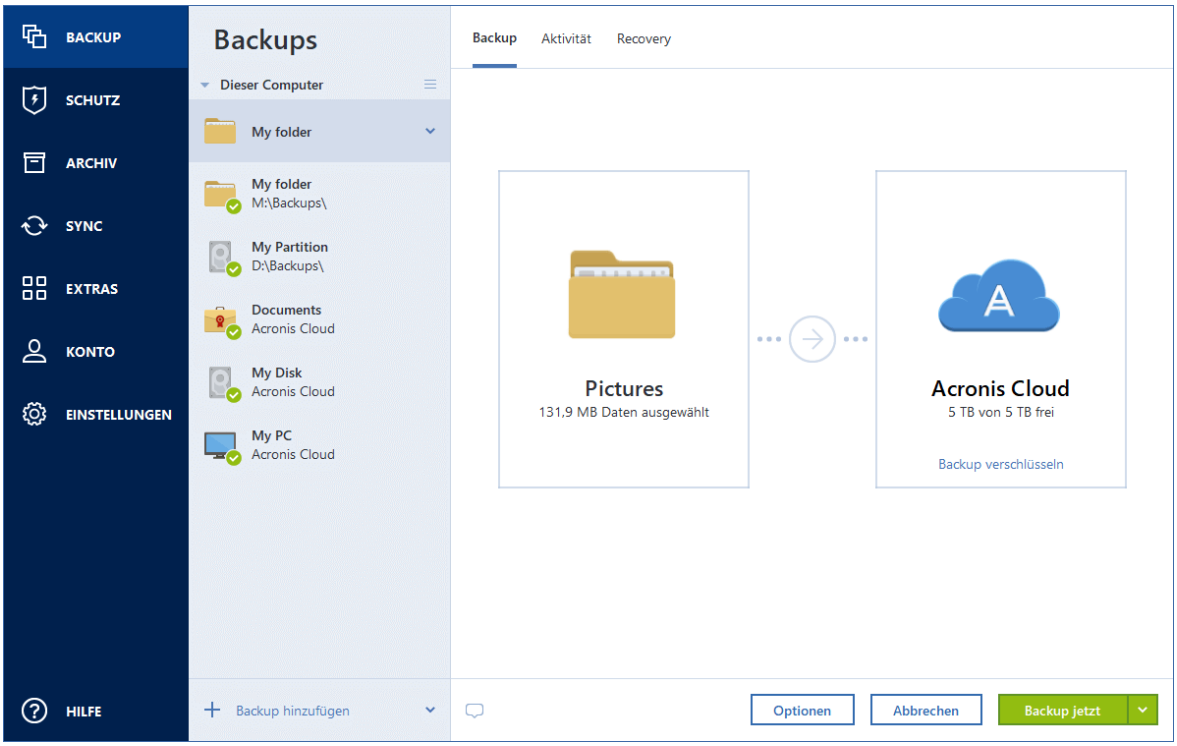
**Hinweis**
Sobald ein Online Backup gestartet wurde, können Sie Acronis Cyber Protect Home Office problemlos schließen. Der eigentliche Backup-Prozess läuft währenddessen als Hintergrundprozess weiter. Wenn Sie das Backup pausieren, Ihren Computer ausschalten oder die Verbindung zum Internet trennen, wird der Backup-Prozess fortgesetzt, sobald Sie auf 'Backup jetzt' klicken oder sobald die Internetverbindung wiederhergestellt ist. Auch wenn ein Backup unterbrochen wurde, werden Ihre Daten nicht doppelt hochgeladen.

# Backup von Dateien und Ordnern

Um bestimmte Dateien wie Dokumente, Fotos, Musik- und Videodateien zu schützen, ist es nicht notwendig, das komplette Volume (welches die Dateien enthält) zu sichern. Sie können auch die einzelnen Dateien und Ordner sichern.

***So können Sie Backups von Dateien und Ordnern erstellen***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Backup**.
3. Klicken Sie auf **Backup hinzufügen**.
4. [Optional] Um ein Backup umzubenennen, müssen Sie zuerst auf den Pfeil neben dem Backup-Namen und dann auf **Umbenennen** klicken. Geben Sie anschließend den gewünschten neuen Namen ein.
5. Klicken Sie auf den Bereich **Backup-Quelle** und wählen Sie dann **Dateien und Ordner**.
6. Aktivieren Sie im geöffneten Fenster die Kontrollkästchen, die neben den zu sichernden Dateien und Ordnern liegen, und klicken Sie dann auf **OK**.




7. Klicken Sie auf den Bereich **Backup-Ziel** und wählen Sie dann einen Zielort für das Backup:
   - **Acronis Cloud** – Melden Sie sich an Ihrem Konto an und klicken Sie dann auf **OK**.

     Sollten Sie noch kein Acronis Konto haben, dann klicken Sie auf **Konto erstellen**, geben Sie Ihre E-Mail-Adresse und ein Kennwort ein – und klicken Sie dann auf die Schaltfläche **Konto erstellen**. Weitere Informationen finden Sie im Abschnitt 'Acronis Konto'.
   - **Ihr externes Laufwerk** – Falls ein externes Laufwerk an Ihrem Computer angeschlossen ist, können Sie dieses aus der Liste auswählen.
   - **NAS** – Wählen Sie ein NAS-Gerät aus der Liste der gefundenen NAS-Geräte. Falls Sie nur ein (1) NAS-Gerät haben, wird Acronis Cyber Protect Home Office vorschlagen, dieses als Standardziel für Backups zu verwenden.
   - **Durchsuchen** – Wählen Sie einen Zielordner aus dem Verzeichnisbaum.
8. [Optionaler Schritt] Klicken Sie auf **Optionen**, um die Einstellungen des betreffenden Backups zu konfigurieren. Zu weiteren Informationen siehe Backup-Optionen.
9. [Optionaler Schritt] Klicken Sie auf das Symbol **Kommentar hinzufügen** und geben Sie dann einen gewünschten Kommentar für die Backup-Version ein. Backup-Kommentare erleichtern Ihnen das Auffinden einer gewünschten Backup-Version, wenn Sie Ihre Daten zu einem späteren Zeitpunkt wiederherstellen wollen.
10. Gehen Sie folgendermaßen vor:
    - Klicken Sie auf **Backup jetzt**, um das Backup umgehend auszuführen.
    - Wenn Sie möchten, dass das Backup zu einem späteren Zeitpunkt oder nach Planung ausgeführt wird, dann klicken Sie auf den rechts neben der Schaltfläche **Backup jetzt** liegenden nach unten zeigenden Pfeil und anschließend auf **Später**.

**Hinweis**
Wenn Sie Ihre Daten in die Acronis Cloud sichern, kann die Fertigstellung des ersten Backups eine längere Zeit in Anspruch nehmen. Spätere Backup-Prozesse werden voraussichtlich schneller ablaufen, da via Internet nur Änderungen an den Dateien gesichert werden.

Zusätzlich können Sie sich englischsprachige Video-Anleitungen unter folgender Adresse anschauen: https://goo.gl/i4J1AN.

# Mobilgeräte per Backup sichern

Falls Sie ein iOS- oder Android-Smartphone haben, können Sie Acronis Cyber Protect Home Office verwenden, um damit Ihre 'mobilen Daten' (wie Fotos, Videos, Kontakte und Kalendereinträge) zu sichern. Ausführlichere Informationen finden Sie im Abschnitt 'Acronis Mobile'.

Bevor Sie ein Backup endgültig starten, müssen Sie festlegen, wo dieses gespeichert werden soll: In der Acronis Cloud oder auf einem lokalen Speichergerät ihres Computers. Sie können den Zielort auch später ändern, aber Sie können nicht beide Backup-Ziele gleichzeitig verwenden. Verwenden Sie die Acronis Mobile App, um Daten in die Acronis Cloud zu sichern. Weitere Informationen finden Sie im Abschnitt 'Backup Ihres Mobilgerätes in die Acronis Cloud'.

***So können Sie Mobilgerätedaten zu einem lokalen Storage auf Ihrem Computer sichern***

1. Folgende Voraussetzungen müssen erfüllt sein:
   - Acronis True Image (2017 oder höher) oder Acronis Cyber Protect Home Office ist auf Ihrem Computer installiert.
   - Auf Ihrem Mobilgerät ist die Acronis Mobile App installiert.
   - Ihr Computer und das Mobilgerät befinden sich im selben (W)LAN.
2. Auf Ihrem Computer:
   a. Starten Sie Acronis True Image (2017 oder höher) oder Acronis Cyber Protect Home Office.
   b. Klicken Sie in der Seitenleiste auf **Backup** und dann auf **Backup hinzufügen**.
   c. Klicken Sie auf den Bereich **Backup-Quelle** und wählen Sie **Mobilgerät**.
      Es wird ein QR-Code angezeigt. Schließen Sie dieses Fenster nicht, weil es gleich benötigt wird.
3. Auf Ihrem Mobilgerät:
   a. Acronis Mobile starten.
   b. Tippen Sie auf ein Plus-Symbol, um ein Backup zu erstellen. Beachten Sie, dass dieser Schritt nicht erscheint, wenn Sie Ihr Mobilgerät das erste Mal per Backup sichern.
   c. Wählen Sie einen Computer als Backup-Ziel.
   d. Tippen Sie auf **QR-Code scannen**, erfassen Sie den QR-Code auf dem Computer-Bildschirm mit Ihrer Kamera – und warten Sie dann, bis das Mobilgerät mit dem Computer verbunden ist.

e. Wählen Sie die Datenkategorien aus, die Sie sichern wollen – oder tippen Sie auf **Bestätigen**, wenn Sie alle Kategorien sichern wollen.
f. Erlauben Sie, dass Acronis Mobile auf Ihre persönlichen Daten zugreifen darf.
g. [Optionaler Schritt] Geben Sie ein Kennwort ein, um das Backup per Verschlüsselung zu schützen. Anderenfalls können Sie auf **Verschlüsselung überspringen** tippen.
h. Tippen Sie auf **Backup starten**.

Wenn das Backup gestartet ist, können Sie dessen Verlauf in beiden Applikationen (auf dem Computer oder Mobilgerät) verfolgen. Fehler und Warnmeldungen werden jedoch nur in der Mobile App angezeigt.

Sie können Acronis Cyber Protect Home Office auf Ihrem Computer und die Acronis Mobile App nun schließen. Das Backup wird automatisch im Hintergrund fortgesetzt.

Wenn Sie möchten, dass Änderungen an den Daten (beispielsweise neue Fotos) automatisch gesichert werden sollen, aktivieren Sie die Einstellung **Kontinuierliches Backup**. Falls diese Einstellung ausgeschaltet ist, werden neue Daten nur dann gesichert, wenn Sie manuell auf **Backup** tippen. Weitere Informationen finden Sie im Abschnitt 'Einstellungen der Mobile App'.

Wenn Sie bei einem Mobilgeräte-Backup das Backup-Ziel von 'lokaler Storage' zu 'Acronis Cloud' ändern, geht die Verbindung zwischen dem Mobilgerät und dem Computer verloren. Acronis Cyber Protect Home Office hört daraufhin damit auf, das Mobilgeräte-Backup in der Liste mit dem Mobilgerät zu assoziieren. Wenn Sie das Ziel dann wieder zurück auf 'lokaler Storage' ändern wollen, müssen Sie die Verbindung erneut aufbauen. Die Verbindung kann außerdem auch aufgrund eines Fehlers verloren gehen. Wählen Sie, um die Verbindung wiederherzustellen, das Mobilgeräte-Backup in der Backup-Liste von Acronis Cyber Protect Home Office aus, klicken Sie auf **Neu verbinden** und scannen Sie anschließend den QR-Code mit Ihrem Mobilgerät. Danach wird das Backup wieder normal mit den gleichen Einstellungen fortgesetzt.

## Acronis Mobile

**Hinweis**
Acronis Cloud ist möglicherweise in Ihrer Region nicht verfügbar. Für weitere Informationen klicken Sie hier: https://kb.acronis.com/content/4541

Mit Acronis Mobile können Sie die Daten Ihres Gerätes in die Acronis Cloud und/oder zu einem lokalen Storage auf Ihrem Computer sichern – um diese von dort (bei Datenverlust oder Datenbeschädigung) wiederherstellen zu können. Beachten Sie, dass Sie zur Backup-Erstellung in den Cloud Storage ein Acronis-Konto und ein Acronis Cloud-Abonnement benötigen.

Weitere Informationen über die Kernfunktionen von Acronis Mobile sowie die unterstützten Geräte finden Sie in der 'Dokumentation für Acronis Mobile'.

## Wo finde ich diese Apps?

Weitere Informationen über Acronis Mobile sowie die Möglichkeit zum Download/zur Installation finden Sie im Apple App Store oder Google Play Store.

- Acronis Mobile für iOS-Geräte: https://go.acronis.com/atimobile/download/iOS
- Acronis Mobile für Android-Geräte: https://go.acronis.com/atimobile/download/Android

## Lokaler Zielort für Backups von Mobilgeräten

Wenn Sie die Daten Ihres Mobilgerätes zu einem Computer sichern, speichert Acronis Mobile die entsprechenden Backups im folgenden Standardordner: *C:\ProgramData\Acronis Mobile Backup Data\acronis-local-data*. Wenn Sie den Standardordner ändern, wird der Ordner *acronis-local-data* zu dem von Ihnen ausgewählten Speicherort als neuer Unterordner verschoben. Alle neu erstellten Mobile Backups werden dann zu dem neuen Speicherort erstellt.

**Hinweis**
Alle Mobile Backups werden immer in demselben Ordner gespeichert und können nicht getrennt werden.

***So können Sie den lokalen Zielort für die Backups von Mobilgeräten ändern:***

1. Klicken Sie in der Seitenleiste auf **Einstellungen** und suchen Sie die Option **Speicherort für Mobile Backup**.
2. Klicken Sie im Bereich **Speicherort für Mobile Backup** auf **Ändern**. Das Fenster **Speicherort ändern** wird angezeigt.
3. Klicken Sie auf **Speicherort auswählen** und bestimmen Sie dann das neue Ziel für die Backups. Beachten Sie, dass Sie nur einen Speicherort (Ordner) auswählen können, der auf einem Ihrer internen Festplattenlaufwerke liegt.

Klicken Sie auf **Auf Standard zurücksetzen**, um den neuen Speicherort wieder zurück auf den ursprünglichen zu ändern.

# Microsoft 365-Daten per Backup sichern

## Warum sollten Sie Microsoft 365-Daten per Backup sichern?

Microsoft 365 für Privatanwender ist zwar ein Set von Cloud-Diensten, ein regelmäßiges Backup bietet aber eine zusätzliche Schutzebene gegen Anwenderfehler und böswillige Angriffe. Acronis Cyber Protect Home Office kann Ihre Microsoft Outlook-Postfächer und Microsoft OneDrive-Daten schützen, indem es diese per Backup in die zuverlässige Acronis Cloud sichert. Außerdem können Sie nach dem Upload in die Acronis Cloud jederzeit und mit jedem internetfähigen Gerät auf all Ihre gesicherten Inhalte zugreifen (sofern das Gerät unterstützt und von Ihnen dazu berechtigt wird). Sie

können gelöschte Elemente auch dann noch aus einem Backup wiederherstellen, wenn die offizielle Microsoft 365-Aufbewahrungsdauer abgelaufen ist.

## Microsoft 365-Daten per Backup sichern

**Diese Daten in Ihrem Outlook-Postfach können Sie sichern:**

- Alle Ordner
- E-Mail-Nachrichten
- Anhänge

**Hinweis**
Sie können keine freigegebenen Postfächer oder Gruppenpostfächer sichern.

**Diese Daten in Ihrem OneDrive können Sie sichern:**

- Alle Dateien und Ordner

**So können Sie Ihre Microsoft 365-Daten sichern**

1. Öffnen Sie das Online Dashboard durch eine der folgenden Aktionen:
   - Folgen Sie diesem Link: https://cloud.acronis.com.
   - Klicken Sie in der Seitenleiste von Acronis Cyber Protect Home Office nacheinander auf **Backup**, **Backup hinzufügen**, dann in den Bereich **Backup-Quelle** und wählen Sie anschließend auf **Cloud Service**.
2. Melden Sie sich an Ihrem Acronis Konto an.
3. Klicken Sie in der Seitenleiste erst auf **Ressourcen**, dann auf **Hinzufügen** und anschließend auf **Microsoft 365 für Privatanwender**.
4. Melden Sie sich bei Aufforderung an Ihrem Microsoft-Konto an.
5. Wählen Sie im Bereich **Backup-Quelle** die Elemente, die per Backup gesichert werden sollen:
   - Komplettes Konto
   - Outlook
   - OneDrive
6. Klicken Sie auf **Fertig**.
7. Im Fensterbereich **Bereinigung** können Sie Bereinigungsregeln für das Backup konfigurieren. Sie können das Backup außerdem verschlüsseln und mit einem Kennwortschutz versehen. Klicken Sie auf **Anwenden**, wenn Sie fertig sind.
8. Klicken Sie zum Starten des Backups auf **Jetzt ausführen**.

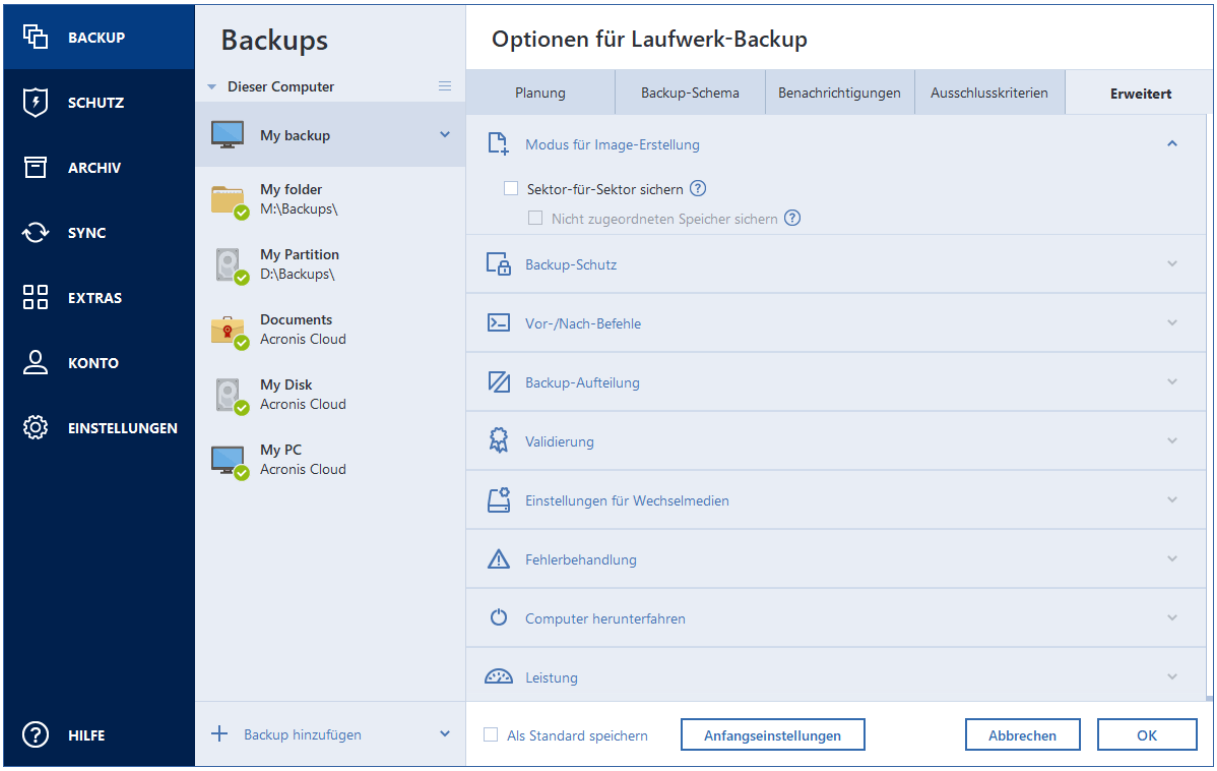
# Backup-Optionen

Sie können bei der Erstellung eines Backups eine Reihe von Optionen ändern und damit eine Feinabstufung des Backup-Prozess vornehmen. Wählen Sie zum Öffnen des entsprechenden

Fensters eine Quelle und ein Ziel für das zu erstellende Backup aus und klicken Sie dann auf **Optionen**.

Beachten Sie, dass die Optionen für die verschiedenen Backup-Typen (Laufwerk-Backup, Datei-Backup, Online Backup, Nonstop Backup) komplett unabhängig voneinander sind und daher von Ihnen einzeln konfiguriert werden sollten.

Alle Optionen werden nach Installation des Programms auf Ihre Anfangswerte eingestellt. Sie können diese für eine aktuelle Backup-Aktion oder für alle zukünftig erstellten Backups ändern. Aktivieren Sie das Kontrollkästchen **Einstellungen als Standard speichern**, um die geänderte Konfiguration für zukünftige Backup-Aktionen als Standard zu übernehmen.



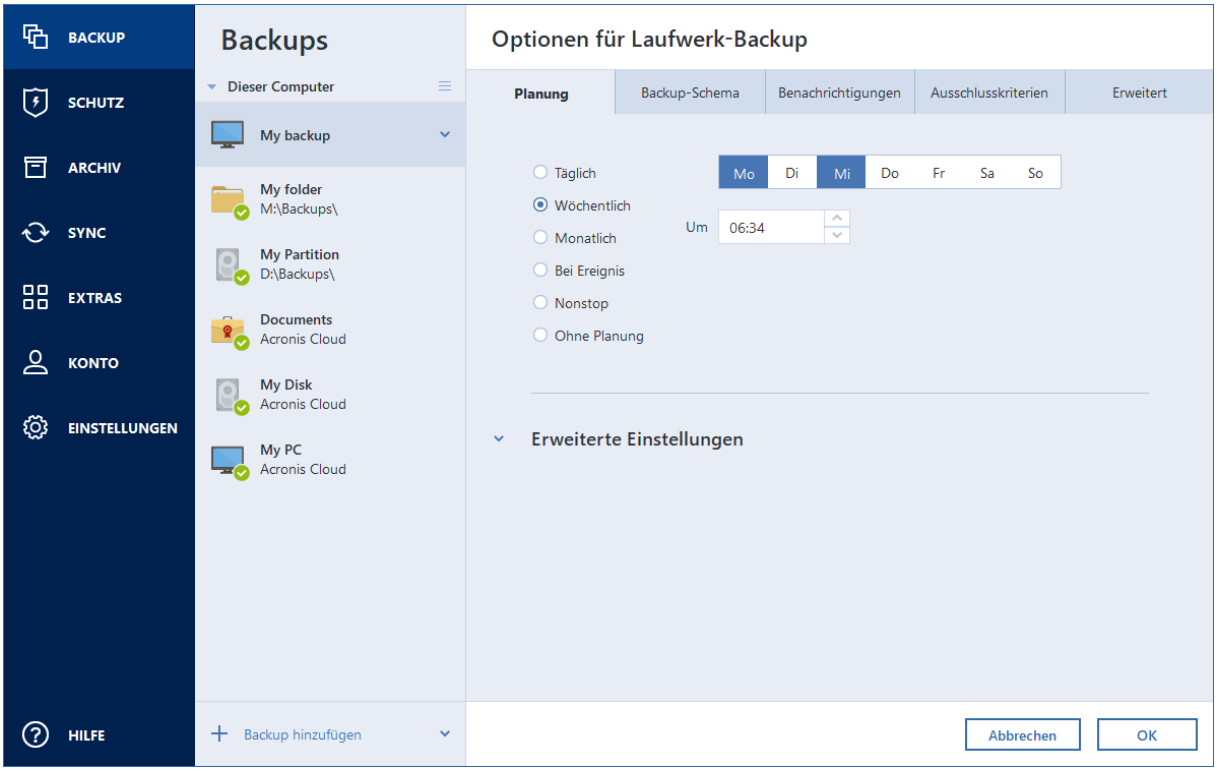

Klicken Sie auf die Schaltfläche **Auf Anfangseinstellungen zurücksetzen**, um alle geänderten Optionen auf ihre anfänglichen Werte (wie bei der Installation des Programms) zurückzusetzen. Beachten Sie, dass dies nur die Einstellungen für das aktuelle Backup zurücksetzt. Sie können die Einstellungen für alle zukünftigen Backups zurücksetzen, indem Sie auf **Auf Anfangseinstellungen zurücksetzen** klicken, dann das Kontrollkästchen **Einstellungen als Standard speichern** aktivieren und abschließend auf **OK** klicken.

Zusätzlich können Sie sich englischsprachige Video-Anleitungen unter folgender Adresse anschauen: https://goo.gl/bKZyaG.

## Planung

Speicherort: **Optionen** –> **Planung**

Die Registerkarte **Planung** ermöglicht Ihnen, Planungseinstellungen für Backups und Validierungen zu spezifizieren.




Sie können eine Planung für regelmäßig zu erstellende oder zu validierende Backups spezifizieren:

- **Täglich** – Die Aktion wird einmal am Tag oder noch häufiger ausgeführt.
- **Wöchentlich** – Die Aktion wird einmal oder mehrmals pro Woche an bestimmten Tagen ausgeführt.
- **Monatlich** – Die Aktion wird einmal oder mehrmals pro Monat an bestimmten Tagen ausgeführt.
- **Bei Ereignis** – Die Aktion wird bei Eintritt des gewählten Ereignisses ausgeführt.
- **Nonstop** – Die Aktion wird alle fünf Minuten ausgeführt.
- **Ohne Planung** – Der Scheduler wird für die aktuelle Aktion ausgeschaltet. In diesem Fall wird das Backup bzw. die Validierung nur ausgeführt, wenn Sie im Hauptfenster auf den Befehl **Backup jetzt** oder **Validieren** klicken.

## Erweiterte Einstellungen

Durch Klicken auf **Erweiterte Einstellungen** können Sie folgende, zusätzliche Optionen zur Planung von Backups und Validierungen einstellen:

- **Nur sichern, wenn der Computer gesperrt ist oder der Bildschirmschoner läuft** – Aktivieren Sie dieses Kontrollkästchen, um eine geplante Aktion auf das nächste Mal zu verschieben, bis der Computer wieder im Leerlauf arbeitet (wenn beispielsweise der Bildschirmschoner angezeigt wird oder der Computer gesperrt ist). Bei der Validierungsplanung wird das Kontrollkästchen zu **Validierung nur ausführen, wenn Computer im Leerlauf ist** geändert.

- **Computer aus Standby/Ruhezustand aufwecken** – Aktivieren Sie dieses Kontrollkästchen, wenn der Computer aus dem Standby- bzw. Ruhezustandsmodus aufweckt werden soll, um die geplante Aktion auszuführen.
- **Computer daran hindern, in Standby/Ruhezustand zu wechseln** – ktivieren Sie dieses Kontrollkästchen, um zu vermeiden, dass ein zeitaufwendiges Backup unterbrochen wird, weil der Computer sonst (normalerweise) in den Standby- oder Ruhezustandsmodus gehen würde.
- **Verpasste Aktionen beim Systemstart mit Verzögerung ausführen (in Minuten)** – Aktivieren Sie dieses Kontrollkästchen, um zu erzwingen, dass versäumte Aktionen beim nächsten Systemstart ausgeführt werden, wenn der Computer zur geplanten Zeit ausgeschaltet war und daher die geplante Aktion nicht ausgeführt wurde.

  Außerdem können Sie eine Zeitverzögerung vorgeben, damit das Backup nach dem Systemstart erstellt wird. Für ein Backup 20 Minuten nach dem Systemstart beispielsweise geben Sie in dem entsprechenden Kästchen die Zahl *20* ein.
- **Verpasste Aktionen ausführen, wenn ein externes Laufwerk angeschlossen wird** [optional, wenn Sie die Erstellung eines Backups zu einem USB-Laufwerk planen – oder die Validierung eines Backups, das auf einem solchen Laufwerk liegt] – Aktivieren Sie dieses Kontrollkästchen, damit eine verpasste Aktion ausgeführt, sobald das entsprechende USB-Laufwerk, welches zum geplanten Zeitpunkt entfernt war, erneut angeschlossen wird.

## Die Parameter für tägliche Backups

Sie können folgende Parameter für Backups einrichten, die täglich erstellt oder validiert werden sollen:

- **Alle** – Wählen Sie die tägliche Periodizität aus dem Listenfeld aus (z.B. alle 2 Stunden).
- **Einmal täglich** – Die Aktion startet einmal pro Tag zur spezifizierten Zeit.
- **Zweimal täglich** – Die Aktion wird zweimal am Tag gestartet. Bestimmen Sie den Zeitpunkt für jede der beiden Aktionen.

Eine Beschreibung der **Erweiterten Einstellungen** finden Sie unter Planung.

## Die Parameter für wöchentliche Backups

Sie können folgende Parameter für Backups einrichten, die wöchentlich erstellt oder validiert werden sollen:

- **Wochentage** – Wählen Sie die Tage aus, an denen die Aktion ausgeführt werden soll.
- **Um** – Bestimmen Sie den Startzeitpunkt der Aktion.

Eine Beschreibung der **Erweiterten Einstellungen** finden Sie unter Planung.

## Die Parameter für monatliche Backups

Sie können folgende Parameter für Backups einrichten, die monatlich erstellt oder validiert werden sollen:

- **Alle** – Wählen Sie eine Ziffer und einen Wochentag aus den Listenfeldern aus. Wählen Sie beispielsweise **Jeden ersten Montag** aus, damit die Aktion an jedem ersten Montag im Monat ausgeführt wird.
- **An bestimmten Tagen des Monats** – Bestimmen Sie das/die Datum/Daten für das Backup. Sie können die Aktion beispielsweise am 10. und am letzten Tag des Monats ausführen lassen.
- **Um** – Bestimmen Sie den Startzeitpunkt der Aktion.

Eine Beschreibung der **Erweiterten Einstellungen** finden Sie unter Planung.

### Parameter zur Ausführung bei einem Ereignis

Sie können folgende Parameter für Backups einrichten, die auf ein bestimmten Ereignis hin erstellt oder validiert werden sollen:

- **Nur einmal pro Tag** – Aktivieren Sie dieses Kontrollkästchen, wenn die Aktion nur beim ersten Auftreten des Ereignisses am aktuellen Tag ausgeführt werden soll.
- Spezifizieren Sie das Ereignis, welches die Backup-Erstellung oder -Validierung auslösen soll:
  - **Wenn ein externes Laufwerk angeschlossen wird** – Die Aktion wird jedes Mal ausgeführt, wenn dasjenige externe Gerät (USB-Stick oder externe Festplatte), welches Sie zuvor als Backup-Ziel verwendet haben, an Ihren Computer angeschlossen wird. Beachten Sie, dass Windows dieses Gerät auch als ein 'externes Gerät' erkennen sollte.
  - **Benutzeranmeldung** – Die Aktion wird jedes Mal ausgeführt, wenn sich der aktuelle Benutzer am Betriebssystem anmeldet.
  - **Benutzerabmeldung** – Die Aktion wird jedes Mal ausgeführt, wenn sich der aktuelle Benutzer vom Betriebssystem abmeldet.
  - **System herunterfahren oder Neustart** – Die Aktion wird vor jedem Herunterfahren oder Neustart des Computers ausgeführt.
  - **Systemstart mit Verzögerung (in Minuten)** – Die Aktion wird bei jedem Start des Betriebssystems und mit der von Ihnen spezifizierte Verzögerungszeit ausgeführt.

Eine Beschreibung der **Erweiterten Einstellungen** finden Sie unter Planung.

## Backup-Schemata

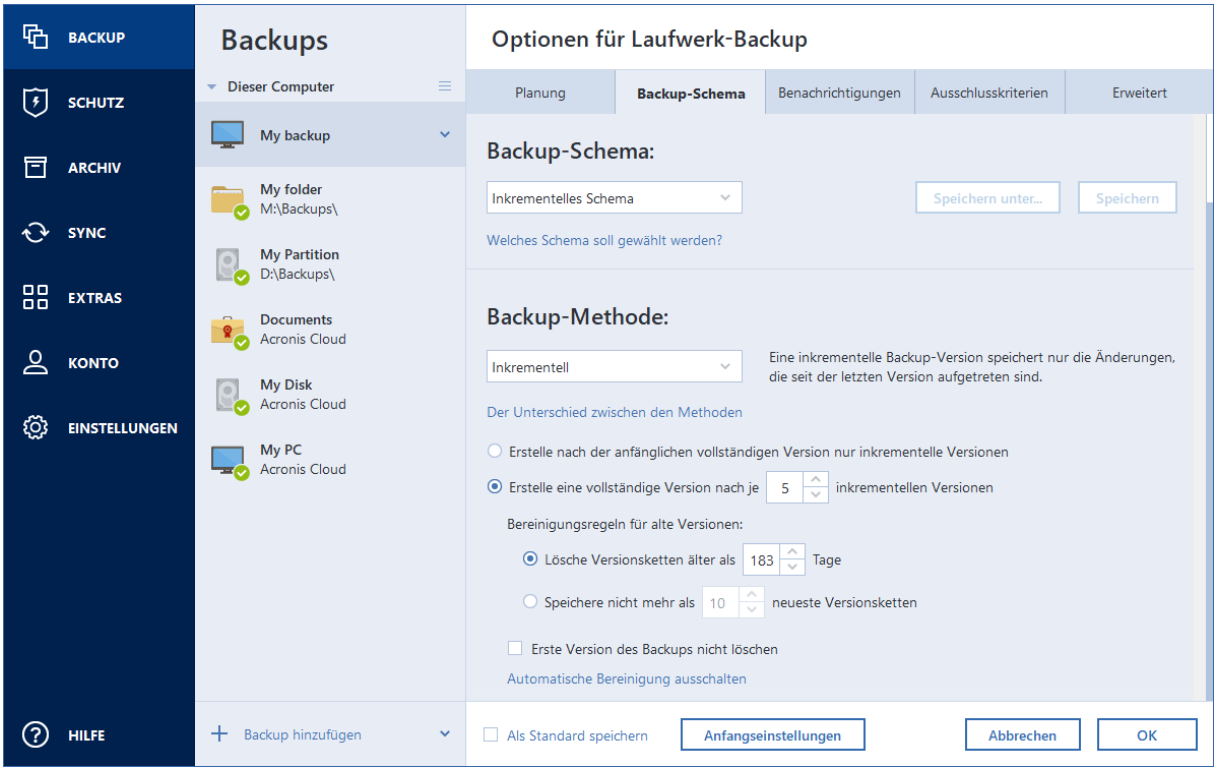
Speicherort: **Optionen** –> **Backup-Schema**

Backup-Schemata helfen Ihnen zusammen mit dem Scheduler, eine für Sie passende Backup-Strategie aufzustellen. Die Schemata ermöglichen Ihnen, die Speicherplatzbelegung des Backup Storages zu optimieren, die Zuverlässigkeit der Datenspeicherung zu verbessern und veraltete Backup-Versionen automatisch löschen zu lassen.

**Hinweis**
Bei Online Backups ist das Backup-Schema voreingestellt und kann nicht geändert werden. Nach dem anfänglichen Voll-Backup werden nur noch inkrementelle Versionen erstellt.

Das Backup-Schema definiert folgende Parameter:

- Die zur Erstellung von Backup-Versionen verwendeten Backup-Methoden (vollständig, differentiell oder inkrementell)
- Die Sequenz der mit verschiedenen Methoden erstellten Backup-Versionen
- Bereinigungsregeln für Versionen




Acronis Cyber Protect Home Office ermöglicht Ihnen, folgende Backup-Schemata zu wählen:

- **Schema 'Eine Version'** – Wählen Sie dieses Schema, wenn Sie den kleinsten Backup Storage verwenden wollen.
- **Schema 'Versionskette'** – Dieses Schema ist in den meisten Fällen optimal.
- **Inkrementelles Schema** – Wählen Sie dieses Schema, damit nach jeweils fünf inkrementellen Versionen eine vollständige erstellt wird. Dies ist das Standardschema.
- **Differentielles Schema** – Wählen Sie dieses Schema, damit nach einem anfänglichen Voll-Backup nur differentielle Backups erstellt werden.
- **Benutzerdefiniertes Schema** – Wählen Sie diese Option, um ein manuelles Backup-Schema zu erstellen.

Sie können auch für ein bereits vorhandenes Backup das Backup-Schema leicht ändern. Die Integrität der Backup-Kette wird dadurch nicht beeinflusst. Sie können Ihre Daten weiterhin aus jeder früheren Backup-Version wiederherstellen.

**Hinweis**
Sie können das Backup-Schema nicht ändern, wenn Sie Backups auf optische Medien wie DVDs/BDs durchführen. In diesem Fall verwendet Acronis Cyber Protect Home Office standardmäßig ein benutzerdefiniertes Schema, bei dem nur Voll-Backups erstellt werden. Hintergrund ist, dass das Programm keine Backups konsolidieren kann, die auf optischen Medien gespeichert sind.

## Schema 'Eine Version'

Dieses Backup-Schema ist für Laufwerk- und Datei-Backups identisch (mit Ausnahme der Planungseinstellungen).

Das Programm erstellt eine Voll-Backup-Version und überschreibt diese jedes Mal – gemäß vorgegebener Planung oder bei manueller Backup-Ausführung. Bei diesem Prozess wird die alte Version nur dann gelöscht, wenn zuvor eine neue erstellt wurde.

**Hinweis**
Die allererste Datei bleibt für Hilfszwecke erhalten, ohne dass Ihre Daten in dieser enthalten sind. Löschen Sie diese bitte nicht!

Planungseinstellungen für Laufwerk-Backups: monatlich.

Planungseinstellungen für Datei-Backups: täglich.

Ergebnis: Sie haben eine einzelne, aktuelle Voll-Backup-Version.

Benötigter Speicherplatz: minimal.

## Schema 'Versionskette'

Dieses Backup-Schema unterscheidet sich für die Backup-Typen 'Laufwerke' und 'Dateien'.

**Versionskette für Laufwerk-Backups**

Das Programm erstellt zuerst die erste Voll-Backup-Version. Diese Version wird solange aufbewahrt, bis Sie sie manuell löschen. Danach erstellt das Programm entsprechend einer vorgegebenen Planung (oder bei manueller Sicherung): 1 Voll- und 5 differentielle Backup-Versionen, danach erneut 1 Voll- und 5 differentielle Backup-Versionen und so weiter. Die Versionen werden für 6 Monate gespeichert. Nach Ablauf dieser Zeitspanne analysiert das Programm, ob die ältesten Backup-Versionen (mit Ausnahme der ersten Voll-Version) gelöscht werden können. Es hängt von der minimalen Versionsanzahl (acht) und der Konsistenz der Versionsketten ab. Das Programm löscht nacheinander die ältesten Versionen, sobald neue Versionen mit derselben Backup-Methode erstellt wurden (beispielsweise wird je die älteste differentielle Version nach Erstellung einer neuen differentiellen Version gelöscht). Zuerst werden die ältesten differentiellen Versionen gelöscht, dann die älteste Voll-Version.

Backup-Planungseinstellungen: monatlich.

Ergebnis: Sie haben monatliche Backup-Versionen der letzten 6 Monate, einschließlich der anfänglichen Voll-Backup-Version (die Sie evtl. für eine längere Zeitspanne bewahren wollen).

Benötigter Speicherplatz: ist abhängig von der Anzahl und Größe der Versionen.

**Versionskette für Datei-Backups**

Entsprechend einer vorgegebenen Planung (oder bei manueller Sicherung) erstellt das Programm: 1 Voll- und 6 inkrementelle Backup-Versionen, danach erneut 1 Voll- und 6 inkrementelle Versionen und so weiter. Die Versionen werden für 1 Monat gespeichert. Nach Ablauf dieser Zeitspanne analysiert das Programm, ob die ältesten Backup-Versionen gelöscht werden können. Dies ist abhängig von der Konsistenz der Versionskette. Das Programm löscht zur Erhaltung der Konsistenz die ältesten Versionen der „1 Voll- und 6 inkrementelle Backup-Versionen"-Ketten, nachdem eine neue, entsprechende Versionskette erstellt wurde.

Backup-Planungseinstellungen: täglich.

Ergebnis: Sie verfügen über Backup-Versionen für jeden Tag des letzten Monats.

Benötigter Speicherplatz: ist abhängig von der Anzahl und Größe der Versionen.

## Benutzerdefinierte Schemata

Mit Acronis Cyber Protect Home Office können Sie auch eigene benutzerdefinierte Backup-Schemata erstellen. Als Basis für die Schemata können die vordefinierten Backup-Schemata dienen. Nehmen Sie am ausgewählten vordefinierten Schema die für Ihre Anforderungen erforderlichen Änderungen vor und speichern Sie dann das geänderte Schema als neues Schema.

**Hinweis**
Sie können die vorhandenen, vordefinierten Backup-Schemata nicht überschreiben.

Es ist außerdem möglich, völlig neue benutzerdefinierte Schemata zu erstellen, die auf vollständigen, differentiellen oder inkrementellen Backup-Versionen basieren.

Wählen Sie daher als erstes eine der Backup-Methoden in der entsprechenden Box.

- Vollständig

  Wählen Sie diese Methode, wenn Sie lediglich Voll-Backup-Versionen erstellen wollen.
- Inkrementell

  Wählen Sie diese Methode, wenn Sie Backup-Ketten erstellen wollen, die nur vollständige und inkrementelle Backup-Versionen enthalten sollen.

  Sie können das Schema unter Verwendung einer der folgenden Optionen konfigurieren:
  - **Erstelle nach der anfänglichen vollständigen Version nur inkrementelle Versionen** – Wählen Sie diese Option, um nur eine Backup-Versionskette zu erstellen. Für diese Option ist die Funktion 'Automatische Bereinigung' nicht verfügbar.
  - **Erstelle eine vollständige Version nach je [n] inkrementellen Versionen** – Wählen Sie diese Option, um mehrere Backup-Versionsketten zu erstellen. Dieses Backup-Schema ist zuverlässiger, benötigt aber auch mehr Speicherplatz.

- Differentiell

  Wählen Sie diese Methode, wenn Sie Backup-Ketten erstellen wollen, die nur vollständige und differentielle Backup-Versionen enthalten sollen.

  Sie können das Schema unter Verwendung einer der folgenden Optionen konfigurieren:
  - **Erstelle nach der anfänglichen vollständigen Version nur differentielle Versionen** – Wählen Sie diese Option, um nur eine Backup-Versionskette zu erstellen. Für diese Option ist die Funktion 'Automatische Bereinigung' nicht verfügbar.
  - **Erstelle eine vollständige Version nach je [n] differentiellen Versionen** – Wählen Sie diese Option, um mehrere Backup-Versionsketten zu erstellen. Dieses Backup-Schema ist zuverlässiger, benötigt aber auch mehr Speicherplatz.

**Automatische Bereinigung einschalten**

- **Bereinigungsregeln für alte Versionen** – Zur automatischen Löschung veralteter Backup-Versionen können Sie eine der folgenden Bereinigungsregeln konfigurieren:
  - **Lösche Versionen älter als [n] Tage** [nur bei der vollständigen Methode verfügbar] – Verwenden Sie diese Option, um das Alter der Backup-Versionen zu begrenzen. Alle Versionen, die älter als die spezifizierte Zeitspanne sind, werden automatisch gelöscht.
  - **Lösche Versionsketten älter als [n] Tage** [nur bei inkrementellen und differentiellen Methoden verfügbar] – Verwenden Sie diese Option, um das Alter der Backup-Versionsketten zu begrenzen. Die älteste Versionskette wird nur dann gelöscht, wenn die jüngste Backup-Version dieser Kette älter als die spezifizierte Zeitspanne ist.
  - **Speichere nicht mehr als [n] neueste Versionen** [nur für vollständige Methode verfügbar] – Wählen Sie diese Einstellung, um die maximale Anzahl an Backup-Versionen zu begrenzen. Wenn die Anzahl an Versionen den angegebenen Wert übersteigt, wird die älteste Backup-Version automatisch gelöscht.
  - **Speichere nicht mehr als [n] neueste Versionsketten** [nur für inkrementelle und differentielle Methoden verfügbar] – Wählen Sie diese Einstellung, um die maximale Anzahl an Backup-Versionsketten zu begrenzen. Wenn die Anzahl an Versionsketten den angegebenen Wert übersteigt, wird die älteste Backup-Versionskette automatisch gelöscht.
  - **Backup nicht größer werden lassen als [vordefinierte Größe]** [nicht für lokale Backups verfügbar] – Verwenden Sie diese Option, um die maximale Größe des Backups zu begrenzen. Das Programm überprüft nach Erstellung einer neuen Backup-Version, ob die Gesamtgröße des Backups den spezifizierten Wert überschreitet. Falls zutreffend, wird die älteste Backup-Version gelöscht.
- **Erste Version des Backups nicht löschen** – Aktivieren Sie dieses Kontrollkästchen, um den anfänglichen Datenbestand zu bewahren. Das Programm wird darauf zwei anfängliche Voll-Backup-Versionen erstellen. Die erste Version wird von der automatischen Bereinigung ausgeschlossen und solange gespeichert, bis Sie es manuell löschen. Wenn Sie sich zur Verwendung einer inkrementellen oder differentiellen Backup-Methode entschieden haben, startet die entsprechende, erste Backup-Kette von der zweiten Voll-Backup-Version. Daher ist nur die dritte Version des Backups eine inkrementelle oder differentielle. Beachten Sie, dass, wenn das Kontrollkästchen für die vollständige Methode aktiviert ist, die Option **Speichere nicht mehr**

**als [n] neueste Versionen** zu **Speichere nicht mehr als 1+[n] neueste Versionen** geändert wird.

## Backup-Schemata verwalten

Wenn Sie an einem vorhandenen Backup-Schema Änderungen vornehmen, können Sie es als neues Backup-Schema speichern. Sie müssen in diesem Fall einen neuen Namen für das Backup-Schema vergeben.

- Sie können vorhandene, benutzerdefinierte Backup-Schemata überschreiben.
- Sie können die vorhandenen, vordefinierten Backup-Schemata nicht überschreiben.
- Im Namen eines Schemas sind alle unter dem Betriebssystem für Dateinamen zulässigen Zeichen erlaubt. Der Name eines Backup-Schemas darf eine maximale Länge von 255 Zeichen haben.
- Sie können bis zu 16 benutzerdefinierte Backup-Schemata erstellen.

Ein benutzerdefiniertes Backup-Schema können Sie nach Erstellen wie jedes andere Backup-Schema für die Konfiguration eines Backups verwenden.

Sie können ein benutzerdefiniertes Backup-Schema auch verwenden, ohne es zu speichern. In diesem Fall ist es nur für das Backup verfügbar, für das es erstellt wurde; Sie können es nicht für andere Backups verwenden.

Wenn Sie ein benutzerdefiniertes Backup-Schema nicht mehr benötigen, können Sie es löschen. Wählen Sie das Schema, das gelöscht werden soll, aus der Liste der Backup-Schemata aus, klicken Sie auf **Löschen** und bestätigen Sie die Aktion im Fenster **Schema löschen**.

**Hinweis**
Vordefinierte Backup-Schemata können nicht gelöscht werden.

## Beispiele für benutzerdefinierte Schemata

### 1. Backup des kompletten PC – Zwei Vollversionen

Typischer Fall: Sie möchten alle Daten auf Ihrem Computer mit zwei Vollversionen sichern und das Backup einmal im Monat aktualisieren. Betrachten wir, wie Sie dies unter Verwendung eines benutzerdefinierten Schemas durchführen können.

1. Starten Sie damit, ein Backup des kompletten PCs zu konfigurieren. Weitere Informationen finden Sie im Abschnitt 'Alle Daten auf Ihrem PC sichern'.
2. Stellen Sie sicher, dass 'Kompletter PC' als Backup-Quelle ausgewählt ist.
3. Klicken Sie auf **Optionen**, öffnen Sie die Registerkarte **Planung**, klicken Sie auf **Monatlich** und spezifizieren Sie dann einen Tag des Monats (beispielsweise den 20.). Als Ergebnis wird jeden Monat – und zwar an dem von Ihnen spezifizierten Tag – eine Backup-Version erstellt. Spezifizieren Sie anschließend einen Startzeitpunkt für die Backup-Aktion.
4. Öffnen Sie die Registerkarte **Backup-Schema** und wählen Sie die Option **Benutzerdefiniertes Schema** (statt **Inkrementelles Schema**).

5. Wählen Sie in der Box **Backup-Methode** das Element **Vollständig** aus dem Listenfeld aus.
6. Wenn Sie die Anzahl der Versionen begrenzen wollen, klicken Sie auf **Speichere nicht mehr als [n] neueste Versionen**, geben Sie **2** ein und klicken Sie abschließend auf **OK**.
   In diesem Fall wird das Programm jeden Monat – und zwar am 20. Tag – eine neue Vollversion erstellen. Nachdem die dritte Version erstellt wurde, wird die älteste der vorhandenen Versionen automatisch gelöscht.
7. Überprüfen Sie die Richtigkeit aller Einstellungen und klicken Sie auf **Backup jetzt**. Wenn Ihr erstes Backup nur zu einem bestimmten Zeitpunkt (laut Planung) ausgeführt werden soll, klicken Sie auf den Pfeil rechts neben der Schaltfläche **Backup jetzt** und wählen Sie dann den Eintrag **Später** aus dem Listenfeld aus.

### 2. Datei-Backup 'Tägliche inkrementelle Version und wöchentliche Vollversion'

Typischer Fall: Sie haben Dateien bzw. Ordner, mit denen Sie täglich arbeiten. Sie müssen die Arbeitsergebnisse eines jeden Tages sichern und möchten in der Lage sein, den jeweiligen Datenzustand für jeden Tag der letzten drei Wochen wiederherzustellen. Betrachten wir, wie Sie dies unter Verwendung eines benutzerdefinierten Schemas durchführen können.

1. Beginnen Sie mit der Konfiguration eines Datei-Backups. Weitere Informationen finden Sie im Abschnitt 'Backup von Dateien und Ordnern'.
2. Klicken Sie auf **Optionen**, öffnen Sie die Registerkarte **Planung**, klicken Sie dann auf **Täglich** und spezifizieren Sie den Startzeitpunkt für die Backup-Aktion. Wenn Sie beispielsweise Ihre tägliche Arbeit um 20:00 Uhr beenden, dann spezifizieren Sie diese Zeit (oder ein bisschen später, z.B. 20:05 Uhr) als Startzeit.
3. Öffnen Sie die Registerkarte **Backup-Schema** und wählen Sie die Option **Benutzerdefiniertes Schema** (statt **Inkrementelles Schema**).
4. Wählen Sie in der Box **Backup-Methode** das Element **Inkrementell** aus dem Listenfeld aus.
5. Klicken Sie auf **Erstelle eine vollständige Version nach je [n] inkrementellen Versionen** und geben Sie als Wert **6** an.
   In diesem Fall wird das Programm zuerst die anfängliche vollständige Backup-Version erstellen (egal wie Sie einen Backup-Prozess aufsetzen, die erste Backup-Version wird immer eine vollständige sein) und danach jeden Tag sechs inkrementelle Versionen. Danach wird es erneut eine Vollversion und sechs inkrementelle Versionen erstellen – und so weiter. Jede neue Vollversion wird also exakt innerhalb der Zeitspanne einer Woche erstellt.
6. Klicken Sie auf **Automatische Bereinigung einschalten**, wenn Sie die Speicherzeit für die Versionen begrenzen wollen.
7. Klicken Sie auf **Lösche Versionsketten älter als [n] Tage**, vergeben Sie als Wert **21** und klicken Sie dann auf **OK**.
8. Überprüfen Sie die Richtigkeit aller Einstellungen und klicken Sie auf **Backup jetzt**. Wenn Ihr erstes Backup nur zu einem bestimmten Zeitpunkt (laut Planung) ausgeführt werden soll, klicken Sie auf den Pfeil rechts neben der Schaltfläche **Backup jetzt** und wählen Sie dann den Eintrag **Später** aus dem Listenfeld aus.

### 3. Laufwerk-Backup 'Vollversion jeden 2. Monat und differentielle Version zweimal pro Monat'

Typischer Fall: Sie müssen Ihr System-Volume zweimal per Monat sichern und jeden zweiten Monat eine neue vollständige Backup-Version erstellen. Sie möchten zusätzlich nicht mehr als 100 GB an Speicherplatz auf dem Laufwerk zum Speichern der Backup-Versionen verwenden. Betrachten wir, wie Sie dies unter Verwendung eines benutzerdefinierten Schemas durchführen können.

1. Beginnen Sie mit der Konfiguration eines Laufwerk-Backups. Weitere Informationen finden Sie im Abschnitt 'Backups von Laufwerken und Volumes'.
2. Wählen Sie Ihr System-Volume (normalerweise C:) als Backup-Quelle aus.
3. Klicken Sie auf **Optionen**, öffnen Sie die Registerkarte **Planung**, klicken Sie dann auf **Monatlich** und spezifizieren Sie beispielsweise den 1. und 15. Tag des Monats. Als Ergebnis wird innerhalb von je zwei Wochen eine Backup-Version erstellt. Spezifizieren Sie anschließend einen Startzeitpunkt für die Backup-Aktion.
4. Öffnen Sie die Registerkarte **Backup-Schema** und wählen Sie die Option **Benutzerdefiniertes Schema** (statt **Inkrementelles Schema**).
5. Wählen Sie in der Box **Backup-Methode** das Element **Differentiell** aus dem Listenfeld aus.
6. Klicken Sie auf **Erstelle eine vollständige Version nach je [n] differentiellen Versionen** und geben Sie als Wert **3** an.
   In diesem Fall wird das Programm zuerst die anfängliche vollständige Backup-Version erstellen (egal wie Sie einen Backup-Prozess konfigurieren, die erste Backup-Version wird immer eine vollständige sein) und danach je innerhalb von zwei Wochen drei differentielle Versionen. Danach wieder eine Vollversion und drei differentielle Versionen – und so weiter. Jede neue Vollversion wird also innerhalb von zwei Monaten erstellt.
7. Klicken Sie auf **Automatische Bereinigung einschalten**, wenn Sie den Speicherplatz für die Versionen begrenzen wollen.
8. Aktivieren Sie **Backup nicht größer werden lassen als [definierte Größe]**, definieren Sie als Wert **100 GB** und klicken Sie dann auf **OK**.

   **Hinweis**
   Wenn die Gesamtgröße der Backups 100 GB übersteigt, wird Acronis Cyber Protect Home Office die vorhandenen Backup-Versionen so bereinigen, dass die verbliebenen Versionen die Speicherbegrenzung einhalten. Das Programm wird die älteste Backup-Kette löschen – bestehend aus einer vollständigen Backup-Version sowie drei differentiellen Backup-Versionen.

9. Überprüfen Sie die Richtigkeit aller Einstellungen und klicken Sie auf **Backup jetzt**. Wenn Ihr erstes Backup nur zu einem bestimmten Zeitpunkt (laut Planung) ausgeführt werden soll, klicken Sie auf den Pfeil rechts neben der Schaltfläche **Backup jetzt** und wählen Sie dann den Eintrag **Später** aus dem Listenfeld aus.

# Benachrichtigungen für Backup-Aktionen

Speicherort: **Optionen** –> **Benachrichtigungen**

Manchmal benötigt ein Backup- oder Recovery-Prozess eine Stunde oder mehr. Acronis Cyber Protect Home Office kann Sie per E-Mail benachrichtigen, wenn die entsprechende Aktion abgeschlossen wurde. Das Programm kann auch Nachrichten reproduzieren, die während der Aktion ausgegeben werden – oder kann Ihnen das vollständige Log nach dem Ende der Aktion senden.

In der Grundeinstellung sind alle Benachrichtigungen deaktiviert.

## Grenzwert für freien Speicherplatz

Sie möchten möglicherweise benachrichtigt werden, wenn der freie Platz auf einem Backup Storage unter einen spezifizierten Grenzwert fällt. Sollte Acronis Cyber Protect Home Office nach dem Start eines Backup-Tasks feststellen, dass der freie Platz am Backup-Speicherort bereits unterhalb des angegebenen Werts liegt, dann beginnt das Programm erst gar nicht mit dem aktuellen Backup-Prozess und wird Sie umgehend mit einer entsprechenden Meldung informieren. Die Meldung bietet drei Wahlmöglichkeiten – sie zu ignorieren und das Backup fortzusetzen, einen anderen Speicherort zu wählen oder das Backup abzubrechen.

Sollte der freie Speicherplatz unter den angegebenen Grenzwert sinken, während das Backup läuft, dann zeigt das Programm dieselbe Meldung an, worauf Sie dieselben Entscheidungen treffen müssen.

Acronis Cyber Protect Home Office kann freien Platz auf folgenden Speichergeräten überwachen: lokale Festplatten, USB-Speicherkarten und -Laufwerke sowie Netzwerkfreigaben (SMB). Für FTP-Server und CD-/DVD-Laufwerke kann diese Option nicht aktiviert werden.

***So können Sie den Grenzwert für den freien Speicherplatz festlegen***

1. Aktivieren Sie das Kontrollkästchen **Quickinfo bei unzureichendem freien Speicherplatz anzeigen**.
2. Geben Sie einen Schwellenwert in das Feld **Benachrichtigen, wenn freier Speicherplatz kleiner ist als** ein.

---

**Hinweis**
Diese Meldung wird nicht angezeigt, wenn das Kontrollkästchen **Während der Durchführung keine Meldungen bzw. Dialoge zeigen (Stiller Modus)** im Bereich **Fehlerbehandlung** der Backup-Optionen aktiviert ist.

---

## E-Mail-Benachrichtigung

1. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen über Aktionsstatus senden**.
2. E-Mail-Einstellungen konfigurieren:

- Geben Sie die E-Mail-Adresse in das Feld **An** ein. Sie können auch mehrere Adressen eingeben, müssen diese aber je per Semikolon trennen.
- Geben Sie die Adresse des Postausgangsservers (SMTP) in das Feld **Server-Einstellungen** ein.
- Tragen Sie die Port-Adresse des Postausgangsservers ein. Standardmäßig ist der Port 25 festgelegt.
- Wählen Sie das gewünschte Verschlüsselungsprotokoll für die E-Mails.
- Aktivieren Sie bei Bedarf das Kontrollkästchen **SMTP-Authentifizierung** und geben Sie dann den Benutzernamen und das Kennwort in die entsprechenden Felder ein.

3. Klicken Sie auf die Schaltfläche **Testnachricht senden**, um zu überprüfen, ob Ihre Einstellungen korrekt sind.

***Wenn das Versenden der Testnachricht fehlschlägt***

1. Klicken Sie auf **Erweiterte Einstellungen anzeigen**.
2. Erweiterte E-Mail-Einstellungen konfigurieren:
   - Geben Sie die E-Mail-Adresse des Absenders das Feld **Von** ein. Falls Sie nicht sicher sind, welche Adresse Sie angeben sollen, dann geben Sie eine gewünschte Adresse im Standardformat vom Typ *aaa@bbb.com* ein.
   - Ändern Sie bei Bedarf den Nachrichtenbetreff im Feld **Betreff**.
     Um die Überwachung des Backup-Status zu vereinfachen, können Sie nützliche, wichtige Informationen in die Betreffzeile der E-Mail-Nachrichten einfügen lassen. Dazu können Sie folgende Textplatzhalter verwenden:
     - %BACKUP_NAME% – Der Backup-Name
     - %COMPUTER_NAME% – Der Name des Computers, wo das Backup gestartet wurde
     - %OPERATION_STATUS% – Das Ergebnis eines Backups oder einer anderen Aktion
       Sie können beispielsweise Folgendes eingeben: *Status von Backup %BACKUP_NAME%: %OPERATION_STATUS% (%COMPUTER_NAME%)*
   - Aktivieren Sie das Kontrollkästchen **Anmeldung beim Posteingangsserver** und geben Sie darunter die Adresse des Posteingangsservers (POP3) an.
   - Legen Sie die Port-Adresse des Posteingangsservers fest. Der Port ist standardmäßig auf 110 eingestellt.
3. Klicken Sie erneut auf die Schaltfläche **Testnachricht senden**.

***Erweiterte Benachrichtigungseinstellungen***

- **Benachrichtigung bei erfolgreichem Abschluss einer Aktion** – Aktivieren Sie dieses Kontrollkästchen, damit eine Benachrichtigung über erfolgreich abgeschlossene Prozesse gesendet wird.
- **Benachrichtigung bei Fehler einer Aktion** – Aktivieren Sie dieses Kontrollkästchen, damit eine Benachrichtigung über fehlgeschlagene Prozesse gesendet wird.

- **Benachrichtigung, wenn Benutzereingriff erforderlich ist** – Aktivieren Sie dieses Kontrollkästchen, damit eine Benachrichtigung gesendet wird, wenn während der Aktion eine Ereignismeldung für den Benutzer angezeigt wurde.
- **Vollständiges Log zur Benachrichtigung hinzufügen** – Aktivieren Sie dieses Kontrollkästchen, damit der Benachrichtigung ein vollständiges Aktionsprotokoll angehängt wird.

**Hinweis**
Sie erhalten nur E-Mail-Benachrichtigungen für ein bestimmtes Backup. Um Benachrichtigungen über all Ihre Backups zu erhalten, müssen Sie die E-Mail-Benachrichtigungen im Online Dashboard einrichten. Weitere Informationen finden Sie im Abschnitt 'E-Mail-Benachrichtigungen'. Beide Methoden funktionieren unabhängig voneinander und können zudem auch gleichzeitig verwendet werden.

## Elemente vom Backup ausschließen

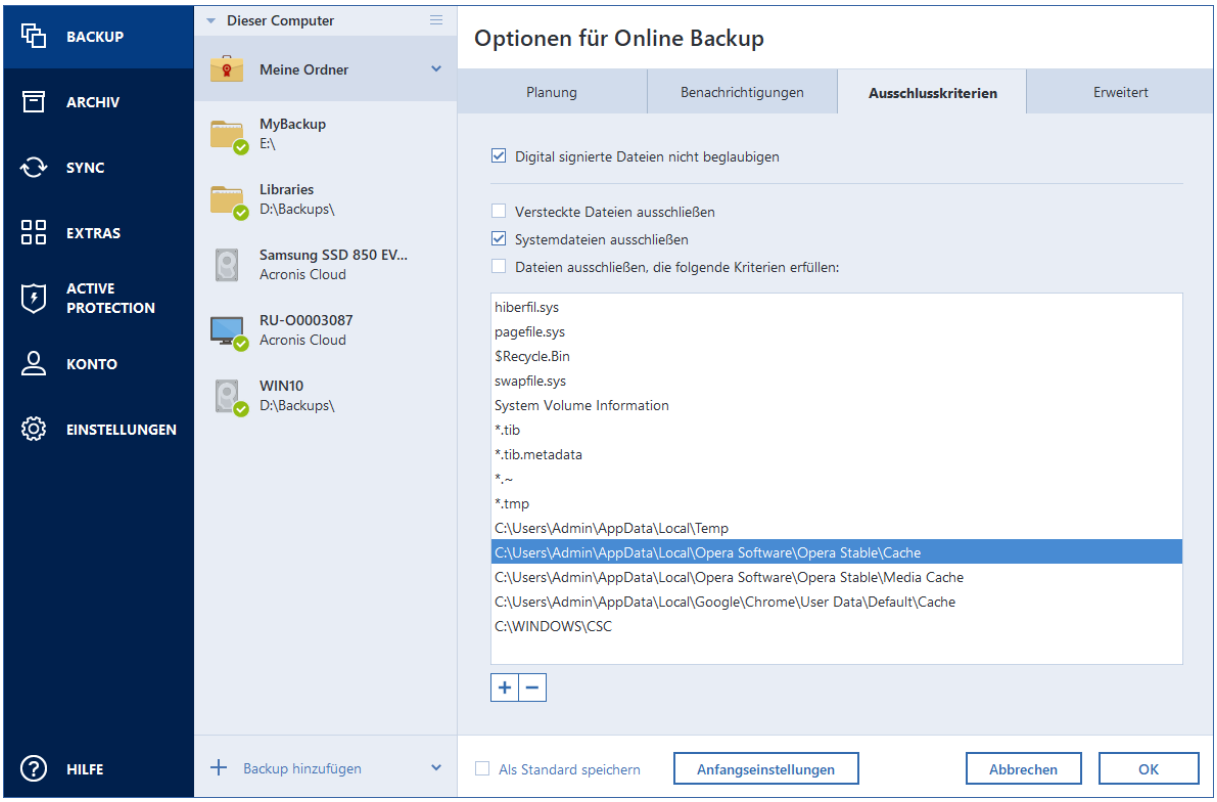
Speicherort: **Optionen** –> **Ausschlusskriterien**

Wenn nicht benötigte Dateien von einem Backup ausgeschlossen werden sollen, dann spezifizieren Sie die entsprechenden Dateitypen in den Backup-Optionen auf der Registerkarte **Ausschlusskriterien**. Sie können solche Ausschlusskriterien für Laufwerk-Backups, Datei-Backups und Online Backups spezifizieren.

Wenn Sie eine bestimmte Datei zum Backup auswählen, kann diese nicht über Ausschlusskriterien ausgeschlossen werden. Diese Einstellungen gelten nur für Dateien, die auf einem Volume, einem Laufwerk oder in einem Ordner liegen, das/der zur Sicherung ausgewählt wurde.

### So verwenden Sie die Standardeinstellungen für die Ausschlusskriterien

Nach Installation der Anwendung sind alle Ausschlusskriterien auf vorgegebene Anfangswerte eingestellt. Sie können diese für eine aktuelle Backup-Aktion oder für alle zukünftig erstellten Backups ändern. Aktivieren Sie das Kontrollkästchen **Einstellungen als Standard speichern**, um die geänderte Konfiguration für zukünftige Backup-Aktionen als Standard zu übernehmen. Klicken Sie auf die Schaltfläche **Auf Anfangseinstellungen zurücksetzen**, um alle geänderten Einstellungen auf ihre anfänglichen Werte (wie bei Installation des Programms) zurückzusetzen.




## Was Sie ausschließen können und was nicht

Sie haben folgende Möglichkeiten, um Dateien von Backups auszuschließen:

- **Digital signierte Dateien nicht beglaubigen** (nur bei beglaubigten Backups verfügbar) – Der Hauptzweck eines Notarized Backups ist der Schutz Ihrer persönlichen Dateien vor unbefugten Veränderungen. Es ist daher nicht unbedingt notwendig, Dateien, die bereits eine digitale Signatur haben (wie Betriebssystemdateien, Applikationsdateien), in einem solchen Backup mitzusichern. Sie können diese Dateien ausschließen, wenn Sie das entsprechende Kontrollkästchen aktivieren.
- **Versteckte Dateien ausschließen** – Aktivieren Sie dieses Kontrollkästchen, wenn Sie verborgenen Dateien und Ordner von einem Datei-Backup ausschließen wollen.
- **Systemdateien ausschließen** – Aktivieren Sie dieses Kontrollkästchen, wenn Sie Dateien und Ordner mit dem Dateiattribut 'System' von einem Datei-Backup ausschließen wollen.

Sie können Dateien ausschließen, die von Ihnen spezifizierte Kriterien erfüllen. Aktivieren Sie dazu das Kontrollkästchen **Dateien ausschließen, die die folgende Kriterien erfüllen**, klicken Sie anschließend auf das Plus-Zeichen (+) und geben Sie dann die Ausschlusskriterien an.

**Hinweis**
Wir raten davon ab, versteckte Dateien und Systemdateien vom Backup Ihrers System-Volumes auszuschließen.

***So können Sie ein Ausschlusskriterium hinzufügen:***

- Sie können eindeutige Dateinamen angeben, damit diese vom Backup ausgeschlossen werden:
  - *file.ext* – alle Dateien mit diesem Namen werden vom Backup ausgeschlossen.
  - *C:\file.ext* – die Datei 'file.ext' auf Laufwerk C: wird ausgeschlossen.
- Sie können Platzhalterzeichen (* und ?) verwenden:
  - **.ext* – Alle Dateien mit der Erweiterung '.ext' werden ausgeschlossen.
  - *??name.ext* – Dateien mit der Erweiterung .ext, deren Namen aus sechs Buchstaben bestehen (beginnend mit zwei beliebigen Zeichen (??) und mit *name* endend), werden ausgeschlossen.
- Um einen Ordner von einem Laufwerk-Backup auszuschließen, klicken Sie zuerst auf das Plus-Zeichen (+) und dann auf die Drei-Punkte-Schaltfläche. Wählen Sie anschließend den auszuschließenden Ordner im Verzeichnisbaum aus und bestätigen Sie die Aktion mit **OK**.

Wenn Sie ein versehentlich hinzugefügtes Kriterium wieder löschen wollen, müssen Sie es auswählen und dann auf das Minus-Zeichen (-) klicken.

## Modus zur Image-Erstellung

Speicherort: **Optionen** –> **Erweitert** –> **Modus zur Image-Erstellung**

Diese Option ist für Backups, die die Acronis Cloud als Speicherziel verwenden, nicht verfügbar.

Sie können diese Parameter verwenden, um von Ihren kompletten Laufwerken bzw. Volumes exakte Kopien zu erstellen (und nicht nur von den Sektoren, die Daten enthalten). Dies kann beispielsweise nützlich sein, wenn Sie ein Volume bzw. ein Laufwerk sichern wollen, welches ein nicht von Acronis Cyber Protect Home Office unterstütztes Betriebssystem enthält. Beachten Sie aber, dass dieser Modus die Durchführung verlängert und üblicherweise zu einer größeren Image-Datei führt.

- Aktivieren Sie das Kontrollkästchen **Sektor-für-Sektor sichern**, um ein Sektor-für-Sektor-Image zu erstellen.
- Aktivieren Sie das Kontrollkästchen **Nicht zugeordneten Speicher sichern**, damit auch der gesamte nicht zugeordnete Speicherplatz des Laufwerks in das Backup aufgenommen wird. Dieses Kontrollkästchen ist nur dann verfügbar, wenn die Option **Sektor-für-Sektor sichern** aktiviert wurde.

## Backup-Schutz

Speicherort: Backup Dashboard –> **Optionen** –> **Erweitert** –> **Backup-Schutz**

**Hinweis**
Dieser Abschnitt bezieht sich auf lokale Backups und Netzwerk-Backups. Informationen zum Schutz von Cloud Backups finden Sie im Abschnitt 'Online Backup-Schutz'.

Der Kennwortschutz für Backups ist standardmäßig nicht aktiviert. Aber Sie können Kennwörter zum Schutz Ihrer Backup-Dateien konfigurieren.

**Hinweis**
Für bereits bestehende Backups kann der Backup-Schutz jedoch nicht nachträglich geändert werden.

***So können Sie ein Backup schützen***

1. Geben Sie das Backup-Kennwort in das entsprechende Feld ein. Wir empfehlen die Verwendung eines Kennworts, das aus mindestens acht Zeichen besteht und sowohl Buchstaben (am besten Groß- und Kleinbuchstaben) wie Zahlen enthält, damit es nicht leicht zu erraten ist.

   **Hinweis**
   Ein Kennwort kann nicht wieder abgerufen werden. Sie sollten das zum Backup-Schutz spezifizierte Kennwort daher gut speichern bzw. erinnern.

2. Bestätigen Sie das zuvor eingegebene Kennwort noch einmal in dem entsprechenden Feld.
3. [Optionaler Schritt] Um die Sicherheit vertraulicher Daten zu gewährleisten, können Sie das Backup mit dem starken Industriestandard AES (Advanced Encryption Standard) verschlüsseln. AES ist in drei Schlüssellängen verfügbar, 128, 192 und 256 Bits, um die gewünschte Balance zwischen Performance und Schutz zu bieten.

   Eine Verschlüsselung mit 128-Bit ist ausreichend für die meisten Anwendungen. Je länger der Schlüssel, desto sicherer sind die Daten. Andererseits verlängern Schlüssel mit der Länge von 192 bzw. 256 Bit den Backup-Prozess signifikant.

   Wenn Sie die AES-Verschlüsselung benutzen möchten, wählen Sie einen der folgenden Schlüssel:
   - **AES 128** – zur Verwendung einer Schlüsselstärke von 128 Bit
   - **AES 192** – zur Verwendung einer Schlüsselstärke von 192 Bit
   - **AES 256** – zur Verwendung einer Schlüsselstärke von 256 Bit

   Wenn Sie das Backup nicht verschlüsseln, sondern nur per Kennwort schützen möchten, dann wählen Sie **Ohne**.
4. Klicken Sie nach Festlegung der Backup-Einstellungen auf **OK**.

## So erhalten Sie Zugriff auf ein kennwortgeschütztes Backup

Acronis Cyber Protect Home Office wird Sie jedes Mal nach dem Kennwort fragen, wenn Sie versuchen, das Backup zu ändern:

- Daten aus dem Backup wiederherstellen
- Einstellungen bearbeiten
- Mounten
- Verschieben

Um auf das Backup zugreifen zu können, müssen Sie das richtige Kennwort eingeben. Aus Sicherheitsgründen gibt es keine Möglichkeit, verlorene/vergessene Kennwörter wiederherzustellen.

## Online Backups schützen

Speicherort: **Optionen** –> **Erweitert** –> **Backup-Schutz**

Damit Ihre Daten in der Acronis Cloud vor unbefugtem Zugriff sicher sind, können Sie eine Verschlüsselung verwenden. In diesem Fall werden Ihre Daten beim Erstellen eines Backups mit dem AES-256-Algorithmus verschlüsselt und dann in der Acronis Cloud gespeichert. Das Programm benötigt ein Kennwort zur Ver- und Entschlüsselung der Daten. Dieses Kennwort muss dann spezifiziert werden, wenn Sie das entsprechende Online Backup konfigurieren. Sie können eine beliebige Zeichenfolge für das Kennwort verwenden. Beachten Sie jedoch unbedingt, dass beim Kennwort zwischen Groß-/Kleinschreibung unterschieden wird.

**Warnung!**
Das Kennwort eines Online Backups kann auf keine Weise irgendwie abgerufen oder wiederhergestellt werden. Sie sollten das zum Backup-Schutz spezifizierte Kennwort daher gut speichern bzw. erinnern.

Das Programm wird Sie bei jedem Zugriff auf die verschlüsselten Daten nach dem von Ihnen eingegebenen Kennwort fragen.

**Hinweis**
Beachten Sie, dass Sie für ein bereits vorhandenes Online Backup kein Kennwort festlegen oder ändern können.

## Befehle vor bzw. nach dem Backup

Speicherort: **Optionen** –> **Erweitert** –> **Vor-/Nach-Befehle**

Diese Option ist für Backups, die die Acronis Cloud als Speicherziel verwenden, nicht verfügbar.

Sie können Befehle spezifizieren (oder Batch-Dateien), die automatisch vor oder nach dem Backup ausgeführt werden.

Damit können Sie z.B. Windows-Prozesse starten oder stoppen oder Ihre Daten vor dem Start des Backups prüfen.

***So können Sie Befehle (Batch-Dateien) spezifizieren***

- Aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Befehle verwenden**.
- Wählen Sie im Feld **Vor-Befehl** den Befehl, der vor dem Backup-Prozess ausgeführt werden soll. Klicken Sie auf **Bearbeiten**, um einen neuen Befehl zu erstellen oder eine neue Batch-Datei auszuwählen.
- Bestimmen Sie im Feld **Nach-Befehl** einen nach Beendigung des Backup-Prozesses auszuführenden Befehl. Klicken Sie auf **Bearbeiten**, um einen neuen Befehl zu erstellen oder eine neue Batch-Datei auszuwählen.

Versuchen Sie nicht, interaktive Befehle auszuführen, d.h. Befehle, die eine Reaktion des Benutzers erfordern (beispielsweise **Pause**). Diese werden nicht unterstützt.

### Benutzerbefehl für Backups bearbeiten

Sie können Befehle spezifizieren (oder Batch-Dateien), die automatisch vor oder nach einem Backup ausgeführt werden:

- Geben Sie im Feld **Befehl** einen Befehl ein oder wählen Sie ihn aus der Liste. Klicken Sie auf '**...**', um eine Batch-Datei zu wählen.
- Geben Sie im Feld **Arbeitsverzeichnis** einen Pfad für die Befehlsausführung ein oder wählen Sie ihn aus der Liste früher gewählter Pfade.
- Geben Sie im Feld **Argumente** die Argumente für die Befehlsausführung ein oder wählen Sie diese aus der Liste aus.

Durch Deaktivieren des standardmäßig aktiviertem Kontrollkästchens **Aktionen nicht ausführen, bis die Befehlsausführung abgeschlossen ist** können Sie den Backup-Prozesse zeitgleich neben der Ausführung Ihrer Befehle laufen lassen.

Die Option **Aktion abbrechen, wenn der Benutzerbefehl fehlschlägt** (standardmäßig eingeschaltet) bricht die Aktion ab, wenn Fehler bei der Ausführung auftreten.

Sie können den Befehl testen, indem Sie auf die Schaltfläche **Befehl testen** klicken.

## Backup-Aufteilung

Speicherort: **Optionen** –> **Erweitert** –> **Backup-Aufteilung**

**Hinweis**
Acronis Cyber Protect Home Office kann keine bereits vorhandenen Backups aufteilen. Backups können nur bei der Erstellung aufgeteilt werden.

Diese Option ist für Backups, die die Acronis Cloud als Speicherziel verwenden, nicht verfügbar.

Große Backups können in mehrere Dateien geteilt werden, die zusammen das Original-Backup bilden. Ein Backup kann auch zum Brennen auf Wechselmedien aufgeteilt werden.

Die Standardeinstellung ist – **Automatisch**. Mit dieser Einstellung wird sich Acronis Cyber Protect Home Office folgendermaßen verhalten:

**Beim Backup auf eine Festplatte oder ähnliches Laufwerk:**

- Wenn das ausgewählte Laufwerk über ausreichend Speicherplatz verfügt und das Dateisystem die geschätzte Dateigröße ermöglicht, erstellt das Programm eine einzelne Backup-Datei.
- Wenn das Speicherlaufwerk zwar über ausreichend Platz verfügt, aber das Dateisystem die geschätzte Dateigröße nicht erlaubt, wird das Programm das Image automatisch in mehrere Dateien splitten.
- Wenn der Speicherplatz nicht ausreicht, um das Image auf Ihrem Laufwerk zu speichern, wird das Programm Sie warnen und auf Ihre Entscheidung warten, wie Sie das Problem beseitigen wollen.

Versuchen Sie, Speicherplatz freizugeben und dann fortzufahren, oder wählen Sie ein anderes Laufwerk aus.

**Beim Backup auf CD-R/RW, DVD-R/RW, DVD+R/RW, BD-R/RE:**

- Acronis Cyber Protect Home Office wird Sie bitten, einen weiteren Datenträger einzulegen, wenn der vorherige voll ist.

Sie können alternativ die gewünschte Dateigröße auch aus dem Listenfeld auswählen. Das Backup wird in mehrere Dateien der angegebenen Größe aufgeteilt. Dies ist nützlich, falls Sie schon beim Speichern des Backups auf ein Laufwerk die Absicht haben, dieses später auf CD-R/RW, DVD-R/RW, DVD+R/RW oder BD-R/RE zu brennen.

**Hinweis**
Das Erstellen von Backups direkt auf eine CD-R/RW, DVD-R/RW, DVD+R/RW, BD-R/RE kann beträchtlich mehr Zeit in Anspruch nehmen als auf Festplatten bzw. ähnlichen Laufwerken.

## Optionen für Backup-Validierung

Speicherort: **Optionen** –> **Erweitert** –> **Validierung**

Diese Option ist für Backups, die die Acronis Cloud als Speicherziel verwenden, nicht verfügbar.

Sie können folgende Einstellungen festlegen:

- **Backup jedes Mal validieren, wenn es abgeschlossen wurde** – Wählen Sie diese Option, um die Integrität der Backup-Version direkt nach der Backup-Durchführung zu überprüfen. Wir empfehlen, diese Option zu aktivieren, wenn Sie wichtige Daten oder das Systemlaufwerk sichern.
  - **Nur die letzte Backup-Version validieren** – Eine schnelle Überprüfung der letzten Backup-Segments (Backup-Slice).
  - **Komplettes Backup validieren**
- **Backup auf Basis einer Planung validieren** – Wählen Sie diese Option, um durch eine geplante Validierung sicherzustellen, dass Ihre Backups weiterhin fehlerfrei sind.
  - **Die letzte Backup-Version, wenn diese abgeschlossen wurde**
  - **Komplettes Backup, wenn dieses abgeschlossen wurde**

  Die Standardeinstellungen sind wie folgt:
  - **Frequenz** – Einmal im Monat
  - **Tag** – Das Datum, an dem das Backup gestartet wurde.
  - **Zeit** — Der Moment, wenn das Backup startet, plus 15 Minuten.

Sie können den Start der Validierung auch manuell über das Backup-Kontextmenü konfigurieren.

Klicken Sie dafür mit der rechten Maustaste auf das Backup und wählen Sie:

- **Alle Versionen validieren**
- **Die letzte Version validieren**

  Beispiel: Sie starten eine Backup-Aktion am 15. Juli um 12:00 Uhr. Die Backup-Version wird um 12:05 Uhr erstellt. Die Validierung wird um 12:15 Uhr ausgeführt, sofern Ihr Computer sich zu diesem Zeitpunkt im 'Bildschirmschonermodus' (Leerlaufbetrieb) befindet. Falls nicht, wird die Validierung nicht ausgeführt. Die Validierung wird in einem Monat (15. August) um 12:15 Uhr erneut gestartet. Ihr Computer muss sich wie zuvor dabei im 'Bildschirmschonermodus' (Leerlaufbetrieb) befinden. Gleiches ereignet sich am 15. September und so weiter.

  Sie können die Standardeinstellungen ändern und so Ihre eigene Planung spezifizieren. Weitere Informationen finden Sie unter 'Planung'.

## Backup-Reservekopie

Speicherort: **Optionen** –> **Erweitert** –> **Backup-Reservekopie**

Diese Option ist für Backups, die die Acronis Cloud als Backup-Ziel verwenden oder für lokale Backups, die mit Acronis True Image (2020 oder 2021) oder Acronis Cyber Protect Home Office erstellt wurden, nicht verfügbar.

Eine Backup-Reservekopie ist eine unabhängige Voll-Backup-Version, die unmittelbar nach einem normalen Backup erstellt wird. Auch wenn Sie eine inkrementelle oder differentielle Backup-Version erstellen (die nur geänderte Daten enthält), wird die Reservekopie dennoch alle Daten enthalten, die für das normale Backup ausgewählt wurden. Sie können Reservekopien Ihrer Backups im normalen Dateisystem, auf einem Netzlaufwerk oder einem USB-Flash-Laufwerk (z.B. einem USB-Stick) speichern.

**Hinweis**
CDs/DVDs werden als Speicherorte für Reservekopien nicht unterstützt.

***So können Sie eine Reservekopie erstellen***

1. Aktivieren Sie das Kontrollkästchen **Reservekopie von Backup erstellen**.
2. Spezifizieren Sie einen Speicherort für die Backup-Kopien.
3. Bestimmen Sie das Format für die Reservekopie. Sie können es als Acronis Backup (.tibx-Dateien) erstellen lassen oder die Quelldateien wie vorliegend (ohne irgendwelche Änderungen) zum ausgewählten Speicherort kopieren.
4. [Optionaler Schritt] Die können die Reservekopie mit einem Kennwort schützen.

   Alle anderen Backup-Optionen werden aus dem Quell-Backup übernommen.

## Einstellungen für Wechselmedien

Speicherort: **Optionen** –> **Erweitert** –> **Einstellungen für Wechselmedien**

Wenn Sie ein Backup auf ein Wechselmedium ausführen, dann können Sie dieses Medium durch Hinzufügen zusätzlicher Komponenten bootfähig machen. Daher benötigen Sie kein zusätzliches Boot-Medium.

**Warnung!**
Wenn ein USB-Stick in NTFS oder exFAT formatiert ist, wird das Erstellen eines Boot-Mediums von Acronis Cyber Protect Home Office nicht unterstützt. Das entsprechende Laufwerk muss FAT16 oder FAT32 als Dateisystem verwenden.

Es stehen folgende Einstellungen zur Verfügung:

- **Acronis Cyber Protect Home Office auf dem Medium speichern** – Wir empfehlen dringend, diese Option zu verwenden, damit USB-, PC-Card- (früher PCMCIA) und SCSI-Schnittstellen sowie die darüber angeschlossenen Storage-Geräte unterstützt werden.
- **Acronis Cyber Protect Home Office (64 Bit) auf dem Medium speichern** – Die selbe Option wie zuvor, nur für 64-Bit-Systeme.
- **Acronis System Report auf dem Medium speichern** – Wählen Sie diese Option, um einen Systembericht zu generieren, der bei Problemen mit dem Programm Informationen über das System sammelt. Die Berichtserstellungsoption steht bereits zur Verfügung, bevor Sie Acronis Cyber Protect Home Office mit dem Boot-Medium gestartet haben (über das Boot-Menü des Mediums). Der generierte Bericht kann auch auf einem USB-Flash-Laufwerk (wie einem USB-Stick) gespeichert werden.
- **Acronis System Report (64 Bit) auf dem Medium speichern** – Die selbe Option wie zuvor, nur für 64-Bit-Systeme.
- **Bei Erstellung eines Backups auf Wechselmedien automatisch nach dem ersten Medium fragen** – Wählen Sie diese Option, damit die Aufforderung **Legen Sie das erste Medium ein** angezeigt wird, wenn Sie ein Backup zu einem Wechselmedium durchführen. Mit der Standardeinstellung (also wenn die Option ausgewählt ist) kann ein Backup auf Wechselmedien bei Abwesenheit des Benutzers unmöglich sein, weil das Programm möglicherweise darauf warten wird, dass der Benutzer zur Bestätigung auf **OK** klickt. Deshalb sollten Sie die Meldung abschalten, wenn Sie ein geplantes Backup auf Wechselmedien ausführen möchten. Wenn das Wechselmedium dann verfügbar ist (z.B. eine CD-R/RW eingelegt ist), kann das Backup unbeaufsichtigt ablaufen.

Wenn andere Produkte von Acronis auf Ihrem Computer installiert sind, werden die bootfähigen Versionen dieser Programme ebenfalls dort zur Auswahl angeboten.

## 32- oder 64-Bit-Komponenten

Achten Sie darauf, welche Version von Acronis Cyber Protect Home Office und Acronis System Report mit Ihrem Computer kompatibel ist.

| | 32-Bit-Komponenten | 64-Bit-Komponenten |
|---|---|---|
| BIOS-basierte 32-Bit-Computer | + | - |

| | | |
|---|---|---|
| BIOS-basierte 64-Bit-Computer | + | + |
| EFI-basierte 32-Bit-Computer | + | - |
| EFI-basierte 64-Bit-Computer | - | + |

## Fehlerbehandlung

Wenn Acronis Cyber Protect Home Office während der Backup-Durchführung einen Fehler feststellt, stoppt es den Backup-Prozess, zeigt anschließend eine entsprechende Meldung an und wartet dann auf die Reaktion des Benutzers, wie der Fehler gehandhabt werden soll. Sie können jedoch Richtlinien für die Fehlerbehandlung definieren, damit Acronis Cyber Protect Home Office den Backup-Prozess nicht einfach stoppt, sondern den Fehler nach den von Ihnen festgelegten Richtlinien behandelt und die Aktion fortsetzt.

**Hinweis**
Dieser Abschnitt bezieht sich auf Backups, die lokale Speicherorte oder Netzwerkfreigaben als Backup-Ziele verwenden. Für Optionen zur Fehlerbehandlung von Backups, bei denen die Acronis Cloud als Backup-Ziel verwendet wird, siehe den Abschnitt 'Fehlerbehandlung für Cloud Backups und Replikate'.

***So können Sie die Fehlerbehandlungsrichtlinie festlegen***

1. Gehen Sie im Backup Dashboard zu **Optionen** –> **Erweitert** –> **Fehlerbehandlung**
2. Konfigurieren Sie die Fehlerbehandlungsrichtlinie:
   - **Während der Durchführung keine Meldungen bzw. Dialoge zeigen (Stiller Modus)** – Aktivieren Sie diese Einstellung, um während einer Backup-Aktion auftretende Fehler zu ignorieren. Dies ist nützlich, wenn Sie keine Möglichkeit haben, den Backup-Prozess zu überwachen bzw. zu steuern.
   - **Fehlerhafte Sektoren ignorieren** – diese Option wird nur bei Backups von Laufwerken/Volumes angezeigt. Diese Option ermöglicht Ihnen, ein Backup auch dann abzuschließen, wenn das Laufwerk fehlerhafte Sektoren hat.
     Wir empfehlen, dieses Kontrollkästchen beispielsweise bei folgenden Laufwerksfehlern zu aktivieren:
     - Ein Festplattenlaufwerk verursacht beim Betrieb Klick- oder Schleifgeräusche.
     - Das S.M.A.R.T.-System hat Laufwerksfehler erkannt und empfiehlt, das Laufwerk so schnell wie möglich per Backup zu sichern.

     Falls Sie das Kontrollkästchen deaktiviert lassen, können Backups fehlschlagen, wenn auf dem Laufwerk fehlerhafte Sektoren sind.
   - **Ältestes Backup löschen, falls in der ASZ nicht genug Speicherplatz ist** (standardmäßig aktiviert) – Wir empfehlen, dieses Kontrollkästchen zu aktivieren, wenn Sie unbeaufsichtigte, geplante Backups in die Acronis Secure Zone erstellen wollen. Sollte die Acronis Secure Zone während einer Backup-Aktion voll sein, wird Acronis Cyber Protect Home Office ansonsten das Backup aussetzen und Ihre Interaktion einfordern. Dieser Dialog wird auch dann angezeigt,

wenn die Einstellung **Während der Durchführung keine Meldungen bzw. Dialoge zeigen (Stiller Modus)** aktiviert ist.

- **Erneuter Versuch, wenn ein Backup fehlschlägt** – Mit dieser Option wird automatisch ein neuer Backup-Versuch unternommen, wenn das Backup aus irgendeinem Grund fehlschlägt. Sie können spezifizieren, wie oft und in welchen Zeitintervallen die Ausführung wiederholt werden soll. Beachten Sie, dass das Backup nicht fertiggestellt wird, wenn der Fehler, der den Backup-Prozess unterbrochen hat, weiterhin besteht.

  **Hinweis**
  Geplante Backup-Aktionen werden solange nicht gestartet, bis alle Versuche abgeschlossen wurden.

3. Klicken Sie auf **OK**.

## Fehlerbehandlung für Cloud Backups und Replikate

Sie können Acronis Cyber Protect Home Office so konfigurieren, dass fehlgeschlagene Backups und Replikationen in die Cloud wiederholt werden.

***So können Sie die Anzahl der Wiederholungsversuche und das Zeitintervall zwischen diesen Versuchen konfigurieren:***

1. Klicken Sie im **Backup** Dashboard zuerst auf ein entsprechendes Cloud Backup, dann auf **Optionen** und gehen Sie anschließend zur Registerkarte **Erweitert**.
2. Aktivieren Sie unter **Fehlerbehandlung** das Kontrollkästchen **Erneuter Versuch, wenn ein Backup fehlschlägt** und bestimmen Sie dann die Anzahl der Versuche (von 1 bis 99) sowie das Zeitintervall zwischen diesen.
3. Klicken Sie auf **OK**.

Die neue Einstellung wird auf alle zukünftigen Backups und Replikationen in die Cloud für das ausgewählte Cloud Backup angewendet.

**Hinweis**
Geplante Backup-Aktionen werden solange nicht gestartet, bis alle Versuche zur Wiederholung des Backups abgeschlossen wurden.

# Dateisicherheitseinstellungen für Backups

Speicherort: **Optionen** –> **Erweitert** –> **Dateisicherheitseinstellungen**

**Hinweis**
Diese Option ist nur für Backups auf Dateiebene verfügbar.

Diese Option ist für Backups, die die Acronis Cloud als Speicherziel verwenden, nicht verfügbar.

Sie können Sicherheitseinstellungen für die gesicherten Dateien spezifizieren:

- **Dateisicherheitseinstellungen in Backups bewahren** – diese Option wird alle Sicherheitseinstellungen (Gruppen oder Benutzern zugewiesene Berechtigungen) der gesicherten Dateien für spätere Wiederherstellungen bewahren.

  Standardmäßig werden Dateien und Ordner im Backup mit ihren ursprünglichen Windows-Sicherheitseinstellungen gespeichert (z.B. für jeden Benutzer oder jede Gruppe die Lese-, Schreib-, Ausführungsrechte usw., wie unter **Eigenschaften** -> **Sicherheit** festgelegt). Wenn Sie auf einem Computer geschützte Dateien bzw. Ordner ohne den in den Berechtigungen angegebenen Benutzer wiederherstellen, werden Sie wahrscheinlich nicht in der Lage sein, diese Dateien bzw. Ordner zu lesen oder zu verändern.

  Um dieses Problem zu umgehen, können Sie den Erhalt der Dateisicherheitseinstellungen ausschalten. Dann erhalten wiederhergestellte Dateien bzw. Ordner immer die Rechte desjenigen Ordners, in dem sie wiederhergestellt wurden (übergeordneter Ordner, wenn ins Stammverzeichnis wiederhergestellt).

  Alternativ können Sie die Sicherheitseinstellungen auch während der Wiederherstellung deaktivieren, selbst wenn sie im Backup verfügbar sind. Das Ergebnis wird dasselbe sein.
- **Verschlüsselte Dateien in Backups unverschlüsselt speichern** (als Voreinstellung deaktiviert) – wählen Sie diese Option, wenn verschlüsselte Dateien im Backup enthalten sind und Sie diese nach der Wiederherstellung für jeden Benutzer verfügbar machen möchten. Anderenfalls wird nur der Benutzer, der die Dateien bzw. Verzeichnisse ursprünglich verschlüsselt hat, darauf zugreifen können. Die Entschlüsselung kann sinnvoll sein, wenn Sie verschlüsselte Dateien auf einem anderen Computer wiederherstellen wollen.

  Wenn Sie die in Windows XP (und späteren Windows-Versionen) verfügbare Verschlüsselungsfunktion nicht nutzen, ignorieren Sie diese Option. (Die Verschlüsselung von Dateien bzw. Ordnern wird eingestellt unter **Eigenschaften** -> **Allgemein** -> **Erweitert** -> **Inhalt verschlüsseln, um Daten zu schützen**).

## Computer herunterfahren

Speicherort: **Optionen** –> **Erweitert** –> **Computer herunterfahren**

Sie können folgende Optionen konfigurieren:

- **Alle laufenden Aktionen stoppen, wenn ich den Computer herunterfahre** – Wenn Sie Ihren Computer ausschalten, während Acronis Cyber Protect Home Office eine längere Aktion (wie z.B. ein Laufwerk-Backup) durchführt, verhindert diese Option, dass der Computer herunterfahren kann. Wenn dieses Kontrollkästchen ausgewählt ist, wird Acronis Cyber Protect Home Office vor einem Herunterfahren automatisch alle aktuellen Aktionen stoppen. Dies kann ca. zwei Minuten dauern. Wenn Sie Acronis Cyber Protect Home Office das nächste Mal ausführen, werden alle gestoppten Backups neu gestartet.
- **Computer herunterfahren, wenn das Backup abgeschlossen ist** – Wählen Sie diese Option, wenn der Backup-Prozess, den Sie konfigurieren, viel Zeit in Anspruch nehmen kann. Sie müssen dann nicht mehr warten, bis die Aktion abgeschlossen wurde. Stattdessen schaltet das Programm den Computer automatisch aus, sobald das Backup abgeschlossen wurde.

Diese Option ist außerdem nützlich, wenn Sie Backups per Planung ausführen. Beispielsweise, wenn Sie Backups am Abend eines jeden Wochentags durchführen wollen, um all Ihre Arbeit zu speichern. Planen Sie das Backup und aktivieren Sie das Kontrollkästchen. Sie können danach, mit Abschluss Ihrer Arbeit, den Computer verlassen, wohl wissend, dass Ihre wichtigen Daten automatisch gesichert werden und der Computer anschließend heruntergefahren wird.

## Die Performance von Backup-Aktionen

Speicherort für Backups zu lokalen Zielen: **Optionen** –> **Erweitert** –> **Performance**

Speicherort für Backups in die Acronis Cloud: **Optionen** –> **Erweitert** –> **Performance und Netzwerk**

### Komprimierungsgrad

Sie können den Komprimierungsgrad für ein Backup spezifizieren:

- **Ohne** – Die Daten werden ohne Komprimierung gesichert, wodurch die Backup-Datei deutlich größer werden kann.
- **Normal** – Der empfohlene und standardmäßig vorgegebene Komprimierungsgrad.
- **Hoch** – Ein höherer Komprimierungsgrad, der jedoch mehr Zeit zur Erstellung eines Backups benötigt.
- **Maximum** – Die maximale Backup-Komprimierung, die jedoch die längste Zeit zur Backup-Erstellung benötigt.

**Hinweis**
Der optimale Komprimierungsgrad hängt vom Typ der Dateien ab, die im Backup gesichert werden. Beispielsweise kann selbst die maximale Komprimierung die Größe eines Backups nicht wesentlich verringern, wenn dieses Dateien enthält, die bereits effektiv komprimiert sind (etwa .jpg-, .pdf- oder .mp3-Dateien).

**Hinweis**
Der Konprimierungsgrad kann nicht für bereits vorhandene Backups festgelegt oder geändert werden.

### Priorität für die Aktion

Durch Änderung der Priorität können Backup- und Recovery-Prozesse schneller oder langsamer als normal ablaufen (je nachdem, wofür Sie sich entscheiden); was aber auch einen Einfluss auf die Performance andere Programme haben kann. Die Priorität eines jeden Prozesses, der in einem System läuft, bestimmt das Ausmaß der CPU-Benutzung und der Systemressourcen, die dem Prozess zugeordnet werden. Durch Herabsetzen der Priorität für Aktionen werden mehr Ressourcen für andere CPU-Tasks freigegeben. Durch Heraufsetzen der Backup- bzw. Recovery-Priorität können entsprechende Aktionen möglicherweise beschleunigt werden, weil Ressourcen

von anderen, aktuell laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-Auslastung und anderen Faktoren.

Sie können die Priorität für Aktionen einstellen:

- **Niedrig** (standardmäßig aktiviert) – Der Backup- oder Recovery-Prozess läuft langsamer, dafür kann aber die Performance anderer Programme besser werden.
- **Normal** – Der Backup- bzw. Recovery-Prozess hat die gleiche Priorität wie andere Prozesse.
- **Hoch** – Der der Backup- bzw. Recovery-Prozess wird schneller durchgeführt, andere Programme laufen dadurch jedoch möglicherweise langsamer. Beachten Sie, dass die Wahl dieser Option zu einer 100%igen CPU-Auslastung durch Acronis Cyber Protect Home Office führen kann.

## Übertragungsrate der Netzwerkverbindung

Wenn Sie Daten in die Acronis Cloud sichern, können Sie festlegen, welche maximale Netzwerkverbindungsgeschwindigkeit Acronis Cyber Protect Home Office dabei verwenden soll. Legen Sie dazu diejenige Verbindungsgeschwindigkeit fest, die es Ihnen ermöglicht, das Internet und andere Netzwerkverbindungen weiter ohne störende Verlangsamung zu nutzen.

Verwenden Sie eine der folgenden Optionen, um die Verbindungsgeschwindigkeit festzulegen:

- **Maximum**
  Die Datenübertragungsrate ist (auf Basis der Grenzen der vorhandenen Systemkonfiguration) maximal.
- **Upload-Geschwindigkeit begrenzen auf**
  Sie können für die Upload-Geschwindigkeit einen maximalen Wert festlegen.

## Snapshot für Backup

**Warnung!**
Diese Option richtet sich nur an erfahrene Anwender. Sie sollten diese Standardeinstellung nur ändern, wenn Sie sicher wissen, was Sie tun und welche Option welchen Effekt hat.

Während ein Laufwerk oder Volume gesichert wird – ein Prozess, der einige Zeit benötigen kann – kommt es möglicherweise vor, dass einige der zu sichernden Dateien gerade verwendet, gesperrt oder in irgendeiner Weise verändert werden. Es kann beispielsweise sein, dass Sie dabei gerade an einem Dokument arbeiten und dieses von Zeit zu Zeit speichern. Falls Acronis Cyber Protect Home Office Dateien nur nacheinander sichern würde, würde die Datei, die Sie geöffnet haben, vermutlich nach dem Start des Backups noch geändert werden – und dann zu einem späteren Zeitpunkt im Backup gespeichert werden. In so einem Fall wären die Daten im Backup nicht konsistent. Um dies zu vermeiden, erstellt Acronis Cyber Protect Home Office einen sogenannten „Snapshot“, der die zu sichernden Daten quasi auf einen bestimmten Zeitpunkt fixiert. Dieser Snapshot wird erstellt, bevor der eigentliche Backup-Prozess startet, und garantiert, dass alle Daten (zueinander) in einem konsistenten Zustand vorliegen.

Wählen Sie eine Option aus der Liste **Snapshot für das Backup**:

- **Kein Snapshot**– Es wird kein Snapshot erstellt. Die Dateien werden nacheinander gesichert – wie bei einer herkömmlichen Kopier-Aktion.
- **VSS** – Diese Option ist die Standardeinstellung für 'Laufwerk-Backups' und 'Backups des kompletten PCs' und gewährleistet, dass die Daten in dem resultierenden Backup konsistent sind.

**Warnung!**
Diese Option wird nur für Backups Ihres Systemlaufwerks empfohlen. Wenn Sie eine Wiederherstellung aus einem Backup mit einem anderen Snapshot-Typ durchführen, kann Ihre Computer möglicherweise nicht mehr richtig starten.

- **Acronis Snapshot** – Die Snapshots werden mithilfe des Acronis Drivers erstellt, der noch in älteren Versionen von Acronis Cyber Protect Home Office standardmäßig verwendet wurde.
- **Keine VSS Writer** – Diese Option ist die Standardeinstellung für 'Datei-Backups'. VSS Writer sind besondere VSS-Komponenten, die Applikationen über die bevorstehende Erstellung des Snapshots benachrichtigen, damit die Applikationen ihre Daten für den Snapshot vorbereiten können. Solche VSS Writer werden nur für bestimmte Applikationen wie Datenbanken benötigt, die viele Dateiaktionen durchführen und deren Daten unbedingt konsistent sein müssen. Da solche Applikationen auf den PCs von Privatanwendern („Home Computer“) üblicherweise nicht installiert sind, werden normalerweise auch keine VSS Writer benötigt. Dies reduziert zudem den Zeitaufwand für die Erstellung eines Datei-Backups.

## Ein Datacenter für Backups auswählen

Speicherort: **Optionen** –> **Erweitert** –> **Datacenter**

**Hinweis**
Diese Option ist nur für Online Backups verfügbar.

Wenn Sie bei der Erstellung eines Backups die Acronis Cloud Cloud als Ziel verwenden, werden Ihre Daten in eines der Acronis Datacenter hochgeladen, die jeweils in verschiedenen Ländern liegen. Beim Erstellen Ihres Acronis Kontos wird anfänglich dasjenige Datacenter für Sie festgelegt, welches Ihrem Standort am nächsten liegt. Anschließend werden Ihre Online Backups und synchronisierten Dateien standardmäßig in genau diesem Datacenter gespeichert.

Wir empfehlen, dass Sie dann ein anderes Datacenter für Ihre Backups manuell festlegen, wenn Sie sich in einem anderen Land befinden – oder das standardmäßig ausgewählte Datacenter doch nicht das nächstliegende ist (bezogen auf Ihren Stand- bzw. Wohnort). Dies kann die Datenrate beim Upload deutlich steigern.

**Hinweis**
Sie können das Datacenter für ein bereits vorliegendes Backup nicht mehr ändern.

## Energieeinstellungen für Notebooks und Tablets

Speicherort: **Einstellungen** –> **Energiesparmodus**

**Hinweis**
Diese Einstellung ist nur auf Computern mit Akkus (wie Notebooks, Tablets, Computer mit einer USV) verfügbar.

Länger ablaufende Backups können den Akku recht stark belasten. Wenn Sie ohne Ladegerät/Netzteil mit Ihrem Notebook oder Tablet arbeiten (weil keines verfügbar ist oder der Computer aufgrund eines Stromausfalls auf eine USV umgeschaltet wurde), kann es angebracht sein, die Akkuladung Ihres Gerätes zu schonen.

***So können Sie Akkuladung einsparen***

- Klicken Sie in der Seitenleiste auf **Einstellungen** –> **Energiesparmodus**, aktivieren Sie das Kontrollkästchen **Kein Backup, wenn der Akkustand niedriger ist als** und verwenden Sie dann den Schieberegler, um den genauen Akkustand festzulegen, ab dem das Energiesparen beginnen soll.

Wenn diese Einstellung aktiviert ist und Sie ohne Ladegerät/Netzteil arbeiten (weil Sie dieses herausgezogen haben oder der Computer aufgrund eines Stromausfalls auf eine USV umgeschaltet wurde) und wenn dann die aktuelle Akkuladung den Wert erreicht, den Sie per Schieberegler festgelegt haben, werden alle gerade laufenden Backups pausiert und in Planung befindliche Backups (vorerst) nicht mehr gestartet. Die pausierten Backups werden fortgesetzt, sobald das Ladegerät/Netzteil wieder angeschlossen wird bzw. die Stromversorgung wieder verfügbar ist. Geplante Backups, die aufgrund der Einstellung ausgesetzt wurden, werden ebenfalls gestartet.

Diese Einstellung blockt die Backup-Funktionalität aber nicht komplett. Denn Sie können ein Backup immer noch manuell starten.

Lokale Backups für Mobilgeräte sind von der Einstellung nicht betroffen. Ihre Mobilgerätedaten werden wie gewohnt zu einem lokalen Speicherort auf Ihrem Computer gesichert.

## WLAN-Verbindungen für Backups in die Acronis Cloud

Speicherort: **Einstellungen** –> **WLAN-Verbindungen für Backup**

Wenn Sie Ihre Daten in die Acronis Cloud sichern wollen, sorgen Sie sich möglicherweise um die Sicherheit Ihrer persönlichen Daten, falls die Übertragung über ein ungeschütztes (z.B. öffentliches) WLAN-Netzwerk erfolgen sollte. Um das Risiko zu vermeiden, dass Ihre persönlichen Daten gestohlen werden, empfehlen wir, dass Sie nur geschützte (nicht öffentliche) WLAN-Verbindungen für Backups verwenden.

***So können Sie Ihre Daten schützen***

1. Klicken Sie in der Seitenleiste auf **Einstellungen** –> **WLAN-Verbindungen für Backup** und klicken Sie anschließend auf **Netzwerke festlegen**.
2. Aktivieren Sie im Fenster **WLAN-Verbindungen für Backup**, in dem alle derzeit verfügbaren (aktiven) sowie auch gespeicherte, aber derzeit nicht verfügbaren (nicht aktiven) WLANs

angezeigt werden, die Kontrollkästchen neben den WLAN-Verbindungen, die zur Sicherung Ihrer Daten in die Cloud verwendet werden dürfen.

Wenn die entsprechenden WLANs ausgewählt sind und Ihr Computer die Verbindung zu einem dieser Netzwerke verliert, werden alle aktuellen Backups pausiert und geplante Backups (vorerst) nicht gestartet. Die pausierten Backups werden wieder fortgesetzt, sobald der Computer wieder mit einem dieser sicheren Netzwerke verbunden ist. Geplante Backups, die aufgrund der Einstellung ausgesetzt wurden, werden ebenfalls gestartet.

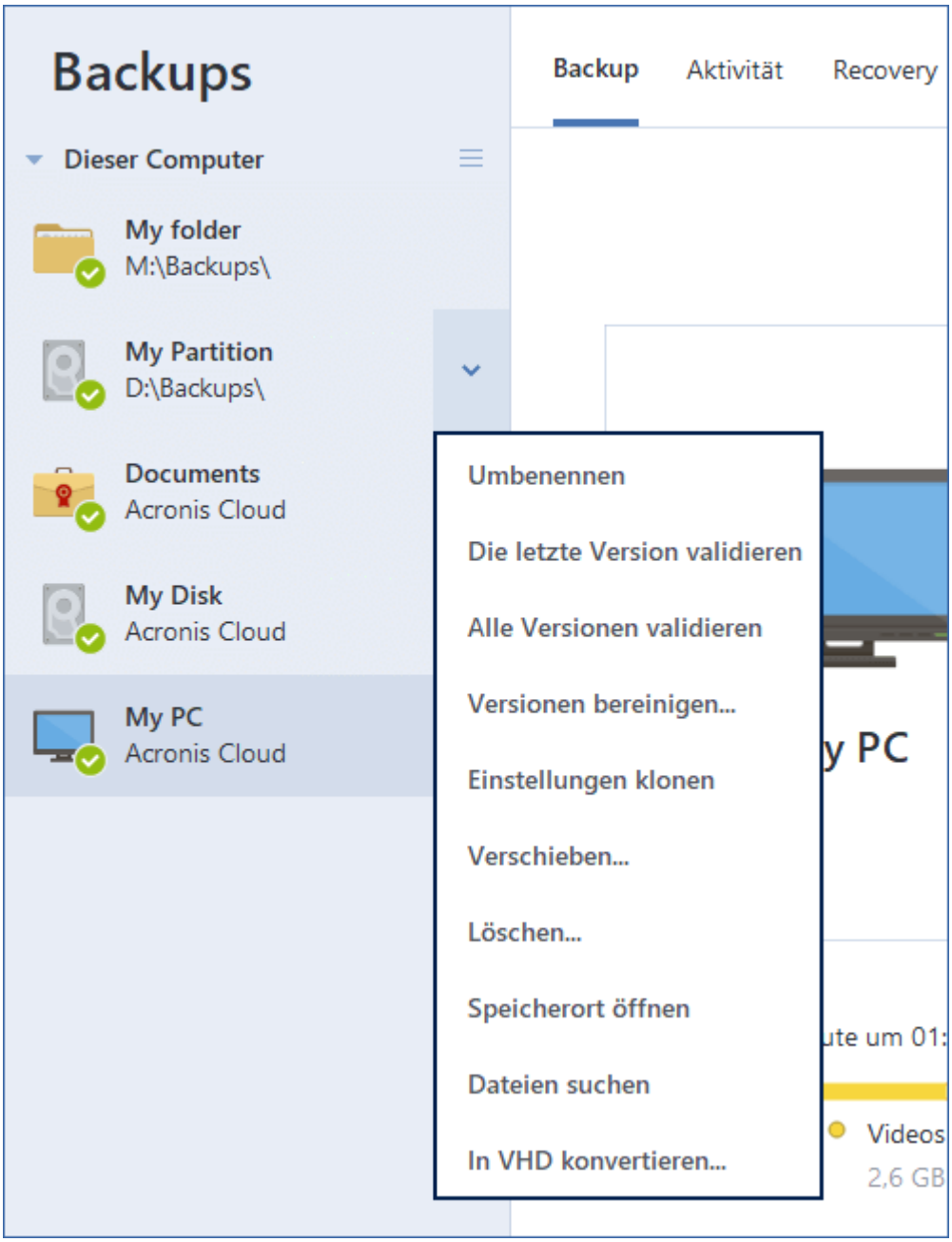
Wenn Sie Ihre Daten über eine neue, noch nicht aufgenommene WLAN-Verbindung sichern wollen, müssen Sie dieses einfach nur im Fenster **WLAN-Verbindungen für Backup** auswählen. Sie können dies jederzeit durchführen, wenn Sie eine neue Netzwerkverbindung benötigen.

Lokale Backups für Mobilgeräte sind von der Einstellung nicht betroffen. Ihre Mobilgerätedaten werden wie gewohnt zu einem lokalen Speicherort auf Ihrem Computer gesichert.

# Aktionen mit Backups

## Das Menü 'Backup-Aktionen'

Das Menü 'Backup-Aktionen' ermöglicht einen Schnellzugriff auf Aktionen, die auf ein ausgewähltes Backup angewendet werden können.




Das Menü 'Backup-Aktionen' kann folgende Elemente enthalten:

- **Umbenennen** (bei Backups in die Acronis Cloud nicht verfügbar) – Legen Sie einen neuen Namen für ein Backup in der Liste fest. Die Backup-Dateien selbst werden nicht umbenannt.
- **Rekonfigurieren** (bei Backups, die der Backup-Liste manuell hinzugefügt wurden) – Konfigurieren Sie die Einstellungen eines Backups, das mit einer früheren Version erstellt wurde. Dieses Element kann auch bei Backups erscheinen, die auf einen anderen Computer erstellt und in die Backup-Liste aufgenommen wurden, ohne dass dabei auch Ihre Backup-Einstellungen importiert wurden.

  Ohne Backup-Einstellungen können Sie ein Backup nicht mit dem Befehl **Backup jetzt** aktualisieren. Außerdem können Sie keine Backup-Einstellungen bearbeiten oder klonen.

- **Rekonfigurieren** (bei Online Backups) – Verbinden Sie ein ausgewähltes Online Backup mit dem aktuellen Computer. Klicken Sie dazu auf das Element und rekonfigurieren Sie Backup-Einstellungen. Beachten Sie, dass auf einem Computer nur ein Online Backup aktiv sein kann.
- **Die letzte Version validieren** – Starten Sie eine schnelle Überprüfung des letzten Backup-Slices.
- **Alle Versionen validieren** – Starten Sie eine Validierung aller Backup-Slices.
- **Versionen bereinigen** – Löschen Sie Backup-Versionen, die Sie nicht mehr benötigen.
- **Einstellungen klonen** – Erstellen Sie eine neue, leere Backup-Box mit den Einstellungen des anfänglichen Backups und der Bezeichnung **(1) [ursprünglicher Backup-Name]**. Ändern Sie die Einstellungen, speichern Sie sie und klicken Sie dann in der geklonten Backup-Box auf **Backup jetzt**.
- **Verschieben** – Verschieben Sie alle Backup-Dateien zu einem anderen Speicherort. Nachfolgende Backup-Versionen werden ebenfalls am neuen Ort gespeichert.

  Wenn Sie das Backup-Ziel durch Bearbeitung der Backup-Einstellungen ändern, werden nur neue Backup-Versionen am neuen Ziel gespeichert. Die älteren Backup-Versionen verbleiben am alten Speicherort.
- **Delete** – Abhängig vom Backup-Typ können Sie das Backup vollständig von seinem Speicherort löschen oder wählen, ob Sie nur die Backup-Box löschen wollen. Wenn Sie eine Backup-Box löschen, verbleiben die Backup-Dateien an ihrem Speicherort und Sie können das Backup der Liste später wieder hinzufügen. Beachten Sie, dass die Löschung nicht zurückgenommen werden kann, wenn Sie ein Backup komplett löschen.
- **Speicherort öffnen** – Öffnen Sie den Ordner, der die Backup-Dateien enthält.
- **Dateien suchen** – Suchen Sie eine bestimmte Dateien bzw. einen bestimmten Ordner in einem Backup, indem Sie den entsprechenden Namen in das Suchfeld eingeben.
- **In VHD-format konvertieren** (nur für Laufwerk-Backups) – Konvertieren Sie eine ausgewählte Acronis Backup-Version (.tibx-Datei) in virtuelles Laufwerke (.vhd(x)-Dateien). Die anfängliche Backup-Version wird nicht geändert.

## Backup-Aktivität und -Statistiken

In den Registerkarten **Aktivität** und **Backup** werden Ihnen weitere Informationen über ein Backup angezeigt – beispielsweise der Backup-Verlauf und die im Backup enthaltenen Dateitypen. Die Registerkarte **Aktivität** enthält eine Liste der Aktionen, die mit dem ausgewählten Backup seit seiner Erstellung durchgeführt wurden. Zusätzlich werden Statusmeldungen und Statistiken zu den Aktionen angezeigt. Das kann praktisch, wenn Sie herausfinden wollen, was mit einem Backup im Hintergrundmodus passiert ist. Angezeigt werden Informationen wie die Anzahl und der Status von geplanten Backup-Aktionen, die Größe der gesicherten Daten, die Ergebnisse von Backup-Validierungen usw.

Wenn Sie die erste Version eines Backups erstellen, wird Ihnen in der Registerkarte **Backup** eine grafische Darstellung über den Backup-Inhalt auf Basis der gesicherten Dateitypen angezeigt.

## Die Registerkarte 'Aktivität'

**Hinweis**
Für Nonstop-Backups und die Backups von Mobilgeräten gibt es keine Aktivitätsinformationen.

***So können Sie sich eine Backup-Aktivität anzeigen lassen***

1. Klicken Sie in der Seitenleiste auf **Backup**.
2. Wählen Sie in der Backup-Liste dasjenige Backup aus, dessen Verlauf Sie sich ansehen wollen.
3. Klicken Sie im rechten Fensterbereich auf **Aktivität**.

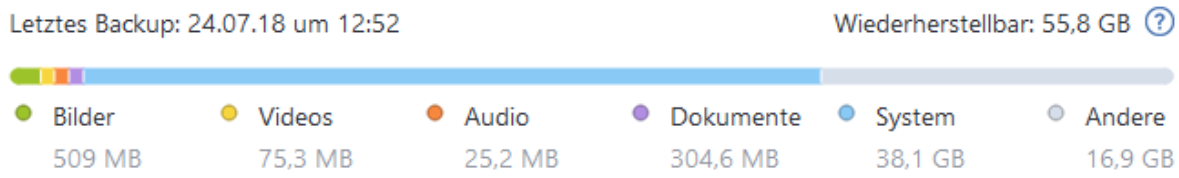

**Was Sie einsehen und analysieren können:**

- Backup-Aktionen und deren Statuszustände (erfolgreich, fehlgeschlagen, abgebrochen, unterbrochen usw.)
- Mit dem Backup durchgeführte Aktionen und deren Statuszustände.
- Fehlermeldungen
- Backup-Kommentare
- Details zu einer Backup-Aktion, einschließlich:
  - **Gesichert** – Größe der Daten, die in der letzten Backup-Version enthalten sind.
    Bei Backups auf Dateiebene berechnet Acronis Cyber Protect Home Office die Größe der zu sichernden Dateien. Der Wert dieses Parameters entspricht bei Voll-Backup-Versionen dem Wert der Daten, die wiederhergestellt werden sollen. Bei differentiellen und inkrementellen Versionen ist der Wert normalerweise niedriger als die Menge der wiederherzustellenden Daten, da Acronis Cyber Protect Home Office hier für die Wiederherstellung zusätzlich auf Daten aus früheren Versionen zurückgreift.
    Bei Backups auf Laufwerksebene berechnet Acronis Cyber Protect Home Office die Größe der Festplattensektoren, die die zu sichernden Daten enthalten. Da diese Sektoren 'feste NTFS-Links' (sogenannte Hard Links) zu Dateien enthalten können, kann der Wert dieses Parameters auch bei vollständigen Laufwerk-Backup-Versionen kleiner sein als der Wert des Parameters für die wiederherzustellenden Daten.
  - **Geschwindigkeit** – Geschwindigkeit der Backup-Aktion.
  - **Dauer** – Zeitdauer, die zur Durchführung der Backup-Aktion benötigt wurde.
  - **Wiederherstellbar** – Größe der Daten, die in der letzten Backup-Version enthalten sind.
  - **Methode** – Art der Backup-Aktion (vollständig, inkrementell oder differentiell).

Weitere Informationen finden Sie in diesem Knowledge Base-Artikel: https://kb.acronis.com/de/content/60104.

## Die Registerkarte 'Backup'

Wenn ein Backup erstellt wird, werden Ihnen hier Statistiken über die Art der gesicherten Dateien angezeigt, die in der letzten Backup-Version enthalten sind:




Zeigen Sie auf ein Farbsegment, um die Anzahl der Dateien und die Gesamtgröße für jede Datenkategorie einzusehen:

- Bilder
- Videodateien
- Audiodateien
- Dokumente
- Systemdateien
- Andere Dateitypen (inkl. versteckte Systemdateien)

**Wiederherzustellende Daten** – zeigt die Größe der ursprünglichen Daten an, die Sie für das Backup ausgewählt haben.

# Backups in der Liste sortieren

Die Backups werden standardmäßig nach Ihrem Erstellungsdatum sortiert, beginnend vom neuesten bis runter zum ältesten. Sie können die Reihenfolge ändern, indem Sie den entsprechenden Sortierungstyp im oberen Bereich der Backup-Liste auswählen. Sie haben folgende Optionen:

| Befehl | | Beschreibung |
|---|---|---|
| **Sortieren nach** | **Name** | Dieser Befehl sortiert alle Backups in alphabetischer Reihenfolge.<br>Wählen Sie **Z —> A**, um die Reihenfolge umzudrehen. |
| | **Erstellungsdatum** | Dieser Befehl sortiert alle Backups von den neuesten zu den ältesten.<br>Wählen Sie **Ältere zuerst**, um die Reihenfolge umzudrehen. |
| | **Aktualisierungszeitpunkt** | Dieser Befehl sortiert alle Backups nach dem Datum der |

| | | |
|---|---|---|
| | | letzten Version. Je neuer die letzte Backup-Version, desto höher wird das Backup in der Liste positioniert.<br>Wählen Sie **Ältere zuerst**, um die Reihenfolge umzudrehen. |
| | **Größe** | Dieser Befehl sortiert die Backups nach Größe, beginnend mit dem größten bis hin zum kleinsten.<br>Wählen Sie **Kleinste zuerst**, um die Reihenfolge umzudrehen. |
| | **Quelltyp** | Dieser Befehl sortiert alle Backups nach dem Quelltyp. |
| | **Zieltyp** | Dieser Befehl sortiert alle Backups nach dem Zieltyp. |

# Backups in die Acronis Cloud replizieren

## Warum sollten Sie ein Backup replizieren?

Ein Backup alleine bietet zwar einen gewissen, aber nicht umfassenden Schutz für Ihre Daten. Daher empfehlen wir, dass Sie alle lokalen Backups zusätzlich in die Acronis Cloud Cloud replizieren, denn so können Sie Ihren Computer noch besser vor Beschädigungen wie zufälligen Desastern schützen. Sie könnten dafür natürlich einfach zwei Backup-Pläne erstellen – einen zur lokalen Sicherung Ihres Computers und einen zur Sicherung in die Acronis Cloud. Mit einer automatischen Replikation sparen Sie jedoch einerseits Zeit bei der Einrichtung von Backup-Plänen und andererseits ist eine Replikation grundsätzlich schneller als die Erstellung eines weiteren Backups. Ein Replikat ist prinzipiell einfach nur eine zusätzliche, identische Kopie Ihres Backups. Diese bietet einen erweiteren Schutz und kann zudem verwendet werden, um von überall auf Ihre Daten zuzugreifen.

## Eine Replikation aktivieren

Die Replikationsoption ist standardmäßig deaktiviert. Sie können die Replikation für jedes lokale Backup eines Laufwerks, Volumes oder kompletten PCs aktivieren, sofern Sie ein lokales Speicherlaufwerk (z.B. eine externe oder interne Festplatte) als Backup-Ziel und Acronis True Image (2020 oder 2021) oder Acronis Cyber Protect Home Office zur Backup-Konfiguration verwenden. Sie können die Replikation über eine spezielle Registerkarte in einem Backup-Plan aktivieren.

***So können Sie die Replikation eines Backups in die Acronis Cloud aktivieren:***

1. Wählen Sie in der Backup-Liste dasjenige Backup aus, das Sie replizieren möchten, und öffnen Sie dann die Registerkarte **Replikat**.
2. Klicken Sie auf **Replizieren**. Jetzt ist die Replikation aktiviert und wird automatisch ausgeführt, sobald das zugrundeliegende Backup erstellt wird. Sie können das Applikationsfenster von Acronis Cyber Protect Home Office jetzt nach Belieben schließen. Das Backup und Replikation werden weiter als Hintergrundprozesse ausgeführt.
3. [Optionaler Schritt] Klicken Sie auf **Optionen** –> **Erweitert** –> **Replikation in die Acronis Cloud**, wenn Sie das Datacenter sehen wollen, wo Ihre Backup-Replikate gespeichert werden – und

wenn Sie Bereinigungseinstellungen für die Acronis Cloud konfigurieren wollen, um die Speicherplatznutzung zu optimieren.

### Der Schutz von replizierten Daten

Replizierte Daten werden per SSL (Secure Socket Layer) in die Acronis Cloud hochgeladen.

In der Cloud werden diese Daten gemäß der von Ihnen festgelegten Verschlüsselungseinstellungen gespeichert. Wenn kein Verschlüsselungskennwort festgelegt wurde, werden die replizierten Daten unverschlüsselt gespeichert. Anderenfalls werden die Daten per AES-256 verschlüsselt.

## Backups validieren

Die Validierungsprozedur überprüft, ob Sie die Daten in einem Backup auch tatsächlich wiederherstellen können.

Die Überprüfung eines Backups ist beispielsweise dann wichtig, wenn Sie Ihr System wiederherstellen wollen. Wenn Sie eine Wiederherstellung mit einem beschädigten Backup durchführen, wird der Prozess fehlschlagen und Ihr Computer ist anschließend möglicherweise nicht mehr bootfähig. Wenn Sie ein Backup Ihres Systemlaufwerks/-volumes validieren wollen, empfehlen wir, dies von einem Boot-Medium aus durchzuführen. Andere Backups können dagegen unter Windows validiert werden. Vergleichen Sie auch die Abschnitte 'Vorbereitungen zur Wiederherstellung' und 'Grundlegende Konzepte'.

***So können Sie ein komplettes Backup unter Windows validieren***

1. Starten Sie Acronis Cyber Protect Home Office und klicken Sie in der Seitenleiste auf **Backup**.
2. Klicken Sie in der Backup-Liste auf den nach unten zeigenden Pfeil neben dem zu validierenden Backup – und wählen Sie dann den Befehl **Validieren**.

***So können Sie eine bestimmte Backup-Version oder ein komplettes Backup mit der autonomen Notfallversion (auf einem Boot-Medium) von Acronis Cyber Protect Home Office validieren:***

1. Suchen Sie in der Registerkarte **Recovery** nach dem Backup, welches die Version enthält, die Sie überprüfen wollen. Sollte das Backup nicht aufgeführt sein, dann klicken Sie auf den Befehl **Nach Backup durchsuchen**. Anschließend können Sie den Pfad zu dem entsprechenden Backup angeben. Acronis Cyber Protect Home Office wird dieses Backup dann der Liste hinzufügen.
2. Klicken Sie mit der rechten Maustaste auf das Backup oder eine bestimmte Version – und danach auf den Befehl **Archiv validieren**. Dies öffnet den **Assistenten zur Validierung**.
3. Klicken Sie auf **Fertigstellen**.

## Backups an verschiedene Plätze

Sie können verschiedene Versionen eines Backups an unterschiedlichen Zielorten speichern, indem Sie beim Bearbeiten der Backup-Einstellungen das Backup-Ziel ändern. Sie können beispielsweise

nach Speicherung des anfänglichen Voll-Backups auf ein externes USB-Laufwerk die Backup-Einstellungen so ändern, dass ein USB-Stick als weiteres Backup-Ziel verwendet wird.

Darauf werden die nachfolgenden inkrementellen und differentiellen Backups auf den USB-Stick geschrieben.

**Hinweis**
Backups auf optische Medien können nicht fortgesetzt werden.

**Hinweis**
Acronis Die Secure Zone und FTP-Server können nur ein komplettes Backup enthalten.

## Backups 'on-the-fly' aufteilen

Sollte der freie Speicherplatz am Ziel (CD-R/RW oder DVD-R/RW) nicht zur Fertigstellung der aktuellen Backup-Aktion ausreichen, dann zeigt das Programm eine Warnmeldung an.

Führen Sie eine der folgenden Aktionen aus, um das Backup abzuschließen

- Geben Sie etwas Speicherplatz auf dem Laufwerk frei und klicken Sie dann auf **Wiederholen**.
- Klicken Sie auf **Durchsuchen** und wählen Sie anschließend ein anderes Speichergerät.
- Klicken Sie auf **Formatieren**, um alle Daten auf dem Laufwerk zu löschen, und fahren Sie dann mit der Backup-Erstellung fort.

Wenn mehrere Versionen eines Backups an unterschiedlichen Speicherplätzen vorliegen, müssen Sie diese während einer Wiederherstellung möglicherweise angeben.

# Ein vorhandenes Backup der Liste hinzufügen

Sie verfügen vielleicht über Backups von Acronis Cyber Protect Home Office, die Sie mit einer früheren Produktversion erstellt haben oder von einem anderen Computer herüberkopiert haben. Acronis Cyber Protect Home Office durchsucht Ihren Computer bei jedem Start nach solchen Backups und fügt diese automatisch zur Backup-Liste hinzu.

Sollten Sie Backups haben, die nicht in der Liste angezeigt werden, so können Sie diese manuell hinzufügen.

***So können Sie Backups manuell hinzufügen:***

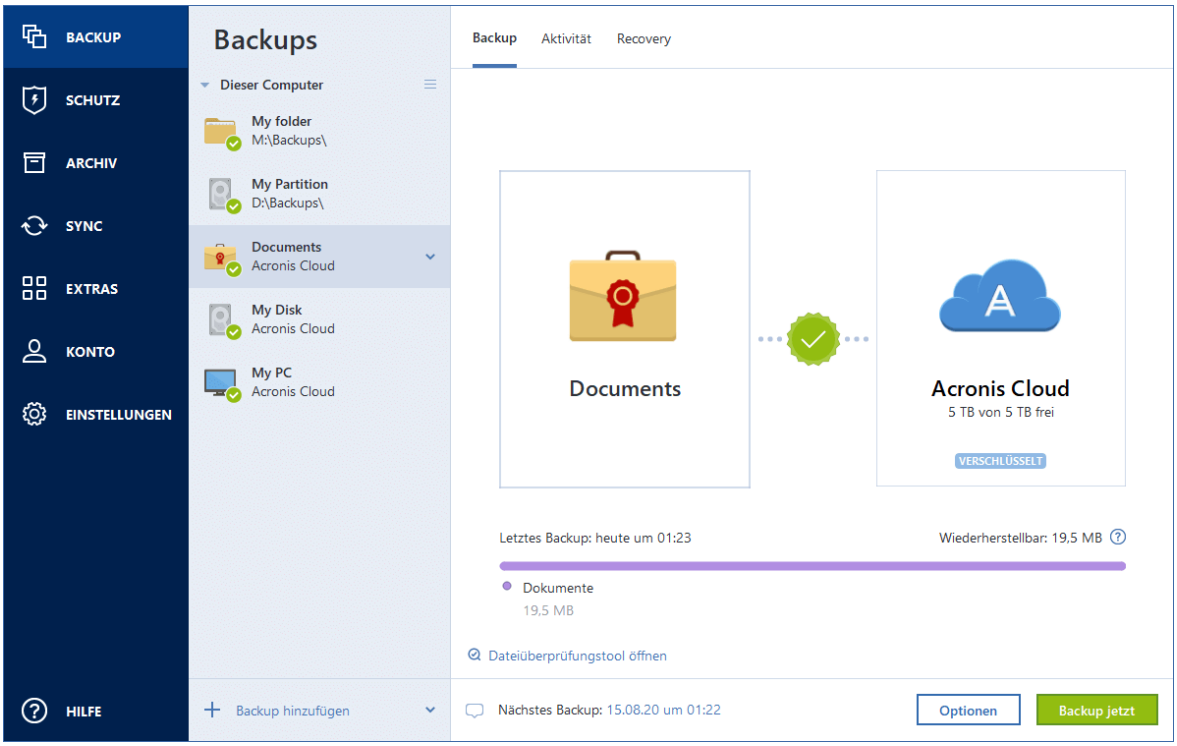
1. Klicken Sie im Bereich **Backup** am unteren Ende der Backup-Liste auf das Pfeilsymbol und anschließend auf den Befehl **Vorhandenes Backup hinzufügen**. Das Programm öffnet ein Fenster, in dem Sie auf Ihrem Computer nach Backups suchen können.
2. Wählen Sie eine Backup-Version (eine .tibx-Datei) aus und klicken Sie dann auf **Hinzufügen**. Daraufhin wird das komplette Backup zur Liste hinzugefügt.

# Notarized Backup

Acronis Cyber Protect Home Office kann mithilfe der Blockchain-Technologie Ihre Dateien vor unbefugten Veränderungen schützen. Sie können damit überprüfen, dass es sich bei einer wiederhergestellten Datei auch wirklich exakt um diejenige Datei handelt, die Sie ursprünglich per Backup gesichert hatten. Wir empfehlen diese Art von Backup insbesondere zum Schutz rechtlich wichtiger Dokumente/Dateien. Sie können damit aber natürlich auch alle anderen Dateien schützen, deren Authentizität Sie überprüfen wollen. Genauere Informationen dazu finden Sie im Abschnitt 'Blockchain-Technologie verwenden'.

***So können Sie ein 'Notarized Backup' (Beglaubigtes Backup) Ihrer Dateien und Ordnern erstellen***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Backup**.
3. Klicken Sie auf **Backup hinzufügen**.
4. [Optional] Um ein Backup umzubenennen, müssen Sie zuerst auf den Pfeil neben dem Backup-Namen und dann auf **Umbenennen** klicken. Geben Sie anschließend den gewünschten neuen Namen ein.
5. Klicken Sie auf den Bereich **Backup-Quelle** und wählen Sie dann **Zu beglaubigende Dateien**.
6. Aktivieren Sie im geöffneten Fenster die Kontrollkästchen, die neben den zu sichernden Dateien und Ordnern liegen, und klicken Sie dann auf **OK**.




7. Klicken Sie auf den Bereich **Backup-Ziel** und wählen Sie dann einen Zielort für das Backup:

- **Acronis Cloud** – Melden Sie sich an Ihrem Acronis Konto an und klicken Sie dann auf **OK**.
  Sollten Sie noch kein Acronis Konto haben, dann klicken Sie auf **Konto erstellen**, geben Sie Ihre E-Mail-Adresse und ein Kennwort ein – und klicken Sie dann auf die Schaltfläche **Konto erstellen**. Weitere Informationen finden Sie im Abschnitt 'Acronis Konto'.
- **Ihr externes Laufwerk** – Falls ein externes Laufwerk an Ihrem Computer angeschlossen ist, können Sie dieses aus der Liste auswählen.
- **NAS** – Wählen Sie ein NAS-Gerät aus der Liste der gefundenen NAS-Geräte. Falls Sie nur ein (1) NAS-Gerät haben, wird Acronis Cyber Protect Home Office vorschlagen, dieses als Standardziel für Backups zu verwenden.
- **Durchsuchen** – Wählen Sie einen Zielordner aus dem Verzeichnisbaum.

8. [Optionaler Schritt] Klicken Sie auf **Optionen**, um die Einstellungen des betreffenden Backups zu konfigurieren. Zu weiteren Informationen siehe Backup-Optionen.
   Wenn Sie Dateien mit einer digitalen Signatur vom Backup ausschließen wollen, aktivieren Sie das Kontrollkästchen **Digital signierte Dateien nicht beglaubigen** auf der Registerkarte **Ausschlusskriterien**. Weitere Details finden Sie im Abschnitt 'Elemente vom Backup ausschließen'.
9. [Optionaler Schritt] Klicken Sie auf das Symbol **Kommentar hinzufügen** und geben Sie dann einen gewünschten Kommentar für die Backup-Version ein. Backup-Kommentare erleichtern Ihnen das Auffinden einer gewünschten Backup-Version, wenn Sie Ihre Daten zu einem späteren Zeitpunkt wiederherstellen wollen.
10. Gehen Sie folgendermaßen vor:
    - Klicken Sie auf **Backup jetzt**, um das Backup umgehend auszuführen.
    - Wenn Sie möchten, dass das Backup zu einem späteren Zeitpunkt oder nach Planung ausgeführt wird, dann klicken Sie auf den rechts neben der Schaltfläche **Backup jetzt** liegenden nach unten zeigenden Pfeil und anschließend auf **Später**.

**Hinweis**
Wenn Sie Ihre Daten in die Acronis Cloud sichern, kann die Fertigstellung des ersten Backups eine längere Zeit in Anspruch nehmen. Spätere Backup-Prozesse werden voraussichtlich schneller ablaufen, da via Internet nur Änderungen an den Dateien gesichert werden.

Zusätzlich können Sie sich englischsprachige Video-Anleitungen unter folgender Adresse anschauen: https://goo.gl/WjUoPZ.

## Blockchain-Technologie verwenden

Acronis Cyber Protect Home Office verwendet die Blockchain-Technologie, um für Ihre per Backup gespeicherten Dateien mit einer zusätzlichen, modernsten Sicherheitsebene zu schützen. Diese Technologie gewährleistet, dass Ihre Dateien von keiner betrügerischen Software (unbemerkt) geändert werden. Denn wenn Sie eine Datei wiederherstellen wollen, können Sie überprüfen, dass es sich wirklich exakt um die Datei handelt, die Sie per Backup gesichert hatten.

## Was ist eine Blockchain?

Eine Blockchain (wörtlich etwa 'Datenblock-Kette') ist eine bestimmte Datenbank, in der Informationen über Transaktion und deren Reihenfolge gespeichert werden. Eine Transaktion entspricht dabei einem Ereignis. Das können beispielsweise Geldüberweisungen oder auch andere Aktionen mit Vermögenswerten (aller Art) sein. Diese Transaktionen werden in Blöcke zusammengefasst, die nacheinander in Form einer Blockchain (Datenblock-Kette) in die Datenbank geschrieben werden. Jede Transaktion und jeder Block hat dabei eine eigene, eindeutige Identifikationsnummer. Wichtig dabei ist, dass jeder Block zudem auch Informationen über alle vorherigen Blöcke in der Kette speichert. Sobald die Information über eine Transaktion in die Datenbank geschrieben wurde, kann diese von niemanden mehr geändert werden. Und auch die Transkationssequenz ist unveränderbar. Jeder Versuch, eine bestimmte Information in der Datenbank zu ändern, kann von jedem Benutzer der Datenbank leicht erkannt werden, weil in den nachfolgenden Blöcken die Informationen über die falsche Transaktion oder falschen Blöcke fehlen. Diese Technologie gewährleistet, dass in der Datenbank gespeicherte Daten gültig sind, zu einer bestimmten Person gehören und von niemanden geändert wurden. Weitere Informationen über die Blockchain-Technologie finden Sie unter der Adresse 'https://de.wikipedia.org/wiki/Blockchain'.

## So verwendet Acronis Cyber Protect Home Office die Blockchain-Technologie

Acronis Cyber Protect Home Office verwendet die Acronis Notary-Technologie, um Ihre Dateien vor unbefugten Veränderungen zu schützen. Dabei handelt es sich um eine universelle Lösung, um beliebige Datenobjekte/Datenströme mit digitalen Zeitstempeln und Fingerabdrücken zu versehen und zu vergleichen. Da es unpraktisch wäre, große Datenmengen in einer Blockchain-Datenbank zu speichern, sendet Acronis Cyber Protect Home Office nur die Hash-Werte von Dateien zum Acronis Notary Service.

Ein Hash-Wert (auch Hash-Code oder kurz einfach Hash) ist eine eindeutige Nummer mit festgelegter Größe, die von einer entsprechenden Hash-Funktion errechnet wird. Dieser Zahlencode ist eine mathematische Definition für einen zufälligen Satz von Daten (beispielsweise von einer Backup-Datei). Jede Veränderung der Backup-Datei resultiert auch in einen abweichenden Hash-Wert. Wenn Sie also überprüfen wollen, ob eine Datei geändert wurde, müssen Sie nur ihre Hash-Werte vergleichen – und je einen Wert für den ursprünglichen Zustand der Datei und einen Wert für den aktuellen Zustand. Stimmen die Werte überein, so ist dies ein Beweis dafür, dass die Datei nicht verändert wurde.

Wenn Acronis Notary die Hash-Werte Ihrer Dateien empfängt, berechnet er einen neuen, einzelnen Hash-Wert und sendet diesen an die Blockchain-Datenbank von Ethereum. Ausführlichere Informationen (in Englisch) über Ethereum finden Sie unter der Adresse 'https://www.ethereum.org/'.

Sobald sich dieser Hash-Wert in der Datenbank befindet, werden die zur Berechnung des Hash-Codes verwendeten Dateien von Acronis Notary beglaubigt. Sie können die Authentizität eine Datei jederzeit leicht mit der im Abschnitt 'Die Authentizität von Dateien überprüfen' beschriebenen Prozedur überprüfen. Jede beglaubigte Datei hat ein Beglaubigungszertifikat (Notarization

Certificate), welches der dokumentarischer Beleg dafür ist, dass diese Datei per Blockchain-Technologie geschützt wird. Ein solches Zertifikat enthält neben allgemeinen Informationen über die Datei außerdem technische Details, mit denen Sie die Dateiauthentizität manuell überprüfen können. Weitere Informationen finden Sie im Abschnitt 'Die Authentizität einer Datei manuell überprüfen'.

## Die Authentizität von Dateien überprüfen

Acronis Cyber Protect Home Office kann mithilfe der Blockchain-Technologie Ihre per Backup gesicherten Dateien vor unbefugten Veränderungen schützen. Sie können damit überprüfen, dass es sich bei einer wiederhergestellten Datei auch wirklich exakt um diejenige Datei handelt, die Sie ursprünglich per Backup gesichert hatten.

***So können Sie die Authentizität einer Datei in Acronis Cyber Protect Home Office überprüfen***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Backup**.
3. Wählen Sie in der Backup-Liste dasjenige 'Notarized Backup' aus, welches die zu überprüfende Datei enthält.
4. Öffnen Sie im rechten Fensterbereich die Registerkarte **Recovery**.
5. Suchen Sie die erforderliche Datei, klicken Sie auf das Menü-Symbol ( ⋮ ) – und wählen Sie anschließend einen der nachfolgenden Befehle:
   - **Zertifikat anzeigen** – Das Zertifikat, welches ausführliche Informationen zur Dateisicherheit enthält, wird in Ihrem Webbrowser geöffnet.
   - **Überprüfen** – Acronis Cyber Protect Home Office wird die Authentizität der Datei verifizieren.

***So können Sie die Authentizität einer Datei im Dateiüberprüfungstool verifizieren:***

1. Öffnen Sie das Dateiüberprüfungstool mit einer der folgenden Methoden:
   - Öffnen Sie in einem Webbrowser die Adresse https://notary.acronis.com/verify.
   - Klicken Sie in der Seitenleiste von Acronis Cyber Protect Home Office auf **Backup**, wählen Sie ein beglaubigtes Backup aus und klicken Sie dann im rechten Fensterbereich auf **Dateiüberprüfungstool öffnen**.
2. Suchen Sie im Windows Explorer die zu überprüfende Datei und ziehen Sie diese in das Webbrowser-Fenster.

Wenn ein Notarized Backup in der Acronis Cloud gespeichert wird, können Sie die Authentizität einer Datei im Backup in der Acronis Cloud-Webapplikation verifizieren.

***So können Sie die Authentizität einer Datei in Acronis Cloud überprüfen***

1. Gehen Sie zu https://www.acronis.com/my/online-backup/webrestore/ und melden Sie sich an Ihrem Acronis Konto an.
2. Klicken Sie in der Seitenleiste auf **Backups**.

3. Wählen Sie in der Backup-Liste dasjenige 'Notarized Backup' aus, welches die zu überprüfende Datei enthält.
4. Wählen Sie die gewünschte Datei über deren Kontrollkästchen aus. Klicken Sie dann in der rechten Seitenleiste auf **Verifizieren**.

## Die Authentizität einer Datei manuell überprüfen

Die einfachste Möglichkeit, die Authentizität einer Datei zu verifizieren, besteht in der Verwendung des Befehls **Überprüfen**, der sowohl in Acronis Cyber Protect Home Office als auch in der Acronis Cloud-Webapplikation verfügbar ist. Ausführliche Informationen dazu finden Sie im Abschnitt 'Die Authentizität von Dateien überprüfen'. Neben dieser einfachen Methode können Sie die Verifizierungsprozedur auch Schritt für Schritt selbst durchführen.

***So können Sie die Authentizität einer Datei manuell überprüfen***

**Schritt 1: Berechnen Sie den MD5-Hash-Wert der Datei**

1. Starten Sie die Windows PowerShell.
2. Um beispielsweise den MD5-Hash-Wert (nachfolgend nur kurz MD5-Hash genannt) einer Datei namens 'picture.png', die im Ordner 'C:\Users' gespeichert ist, zu berechnen, geben Sie folgenden Befehl ein:

   ```
   $($(CertUtil -hashfile "C:\Users\picture.png" MD5)[1] -replace " ","")
   ```

   Beispiel für einen MD5-Hash: eea16ade1edf2750a46bb6bffb2e45a2
3. Überprüfen Sie, dass der berechnete MD5-Hash identisch ist mit einem eTag im Feld 'DATEN' in Ihrem Beglaubigungszertifikat (englisch auch als „Notarization Certificate“ bezeichnet). Informationen darüber, wie Sie ein Dateizertifikat abrufen können, finden Sie im Abschnitt 'Die Authentizität von Dateien überprüfen.

**Schritt 2. Überprüfen Sie, dass ein ROOT-Wert in der Blockchain gespeichert ist**

1. Öffnen Sie einen Blockchain-Explorer (beispielsweise https://etherscan.io/).
2. Geben Sie die TRANSAKTIONS-ID aus dem Zertifikat in das Suchfeld ein.
3. Überprüfen Sie, dass das Datenfeld in der Ereignisprotokoll-Registerkarte mit dem STAMMVERZEICHNIS (ROOT)-Wert in Ihrem Zertifikat übereinstimmt.

**Schritt 3. Überprüfen Sie, dass der Hash-Wert im Hash-Verzeichnisbaum enthalten ist**

1. Laden Sie das Befehlszeilenwerkzeug vom GitHub-Repository herunter: https://github.com/acronis/notary-verifyhash/releases.
2. Befolgen Sie die Anweisungen unter: https://github.com/acronis/notary-verifyhash.

## Acronis ASign:

### Was ist Acronis ASign?

Acronis ASign ist ein Online Service, der es ermöglicht, dass mehrere Personen eine Datei elektronisch signieren können. Die betreffende Datei sollte zuvor per Backup, Archivierung oder Synchronisierung in die Acronis Cloud hochgeladen werden. Um die signierten Dateien noch weiter schützen zu können, werden sie mithilfe von Acronis Notary beglaubigt und geschützt.

ASign kann zum Signieren beliebiger elektronischer Dokumente – wie Verträge, Vereinbarungen, Zertifikate, Finanzdokumente oder offizielle Briefe – verwendet werden.

### Eine Datei signieren

***So können Sie eine Datei in der Acronis Cloud signieren***

1. Gehen Sie zu https://www.acronis.com/my/online-backup/webrestore/ und melden Sie sich an Ihrem Acronis Konto an.
2. Suchen Sie die gewünschte Datei, klicken Sie auf den Dateinamen und wählen Sie dann im geöffneten Menü den Befehl **Zur Unterschrift senden**.
3. Geben Sie die E-Mail-Adressen der Personen ein, die die Datei signieren sollen, und senden Sie diesen Personen dann Einladungen.
   Nachdem die Datei von den Unterzeichnern signiert wurde, beglaubigt Acronis Notary die Datei und generiert ein Signaturzertifikat.

Eine vollständige Beschreibung der Funktionalität finden Sie auf der englischsprachigen Webhilfe zu Acronis ASign (unter: https://www.acronis.com/en-us/support/documentation/ATI2017ASign/).

# Backups, Backup-Versionen und Replikate bereinigen

Wenn Sie nicht mehr benötigte Backups und Backup-Versionen löschen wollen, sollten Sie dies nur mit den von Acronis Cyber Protect Home Office dafür bereitgestellten Befehlen tun.

Acronis Cyber Protect Home Office speichert Informationen über Backups in einer Datenbank für Metadaten-Informationen. Wenn Sie nicht mehr benötigte Backup-Dateien daher einfach in einem Windows-Dateimanager (wie dem Windows Explorer) löschen, werden die Metadaten-Informationen dieser Backups nicht auch aus der Datenbank entfernt. Das führt zu Fehlern, wenn das Programm versucht, Aktionen mit nicht mehr existierenden Backups auszuführen.

## Ein komplettes Backup und dessen Replikat löschen

Klicken Sie im Bereich **Backup** auf den nach unten zeigenden Pfeil neben dem zu löschenden Backup – und wählen Sie dann den Befehl **Löschen**.

Abhängig vom Backup-Typ löscht dieser Befehl das Backup vollständig von seinem Speicherort oder erlaubt es Ihnen zu wählen, ob Sie das Backup vollständig (mit all seinen Dateien) löschen oder nur aus der Backup-Liste entfernen wollen. Wenn Sie das Backup aus der angezeigten Liste entfernen,

verbleiben die dazugehörigen Backup-Dateien an ihrem Speicherort, sodass Sie das Backup auch zu einem späteren Zeitpunkt wieder in die Liste aufnehmen können. Beachten Sie, dass die Löschung nicht rückgängig gemacht werden kann, wenn Sie ein Backup komplett löschen.

Wenn Sie ein Backup löschen, wird automatisch auch dessen Replikat gelöscht. Sie können eine lokale Backup nicht löschen und dabei trotzdem dessen Replikat bewahren. Umgekehrt können Sie jedoch das Replikat alleine löschen und das lokale Backup behalten.

## Ein komplettes Backup-Replikat löschen

Sie können ein Replikat separat löschen oder zusammen mit seinem Original-Backup. Wenn Sie es mit dem Backup zusammen löschen wollen, löschen Sie (wie oben beschrieben) das Backup.

Wenn Sie ein Replikat löschen wollen, ohne das entsprechenden Backup zu entfernen, dann müssen Sie im Bereich **Backup** auf den nach unten zeigenden Pfeil neben dem Backup, zu dem das zu löschende Replikat gehört, klicken und anschließend den Befehl **Replikat löschen** auswählen.

## Backup-Versionen automatisch bereinigen

1. Gehen Sie in den Programmbereich **Backup**.
2. Wählen Sie aus der Backup-Liste dasjenige Backup aus, dessen Replikat-Versionen Sie bereinigen wollen, und klicken Sie dann auf **Optionen**.
3. Wählen Sie in der Registerkarte **Backup-Schema** die Option **Benutzerdefiniertes Schema**, wählen Sie eine Backup-Methode aus und klicken Sie anschließdend auf **Automatische Bereinigung einschalten**.
4. Konfigurieren Sie die Bereinigungsregeln für das Backup.
   Weitere Informationen finden Sie im Abschnitt 'Benutzerdefinierte Schemata'.

**Hinweis**
Nach der Bereinigung können einige Hilfsdateien im Storage übrigbleiben. Löschen Sie diese bitte nicht!

## Replikat-Versionen automatisch bereinigen

1. Gehen Sie in den Programmbereich **Backup**.
2. Wählen Sie aus der Backup-Liste dasjenige Backup aus, dessen Replikat-Versionen Sie bereinigen wollen, und klicken Sie dann auf **Optionen**.
3. Öffnen Sie über die Registerkarte **Erweitert** die Registerkarte **Acronis Cloud -Bereinigung**.
   - Verwenden Sie die Option **Nicht mehr speichern als ... neueste Backup-Versionen**, um einen Wert festzulegen, der die Gesamtanzahl aller gespeicherten Replikat-Versionen begrenzt.
   - Klicken Sie auf das Kontrollkästchen **Backup-Versionen löschen, die älter sind als** und geben Sie einen Wert an, der das Versionsalter entsprechend begrenzt. Die neuesten Versionen werden aufbewahrt, während alle anderen (älteren) Versionen automatisch gelöscht werden.

## Backup-Versionen manuell bereinigen

Wenn Sie nicht mehr benötigte Backup-Versionen löschen wollen, sollten Sie dies nur mit den von der Applikation dafür bereitgestellten Befehlen tun. Wenn Sie Backup-Versionen außerhalb von Acronis Cyber Protect Home Office löschen (beispielsweise über den Windows Explorer), wird dies zu Fehlern führen, wenn Sie mit den Backups weitere Aktionen durchführen wollen.

Die Versionen folgender Backups können nicht manuell gelöscht werden:

- Backups, die auf CD, DVD, BD oder in der Acronis Secure Zone gespeichert sind
- Nonstop Backups.
- Beglaubigte Backups (Notarized Backups).

***So können Sie bestimmte Backup-Versionen bereinigen***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie im Bereich **Backup** auf den nach unten zeigenden Pfeil neben dem zu bereinigenden Backup – und wählen Sie dann den Befehl **Versionen bereinigen**.
   Das Fenster **Backup-Versionen bereinigen** wird geöffnet.
3. Wählen Sie die gewünschten Versionen aus und klicken Sie dann auf **Löschen**.
4. Klicken Sie im Bestätigungsfenster auf **Löschen**.

Warten Sie, bis die Bereinigungsaktion abgeschlossen wurde. Nach der Bereinigung können einige Hilfsdateien im Storage übrigbleiben. Löschen Sie diese bitte nicht.

**Versionen bereinigen, die abhängige Versionen haben**

Wenn Sie eine Backup-Version zum Löschen auswählen, sollten Sie beachten, dass zu dieser Versionen noch weitere, abhängige Versionen gehören können. In diesem Fall werden auch die abhängigen Versionen zum Löschen ausgewählt, da von diesen Versionen ohnehin keine Wiederherstellung mehr möglich ist.

- **Wenn Sie eine Voll-Backup-Version auswählen** – wählt das Programm ebenfalls alle abhängigen inkrementellen und differentiellen Versionen aus (bis zur nächsten vollständigen Version). Oder mit anderen Worten: die komplette Backup-Versionskette wird gelöscht.
- **Wenn Sie eine differentielle Version auswählen** – wählt das Programm ebenfalls alle abhängigen inkrementellen Versionen innerhalb der Backup-Versionskette aus.
- **Wenn Sie eine inkrementelle Version auswählen** – wählt das Programm ebenfalls alle abhängigen inkrementellen Versionen innerhalb der Backup-Versionskette aus.

**Siehe auch**

Vollständige, inkrementelle und differentielle Backups.

Daten aus der Acronis Cloud entfernen.

## Speicherplatz in der Acronis Cloud bereinigen

1. Gehen Sie zu https://www.acronis.com/my/online-backup/webrestore/ und melden Sie sich an Ihrem Acronis Konto an. Daraufhin wird die Acronis Cloud-Webapplikation geöffnet.
2. Klicken Sie in der linken Seitenleiste der Webapplikation auf **Konto**.
3. Klicken Sie in der Zeile der **Acronis Cloud** auf den Befehl **Bereinigen**.
4. Wählen Sie, welche Versionen Sie löschen möchten:
   - Versionen, die älter als ein bestimmter Zeitraum sind.
   - Alle alten Versionen, außer einigen neuen.

**Warnung!**
Achtung! Gelöschte Versionen können nicht wiederhergestellt werden.

Eine weitere Möglichkeit zur Bereinigung besteht darin, dass Sie ein nicht mehr benötigtes Cloud Backup löschen. In diesem Fall wird der komplette Versionsverlauf des betreffenden Backups aus der Acronis Cloud gelöscht.

## Daten aus der Acronis Cloud entfernen

Da der in der Acronis Cloud verfügbare Speicherplatz begrenzt ist, müssen Sie Ihren Cloud-Speicherplatz verwalten, indem Sie ihn von veralteten oder nicht mehr benötigten Daten bereinigen. Die Bereinigung kann in Acronis Cyber Protect Home Office durchgeführt werden – oder auch über die Acronis Cloud-Webapplikation.

### Ein komplettes Backup löschen

Die drastischste Möglichkeit besteht darin, das komplette Backup in der Acronis Cloud zu löschen. Wenn ein Backup gelöscht wird, werden damit auch all seine Daten dauerhaft gelöscht. Gelöschte Daten können nicht wiederhergestellt werden.

In **Acronis Cyber Protect Home Office**:

Klicken Sie neben dem zu löschenden Backup auf den nach unten zeigenden Pfeil und anschließend auf den Befehl **Löschen**. Das Backup wird – mit all seinen Versionen, Einstellungen und der Planung – gelöscht.

In der **Acronis Cloud-Webapplikation**:

1. Gehen Sie zu https://www.acronis.com/my/online-backup/webrestore/ und melden Sie sich an Ihrem Acronis Konto an.
2. Bewegen Sie auf der Registerkarte **Backups** den Mauszeiger über das Backup, das Sie löschen wollen.
3. Klicken Sie auf die Größe des Backups, woraufhin die Detailansicht angezeigt wird.
4. Klicken Sie in der Detailansicht auf **Löschen**.

Beachten Sie, dass zwar das Backup aus der Acronis Cloud gelöscht wird, aber seine Einstellungen und seine Planung bleiben in der Acronis Cyber Protect Home Office-Applikation erhalten.

## Die Versionen eines Backups in die Cloud löschen

In **Acronis Cyber Protect Home Office**:

1. Klicken Sie neben dem Backup, dessen Versionen Sie löschen wollen, auf den nach unten zeigenden Pfeil und anschließend auf den Befehl **Versionen bereinigen**.
   Die Liste der Backup-Versionen wird angezeigt.
2. Wählen Sie die Versionen aus, die Sie löschen wollen, und klicken Sie dann auf den Befehl **Löschen**.

**Hinweis**
Es kann bis zu einem Tag dauern, bis die Quota in der Acronis Cloud entsprechend aktualisiert wird.

In der **Acronis Cloud-Webapplikation**:

1. Gehen Sie zu https://www.acronis.com/my/online-backup/webrestore/ und melden Sie sich an Ihrem Acronis Konto an.
2. Klicken Sie in der Registerkarte **Backups** auf die Größenangabe des Backups, dessen Versionen Sie löschen wollen.
   Die Detailansicht für das Backup wird geöffnet.
3. Klicken Sie in der Detailansicht auf den Befehl **Bereinigen**.
   Sie können bestimmen, ob Versionen gelöscht werden sollen, die älter als ein von Ihnen festgelegter Zeitraum sind – oder ob Sie alle Versionen bereinigen wollen, wobei einige neuere Versionen ausgenommen werden können.
4. Konfigurieren Sie, was gelöscht werden soll, und klicken Sie dann auf **Jetzt bereinigen**.
5. Klicken Sie im Bestätigungsdialog auf **Löschen**.

Der Status des Bereinigungsprozedur wird angezeigt, wenn die Aktion abgeschlossen wurde.

## Die Versionen eines Backup-Replikats in die Cloud löschen

In **Acronis Cyber Protect Home Office**:

1. Suchen Sie im Bereich **Backup** ein lokales Backup, das in die Cloud repliziert wird. Klicken Sie anschließend auf den nach unten zeigenden Pfeil und wählen Sie den Befehl **Versionen bereinigen**.
   Das Dialogfenster 'Backup-Versionen bereinigen' wird geöffnet.
2. Wählen Sie bei **Versionen aus ... löschen** die Option **Acronis Cloud**.
   Die Liste der Backup-Replikat-Versionen wird angezeigt.
3. Wählen Sie die Replikat-Versionen aus, die Sie löschen wollen, und klicken Sie dann auf den Befehl **Löschen**.
4. Klicken Sie im Bestätigungsdialog auf **Löschen**.

**Hinweis**
Es kann bis zu einem Tag dauern, bis die Quota in der Acronis Cloud entsprechend aktualisiert wird.

In der **Acronis Cloud-Webapplikation**:

1. Gehen Sie zu https://www.acronis.com/my/online-backup/webrestore/ und melden Sie sich an Ihrem Acronis Konto an.
2. Klicken Sie in der Registerkarte **Backups** auf die Größenangabe des Replikats, dessen Versionen Sie löschen wollen.
   Die Detailansicht für das Backup-Replikat wird geöffnet.
3. Klicken Sie in der Detailansicht auf den Befehl **Bereinigen**.
   Sie können bestimmen, ob Versionen gelöscht werden sollen, die älter als ein von Ihnen festgelegter Zeitraum sind – oder ob Sie alle Versionen bereinigen wollen, wobei einige neuere Versionen ausgenommen werden können.
4. Konfigurieren Sie, was gelöscht werden soll, und klicken Sie dann auf **Jetzt bereinigen**.
5. Klicken Sie im Bestätigungsdialog auf **Löschen**.

Der Status des Bereinigungsprozedur wird angezeigt, wenn die Aktion abgeschlossen wurde.

## Einmalige Bereinigung

Wenn die Acronis Cloud voll ist oder ihr Speicherplatz ausgeht, empfehlen wir die Verwendung des Bereinigungswerkzeugs in der Acronis Cloud-Webapplikation. Dieses Tool ermöglicht Ihnen, schnell und einfach eine beträchtliche Menge an Speicherplatz in der Cloud freizugeben.

**Hinweis**
Sie können die Backups einzeln nacheinander bereinigen, auch die verschlüsselten Backups. Das Kennwort wird abgefragt.

1. Gehen Sie zu https://www.acronis.com/my/online-backup/webrestore/ und melden Sie sich an Ihrem Acronis Konto an.
2. Bewegen Sie auf der Registerkarte **Backups** den Mauszeiger über das Backup, das Sie löschen wollen.
3. Klicken Sie auf die Schaltfläche **Bereinigen**.
4. Konfigurieren Sie im angezeigten Fenster die Bereinigungseinstellungen und klicken Sie dann auf **Jetzt bereinigen**

Verwenden Sie die folgende Option, um eine einmalige Bereinigung von allen unverschlüsselten Backups durchzuführen:

1. Gehen Sie zur Registerkarte **Konto**.
2. Klicken Sie auf die Schaltfläche **Bereinigen**.

# Daten wiederherstellen

## Laufwerke und Volumes wiederherstellen

### Ihr System nach einem Absturz wiederherstellen

Wenn Ihr Computer nicht mehr in der Lage ist zu booten, ist es ratsam, als erstes mit den im Abschnitt 'Versuche zur Bestimmung der Absturzursache' gemachten Vorschlägen nach dem entsprechenden Grund zu suchen. Wenn die Ursache des Absturzes in einer Beschädigung des Betriebssystems liegt, dann sollten Sie ein Backup verwenden, um Ihr System wiederherzustellen. Führen Sie die im Abschnitt 'Vorbereitungen zur Wiederherstellung' beschriebenen Maßnahmen durch und fahren Sie dann mit der Wiederherstellung Ihres Systems fort.

### Versuche zur Bestimmung der Absturzursache

Die meisten Systemabstürze beruhen auf zwei grundsätzlichen Faktoren:

- **Hardware-Fehler**

  In diesem Szenario sollten Sie die Reparatur am besten von einem Service-Center ausführen lassen. Möglicherweise möchten Sie aber auch selbst einige typische Tests zur Klärung durchführen. Überprüfen Sie die Kabel, Stecker, die Stromversorgung externer Geräte etc. Versuchen Sie danach, den Computer neu zu starten. Beim Vorliegen eines Hardware-Problems gibt Ihnen möglicherweise die POST-Routine (Power-On Self Test) Informationen über den Fehler. Bringt der POST jedoch keinen Hardware-Fehler zu Tage, dann sollten Sie als Nächstes ins BIOS gehen und dort überprüfen, ob Ihr System-Laufwerk erkannt wird. Um in das BIOS zu gelangen, müssen Sie eine bestimmte Tastenkombination drücken (**Entf**, **F1**, **Strg+Alt+Esc**, **Strg+Esc** oder eine andere Kombination, abhängig von vorliegenden BIOS) Üblicherweise wird eine Meldung zur benötigten Tastenkombination während des Starts angezeigt. Durch Drücken dieser Tastenkombination gelangen Sie in das Setup-Menü Ihres BIOS. Gehen Sie zum Werkzeug für die automatische Laufwerkserkennung (Hard Disk Autodetection, die meisten BIOS-Versionen sind englischsprachig), das Sie üblicherweise im Menüpunkt 'Standard CMOS Setup' oder 'Advanced CMOS Setup' finden (ebenfalls üblicherweise englisch). Falls das Werkzeug Ihr System-Laufwerk nicht erkennt, dürfte dieses beschädigt sein und sollte von Ihnen ausgetauscht werden.
- **Beschädigung des Betriebssystems (Windows kann nicht starten)**

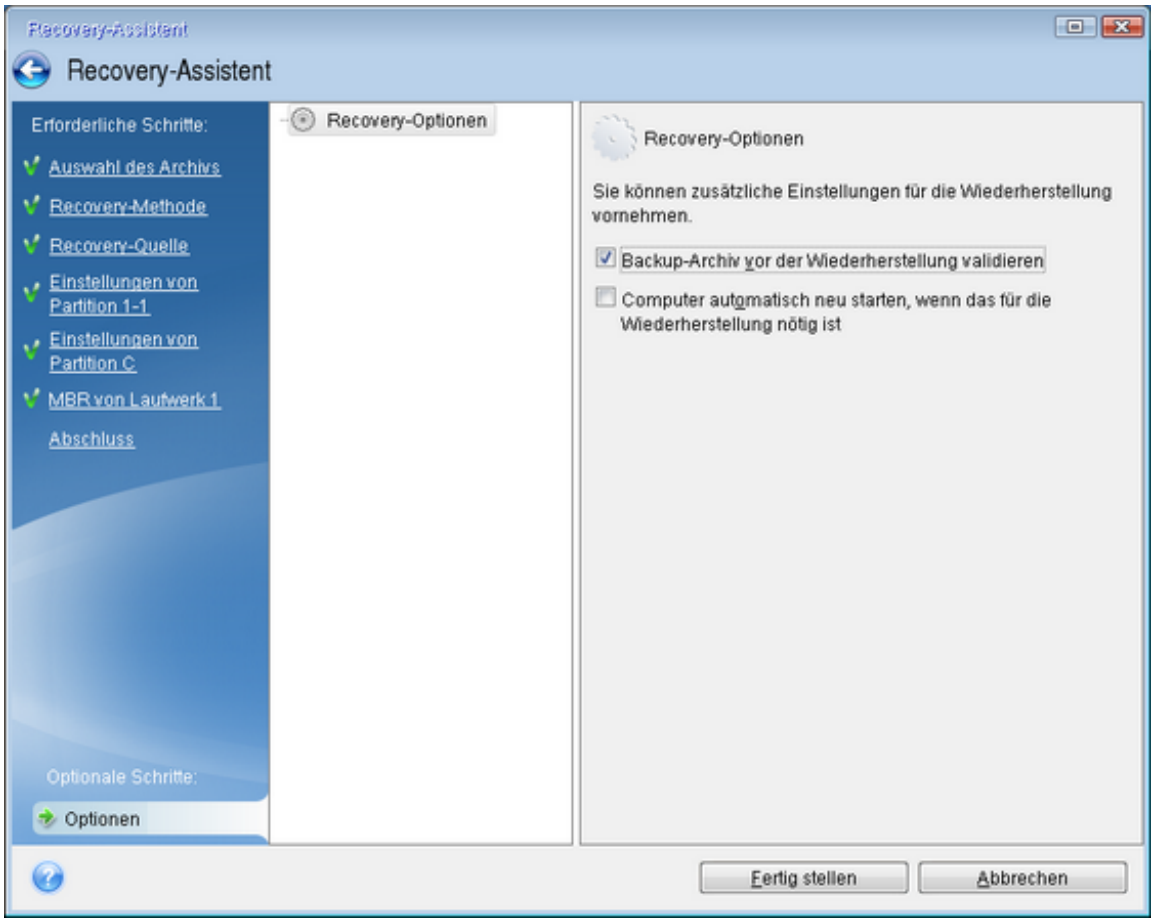
  Falls die POST-Routine Ihr System-Laufwerk jedoch korrekt erkennt, ist die Absturzursache vermutlich Software-basiert – beispielsweise durch ein Virus (oder ähnliches Schadprogramm) oder weil eine zum Booten benötigte Systemdatei beschädigt ist. In diesem Fall sollten Sie Ihr System durch Verwendung eines Backups (von Ihrem System-Laufwerk bzw. -Volume) wiederherstellen. Weitere Details finden Sie im Abschnitt 'Ihr System wiederherstellen'.

### Wiederherstellung vorbereiten

Wir empfehlen, dass Sie vor der Wiederherstellung folgende Aktionen durchführen:

- Überprüfen Sie den Computer auf Viren (oder ähnliche Schadprogramme), sofern Sie vermuten, dass diese für den Systemabsturz verantwortlich sein könnten.
- Versuchen Sie mit einem Boot-Medium eine Testwiederherstellung auf ein überzähliges, freies Laufwerk durchzuführen (sofern ein solches verfügbar ist).
- Validieren Sie das Image unter Verwendung eines Boot-Mediums. Ein unter Windows bei der Validierung lesbares Backup **muss nicht immer auch unter einer Linux-Umgebung (Boot-Medium) lesbar sein**.

  **Bei einem Boot-Medium gibt es zwei Möglichkeiten, ein Backup zu validieren:**
  - Klicken Sie zur manuellen Validierung eines Backups in der Registerkarte **Recovery** mit der rechten Maustaste auf ein Backup und wählen Sie **Archiv validieren**.
  - Aktivieren Sie zur automatischen Validierung eines Backups vor einer Wiederherstellung im Schritt **Optionen** des **Recovery-Assistenten** das Kontrollkästchen **Backup-Archiv vor der Wiederherstellung validieren**.




- Weisen Sie allen Volumes auf Ihren Laufwerken eindeutige Namen (Bezeichnungen) zu. Dadurch ist es auch einfacher, die Laufwerke, die die Backups enthalten, zu finden.

  Wenn Sie ein Boot-Medium verwenden, vergibt dieses Laufwerksbuchstaben, die sich möglicherweise von denen, die Windows verwendet, unterscheiden. So könnte beispielsweise die Zuordnung des Laufwerks D: unter dem Boot-Medium dem Laufwerk E: unter Windows entsprechen.

## Ein System auf demselben Laufwerk wiederherstellen

Wir empfehlen, dass Sie vor dem Beginn die im Abschnitt 'Vorbereitungen zur Wiederherstellung' beschriebenen Aktionen durchführen.

***So können Sie Ihr System wiederherstellen***

1. Schließen Sie ein externes Laufwerk an, wenn dieses das für die Wiederherstellung zu verwendende Backup enthält und schalten Sie es ein.
2. Konfigurieren Sie die Boot-Reihenfolge in Ihrem BIOS so, dass das Gerät/Laufwerk Ihres Acronis Boot-Mediums (CD, DVD oder USB-Stick) das primäre Boot-Gerät ist. Siehe auch den Abschnitt 'Boot-Reihenfolge im BIOS oder UEFI-BIOS arrangieren'.

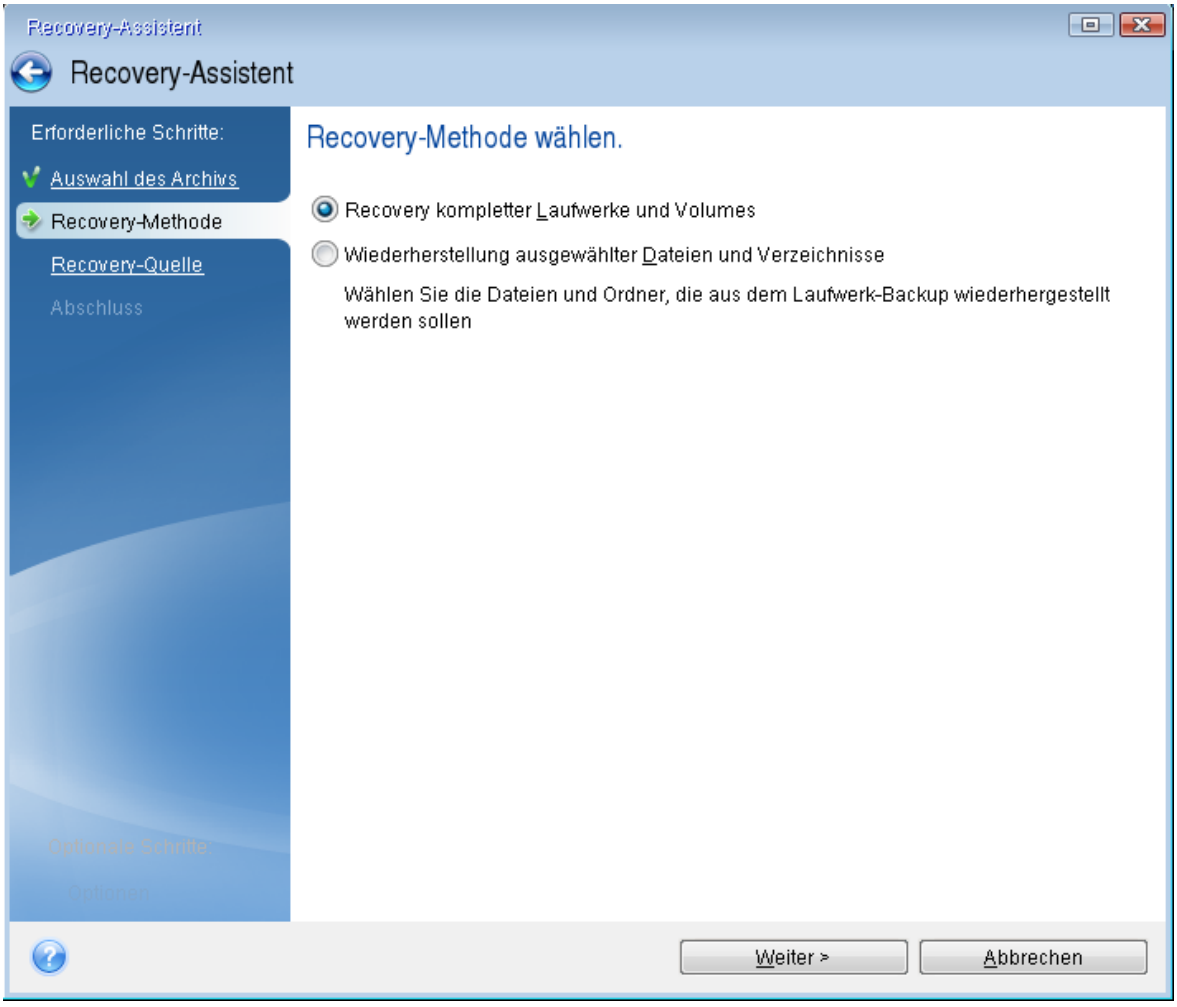
   Wenn Sie einen UEFI-Computer verwenden, sollten Sie darauf achten, welcher Boot-Modus für das Boot-Medium im UEFI-BIOS eingestellt ist. Der Boot-Modus sollte normalerweise mit dem Typ des Systems im Backup übereinstimmen. Wenn das Backup ein BIOS-System enthält, sollten Sie das Boot-Medium im BIOS-Modus starten. Wenn es sich um ein UEFI-System handelt, sollten Sie das Medium im UEFI-Modus booten.
3. Starten Sie den Computer mit dem Acronis Boot-Medium und wählen Sie **Acronis Cyber Protect Home Office**.
4. Wählen Sie in der **Startseite** den Befehl **Laufwerke** (unterhalb des Elements **Recovery**).


5. Wählen Sie das Systemlaufwerk- oder Volume-Backup aus, welches Sie für die Wiederherstellung verwenden wollen.

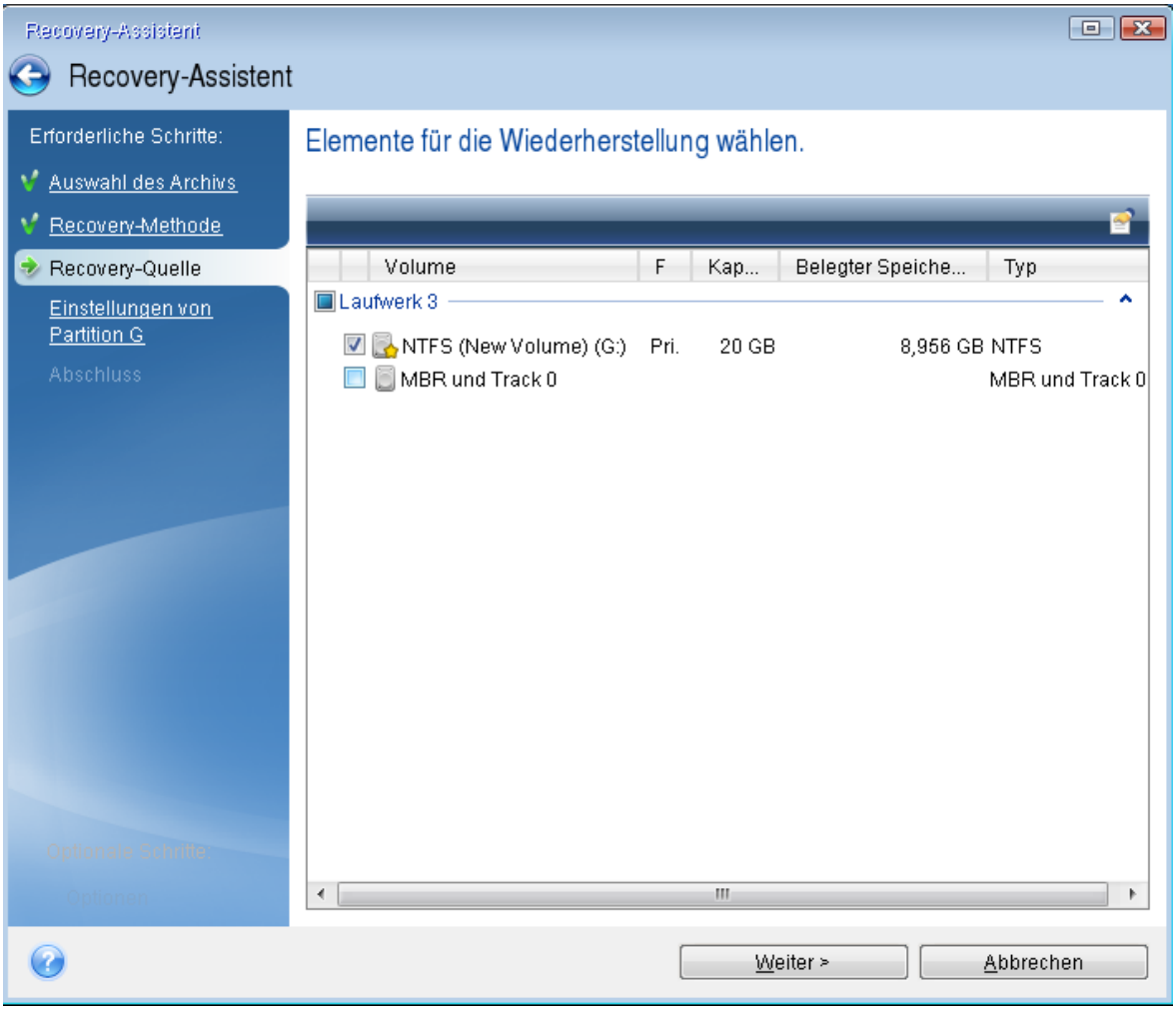
Sollte das Backup nicht angezeigt werden, dann klicken Sie auf **Durchsuchen** und geben Sie den Pfad zum Backup manuell an.

**Hinweis**
Wenn sich das Backup auf einem USB-Laufwerk befindet und das Laufwerk nicht richtig erkannt wird, sollten Sie die Version des USB-Anschluss überprüfen. Falls es sich um einen USB 3.0- oder USB 3.1-Anschluss handelt, sollten Sie versuchen, das Laufwerk alternativ über einen USB 2.0-Anschluss zu verbinden.

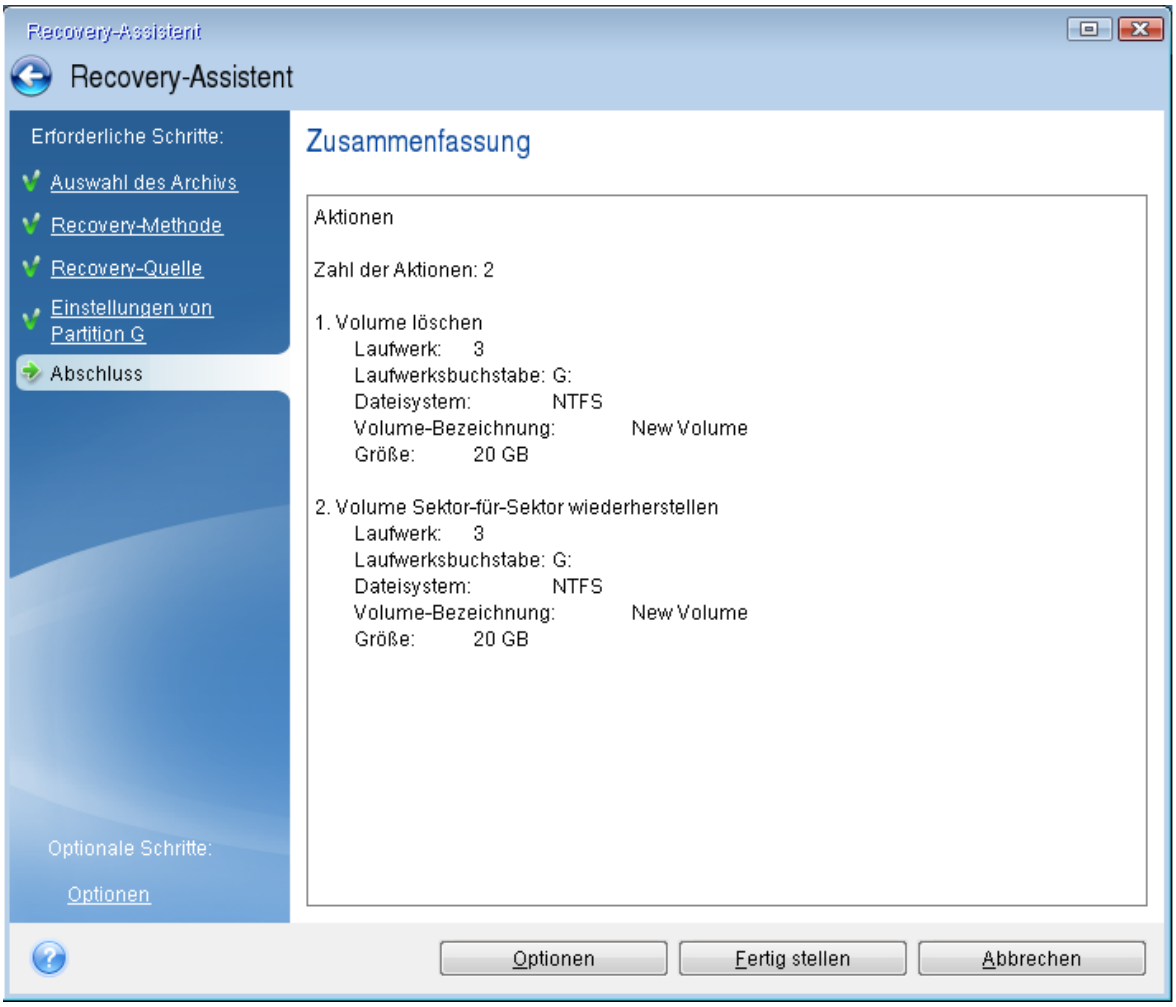
6. Wählen Sie im Schritt **Recovery-Methode** den Befehl **Recovery kompletter Laufwerke und Volumes**.




7. [Optional] Wählen Sie bei **Recovery-Punkt** denjenigen Zeitpunkt, an dem das Backup erstellt wurde und zu dem Sie das System zurücksetzen wollen.
8. Wählen Sie in der Anzeige **Recovery-Quelle** die Systempartition aus (üblicherweise C). Wenn das System-Volume einen anderen Buchstaben hat, wählen Sie das Volume über die Spalte **Flags** (Englisch für Kennzeichnungen) aus. Die Kennzeichnungen **Primär** und **Aktiv** müssen gesetzt sein. Sollte bei Ihnen ein verstecktes Volume vorliegen (beispielsweise das Volume 'System-reserviert'), dann wählen Sie auch dieses aus.




9. Überprüfen Sie beim Schritt **Einstellungen des Volumes C:** (bzw. dem Laufwerksbuchstaben des System-Volumes, sofern abweichend) die Standardeinstellungen und klicken Sie auf **Weiter**, wenn diese korrekt sind. Ändern Sie anderenfalls die Einstellungen wie benötigt, bevor Sie auf **Weiter** klicken. Eine Änderung der Einstellung kann nötig werden, wenn Sie eine Wiederherstellung auf ein neues Laufwerk mit abweichender Kapazität durchführen wollen.
10. Lesen Sie die Zusammenfassung der Aktionen im Schritt **Fertigstellen** aufmerksam durch. Wenn Sie die Volume-Größe nicht verändert haben, müssen die Größen in den Elementen **Volume löschen** und **Volume wiederherstellen** übereinstimmen. Klicken Sie auf **Fertigstellen**, wenn Sie die angezeigte Zusammenfassung überprüft haben.




11. Beenden Sie nach Abschluss der Aktion die autonome Notfallversion von Acronis Cyber Protect Home Office, entnehmen/entfernen Sie das Acronis Boot-Medium und booten Sie dann das wiederhergestellte System-Volume. Wenn Sie sich vergewissert haben, dass Sie Windows zu dem von Ihnen gewünschten Stadium wiederhergestellt haben, können Sie die ursprüngliche Boot-Reihenfolge im BIOS wieder einrichten.

## Ein System mit einem Boot-Medium auf einem neuen Laufwerk wiederherstellen

Wir empfehlen, dass Sie vor dem Beginn die im Abschnitt 'Vorbereitungen zur Wiederherstellung' beschriebenen Aktionen durchführen. Sie müssen das neue Laufwerk nicht formatieren, da dies durch den Recovery-Prozess quasi übernommen wird.

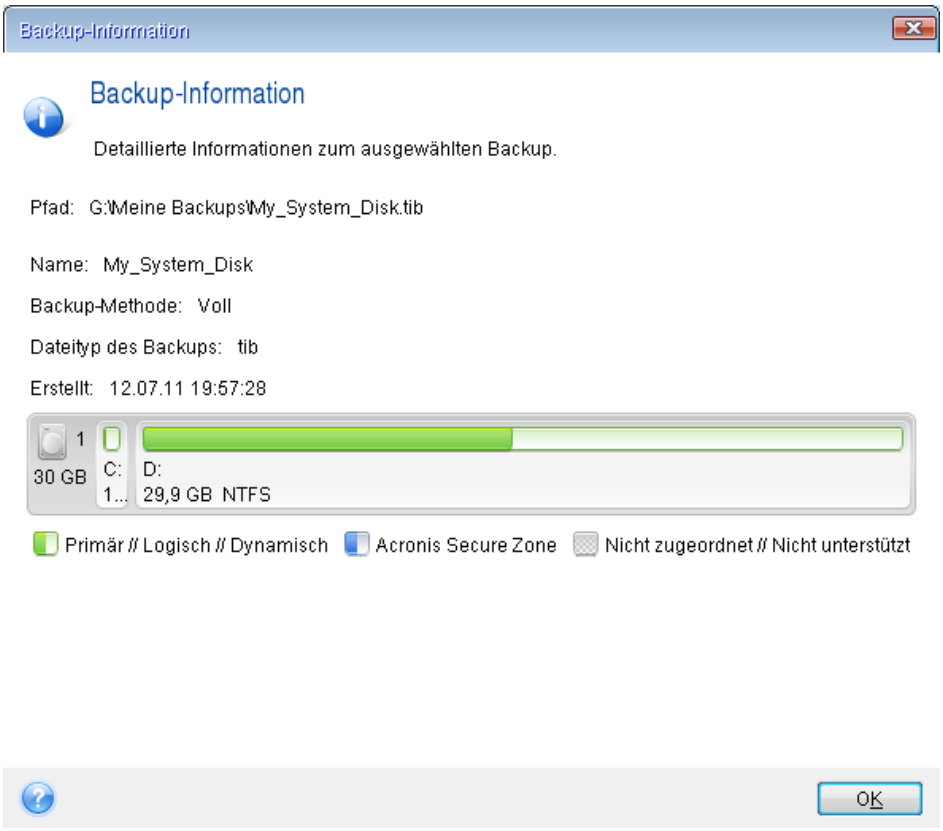
**Hinweis**
Es wird empfohlen, dass das alte und neue Laufwerk im selben 'Controller-Modus' (beispielsweise 'IDE' oder 'AHCI') arbeiten. Anderenfalls wird Ihr Computer möglicherweise nicht von dem neuen Laufwerk booten können.

***So können Sie Ihr System auf einem neuen Laufwerk wiederherstellen***

1. Bauen Sie das neue Laufwerk möglichst an derselben Position im Computer ein und verwenden Sie dabei auch das Kabel und den Stecker des ursprünglichen Laufwerks. Sollte dies nicht möglich sein, dann bauen Sie das neue Laufwerk dort ein, wo Sie es später verwenden möchten.
2. Schließen Sie ein externes Laufwerk an, wenn dieses das für die Wiederherstellung zu verwendende Backup enthält und schalten Sie es ein.
3. Konfigurieren Sie die Boot-Reihenfolge in Ihrem BIOS so, dass das Gerät/Laufwerk Ihres Boot-Mediums (CD, DVD oder USB-Stick) das primäre Boot-Gerät ist. Siehe auch den Abschnitt 'Boot-Reihenfolge im BIOS oder UEFI-BIOS arrangieren'.

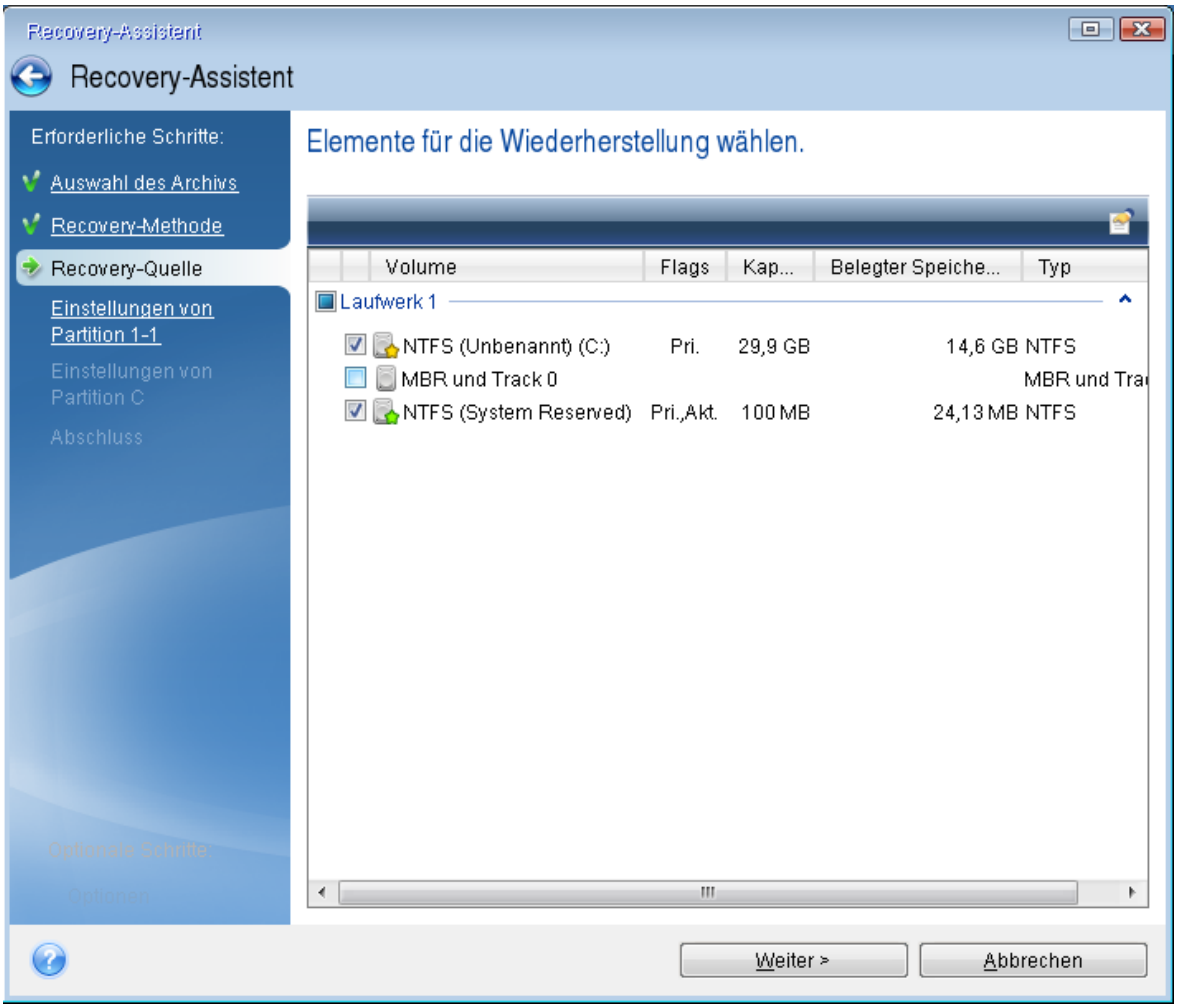
   Wenn Sie einen UEFI-Computer verwenden, sollten Sie darauf achten, welcher Boot-Modus für das Boot-Medium im UEFI-BIOS eingestellt ist. Der Boot-Modus sollte normalerweise mit dem Typ des Systems im Backup übereinstimmen. Wenn das Backup ein BIOS-System enthält, sollten Sie das Boot-Medium im BIOS-Modus starten. Wenn es sich um ein UEFI-System handelt, sollten Sie das Medium im UEFI-Modus booten.
4. Starten Sie den Computer mit dem Boot-Medium und wählen Sie **Acronis Cyber Protect Home Office**..
5. Wählen Sie in der **Startseite** den Befehl **Laufwerke** (unterhalb des Elements **Recovery**).
6. Wählen Sie das Systemlaufwerk- oder Volume-Backup aus, welches Sie für die Wiederherstellung verwenden wollen. Sollte das Backup nicht angezeigt werden, dann klicken Sie auf **Durchsuchen** und geben Sie den Pfad zum Backup manuell an.

   **Hinweis**
   Wenn sich das Backup auf einem USB-Laufwerk befindet und das Laufwerk nicht richtig erkannt wird, sollten Sie die Version des USB-Anschluss überprüfen. Falls es sich um einen USB 3.0- oder USB 3.1-Anschluss handelt, sollten Sie versuchen, das Laufwerk alternativ über einen USB 2.0-Anschluss zu verbinden.
7. Sollte bei Ihnen ein verstecktes Volume vorliegen (beispielsweise das Volume 'System-reserviert' oder ein vom PC-Hersteller erstelltes Volume), dann klicken Sie in der Symbolleiste des Assistenten auf **Details**. Merken bzw. notieren Sie sich die Position und Größe des versteckten Volumes, da diese Parameter auf dem neuen Laufwerk identisch sein müssen.



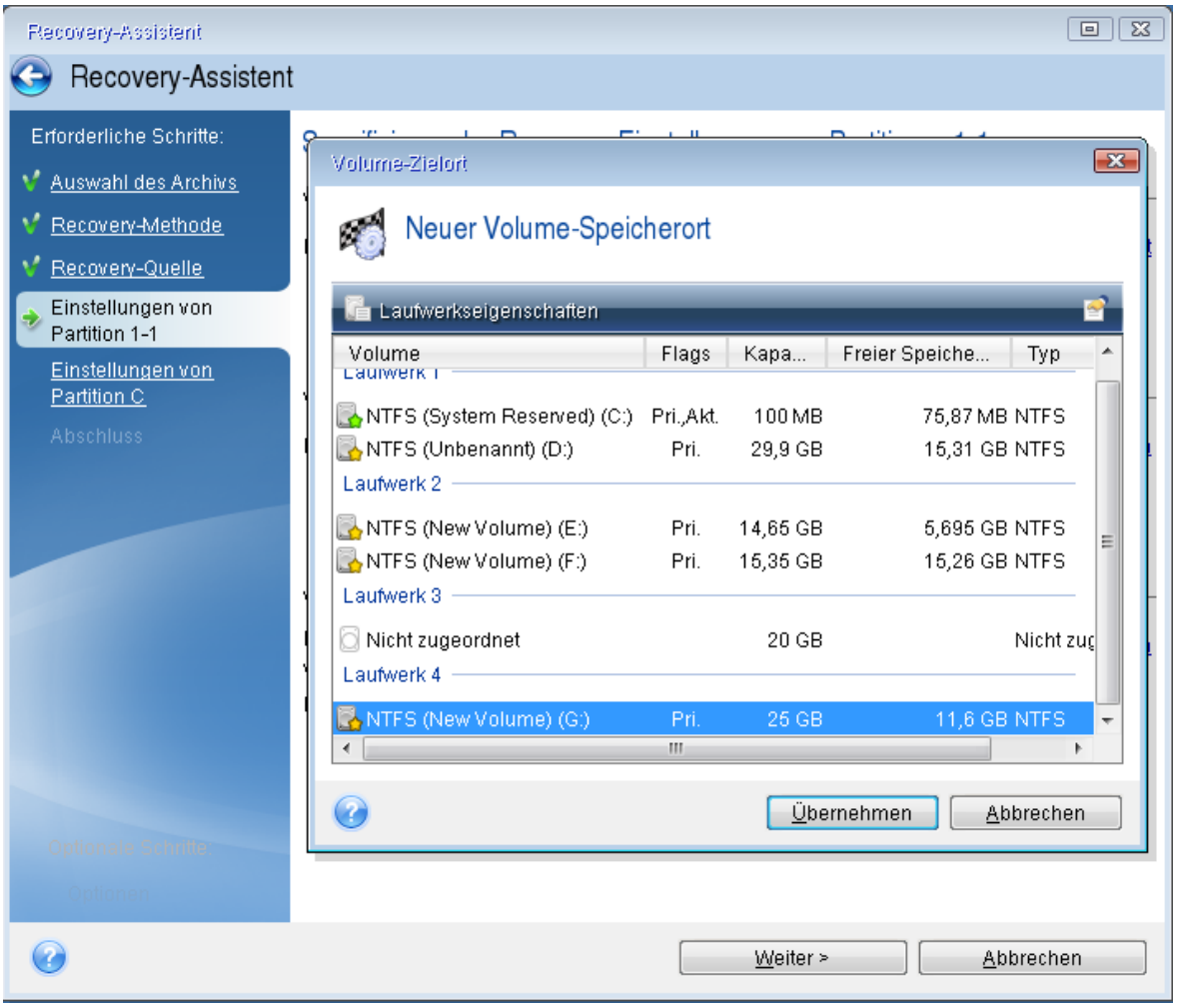

8. Wählen Sie im Schritt **Recovery-Methode** den Befehl **Recovery kompletter Laufwerke und Volumes**.
9. Aktivieren Sie im Schritt **Recovery-Quelle** die Kontrollkästchen der wiederherzustellenden Volumes.

   Wenn Sie ein komplettes Laufwerk auswählen, werden der MBR und Track 0 des Laufwerks ebenfalls mit wiederhergestellt.

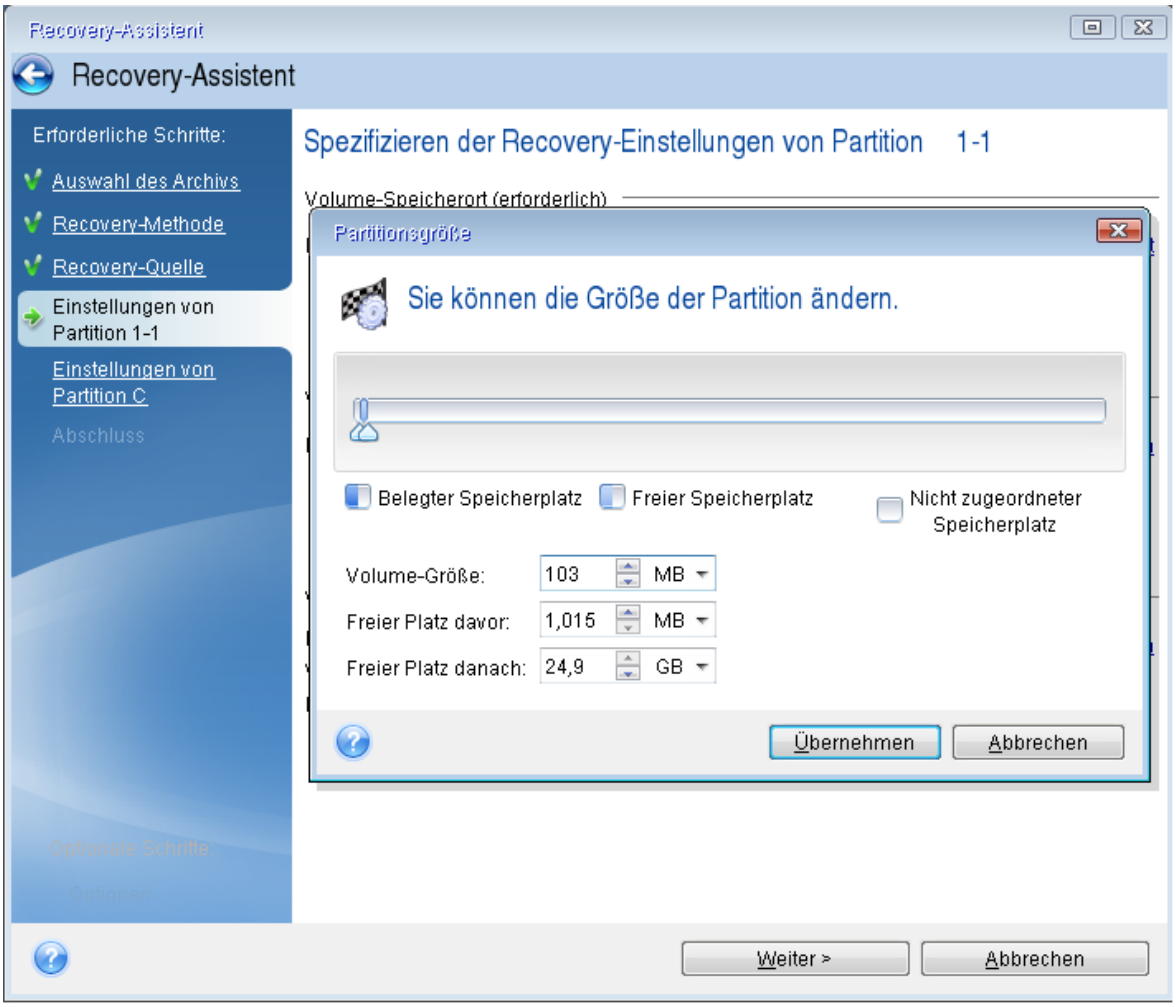



Über das Auswählen der Volumes gelangen Sie zu den Schritten **Einstellungen des Volumes**. Beachten Sie, dass diese Schritte mit den Volumes beginnen, die keinen Laufwerksbuchstaben zugewiesen haben (wie es normalerweise bei versteckten Volumes der Fall ist). Die Volumes nehmen dann eine aufsteigende Reihenfolge gemäß ihrer Laufwerksbuchstaben an. Diese Reihenfolge kann nicht geändert werden. Diese Reihenfolge kann sich von der physischen Reihenfolge der Volumes auf dem Laufwerk unterscheiden.

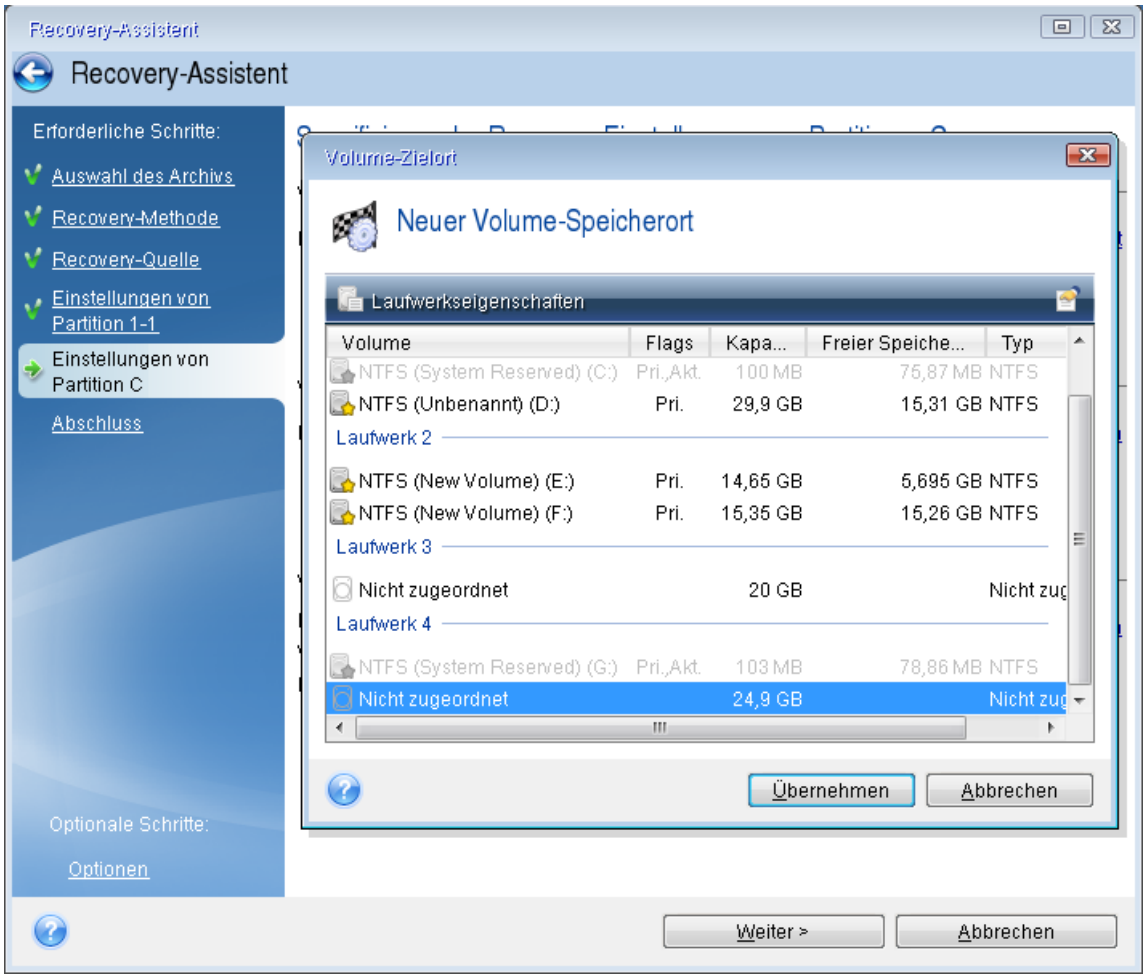
10. Spezifizieren Sie beim Schritt zur Konfiguration des versteckten Volumes (üblicherweise mit 'Einstellungen von Volume 1-1' bezeichnet) folgende Optionen:
    - **Speicherort** – Klicken Sie auf **Neuer Speicherort**, wählen Sie das neue Laufwerk anhand seiner Bezeichnung oder Kapazität aus und klicken Sie dann auf **Übernehmen**.



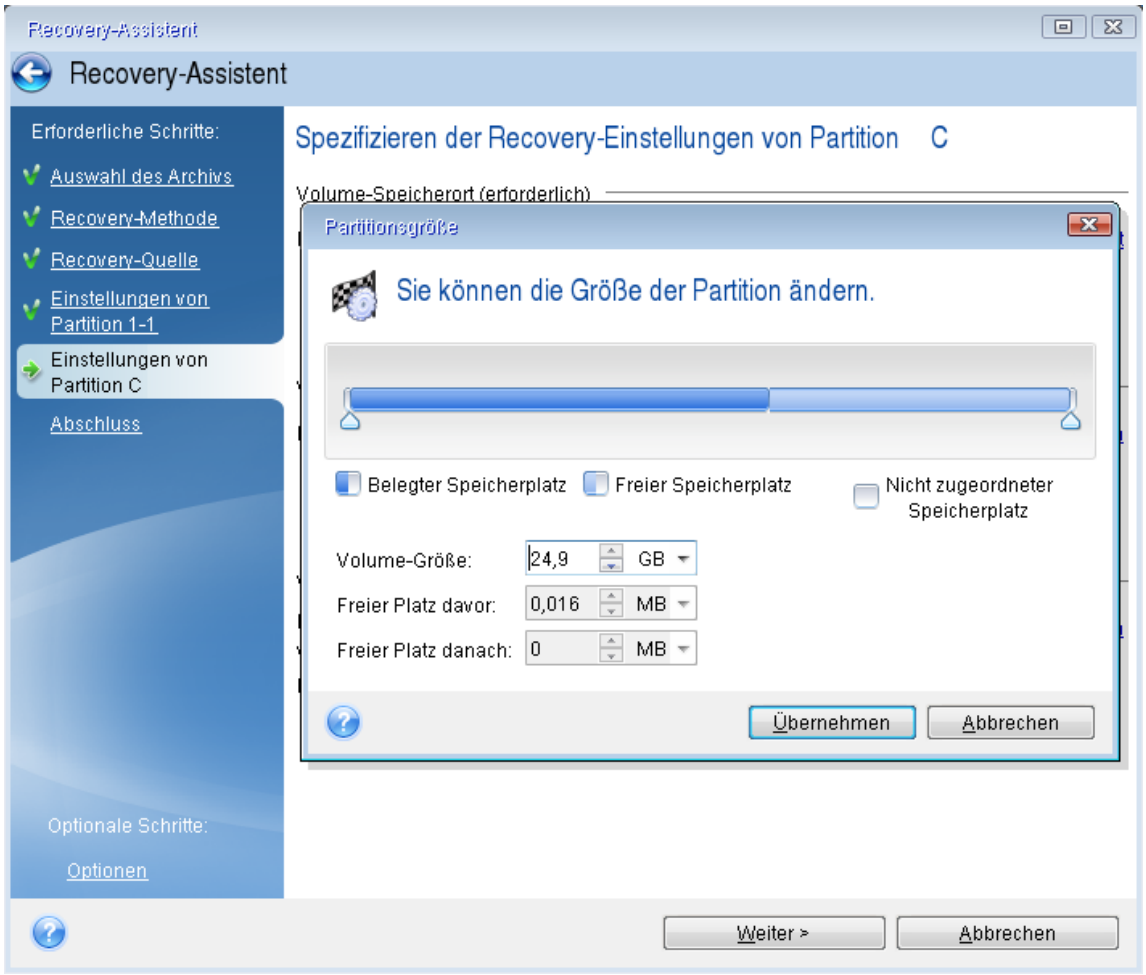

- **Typ** – Überprüfen Sie den Volume-Typ (Partitionstyp) und ändern Sie diesen bei Bedarf. Überprüfen Sie, dass das Volume 'System-reserviert' (sofern vorhanden) als 'Primär' und 'Aktiv' gekennzeichnet ist.
- **Größe** – Klicken Sie im im Bereich 'Volume-Größe' auf **Standard ändern**. Standardmäßig belegt das Volume das komplette neue Laufwerk. Geben Sie im Feld zur Volume-Größe den korrekten Wert ein (Sie können diese Wert im Schritt **Recovery-Quelle** einsehen). Ziehen Sie dann (sofern nötig) dieses Volume an dieselbe Position, die Sie im Fenster 'Backup-Informationen' gesehen haben. Klicken Sie auf **Übernehmen**.




11. Spezifizieren Sie im Schritt **Einstellungen von Volume C** die Einstellungen für das zweite Volume (welches in diesem Fall Ihr System-Volume ist).
    - Klicken Sie auf **Neuer Speicherort** und wählen Sie dann auf dem Ziellaufwerk den 'nicht zugeordneten' Speicherplatz aus, der das Volume aufnehmen soll.




- Ändern Sie (sofern nötig) den Volume-Typ (Partitionstyp). Es muss ein primäres System-Volume sein.
- Spezifizieren Sie die Volume-Größe; als Standard wird die ursprüngliche Größe vorgegeben. Normalerweise gibt es hinter dem Volume keinen freien Speicherplatz, weisen Sie dem zweiten Volume daher den kompletten 'nicht zugeordneten' Speicherplatz des neuen Laufwerks zu. Klicken Sie auf **Übernehmen** und dann auf **Weiter**.




12. Lesen Sie die Zusammenfassung der durchzuführenden Aktionen aufmerksam durch und klicken Sie auf **Fertigstellen**.

## Nach Abschluss der Wiederherstellung

Trennen Sie die Verbindung zu Ihrem alten Laufwerk (sofern vorhanden), bevor Sie den Computer booten. Falls Windows beim Boot-Vorgang sowohl das neue wie auch das alte Laufwerk 'sieht', kann dies dazu führen, dass Windows Probleme beim Booten bekommt. Wenn Sie ein Upgrade des alten Laufwerks auf ein neues mit größerer Kapazität ausführen, trennen Sie das alte Laufwerk, bevor Sie das erste Mal booten.

Entfernen Sie das Boot-Medium und starten Sie den Computer mit Windows. Möglicherweise wird gemeldet, dass neue Hardware (das Laufwerk) gefunden wurde und Windows neu gestartet werden muss. Stellen Sie die ursprüngliche Boot-Reihenfolge wieder her, nachdem Sie sich vergewissert haben, dass das System normal arbeitet.

## Acronis Universal Restore

Wenn Sie Ihr System auf einem Zielcomputer mit abweichender Hardware wiederherstellen, wird dieser möglicherweise (noch) nicht booten können. Grund ist, dass die neue Hardware inkompatibel zu den wichtigsten, im Image enthaltenen Treibern ist. Sie können den neuen Zielcomputer aber

mithilfe von Acronis Universal Restore bootfähig machen. Weitere Details finden Sie im Abschnitt 'Acronis Universal Restore'.

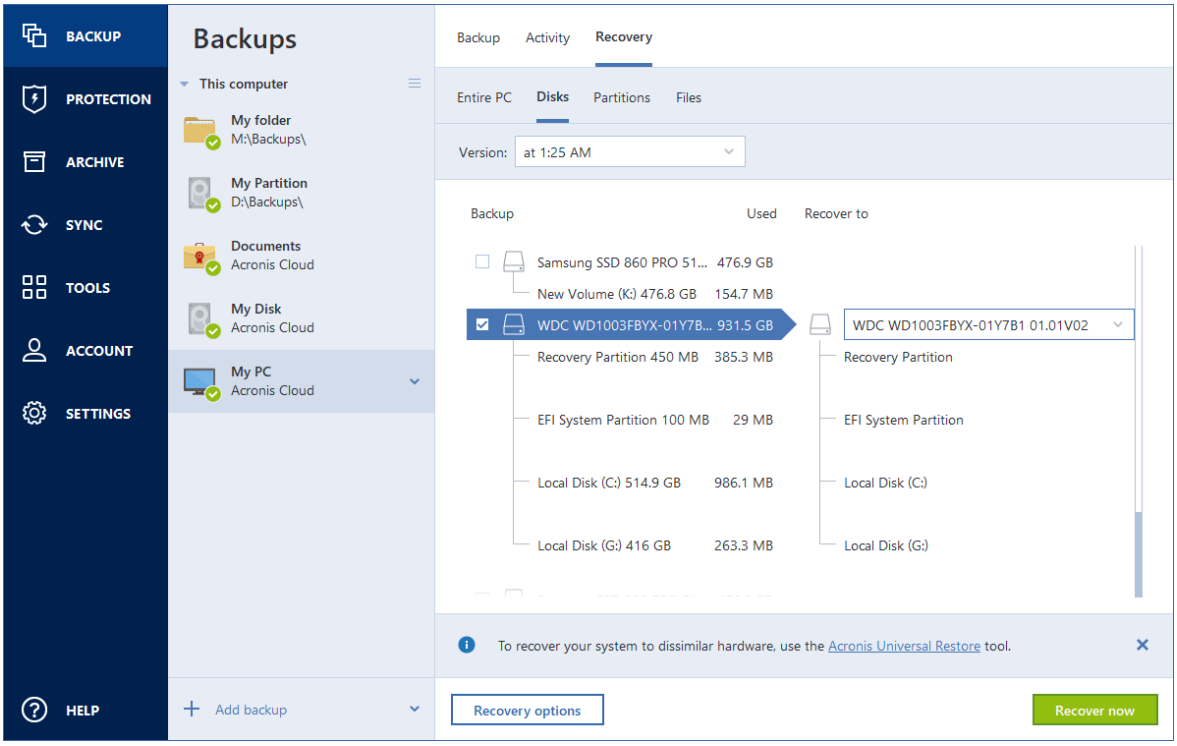
## Volumes und Laufwerke wiederherstellen

Sie können zur Wiederherstellung Ihrer Laufwerke Backups verwenden, die sich auf einem lokalen Storage, einem Netzwerk-Storage oder in der Acronis Cloud befinden.

**Hinweis**
Die Wiederherstellung eines Laufwerks aus der Acronis Cloud kann in Abhängigkeit von Ihrer Internetgeschwindigkeit eine längere Zeit in Anspruch nehmen.

***So können Sie Volumes oder Laufwerke wiederherstellen***

1. Acronis Cyber Protect Home Office starten.
2. Um Ihre Daten aus der Acronis Cloud wiederherstellen zu können, müssen Sie sich an Ihrem Acronis Konto angemeldet haben.
3. Wählen Sie im Bereich **Backup** dasjenige Backup aus, welches die wiederherzustellenden Volumes oder Laufwerke enthält. Öffnen Sie anschließend die Registerkarte **Recovery** und klicken Sie auf **Laufwerke wiederherstellen**.
4. Wählen Sie in der Liste **Backup-Version** die wiederherzustellende Backup-Version anhand des Zeitpunkts ihrer Erstellung aus.




5. Wählen Sie die Registerkarte **Laufwerke**, um Laufwerke wiederherzustellen – oder die Registerkarte **Volumes**, wenn Sie bestimmte Volumes (Partitionen) wiederherstellen wollen. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen.

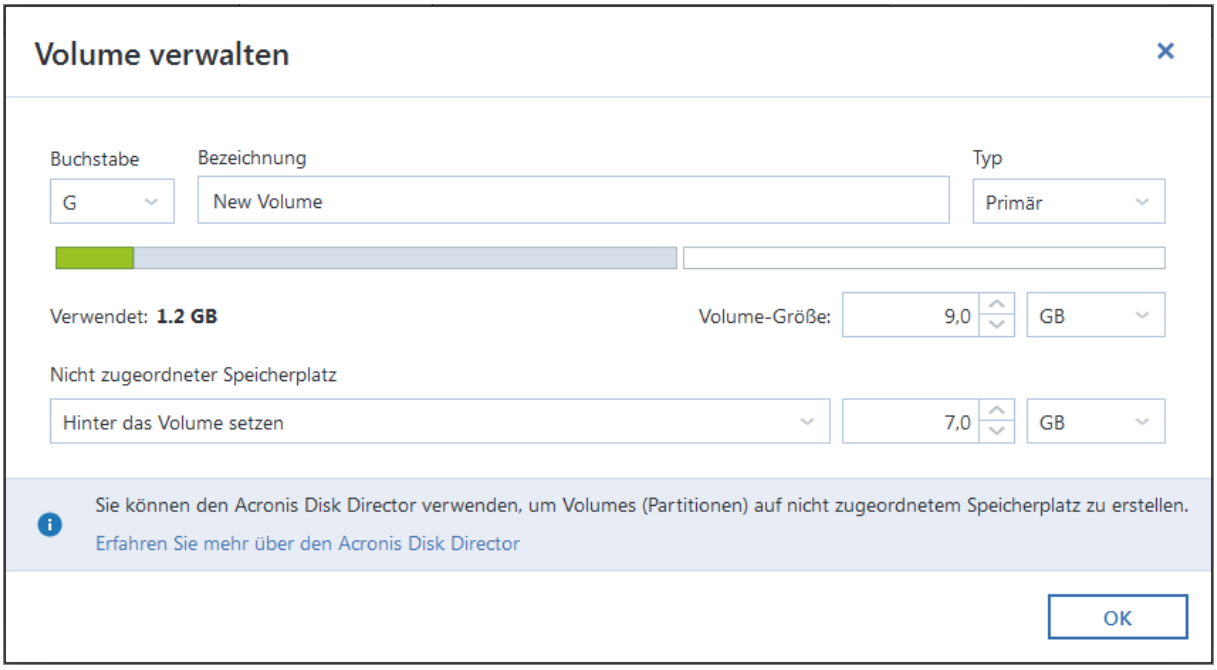
6. Bestimmen Sie im Feld 'Recovery-Ziel' (unterhalb der Volume-Bezeichnung) das Ziel-Volume. Nicht passende Volumes sind dagegen mit einem roten Rahmen gekennzeichnet. Beachten Sie, dass alle Daten auf dem Ziel-Volume verloren gehen, weil sie durch die wiederherzustellenden Daten (mitsamt Dateisystem) ersetzt werden.

   **Hinweis**
   Um das ursprüngliche Volume wiederherstellen zu können, muss mindestens 5% des Volume-Speicherplatzes frei sein. Anderenfalls ist die Schaltfläche **Recovery jetzt** nicht verfügbar.

7. [Optional] Klicken Sie zum Festlegen zusätzlicher Parameter für den Laufwerkswiederherstellungsprozess auf den Befehl **Recovery-Optionen**.
8. Klicken Sie nach Abschluss Ihrer Auswahl auf **Recovery jetzt**, um die Wiederherstellung zu starten.

## Volume-Eigenschaften

Wenn Sie Volumes (Partitionen) auf einem Laufwerk vom Typ 'Basisdatenträger' wiederherstellen, können Sie bestimmte Eigenschaften dieser Volumes ändern. Klicken Sie zum Öffnen des Fensters **Volume-Eigenschaften** neben dem ausgewählten Ziel-Volume auf **Eigenschaften**.




Sie können folgende Volume-Eigenschaften ändern:

- **Laufwerksbuchstabe**
- **Bezeichnung**
- **Typ**
  Sie können das Volume als 'primär', 'primär aktiv' oder 'logisch' festlegen.
- **Größe**

Sie können die Volume-Größe leicht ändern, indem Sie die Begrenzung der grafischen Volume-Darstellung (horizontaler Balken) mit Ihrer Maus verschieben. Um dem Volume direkt eine spezifische Größe zuzuweisen, können Sie den entsprechenden Zahlenwert in das Feld **Volume-Größe** eingeben. Sie können außerdem die Position des nicht zugeordneten Speicherplatzes festlegen – und zwar vor oder hinter dem Volume.

## Unified Extensible Firmware Interface (UEFI)

Sie können mit Acronis Cyber Protect Home Office zudem **BIOS**- zu **UEFI**-Systemen konvertieren.

### Was ist UEFI?

**Unified Extensible Firmware Interface** (UEFI) ist eine Spezifikation, die eine bessere Software-Interoperabilität durch eine Standard-Syntax für Boot- und Laufzeit-Dienste ermöglicht. Weitere Informationen über UEFI finden Sie unter https://www.uefi.org.

Folgende Betriebssysteme unterstützen die UEFI-Technologie:

- Windows 8 (x86) und frühere x86-Editionen von Windows.
- Windows Vista SP1 (x64) spätere x64-Editionen von Windows

### Warum UEFI?

- **Kompatibilität mit BIOS** – UEFI-basierte Systeme können weiterhin BIOS-basierte Betriebssysteme durch ein 'Compatibility Support Module' (CSM) booten.
- **Booten von großen Laufwerken** – UEFI-basierte Systeme unterstützen das GPT-Partitionierungsschema, welches Laufwerksgrößen mit mehr als 2^32 Sektoren erlaubt.
- **CPU-unabhängige Architektur** – UEFI ist für alle Prozessor-Architekturen ähnlich.
- **CPU-unabhängige Treiber** – die UEFI-Spezifikation enthält einen 'EFI Byte Code' (EBC) und ermöglicht die Erstellung von 'EBC-Images' (Treibern), die auf jedem System ausgeführt werden können.
- **Flexible 'Pre-OS'-Umgebung** (Umgebung vor Laden des Betriebssystems) – UEFI-basierte Systeme können von jeder Hardware booten.
- **Modulares Design** – UEFI ermöglicht ein Update einzelner Komponenten ohne Beeinflussung anderer Komponenten.

**Hinweis**
Da UEFI eine neue Technologie ist, wird dessen Verwendung nicht von allen Systemen unterstützt. Wenden Sie sich an Ihren Hardware-Hersteller, um herauszufinden, ob Ihr Computer UEFI unterstützt.

### Wie können Sie UEFI im BIOS aktivieren?

Nachfolgend finden Sie eine Beschreibung für einen typischen Ansatz zur (De)Aktivierung von UEFI im BIOS:

1. Wechseln Sie in das BIOS-Setup-Programm, indem Sie die während der Boot-Meldungen angezeigte Taste drücken. Üblicherweise handelt es sich dabei um die Taste [Entf] oder [F2].
2. Gehen Sie durch die Pfeiltasten in das Menü **Boot Options** (BIOS-Befehle sind bei den meisten Mainboards in Englisch).
3. Gehen Sie zum Element **UEFI Booting** und wählen Sie *Enable* (oder *Disable*, wenn Sie UEFI für Ihr System **Deaktivieren** wollen).
4. Navigieren Sie zum Menüpunkt **Save & Exit Setup** und drücken Sie die **Eingabe-Taste**, damit die Änderungen gespeichert werden und das System neu startet.

Wenn Sie zum Einschalten der UEFI-Option Unterstützung benötigen, kontaktieren Sie bitte Ihren Hardware-Hersteller.

## Wie können Sie ein ursprüngliches System auf ein größeres Festplattenlaufwerk migrieren?

Acronis Cyber Protect Home Office ermöglicht die Migration oder Wiederherstellung eines Systems von einem zuvor erstellten Backup-Archiv auf Festplattenlaufwerke, die größer sind als 2^32 Byte (entspricht 2 TB bei Laufwerken mit der Standardsektorgröße von 512 Byte – oder 16 TB bei Laufwerken mit einer logischen Sektorgröße von 4096 Byte).

Sie können dies unter Verwendung eines Acronis Boot-Mediums tun – oder durch Booten eines UEFI-basierten Betriebssystems, auf dem Acronis Cyber Protect Home Office installiert ist:

***So können Sie ein System mithilfe eines Acronis Boot-Mediums migrieren***

1. Booten Sie Ihr System mit einem Acronis Boot-Medium.
2. Wählen Sie im Boot-Menü **Acronis Cyber Protect Home Office (Vollständige Version)** aus, damit die entsprechende autonome Notfallversion des Produkts gestartet wird.
3. Wechseln Sie zum benötigten Assistenten (**Recovery** oder **Klonen**) und folgen Sie dessen Anweisungen.

***So können Sie ein System unter einem UEFI-basierten Betriebssystem migrieren***

1. Booten Sie ein UEFI-fähiges Windows-Betriebssystem.
2. Führen Sie Acronis Cyber Protect Home Office aus, gehen Sie zur Registerkarte **Backup und Recovery**, klicken Sie in der Symbolleiste auf **Recovery** – und folgen Sie den angezeigten Anweisungen.

## Partitionslayouts

Ein Partitionslayout definiert, wie ein Betriebssystem seine Partitionen (Volumes) auf einer Festplatte (oder ähnlichem Laufwerk) organisiert:

- **MBR (Master Boot Record)** – ein 512 Byte großer Boot-Sektor, der als erster Sektor auf dem entsprechenden Laufwerk liegt und dessen primäre Partitionstabelle enthält.
  MBR ist ein Standard-Partitionierungsschema (auch Partitionslayout genannt) und wird auf den meisten Festplattenlaufwerken verwendet. Wesentliche MBR-Begrenzung ist, dass nur

Laufwerksgrößen bis 2 TB unterstützt werden, wodurch die Nutzung moderner, großer Festplatten unmöglich wird – denn der Anwender erhält keinen Zugriff auf den Speicherplatz oberhalb von 2 TB.

- **GPT (GUID-Partitionstabelle)** – ein neuerer Standard für das Partitionstabellenlayout (auch Partitionsschema genannt) von Festplatten und verwandten Laufwerken.

  GPT ermöglicht Laufwerke/Volumes mit einer Größe bis zu 9,4 ZB (9,4 x 10^21 Byte).

  Die untere Tabelle verdeutlicht, welche Betriebssysteme das Lesen und/oder Booten von GPT-Laufwerken unterstützen:

| | **Betriebssystem kann von GPT-Laufwerken lesen** | **Betriebssystem kann von GPT-Laufwerken booten** |
|---|---|---|
| **Windows XP x32** | NEIN | NEIN |
| **Windows XP x64** | JA | NEIN |
| **Windows Vista x32** | JA | NEIN |
| **Windows Vista x64** | JA | NEIN |
| **Windows Vista x64 SP1 oder später** | JA | JA |
| **Windows 7 x32** | JA | NEIN |
| **Windows 7 x64** | JA | JA |
| **Windows 8 x32** | JA | JA |
| **Windows 8 x64** | JA | JA |
| **Windows 8.1 x32** | JA | JA |
| **Windows 8.1 x64** | JA | JA |
| **Windows 10 x32** | JA | JA |
| **Windows 10 x64** | JA | JA |
| **Windows 11** | JA | JA |

### Tabelle 1: Ziellaufwerk ist größer als 2 TB

Die nachfolgende Tabelle demonstriert die verfügbaren Optionen, wenn Sie ein Quelllaufwerk auf ein großes Laufwerk mit mehr als 2 TB migrieren wollen.

Sofern Ihr Quelllaufwerk vom Typ MBR ist, müssen Sie wählen, ob das Ziellaufwerk ebenfalls MBR beibehalten soll – oder ob Sie es unter Verwendung von Acronis Cyber Protect Home Office zu GPT konvertieren wollen.

Jede Wahl hat, abhängig von den Parametern Ihres Systems, bestimmte Vorteile und Einschränkungen. Sie betreffen hauptsächlich die Bootfähigkeit des Ziellaufwerks sowie die Möglichkeit, auf großen Laufwerken den kompletten Speicherplatz nutzen zu können.

| | **Mein System wird per BIOS gebootet (Windows oder Acronis Boot-Medium)** | **Mein System wird per UEFI gebootet (Windows oder Acronis Boot-Medium)** |
|---|---|---|
| **Mein Quelllaufwerk ist MBR und mein Betriebssystem unterstützt kein UEFI** | Das Partitionierungsschema verbleibt nach dem Klonen vom Typ MBR, der Acronis-Bus-Treiber wird auf dem geklonten Betriebssystem installiert. Sie können zudem den Speicherplatz oberhalb von 2 TB nicht verwenden, da MBR keine Festplatten mit mehr als 2 TB unterstützt. Um den kompletten Speicherplatz nutzen zu können, müssen Sie das Partitionierungsschema zu GPT ändern – oder Acronis Cyber Protect Home Office nach Abschluss der Aktion neu starten und den Acronis Extended Capacity Manager verwenden, um den Speicherplatz oberhalb von 2 TB für das Werkzeug 'Neues Laufwerk hinzufügen' sichtbar zu machen. | *Sie können eine der benötigten Migrationsmethoden wählen:*<br>• **Partition ohne Änderungen kopieren**<br>Als Partitionierungsschema wird weiterhin MBR verwendet, jedoch kann das Betriebssystem nach Abschluss der Aktion nicht per UEFI booten. Der Acronis-Bus-Treiber wird auf dem geklonten Betriebssystem installiert. Sie können zudem den Speicherplatz oberhalb von 2 TB nicht verwenden, da MBR keine Festplatten mit mehr als 2 TB unterstützt. Um den kompletten Speicherplatz nutzen zu können, müssen Sie das Partitionierungsschema zu GPT ändern – oder Acronis Cyber Protect Home Office nach Abschluss der Aktion neu starten und den Acronis Extended Capacity Manager verwenden, um den Speicherplatz oberhalb von 2 TB für das Werkzeug 'Neues Laufwerk hinzufügen' sichtbar zu machen.<br>• **Partitionierungsschema zu GPT konvertieren**<br>Das Ziel-Volume (Ziel-Partition) wird zum GPT-Schema konvertiert. Es ist nur eine Verwendung als 'Nicht-System'-Laufwerk möglich, da das Betriebssystem kein UEFI unterstützt. Der komplette Speicherplatz ist verfügbar. |
| **Mein Quelllaufwerk ist MBR und mein Betriebssystem unterstützt UEFI** | Das Partitionierungsschema verbleibt nach der Migration vom Typ MBR. Der Acronis-Bus-Treiber wird auf dem geklonten Betriebssystem installiert. Sie können den Speicherplatz oberhalb von 2 TB nicht verwenden, | Das Partitionierungsschema Ihres Ziellaufwerks wird automatisch zu GPT konvertiert. Dieses Laufwerk kann auch zum Booten per UEFI verwendet werden. Außerdem ist der komplette Speicherplatz verfügbar. |

| | | |
|---|---|---|
| | da MBR keine Festplatten mit mehr als 2 TB unterstützt. Um den kompletten Speicherplatz nutzen zu können, müssen Sie das Partitionierungsschema zu GPT ändern – oder Acronis Cyber Protect Home Office nach Abschluss der Aktion neu starten und den Acronis Extended Capacity Manager verwenden, um den Speicherplatz oberhalb von 2 TB für das Werkzeug 'Neues Laufwerk hinzufügen' sichtbar zu machen. | |
| **Mein Quelllaufwerk ist MBR und mein Betriebssystem ist 'Nicht-Windows' oder 'Kein Betriebssystem'** | *Sie können eine der benötigten Migrationsmethoden wählen:*<br>• **Partition ohne Änderungen kopieren**<br>Als Partitionierungsschema wird weiterhin MBR verwendet, aber Sie können den Speicherplatz oberhalb von 2 TB nicht verwenden, da MBR keine Festplatten mit mehr als 2 TB unterstützt. Um den kompletten Speicherplatz nutzen zu können, müssen Sie das Partitionierungsschema zu GPT ändern – oder Acronis Cyber Protect Home Office nach Abschluss der Aktion neu starten und den Acronis Extended Capacity Manager verwenden, um den Speicherplatz oberhalb von 2 TB für das Werkzeug 'Neues Laufwerk hinzufügen' sichtbar zu machen.<br>• **Partitionierungsschema zu GPT konvertieren**<br>Das Partitionierungsschema wird mit Abschluss der Aktion zu GPT konvertiert. Das Ziellaufwerk kann nicht zum Booten verwendet werden, da kein Windows-Betriebssystem auf Ihrem Quelllaufwerk installiert ist. Der komplette Speicherplatz ist verfügbar. | *Sie können eine der benötigten Migrationsmethoden wählen:*<br>• **Partition ohne Änderungen kopieren**<br>Als Partitionierungsschema wird weiterhin MBR verwendet, aber Sie können den Speicherplatz oberhalb von 2 TB nicht verwenden, da MBR keine Festplatten mit mehr als 2 TB unterstützt. Um den kompletten Speicherplatz nutzen zu können, müssen Sie das Partitionierungsschema zu GPT ändern – oder Acronis Cyber Protect Home Office nach Abschluss der Aktion neu starten und den Acronis Extended Capacity Manager verwenden, um den Speicherplatz oberhalb von 2 TB für das Werkzeug 'Neues Laufwerk hinzufügen' sichtbar zu machen.<br>• **Partitionierungsschema zu GPT konvertieren**<br>Das Ziel-Volume (Ziel-Partition) wird zum GPT-Schema konvertiert. Das Ziellaufwerk kann nicht zum Booten verwendet werden, da kein Windows-Betriebssystem auf Ihrem Quelllaufwerk installiert ist. Außerdem ist der komplette Speicherplatz verfügbar. |

| | | |
|---|---|---|
| **Mein Quelllaufwerk ist GPT und mein Betriebssystem unterstützt UEFI** | Das Partitionierungsschema verbleibt nach der Migration vom Typ GPT. Nach Abschluss der Aktion kann das System nicht mehr per BIOS booten, da Ihr Betriebssystem das Booten von GPT per BIOS nicht unterstützt. Der komplette Speicherplatz ist verfügbar. | Die Aktion hat weder Einfluss auf das Partitionierungsschema noch die Bootfähigkeit des Laufwerks: als Partitionierungsschema wird weiterhin GPT verwendet, das Ziellaufwerk ist per UEFI bootfähig. Der komplette Speicherplatz ist verfügbar. |
| **Mein Quelllaufwerk ist GPT und mein Betriebssystem ist 'Nicht-Windows' oder 'Kein Betriebssystem'** | Die Aktion hat weder Einfluss auf das Partitionierungsschema noch die Bootfähigkeit des Laufwerks: als Partitionierungsschema wird weiterhin GPT verwendet, das Ziellaufwerk ist nicht bootfähig. Der komplette Speicherplatz ist verfügbar. | Die Aktion hat weder Einfluss auf das Partitionierungsschema noch die Bootfähigkeit des Laufwerks: als Partitionierungsschema wird weiterhin GPT verwendet, das Ziellaufwerk ist nicht per UEFI bootfähig. Der komplette Speicherplatz ist verfügbar. |

### Tabelle 2: Ziellaufwerk ist kleiner als 2 TB

Die nachfolgende Tabelle demonstriert die verfügbare Option, wenn Sie ein Quelllaufwerk auf ein Laufwerk mit weniger als 2 TB migrieren wollen.

Sofern Ihr Quelllaufwerk vom Typ MBR ist, müssen Sie wählen, ob das Ziellaufwerk ebenfalls MBR beibehalten soll – oder ob Sie es unter Verwendung von Acronis Cyber Protect Home Office zu GPT konvertieren wollen.

Jede Wahl hat, abhängig von den Parametern Ihres Systems, bestimmte Vorteile und Einschränkungen. Dies betrifft hauptsächlich die Bootfähigkeit des Ziellaufwerks.

| | **Mein System wird per BIOS gebootet (Windows oder Acronis Boot-Medium)** | **Mein System wird per UEFI gebootet (Windows oder Acronis Boot-Medium)** |
|---|---|---|
| **Mein Quelllaufwerk ist MBR und mein Betriebssystem unterstützt kein UEFI** | Die Aktion hat weder Einfluss auf das Partitionierungsschema noch die Bootfähigkeit des Laufwerks: das Partitionierungsschema verbleibt vom Typ MBR, das Ziellaufwerk ist per BIOS bootfähig. Der komplette Speicherplatz ist verfügbar. | Das Partitionierungsschema verbleibt nach Abschluss der Aktion vom Typ MBR, das Betriebssystem kann jedoch nicht per UEFI booten, da es dieses nicht unterstützt. |
| **Mein Quelllaufwerk ist MBR und mein Betriebssystem unterstützt UEFI** | Die Aktion hat weder Einfluss auf das Partitionierungsschema noch die Bootfähigkeit des Laufwerks: das Partitionierungsschema verbleibt vom Typ MBR, das Ziellaufwerk ist per BIOS bootfähig. Der komplette Speicherplatz ist verfügbar. | Das Ziel-Volume wird zum GPT-Schema konvertiert, wodurch das Ziellaufwerk per UEFI bootfähig wird. Der komplette Speicherplatz ist verfügbar. |
| **Mein Quelllaufwerk ist** | *Sie können eine der benötigten Migrationsmethoden wählen:* | *Sie können eine der benötigten Migrationsmethoden wählen:* |

| | | |
|---|---|---|
| **MBR und mein Betriebssystem ist 'Nicht-Windows' oder 'Kein Betriebssystem'** | • **Partition ohne Änderungen kopieren**<br>Das Partitionierungsschema verbleibt vom Typ MBR. Das Ziellaufwerk wird nicht bootfähig sein, da in Ihrem System kein Windows-Betriebssystem erkannt wird.<br>• **Partitionierungsschema zu GPT konvertieren**<br>Das Ziellaufwerk wird zum GPT-Schema konvertiert und als 'Nicht-System'-Laufwerk verwendet, da Ihr Betriebssystem das Booten von GPT-Laufwerken per BIOS nicht unterstützt. | • **Partition ohne Änderungen kopieren**<br>Das Partitionierungsschema verbleibt vom Typ MBR. Das Ziellaufwerk wird nicht bootfähig sein, da in Ihrem System kein Windows-Betriebssystem erkannt wird.<br>• **Partitionierungsschema zu GPT konvertieren**<br>Das Ziel-Volume wird zum GPT-Schema konvertiert und als 'Nicht-System'-Laufwerk verwendet, da in Ihrem System kein Windows-Betriebssystem erkannt wird. |
| **Mein Quelllaufwerk ist GPT und mein Betriebssystem unterstützt UEFI** | Das Partitionierungsschema verbleibt nach Abschluss der Aktion vom Typ GPT, das System kann nicht per BIOS booten, da Ihr Betriebssystem das Booten von GPT per BIOS nicht unterstützt. | Das Partitionierungsschema verbleibt nach Abschluss der Aktion vom Typ GPT, das Betriebssystem wird per UEFI bootfähig sein. |
| **Mein Quelllaufwerk ist GPT und mein Betriebssystem ist 'Nicht-Windows' oder 'Kein Betriebssystem'** | Das Partitionierungsschema verbleibt nach Abschluss der Aktion vom Typ GPT, das System kann nicht per BIOS booten, da Ihr Betriebssystem das Booten von GPT per BIOS nicht unterstützt. | Das Partitionierungsschema verbleibt nach Abschluss der Aktion vom Typ GPT, das System wird nicht mehr booten, da in Ihrem System kein Windows-Betriebssystem erkannt wird. |

## Migrationsmethode

Acronis Cyber Protect Home Office ermöglicht Ihnen, nach Abschluss einer Wiederherstellungsaktion für ein Ziellaufwerk das Partitionierungsschema zu wählen:

- **MBR (Master Boot Record)** – ein 512 Byte großer Boot-Sektor, der als erster Sektor auf dem entsprechenden Laufwerk liegt und dessen primäre Partitionstabelle enthält.
- **GPT (GUID-Partitionstabelle)** – ein Standard für das Partitionstabellenlayout (auch Partitionierungsschema genannt) von Festplatten und verwandten Laufwerken. GPT ermöglicht Laufwerke/Volumes mit einer Größe bis zu 9,4 ZB (9,4 x 10^21 Byte).

Durch Verwendung dieses Assistenten können Sie während einer Recovery-Aktion das Partitionierungsschema konvertieren oder wie vorliegend belassen.

- **Partitionen ohne Änderungen kopieren** – wählen Sie diese Option, um Ihr System wie vorliegend (also ohne Änderung des Partitionierungsschemas) zu migrieren. Beachten Sie, dass in diesem Fall der Speicherplatz oberhalb von 2 TB nicht verfügbar ist. Sie können den Acronis

Extended Capacity Manager verwenden, um den Speicherplatz oberhalb von 2 TB zuzuweisen.

- **Volumes kopieren und ein Laufwerk als 'Nicht-System' (GPT-Schema) verwenden** – wählen Sie diese Option, um Ihre Partition (Volume) zum GPT-Layout zu konvertieren.

Sie können mit Acronis Cyber Protect Home Office zudem **BIOS**- zu **UEFI**-Systemen konvertieren.

### Per BIOS gebootetes System, MBR, UEFI nicht unterstützt

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

#### Aktuell enthält Ihr System:

**System**: Per BIOS gebootet

**Quell-Partitionierungsschema**: MBR

**Betriebssystem auf dem Quelllaufwerk**: Windows, Booten per UEFI wird nicht unterstützt

**Größe des Ziellaufwerks**: weniger als 2 TB

#### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: Per BIOS gebootet

**Partitionierungsschema**: MBR

**Betriebssystem**: Windows, Booten per UEFI wird nicht unterstützt

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

### Per BIOS gebootetes System, MBR, UEFI unterstützt

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

#### Aktuell enthält Ihr System:

**System**: Per BIOS gebootet

**Quell-Partitionierungsschema**: MBR

**Betriebssystem auf dem Quelllaufwerk**: Windows, Booten per UEFI wird unterstützt

**Größe des Ziellaufwerks**: weniger als 2 TB

#### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: Per BIOS gebootet

**Partitionierungsschema**: MBR

**Betriebssystem**: Windows, Booten per UEFI wird unterstützt

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per BIOS gebootetes System, MBR, 'Nicht-Windows'

Acronis Cyber Protect Home Office ermöglicht Ihnen, nach Abschluss einer Aktion das Partitionslayout für ein Ziellaufwerk zu bestimmen.

### Aktuell enthält Ihr System:

**System**: Per BIOS gebootet

**Quell-Partitionierungsschema**: MBR

**Betriebssystem auf dem Quelllaufwerk**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Größe des Ziellaufwerks**: weniger als 2 TB

### Mit diesen Systemparametern können Sie Folgendes wählen:

1. **Volumes ohne Änderungen kopieren**

Sie können das MBR-Partitionierungsschema auf dem Ziellaufwerk belassen.

**Ziellaufwerk nach Migration:**

**System**: Per BIOS gebootet

**Partitionierungsschema**: MBR

**Betriebssystem**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

2. **Volumes kopieren und ein Laufwerk als 'Nicht-System' (GPT-Schema) verwenden**

Sie können das Partitionierungsschema zu GPT konvertieren.

**Ziellaufwerk nach Migration:**

**System**: nicht bootfähig per BIOS

**Partitionierungsschema**: GPT

**Betriebssystem**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

**Warnung!**
Das Ziellaufwerk kann nach der Migration nur als 'Nicht-System'-Laufwerk genutzt werden. Diese Option ist nicht verfügbar, falls Acronis Cyber Protect Home Office unter Windows XP x86 (32-Bit) als Betriebssystem ausgeführt wird.

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per BIOS gebootetes System, GPT, UEFI unterstützt

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

### Aktuell enthält Ihr System:

**System**: Per BIOS gebootet

**Quell-Partitionierungsschema**: GPT

**Betriebssystem auf dem Quelllaufwerk**: Windows, Booten per UEFI wird unterstützt

### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: nicht bootfähig per BIOS

**Partitionierungsschema**: GPT

**Betriebssystem**: Windows, Booten per UEFI wird unterstützt

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

---

**Warnung!**
Das Betriebssystem kann nach der Migration nicht mehr per BIOS vom Ziellaufwerk booten. Wenn Sie nach der Migration vom Ziellaufwerk booten wollen, müssen Sie in Ihrem System das Booten per UEFI aktivieren (siehe den Abschnitt zu 'Unified Extensible Firmware Interface'). Starten Sie die Aktion anschließend neu.

---

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per BIOS gebootetes System, GPT, 'Nicht-Windows'

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

### Aktuell enthält Ihr System:

**System**: Per BIOS gebootet

**Quell-Partitionierungsschema**: GPT

**Betriebssystem auf dem Quelllaufwerk**: 'Nicht-Windows' oder 'Kein Betriebssystem'

### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: Per BIOS gebootet

**Partitionierungsschema**: GPT

**Betriebssystem**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per UEFI gebootetes System, MBR, UEFI nicht unterstützt

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

### Aktuell enthält Ihr System:

**System**: Per UEFI gebootet

**Quell-Partitionierungsschema**: MBR

**Betriebssystem auf dem Quelllaufwerk**: Windows, Booten per UEFI wird nicht unterstützt

**Größe des Ziellaufwerks**: weniger als 2 TB

### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: nicht bootfähig per UEFI

**Partitionierungsschema**: MBR

**Betriebssystem**: Windows, Booten per UEFI wird nicht unterstützt

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

**Warnung!**
Das Betriebssystem kann möglicherweise nicht per UEFI vom Ziellaufwerk booten.

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per UEFI gebootetes System, MBR, UEFI wird unterstützt

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

### Aktuell enthält Ihr System:

**System**: Per UEFI gebootet

**Quell-Partitionierungsschema**: MBR

**Betriebssystem auf dem Quelllaufwerk**: Windows, Booten per UEFI wird unterstützt

### Falls Sie das System auf das gewählte Laufwerk migrieren:

Das Partitionierungsschema des Ziellaufwerks wird nach der Migration zu GPT konvertiert und Sie können dann von diesem booten.

**Ziellaufwerk nach Migration:**

**System**: Per UEFI gebootet

**Partitionierungsschema**: GPT

**Betriebssystem**: Windows, Booten per UEFI wird unterstützt

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per UEFI gebootetes System, MBR, 'Nicht-Windows'

Acronis Cyber Protect Home Office ermöglicht Ihnen, nach Abschluss einer Aktion das Partitionslayout für ein Ziellaufwerk zu bestimmen.

### Aktuell enthält Ihr System:

**System**: Per UEFI gebootet

**Quell-Partitionierungsschema**: MBR

**Betriebssystem auf dem Quelllaufwerk**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Größe des Ziellaufwerks**: weniger als 2 TB

### Mit diesen Systemparametern können Sie Folgendes wählen:

1. **Volumes ohne Änderungen kopieren**

Sie können das MBR-Partitionierungsschema auf dem Ziellaufwerk belassen.

**Ziellaufwerk nach Migration:**

**System**: Per UEFI gebootet

**Partitionierungsschema**: MBR

**Betriebssystem**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

2. **Volumes kopieren und ein Laufwerk als 'Nicht-System' (GPT-Schema) verwenden**

Sie können das Partitionierungsschema zu GPT konvertieren.

**Ziellaufwerk nach Migration:**

**System**: nicht bootfähig per UEFI

**Partitionierungsschema**: GPT

**Betriebssystem**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

**Warnung!**
Das Ziellaufwerk kann nach der Migration nur als 'Nicht-System'-Laufwerk genutzt werden.

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per UEFI gebootetes System, GPT, UEFI wird unterstützt

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

### Aktuell enthält Ihr System:

**System**: Per UEFI gebootet

**Quell-Partitionierungsschema**: GPT

**Betriebssystem:** Windows, Booten per UEFI wird unterstützt

### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: Per UEFI gebootet

**Partitionierungsschema**: GPT

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

### Per UEFI gebootetes System, GPT, 'Nicht-Windows'

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

#### Aktuell enthält Ihr System:

**System**: Per UEFI gebootet

**Quell-Partitionierungsschema**: GPT

**Betriebssystem**: 'Nicht-Windows' oder 'Kein Betriebssystem'

#### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: Per UEFI gebootet

**Partitionierungsschema**: GPT

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Recovery von Laufwerken und Volumes vom Typ 'Dynamisch' oder 'GPT'

### Recovery von dynamischen Volumes

Sie können bei der Wiederherstellung dynamischer Volumes auf lokale Laufwerke folgende Speicherorte verwenden:

- **Dynamisches Volume.**

  **Hinweis**
  Bei der Wiederherstellung auf dynamische Datenträgern wird eine manuelle Größenanpassung der dynamischen Volumes nicht unterstützt. Wenn es für Sie notwendig ist, ein dynamisches Volumes während der Wiederherstellung in der Größe anzupassen, dann sollten Sie es zu einem Basis-Laufwerk wiederherstellen.

  - **Den ursprünglichen Speicherort (zum selben dynamischen Volume).**
    Der Typ des Ziel-Volumes ändert sich nicht.
  - **Einen anderen dynamischen Datenträger oder anderes Volume.**
    Der Typ des Ziel-Volumes ändert sich nicht. Wenn beispielsweise ein dynamisches Stripeset-Volume über ein dynamisches Volume vom Typ 'Übergreifend' wiederhergestellt wird, behält das Ziel-Volume den Typ 'Übergreifend' bei.
  - **Nicht zugeordneter Speicherplatz einer dynamischen Gruppe.**
    Der Typ des wiederhergestellten Volumes bleibt derselbe wie der im Backup.

- **Ein Volume oder Laufwerk vom Typ 'Basis'.**
  Das Ziel-Volume behält den Typ 'Basis' bei.
- **Fabrikneue Hardware (Bare Metal Recovery).**
  Bei der Wiederherstellung dynamischer Volumes auf fabrikneue Hardware (Bare Metal Recovery - entspricht einem neuen, unformatierten Laufwerk) erhalten die wiederhergestellten Volumes den Typ 'Basis'. Wenn Sie wollen, dass die wiederhergestellten Datenträger bzw. Laufwerke den Typ 'Dynamisch' beibehalten, dann sollten die Ziellaufwerke vor der Wiederherstellung so vorbereitet werden (partitioniert und formatiert), dass sie vom Typ 'Dynamisch' sind. Sie können dazu die Tools von Drittherstellern verwenden, beispielsweise die in Windows integrierte Datenträgerverwaltung.

## Volumes und Laufwerke vom Typ 'Basis' wiederherstellen

- Wenn ein Basis-Volume auf 'nicht zugeordnetem' Speicherplatz einer dynamischen Gruppe wiederhergestellt wird, dann wird das wiederhergestellte Volume 'Dynamisch'.
- Wenn ein Basis-Laufwerk auf einem dynamischen Datenträger einer aus zwei Laufwerken bestehenden dynamischen Gruppe wiederhergestellt wird, dann behält das wiederhergestellte Laufwerk den Typ 'Basis'. Der als Wiederherstellungsziel dienende dynamische Datenträger erhält den Status 'fehlend' und das dynamische Volume (übergreifend oder Stripeset) auf dem zweiten Laufwerk erhält den Status 'fehlgeschlagen'.

## Das Partitionierungsschema nach der Wiederherstellung

Das Partitionierungsschema des Ziellaufwerkes hängt davon ab, ob Ihr Computer UEFI unterstützt – und davon, ob Ihr System per BIOS oder per UEFI gebootet wird. Vergleichen Sie die nachfolgende Tabelle:

| | **Mein System wird per BIOS gebootet (Windows oder Acronis Boot-Medium)** | **Mein System wird per UEFI gebootet (Windows oder Acronis Boot-Medium)** |
|---|---|---|
| **Mein Quelllaufwerk ist MBR und mein Betriebssystem unterstützt kein UEFI** | Die Aktion hat weder Einfluss auf das Partitionierungsschema noch die Bootfähigkeit des Laufwerks: das Partitionierungsschema verbleibt vom Typ MBR, das Ziellaufwerk ist per BIOS bootfähig. | Das Partitionierungsschema wird nach Abschluss der Aktion in das GPT-Schema konvertiert. Das Betriebssystem kann jedoch nicht per UEFI booten, da es dieses nicht unterstützt. |
| **Mein Quelllaufwerk ist MBR und mein Betriebssystem unterstützt UEFI** | Die Aktion hat weder Einfluss auf das Partitionierungsschema noch die Bootfähigkeit des Laufwerks: das Partitionierungsschema verbleibt vom Typ MBR, das Ziellaufwerk ist per BIOS bootfähig. | Das Ziel-Volume wird zum GPT-Schema konvertiert, wodurch das Ziellaufwerk per UEFI bootfähig wird. Siehe 'Beispiel für die Wiederherstellung auf ein UEFI-System'. |
| **Mein** | Das Partitionierungsschema verbleibt | Das Partitionierungsschema verbleibt |

| | Mein System wird per BIOS gebootet (Windows oder Acronis Boot-Medium) | Mein System wird per UEFI gebootet (Windows oder Acronis Boot-Medium) |
|---|---|---|
| **Quelllaufwerk ist GPT und mein Betriebssystem unterstützt UEFI** | nach Abschluss der Aktion vom Typ GPT, das System kann nicht per BIOS booten, da Ihr Betriebssystem das Booten von GPT per BIOS nicht unterstützt. | nach Abschluss der Aktion vom Typ GPT, das Betriebssystem wird per UEFI bootfähig sein. |

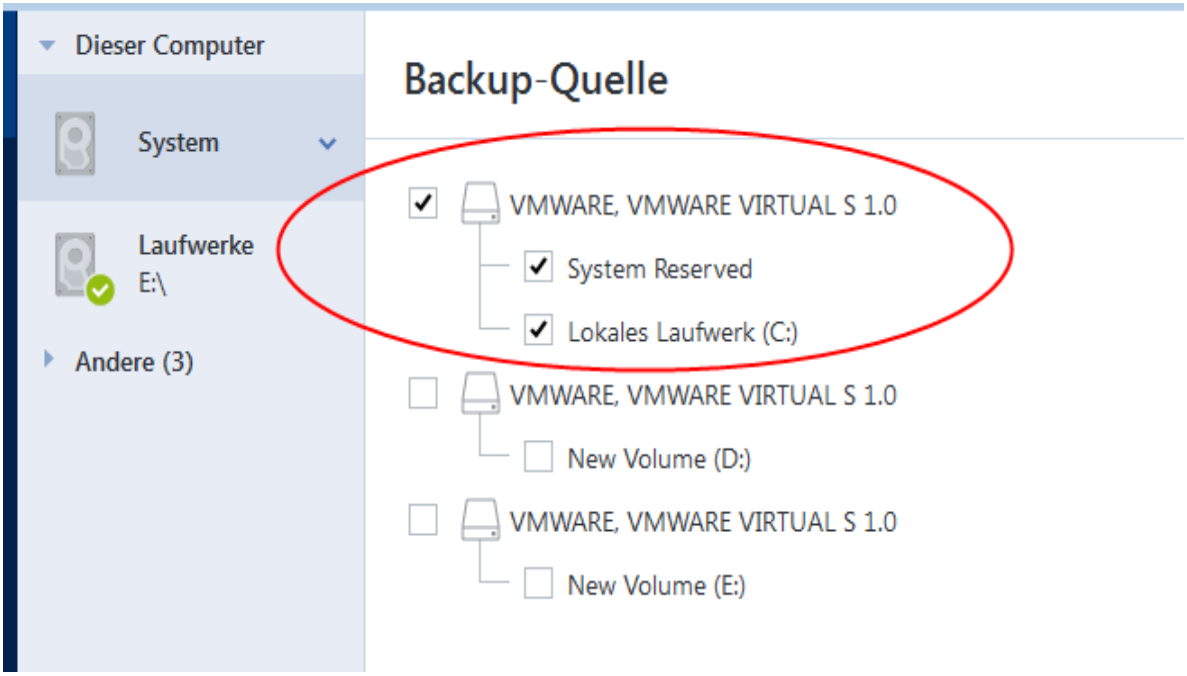
## Beispiel für eine Wiederherstellung auf UEFI-Systemen

Dies ist ein Beispiel, wie Sie ein System unter folgenden Bedingungen (von einem anderen System) übertragen können:

- Das Quelllaufwerk hat den Typ 'MBR' und das Betriebssystem unterstützt UEFI.
- Das Zielsystem wird per UEFI gebootet.
- Das alte und neue Laufwerk arbeiten im selben 'Controller-Modus' (beispielsweise 'IDE' oder 'AHCI').

Überprüfen Sie vor Beginn der Prozedur, dass Sie Folgendes haben:

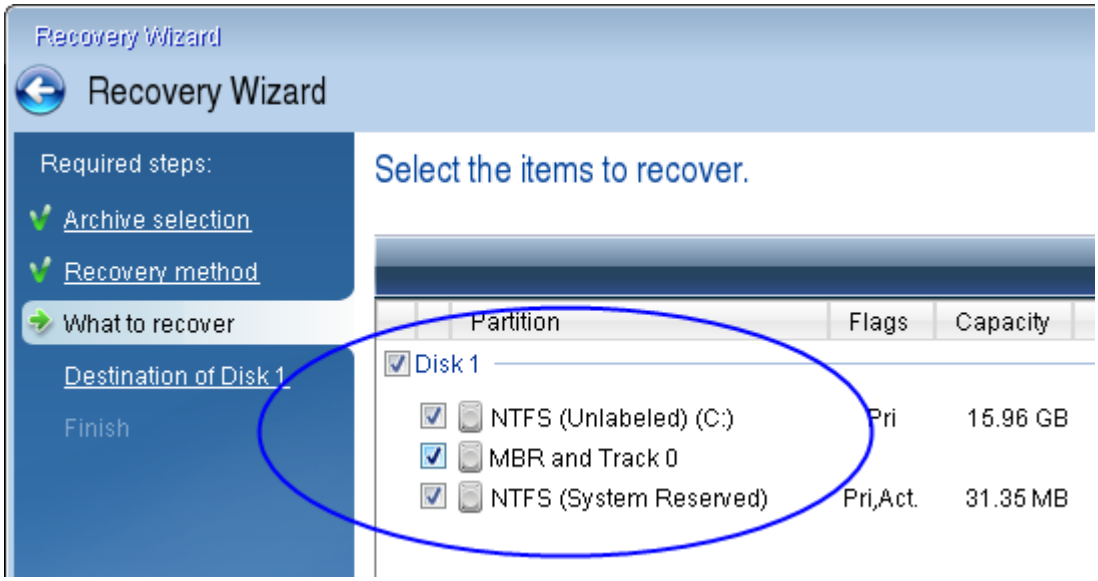
- **Acronis Boot-Medium.**
  Weitere Informationen finden Sie im Abschnitt 'Ein Acronis Boot-Medium erstellen'.
- **Backup Ihres Systemlaufwerkes, welches im 'Laufwerk-Modus' erstellt wurde.**
  Wechseln Sie zur Erstellung dieses Backups in den 'Laufwerk-Modus' – und wählen Sie dann das Festplattenlaufwerk aus, welches Ihr System-Volume (auch System-Partition genannt) enthält.
  Weitere Informationen finden Sie im Abschnitt 'Backup von Laufwerken und Volumes'.



***So können Sie Ihr System von einem MBR-Laufwerk auf einen per UEFI gebooteten Computer übertragen***

1. Starten Sie den Computer mit dem Acronis Boot-Medium im UEFI-Modus und wählen Sie den Eintrag 'Acronis Cyber Protect Home Office'.
2. Starten Sie den **Recovery-Assistenten** und befolgen Sie die im Abschnitt 'Wiederherstellung Ihres Systems' beschriebenen Anweisungen.
3. Aktivieren Sie im Schritt **Recovery-Quelle** das Kontrollkästchen neben dem Laufwerksnamen, um das komplette Systemlaufwerk auszuwählen.

   Im unteren Bespiel müssen Sie das Kontrollkästchen **Laufwerk 1** aktivieren:




4. Klicken Sie im Schritt **Abschluss** auf den Befehl **Fertigstellen**.

Das Ziellaufwerk wird nach Abschluss der Aktion in das GPT-Schema konvertiert sein, sodass es per UEFI gebootet werden kann.

Überprüfen Sie daher nach der Wiederherstellung, ob Ihr Computer auch im UEFI-Modus bootet. Möglicherweise müssen Sie den Boot-Modus Ihres Systemlaufwerkes in der Benutzeroberfläche des UEFI-Boot-Managers ändern.

## Boot-Reihenfolge im BIOS oder UEFI-BIOS arrangieren

Um Ihren Computer mit einem Acronis Boot-Medium starten zu können, müssen Sie die Boot-Reihenfolge so konfigurieren, dass das Medium das primäre Boot-Gerät ist. Diese Boot-Reihenfolge wird – abhängig von Firmware-Schnittstelle Ihres Computers – entweder im BIOS (älterer Computer) oder UEFI-BIOS (neuere Computer) festgelegt. Die Vorgehensweise ist in beiden Fällen quasi identisch:

***So können Sie den Computer mit einem Acronis Boot-Medium starten***

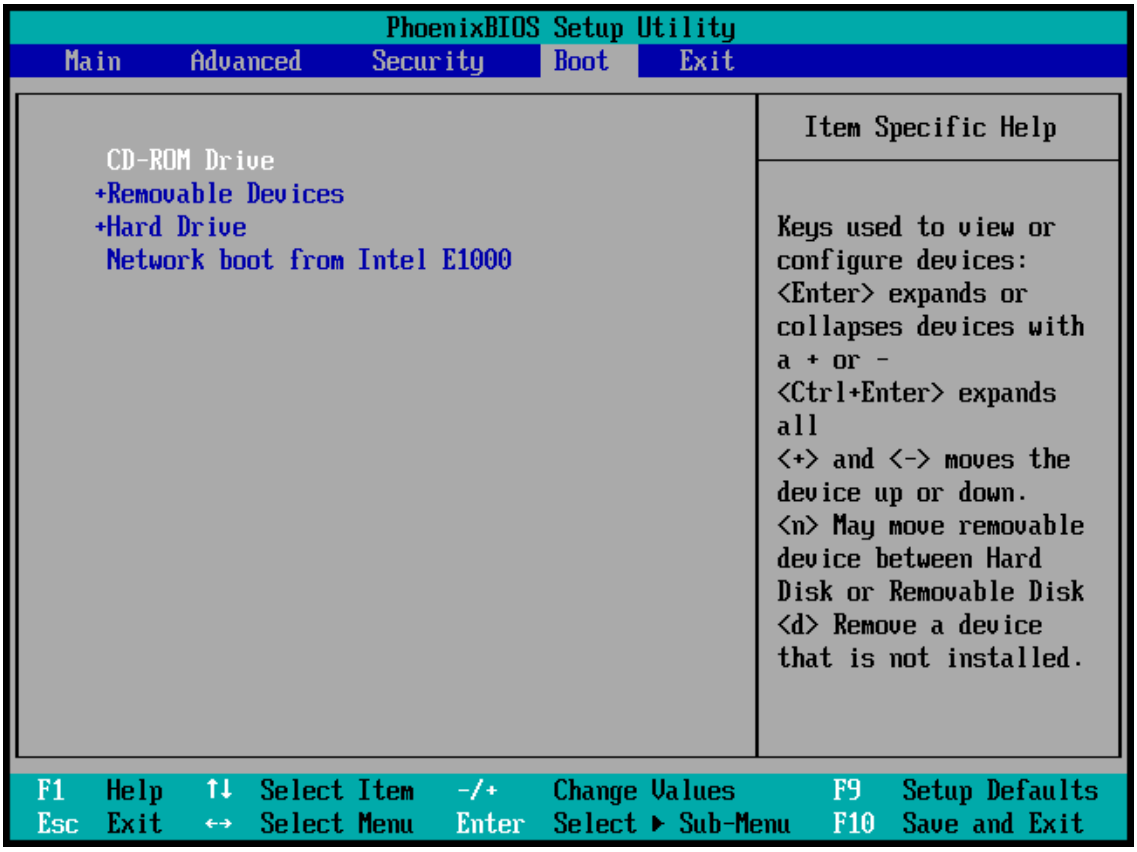
1. Sollten Sie einen USB-Stick oder ein externes Lafuwerk als Boot-Medium verwenden, dann stecken Sie diesen in einen entsprechenden USB-Anschluss.

2. Schalten Sie Ihren Computer ein. Ihnen wird während der sogenannten POST-Routine (Power-On Self Test) eine Tastenkombination angezeigt, die Sie drücken müssen, um das BIOS oder UEFI-BIOS aufzurufen.
3. Geben Sie diese Tastenkombination ein (beispielsweise **Entf, F2, Strg+Alt+Esc, Strg+Esc**). Die Benutzeroberfläche (englisch auch 'Setup Utility' genannt) des BIOS oder UEFI-BIOS wird geöffnet. Beachten Sie, dass sich diese (UEFI-)BIOS-Benutzeroberfläche in der Darstellung, Anordnung der Elemente und Bezeichungen je nach Hersteller unterscheiden kann.

   **Hinweis**
   Bei manchen Mainboards können Sie zudem auch ein sogenanntes Boot-Menü öffnen, wenn Sie beim Booten eine bestimmte Taste(nkombination) drücken – beispielsweise **F12**. Dieses Boot-Menü gibt Ihnen die Möglichkeit, ein gewünschtes Boot-Gerät direkt aus einer Liste bootfähiger Geräte auszuwählen, ohne die komplette BIOS- bzw. UEFI-BIOS-Benutzeroberfläche aufrufen zu müssen (und dabei möglicherweise noch andere Einstellungen zu ändern).

4. Sollten Sie eine CD oder DVD als Boot-Medium verwenden, dann legen Sie diese in das entsprechende Laufwerk ein.
5. Legen Sie fest, dass das Boot-Medium (CD, DVD oder USB-Stick) bzw. dessen Laufwerk das 'primäre' Boot-Gerät ist.
   a. Wechseln Sie mit den Pfeiltasten Ihrer Tastatur (bei modernen Rechnern evtl. auch mit dem Mauszeiger) zu den Einstellungen für die Boot-Reihenfolge.
   b. Platzieren Sie den Cursor (oder den Mauszeiger) auf das entsprechende Gerät Ihres Boot-Mediums und setzen Sie es an die Spitze dieser Liste. Üblicherweise können Sie die

Reihenfolge mit den Plus-Tasten (+) und Minus-Tasten (-) ändern.




6. Verlassen Sie das BIOS bzw. UEFI-BIOS und speichern Sie die dabei vorgenommenen Änderungen. Der Computer wird nun mit dem Acronis Boot-Medium gestartet.

**Hinweis**
Falls der Computer mit dem ersten Gerät nicht booten kann, versucht er das zweite Gerät aus der Liste zu verwenden – und so weiter.

## Laufwerk-Recovery aus der Cloud

Die Wiederherstellung eines Laufwerk-Backups aus der Acronis Cloud ist einer herkömmlichen Laufwerkswiederherstellung sehr ähnlich.

- Wenn Sie Windows und Acronis Cyber Protect Home Office starten können, dann orientieren Sie sich am Abschnitt 'Volumes und Laufwerke wiederherstellen'.
- Wenn Windows nicht mehr starten kann, dann orientieren Sie sich am Abschnitt 'Ihr System aus der Acronis Cloud wiederherstellen'.

### Und so funktioniert es

Ihr Computer sollte per Netzwerkkabel oder WLAN mit dem Internet verbunden sein. Acronis Cyber Protect Home Office unterstützt mehrere WLAN-Sicherheitsprotokolle, einschließlich WPA-Personal, WPA2-Personal und WPA2-Enterprise.

**Am ursprünglichen Speicherort wiederherstellen**

Wenn Sie ein Laufwerk zu seinem ursprünglichen Speicherort wiederherstellen, lädt Acronis Cyber Protect Home Office nicht den kompletten Speicherplatz des Laufwerks auf Ihren Computer herunter. Ihr Laufwerk wird auf Datenänderungen untersucht und es werden nur solche Dateien wiederhergestellt, die sich von denen im Image unterscheiden. Diese Technologie reduziert die Datenmenge deutlich, die Sie zur Wiederherstellung Ihres Laufwerks herunterladen müssen.

**Recovery zu einem neuen Speicherort**

Wenn Sie ein Laufwerk zu einem anderen Speicherort oder auf einem 'nicht zugeordneten' Speicherplatz wiederherstellen, gleicht der resultierende Prozess sehr dem einer Wiederherstellung von einem lokalen Storage (Datenspeicher). Der einzige Unterschied besteht in der Art, wie die Daten geschrieben werden. Die Daten werden von Acronis Cyber Protect Home Office nicht kontinuierlich, sondern blockweise heruntergeladen und geschrieben. Diese Technologie erhöht die Wiederherstellungsgeschwindigkeit und Zuverlässigkeit des kompletten Prozesses.

## Was passiert, wenn die Wiederherstellung unterbrochen wurde?

Da die Laufwerkswiederherstellung aus der Acronis Cloud eine Internetverbindung verwendet und üblicherweise eine längere Zeit benötigt, ist die Wahrscheinlichkeit, dass die Wiederherstellung unterbrochen wird, höher als wenn eine herkömmliche Festplatte als Recovery-Quelle dient.

Mögliche Gründe einer Wiederherstellungsunterbrechung:

- Verlust der Internetverbindung.
- Die Verbindung mit der Acronis Cloud ging verloren.
- Sie haben die Wiederherstellung selbst abgebrochen (absichtlich oder versehentlich).
- Probleme bei der Stromversorgung.

Wenn die Wiederherstellung aufgrund eines Verbindungsproblems nicht abgeschlossen wurde, versucht Acronis Cyber Protect Home Office automatisch, eine neue Verbindung zur Acronis Cloud aufzubauen und den Recovery-Prozess fortzusetzen. Wir empfehlen, dass Sie in diesem Fall Ihre Internetverbindungseinstellungen überprüfen. Sollten alle automatischen Versuche fehlschlagen, dann führen Sie die Wiederherstellung manuell aus, sobald die Verbindung wieder besteht.

Führen Sie in allen anderen Fällen die Wiederherstellung erneut manuell aus und überprüfen Sie, dass die Wiederherstellung abgeschlossen wurde.

Unabhängig vom Grund der Unterbrechung startet Acronis Cyber Protect Home Office den Recovery-Prozess nicht wieder ganz von vorne. Es nimmt den Prozess wieder auf und lädt nur solche Daten herunter, die bisher nicht wiederhergestellt wurden.

## Ihr System aus der Acronis Cloud wiederherstellen

**Hinweis**
Die Wiederherstellung eines Laufwerks aus der Acronis Cloud kann in Abhängigkeit von Ihrer Internetgeschwindigkeit eine längere Zeit in Anspruch nehmen.

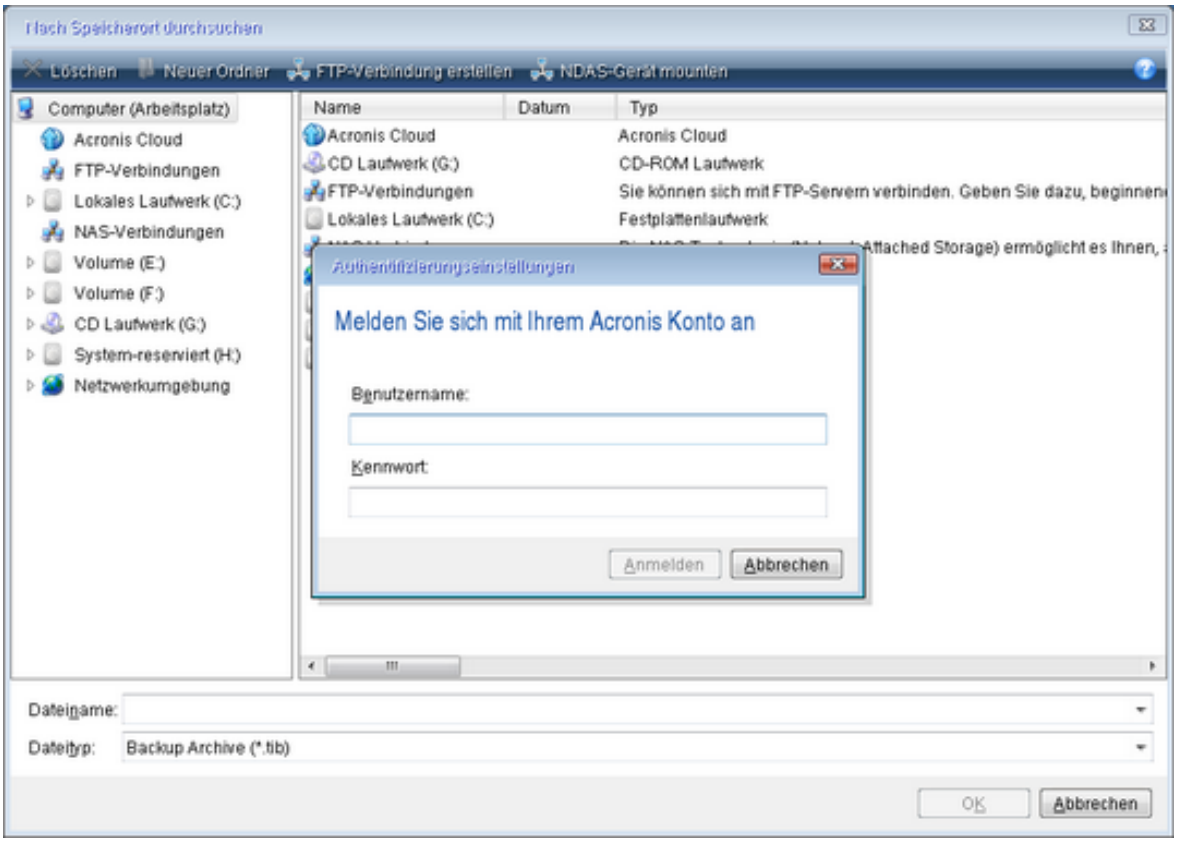
Wir empfehlen, dass Sie vor dem Beginn die im Abschnitt 'Vorbereitungen zur Wiederherstellung' beschriebenen Aktionen durchführen. Falls Sie Ihr System auf einem neuen Laufwerk wiederherstellen, müssen Sie dieses nicht formatieren, da das vom Recovery-Prozess übernommen wird.

Stellen Sie vor dem Start dieser Prozedur sicher, dass Ihr Computer per Netzwerkkabel oder WLAN mit dem Internet verbunden ist.

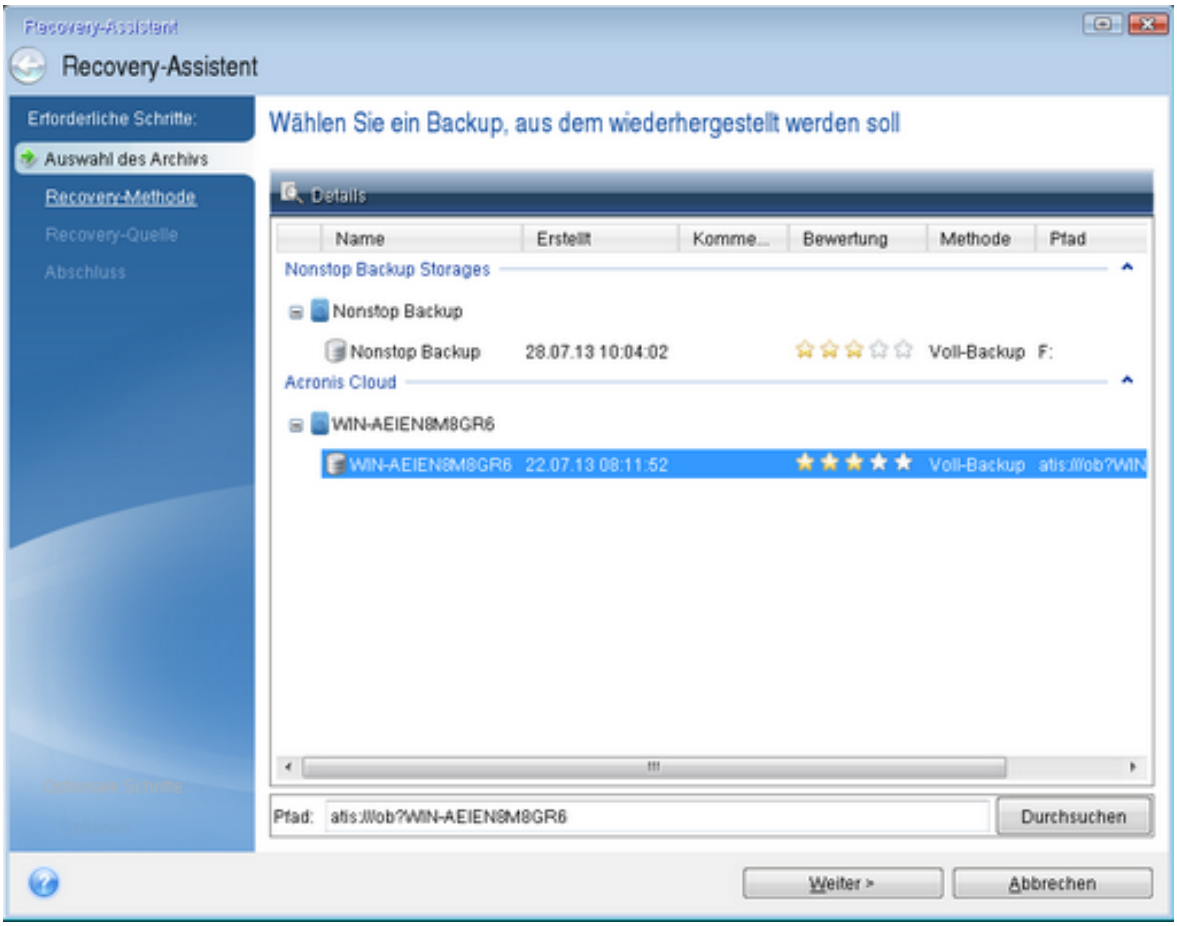
***So können Sie ein Systemlaufwerk Acronis Cloud wiederherstellen***

1. Konfigurieren Sie die Boot-Reihenfolge in Ihrem BIOS so, dass das Gerät/Laufwerk Ihres Acronis Boot-Mediums (CD, DVD oder USB-Stick) das primäre Boot-Gerät ist. Siehe Boot-Reihenfolge im BIOS arrangieren.
2. Starten Sie den Computer mit dem Boot-Medium und wählen Sie **Acronis Cyber Protect Home Office**..
3. Wählen Sie in der **Startseite** den Befehl **Laufwerke** (unterhalb des Elements **Recovery**).

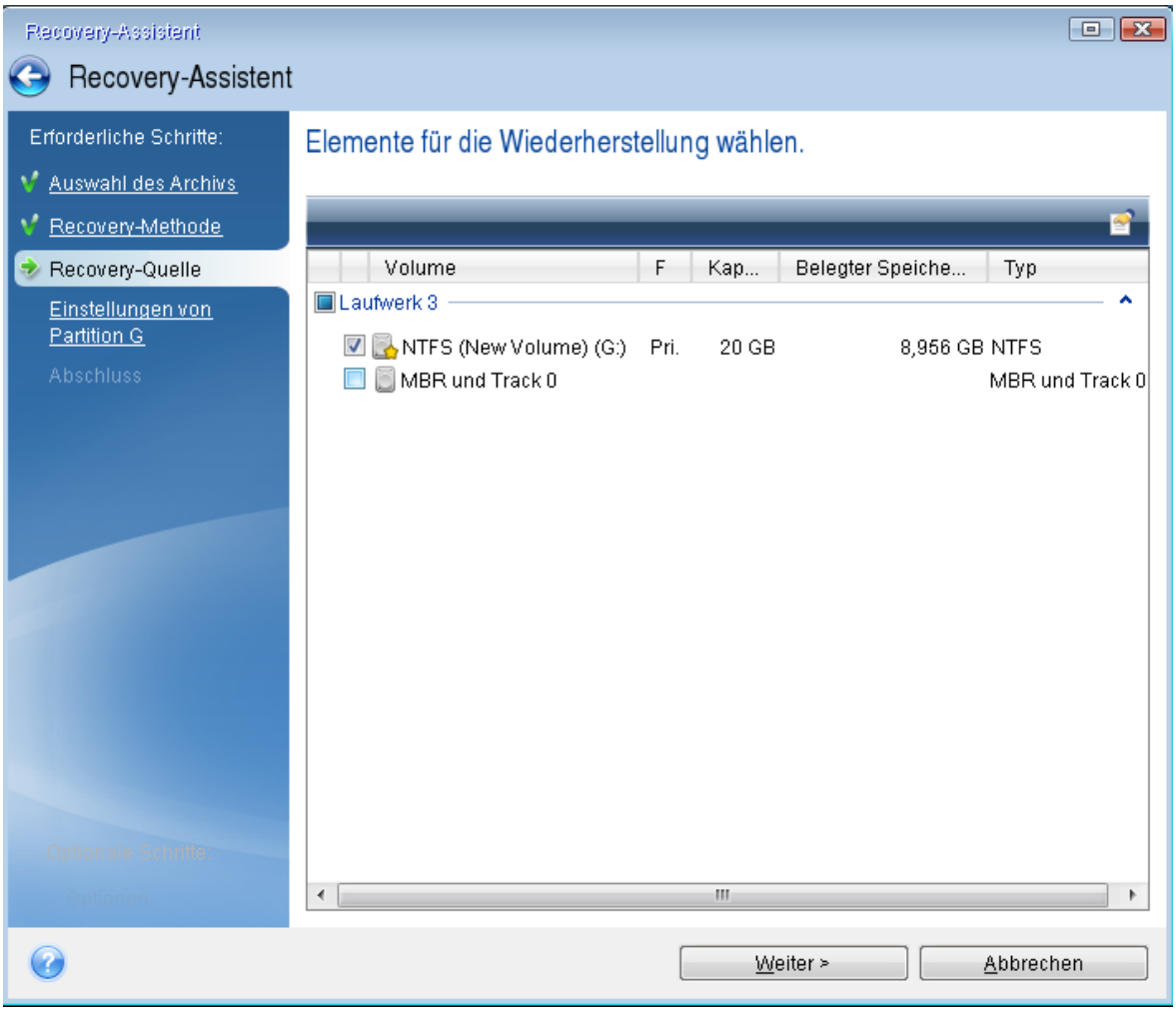

4. Klicken Sie auf **Durchsuchen**, um das Online Backup des Systemlaufwerks bzw. System-Volumes zur Liste der verfügbaren Backups hinzuzufügen.
5. Wählen Sie im Verzeichnisbaum des geöffneten Fensters die Acronis Cloud aus und geben Sie die Anmeldedaten für Ihr Acronis Konto an.




6. Wählen Sie das Backup aus, welches Sie für die Wiederherstellung verwenden möchten, und klicken Sie auf **OK**.
7. Wählen Sie im Schritt **Auswahl des Archivs** das Online Backup aus und klicken Sie dann auf **Weiter**.




8. Wählen Sie im Schritt **Recovery-Methode** den Befehl **Recovery kompletter Laufwerke und Volumes** aus.
9. Wählen Sie beim Schritt **Recovery-Quelle** das System-Volume (üblicherweise C) sowie das Volume 'System-reserviert' (sofern vorhanden). Sie können diese Volumes auch anhand der Kennzeichnungen (Flags) **Pri.** und **Akt.** identifizieren.



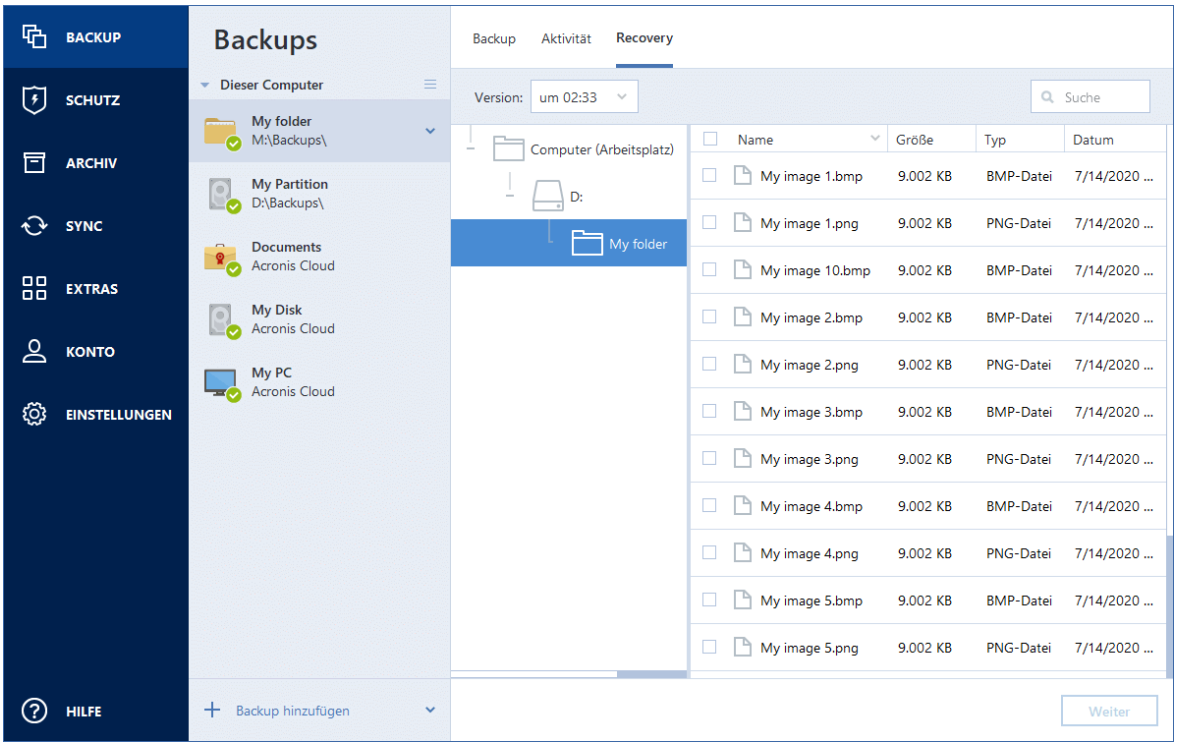

10. Ändern Sie bei Bedarf im Schritt **Einstellungen von Volume C** (oder, falls abweichend, für den tatsächlichen Laufwerksbuchstaben des System-Volumes) die Einstellungen. Sie müssen die Einstellungen beispielsweise ändern, wenn Sie eine Wiederherstellung auf einem neuen Laufwerk mit anderer Kapazität durchführen wollen.
11. Lesen Sie die Zusammenfassung der Aktionen im Schritt **Fertigstellen** aufmerksam durch. Wenn Sie die Volume-Größe nicht verändert haben, müssen die Größen in den Elementen **Volume löschen** und **Volume wiederherstellen** übereinstimmen. Klicken Sie auf **Fertigstellen**.
12. Beenden Sie nach Abschluss der Wiederherstellung die autonome Notfallversion von Acronis Cyber Protect Home Office und entfernen Sie das Boot-Medium. Booten Sie das wiederhergestellte System-Volume. Wenn Sie sich vergewissert haben, dass Sie Windows zu dem von Ihnen gewünschten Stadium wiederhergestellt haben, können Sie die ursprüngliche Boot-Reihenfolge im BIOS wieder einrichten.

# Dateien und Ordner wiederherstellen

Sie können gesicherte Dateien und Ordner über Acronis Cyber Protect Home Office, einen Datei-Manager (wie dem Windows Explorer) oder in der Acronis Cloud durchsuchen und über bzw. aus dieser wiederherstellen. Sie können Dateien und Ordner sowohl aus Datei- wie auch Laufwerk-Backups wiederherstellen.

***So können Sie Daten von der Acronis Cyber Protect Home Office aus wiederherstellen***

1. Klicken Sie in der Seitenleiste auf **Backup**.
2. Wählen Sie das Backup, welches die wiederherzustellenden Dateien und Ordner enthält, aus der Backup-Liste aus und öffnen Sie dann die Registerkarte **Recovery**.
3. [Optional] Wählen Sie auf der Symbolliste im Listenfeld **Version** den gewünschten Backup-Zeitpunkt (anhand von Datum und Uhrzeit). Standardmäßig wird das jüngste Backup wiederhergestellt.
4. Aktivieren Sie das Kontrollkästchen für die entsprechenden Dateien oder Ordner, die Sie wiederherstellen wollen, und klicken Sie dann auf **Weiter**.




5. [Optional] Die Daten werden standardmäßig an ihrem ursprünglichen Speicherort wiederhergestellt. Sie können dies ändern, wenn Sie in der Symbolleiste auf **Durchsuchen** klicken und dann den gewünschten alternativen Zielordner auswählen.
6. [Optional] Sie können bei Bedarf die Optionen für den Recovery-Prozess (Priorität des Wiederherstellungsprozesses, Sicherheitseinstellungen auf Dateiebene usw.) festlegen. Klicken Sie zum Konfigurieren der Optionen auf den Befehl **Recovery-Optionen**. Die hier eingestellten Optionen gelten nur für die aktuelle Recovery-Aktion.
7. Klicken Sie auf die Schaltfläche **Recovery jetzt**, um den Wiederherstellungsprozess zu starten.

   Die ausgewählte Dateiversion wird zum spezifizierten Ziel heruntergeladen.

   Sie können die Wiederherstellung durch Klick auf **Abbrechen** stoppen. Denken Sie daran, dass die abgebrochene Wiederherstellung dennoch zu Veränderungen im Zielordner führen kann.

***So können Sie Dateien über den Windows Explorer wiederherstellen***

1. Klicken Sie doppelt auf die entsprechende .tibx-Datei und suchen Sie anschließend die wiederherzustellenden Datei(en) bzw. Ordner.

2. Kopieren Sie die Datei bzw. den Ordner auf ein Festplattenlaufwerk.

**Hinweis**
Die kopierten Dateien verlieren die Attribute 'Komprimiert' und 'Verschlüsselt'. Wenn es notwendig ist, diese Attribute zu behalten, dann empfiehlt sich eine richtige Wiederherstellung des Backups.

***So können Sie Daten von der Acronis Cloud aus wiederherstellen***

1. Klicken Sie in der linken Seitenleiste auf **BACKUPS**.
2. Wählen Sie das Backup, welches die wiederherzustellenden Daten enthält, aus der Backup-Liste aus.
3. Wählen Sie die Backup-Version aus, die die gewünschten Daten enthält. Sehen Sie sich dafür das Datum der letzten Backup-Aktion an.
4. Wählen Sie die wiederherzustellenden Dateien bzw. Ordner aus der entsprechenden Liste aus.
5. [Optional] Sie können von einer Datei (gilt nicht für Ordner) auch eine bestimmte Version wiederherstellen. Klicken Sie dafür zuerst in der rechten Seitenleiste auf **Versionen** und dann in der gewünschten Versionszeile auf das Download-Symbol.
6. Klicken Sie in der rechten Seitenleise auf **DOWNLOAD**, um den Wiederherstellungsprozess zu starten.
   Die ausgewählten Daten werden zum vorgegebenen Download-Ordner kopiert.

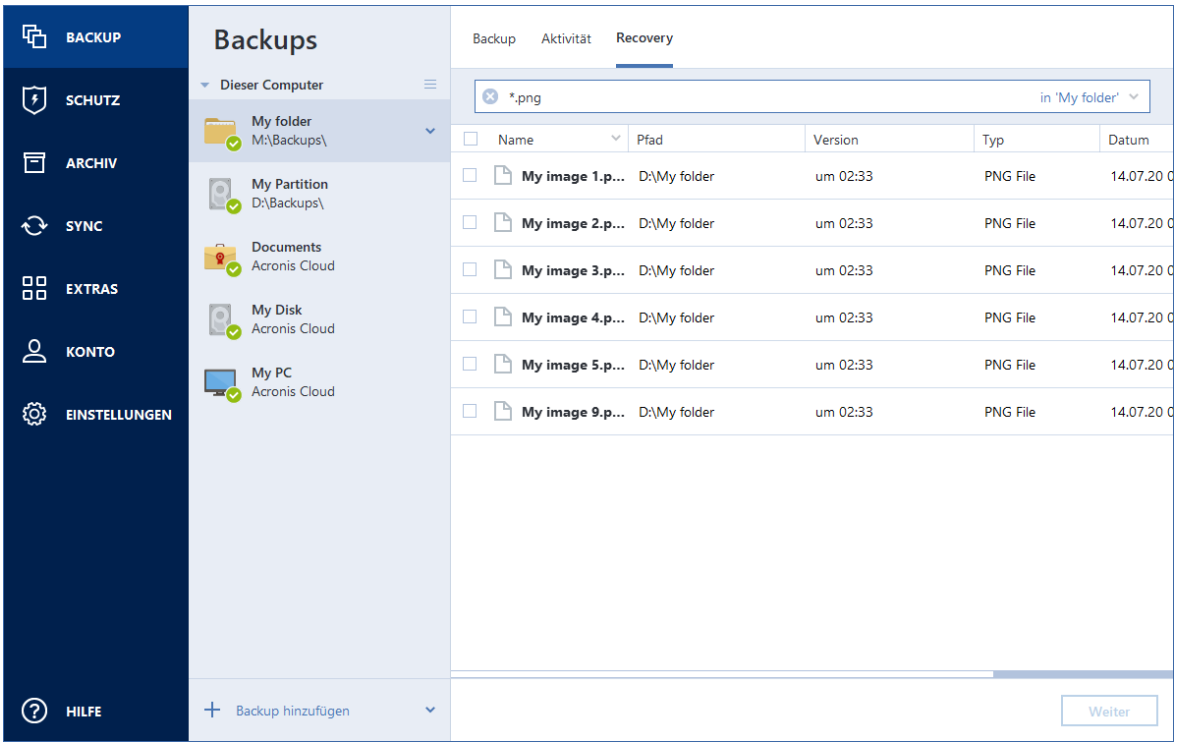
**Hinweis**
Sollten Sie mehrere Dateien und Ordner auswählen, dann werden diese in einem ZIP-Archiv zusammengefasst.

# Backup-Inhalte durchsuchen

Wenn Sie Daten aus einem lokalen Backup wiederherstellen, können Sie eine Suchfunktion verwenden, um bestimmte Dateien/Ordner zu finden, die im ausgewählten Backup gespeichert sind.

***So können Sie nach Dateien und Ordnern suchen***

1. Starten Sie eine Datenwiederherstellung wie im Abschnitt 'Volumes und Laufwerke wiederherstellen' oder 'Dateien und Verzeichnisse wiederherstellen' beschrieben.
2. Geben Sie bei der Auswahl der wiederherzustellenden Dateien/Ordner den gewünschten Datei-/Ordnernamen in das Feld **Suche** ein. Das Programm zeigt daraufhin Suchergebnisse an.
   Sie können dabei auch die üblichen Windows-Wildcards verwenden: '*' und '?'. Wenn Sie beispielsweise alle Dateien mit der Erweiterung **.exe** finden möchten, geben Sie ***.exe** ein. Mit der Eingabe **Meine???.exe** werden alle Dateien mit der Erweiterung '.exe' gefunden, die aus acht Zeichen bestehen und zudem mit 'Meine' beginnen.




3. Acronis Cyber Protect Home Office durchsucht standardmäßig den im vorherigen Schritt ausgewählten Ordner. Wenn Sie Backup vollständig durchsuchen wollen, klicken Sie auf den 'Pfeil nach unten' und dann auf den Befehl **im kompletten Backup**.

   Wenn Sie zum vorherigen Schritt zurückkehren wollen, löschen Sie den Suchttext und klicken Sie dann auf das Symbol mit dem Kreuz.
4. Wenn die Suche abgeschlossen wurde, können Sie die wiederherzustellenden Dateien auswählen und auf **Weiter** klicken.

**Hinweis**
Achten Sie auf die Spalte Version. Dateien und Ordner, die zu unterschiedlichen Backup-Versionen gehören, können nicht gleichzeitig wiederhergestellt werden.

# Microsoft 365-Daten wiederherstellen

Mit Acronis Cyber Protect Home Office können Sie Ihr persönliches Microsoft 365-Konto per Backup davor schützen, dass Sie Ihre E-Mail-Nachrichten, Dateien und Ordner, Profil-Informationen und andere Daten verlieren. Wenn Sie Ihre Kontodaten per Cloud Backup gesichert haben, können Sie das Backup bei Bedarf in der Cloud durchsuchen und dabei einzelne Elemente direkt wiederherstellen.

## Welche Elemente können wiederhergestellt werden?

**Folgende Elemente können aus einem Postfach-Backup wiederhergestellt werden:**

- Komplettes Postfach
- E-Mail-Nachrichten

- Anhänge

**Folgende Elemente können aus einem OneDrive-Backup wiederhergestellt werden:**

- Kompletter OneDrive-Ordner
- Alle Dateien und Ordner, die im Backup gesichert wurden

## Microsoft 365-Daten wiederherstellen

***So können Sie Ihre Daten durchsuchen und wiederherstellen***

1. Öffnen Sie das Online Dashboard durch eine der folgenden Aktionen:
   - Folgen Sie diesem Link: https://cloud.acronis.com.
   - Klicken Sie in der Seitenleiste von Acronis Cyber Protect Home Office auf den Befehl **Konto** und anschließend auf **Online Dashboard öffnen**.
2. Melden Sie sich an Ihrem Acronis Konto an.
3. Klicken Sie in der Seitenleiste auf **Ressourcen**, suchen Sie die Microsoft 365-Backup-Box und klicken Sie dann auf **Recovery**.
4. Durchsuchen Sie die Liste Ihrer Backups. Verwenden Sie bei Bedarf die Filterfunktion, um bestimmte Inhalte im Backup zu finden.
5. Klicken Sie nach der Auswahl des Backups auf **Wiederherstellen...** und bestimmen Sie, welche Daten genau Sie wiederherstellen wollen:
   - Das komplette OneDrive oder bestimmte Dateien bzw. Ordner.
   - Das komplette Postfach oder bestimmte Nachrichten.

   Wenn Sie sich zur Wiederherstellung bestimmter Elemente entschlossen haben, wird das Online Dashboard eine Liste der gesicherten Elemente öffnen. Sie können diese nun durchsuchen, die entsprechende Inhalte anzeigen lassen und eine Suchfunktion benutzen, um bestimmte Elemente zu finden (wird nicht für alle Datentypen unterstützt).

   Nachdem Sie die Elemente ausgewählt haben, können Sie bestimmen, welche Aktion(en) mit diesen durchgeführt werden soll (je nach Datentyp sind einige Aktionen nicht verfügbar):
   - **Inhalt anzeigen** – mit diesem Befehl werden Elementinformationen angezeigt oder das Element im Vollbild geöffnet.
   - **Als E-Mail senden** – mit diesem Befehl können Sie die Nachricht an bestimmte Empfänger übermitteln.
   - **Versionen anzeigen** – mit diesem Befehl können Sie sich die Versionen des Elements anzeigen lassen.
   - **Recovery** – mit diesem Befehl können Sie den Zielspeicherort für die wiederherzustellenden Elemente festlegen. Für einige Elemente können Sie auch Freigabe-Berechtigungen wiederherstellen.
   - **Download** – mit diesem Befehl können Sie eine ausgewählte Datei herunterladen.
6. Klicken Sie auf **Recovery starten**.

# Recovery-Optionen

Sie können Optionen für die Wiederherstellungsprozesse von Laufwerken/Volumes und von Dateien konfigurieren. Alle Optionen werden nach Installation des Programms auf Ihre Anfangswerte eingestellt. Sie können sie allein für Ihre aktuelle Recovery-Aktion ändern oder aber auch für alle zukünftigen Recovery-Aktionen. Aktivieren Sie das Kontrollkästchen **Einstellungen als Standard speichern**, um geänderte Einstellungen für alle zukünftigen Recovery-Aktionen als Vorgabe zu übernehmen.

Beachten Sie, dass die Optionen zur Wiederherstellung von Laufwerken und Dateien komplett unabhängig voneinander sind und daher von Ihnen je separat konfiguriert werden sollten.

Klicken Sie auf die Schaltfläche **Auf Anfangseinstellungen zurücksetzen**, wenn Sie alle geänderten Optionen auf ihre anfänglichen Werte (wie bei Installation des Programms) zurücksetzen wollen.

## Recovery-Modus 'Laufwerk'

Speicherort: **Recovery-Optionen** –> **Erweitert** –> **Recovery-Modus 'Laufwerk'**

Sie können mit dieser Option den Laufwerkswiederherstellungsmodus bei Image-Backups wählen.

- **'Sektor-für-Sektor' wiederherstellen** – aktivieren Sie dieses Kontrollkästchen, wenn Sie von Ihren Laufwerke bzw. Volumes alle Sektoren (benutzte und unbenutzte) wiederherstellen lassen möchten. Diese Option ist nur dann wirksam, wenn Sie für die Wiederherstellung auch ein entsprechendes 'Sektor-für-Sektor-Backups' auswählen.

## Vor-/Nach-Befehle für Wiederherstellung

Speicherort: **Recovery-Optionen** –> **Erweitert** –> **Vor-/Nach-Befehle**

Sie können Befehle (oder Batch-Dateien) spezifizieren, die automatisch vor oder nach der Wiederherstellung ausgeführt werden.

Damit können Sie z.B. Windows-Prozesse starten bzw. stoppen oder Ihre Daten vor dem Start der Wiederherstellung auf Viren prüfen.

Um Befehle (Batch-Dateien) zu spezifizieren:

- Wählen Sie im Feld **Vor-Befehl** den Befehl, der vor dem Recovery-Prozess ausgeführt werden soll. Klicken Sie auf **Bearbeiten**, um einen neuen Befehl zu erstellen oder eine neue Batch-Datei auszuwählen.
- Bestimmen Sie im Feld **Nach-Befehl** einen nach Beendigung des Recovery-Prozesses auszuführenden Befehl. Klicken Sie auf **Bearbeiten**, um einen neuen Befehl zu erstellen oder eine neue Batch-Datei auszuwählen.

Versuchen Sie nicht, interaktive Befehle auszuführen, d.h. Befehle, die eine Reaktion des Benutzers erfordern (beispielsweise 'Pause'). Diese werden nicht unterstützt.

### Benutzerbefehl für Wiederherstellung bearbeiten

Sie können Befehle angeben (oder Batch-Dateien), die automatisch vor oder nach einer Wiederherstellung ausgeführt werden:

- Geben Sie im Feld **Befehl** einen Befehl ein oder wählen Sie einen aus der Liste. Klicken Sie auf '**...**', um eine Batch-Datei zu wählen.
- Geben Sie im Feld **Arbeitsverzeichnis** einen Pfad für die Befehlsausführung ein oder wählen Sie diesen aus der Liste zuvor bereits gewählter Pfade.
- Geben Sie im Feld **Argumente** die Argumente für die Befehlsausführung ein oder wählen Sie diese aus der Liste aus.

Das Deaktivieren des standardmäßig aktivierten Kontrollkästchens **Aktionen nicht ausführen, bis die Befehlsausführung abgeschlossen ist** erlaubt es, dass Wiederherstellungsprozesse zeitgleich neben der Ausführung Ihrer Befehle laufen können.

Die Option **Aktion abbrechen, wenn der Benutzerbefehl fehlschlägt** (standardmäßig eingeschaltet) bricht die Aktion ab, wenn Fehler bei der Ausführung auftreten.

Sie können den Befehl testen, indem Sie auf die Schaltfläche **Befehl testen** klicken.

## Optionen für Validierung

Speicherort: **Recovery-Optionen** –> **Erweitert** –> **Validierung**

- **Backup vor der Wiederherstellung validieren** – Aktivieren Sie diese Option, um die Integrität des Backups vor der Wiederherstellung zu überprüfen.
- **Dateisystem nach Wiederherstellung prüfen** – Aktivieren Sie diese Option, um die Integrität des Dateisystems auf dem wiederhergestellten Volume zu überprüfen.

**Hinweis**
Nur die Dateisysteme FAT16/32 und NTFS können überprüft werden.

**Hinweis**
Das Dateisystem wird nicht geprüft, falls während der Wiederherstellung ein Neustart erforderlich ist, z.B. wenn die Systempartition an ihren ursprünglichen Platz wiederhergestellt wird.

## Computer-Neustart

Speicherort: **Recovery-Optionen** –> **Erweitert** –> **Computer-Neustart**

Aktivieren Sie das Kontrollkästchen **Computer automatisch neu starten, wenn für Wiederherstellung erforderlich**, wenn Sie wollen, dass Ihr Computer während einer Recovery-Aktion automatisch gestartet wird, falls dies zur Fertigstellung benötigt wird. Dies ist beispielsweise der Fall, wenn ein Volume wiederhergestellt werden muss, welches vom Betriebssystem gesperrt wird.

## Optionen für Datei-Recovery

Speicherort: **Recovery-Optionen** –> **Erweitert** –> **Optionen für Datei-Recovery**

Sie können folgende Optionen für Datei-Recovery wählen:

- **Dateien mit ihren ursprünglichen Sicherheitseinstellungen wiederherstellen** – wenn die Sicherheitseinstellungen der Dateien während des Backups beibehalten wurden (siehe 'Dateisicherheitseinstellungen für Backups') , dann können Sie wählen, ob die Dateien mit ihren Sicherheitseinstellungen wiederhergestellt werden oder ob sie die Sicherheitseinstellungen von dem Ordner erben sollen, in den sie wiederhergestellt werden. Diese Option gilt nur bei Wiederherstellung von dateibasierten Backups.
- **Aktuelles Datum und Zeit für wiederhergestellte Dateien festlegen** – Sie können entscheiden, ob der Zeitstempel der wiederhergestellten Dateien aus dem Backup übernommen wird oder ob den Dateien das aktuelle Datum und die aktuelle Zeit zugewiesen werden. Standardmäßig wird den Dateien das Datum und die Zeit aus dem Backup zugewiesen.

## Optionen für das Überschreiben von Dateien

Speicherort: **Recovery-Optionen** –> **Erweitert** –> **Optionen für das Überschreiben von Dateien**

Bestimmen Sie, was das Programm tun soll, wenn es im Zielverzeichnis Dateien mit gleichen Namen findet, wie diejenigen, die aus dem Backup wiederhergestellt werden sollen.

**Hinweis**
Diese Option ist nur bei der Wiederherstellung von Dateien und Ordnern verfügbar (nicht von Laufwerken und Volumes).

Aktivieren Sie das Kontrollkästchen **Vorhandene Dateien überschreiben**, wenn die Dateien auf Ihrem Festplattenlaufwerk durch die Dateien aus dem Backup überschrieben werden sollen. Wenn das Kontrollkästchen deaktiviert ist, werden die aktuelleren Dateien/Ordner auf dem Laufwerk beibehalten.

Dazu gehen Sie folgendermaßen vor:

- Aktivieren Sie das Kontrollkästchen **Versteckte Dateien und Ordner**, um zu verhindern, dass versteckte Dateien/Ordner überschrieben werden. Diese Option ist für Datei-Backups verfügbar, die lokale Speicherorte und Netzwerkfreigaben als Ziel verwenden.
- Aktivieren Sie das Kontrollkästchen **Systemdateien und Systemordner**, um zu verhindern, dass Dateien/-Ordner mit der Kennzeichnung 'System' überschrieben werden. Diese Option ist für Datei-Backups verfügbar, die lokale Speicherorte und Netzwerkfreigaben als Ziel verwenden.
- Aktivieren das Kontrollkästchen **Neuere Dateien und Ordner**, um zu verhindern, dass neuere Dateien/Ordner überschrieben werden.
- Klicken Sie auf **Bestimmte Dateien und Ordner hinzufügen**, um die Liste benutzerdefinierter Dateien bzw. Ordner zu verwalten, die nicht überschrieben werden sollen. Diese Option ist für Datei-Backups verfügbar, die lokale Speicherorte und Netzwerkfreigaben als Ziel verwenden.

- Um zu verhindern, dass bestimmte Dateien überschrieben werden, müssen Sie auf das Plus-Zeichen (+) klicken, um ein Ausschlusskriterium zu definieren.
- Bei Spezifizierung der Kriterien können Sie die üblichen Windows-Wildcards verwenden. Wenn Sie z.B. alle Dateien mit der Erweiterung **.exe** schützen wollen, fügen Sie ***.exe** hinzu. Indem Sie **Meine???.exe** hinzufügen, werden alle Dateien mit der Erweiterung .exe geschützt, die außerdem aus acht Zeichen bestehen und mit „Meine“ beginnen.

Wenn Sie ein Kriterium löschen wollen, können Sie es in der Liste auswählen und durch Klick auf das Minus-Zeichen (-) entfernen.

## Die Performance von Recovery-Aktionen

Speicherort: **Recovery-Optionen** –> **Erweitert** –> **Performance**

Sie können folgende Einstellungen konfigurieren:

### Priorität für die Aktion

Durch Änderung der Priorität können Backup- und Recovery-Prozesse schneller oder langsamer als normal ablaufen (je nachdem, wofür Sie sich entscheiden); was aber auch einen Einfluss auf die Performance andere Programme haben kann. Die Priorität eines jeden Prozesses, der in einem System läuft, bestimmt das Ausmaß der CPU-Benutzung und der Systemressourcen, die dem Prozess zugeordnet werden. Durch Herabsetzen der Priorität für Aktionen werden mehr Ressourcen für andere CPU-Tasks freigegeben. Durch Heraufsetzen der Backup- bzw. Recovery-Priorität können entsprechende Aktionen möglicherweise beschleunigt werden, weil Ressourcen von anderen, aktuell laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-Auslastung und anderen Faktoren.

Sie können die Priorität für Aktionen einstellen:

- **Niedrig** (standardmäßig aktiviert) – Der Backup- oder Recovery-Prozess läuft langsamer, dafür kann aber die Performance anderer Programme besser werden.
- **Normal** – Der Backup- bzw. Recovery-Prozess hat die gleiche Priorität wie andere Prozesse.
- **Hoch** – Der der Backup- bzw. Recovery-Prozess wird schneller durchgeführt, andere Programme laufen dadurch jedoch möglicherweise langsamer. Beachten Sie, dass die Wahl dieser Option zu einer 100%igen CPU-Auslastung durch Acronis Cyber Protect Home Office führen kann.

## Benachrichtigungen für Recovery-Aktionen

Speicherort: **Recovery-Optionen** –> **Benachrichtigungen**

Manchmal benötigt eine Backup- oder Recovery-Prozedur länger als eine Stunde. Acronis Cyber Protect Home Office kann Sie per E-Mail benachrichtigen, wenn Aktionen abgeschlossen wurden. Das Programm kann auch Nachrichten reproduzieren, die während der Aktion ausgegeben werden – oder kann Ihnen das vollständige Log nach dem Ende der Aktion senden.

In der Grundeinstellung sind alle Benachrichtigungen deaktiviert.

## Grenzwert für freien Speicherplatz

Sie möchten möglicherweise benachrichtigt werden, wenn der freie Platz auf einem Recovery Storage unter einen spezifizierten Grenzwert fällt. Sollte Acronis Cyber Protect Home Office nach dem Start eines Backup-Tasks feststellen, dass der freie Platz am Backup-Speicherort bereits unterhalb des angegebenen Werts liegt, dann beginnt das Programm erst gar nicht mit dem aktuellen Wiederherstellungsprozess und wird Sie umgehend mit einer entsprechenden Meldung informieren. Die Meldung bietet drei Wahlmöglichkeiten – sie zu ignorieren und die Wiederherstellung fortzusetzen, einen anderen Speicherort zu wählen oder die Wiederherstellung abzubrechen.

Sollte der freie Speicherplatz unter den angegebenen Grenzwert sinken, während die Wiederherstellung läuft, dann zeigt das Programm dieselbe Meldung an, worauf Sie dieselben Entscheidungen treffen müssen.

***So können Sie den Grenzwert für den freien Speicherplatz festlegen***

- Aktivieren Sie das Kontrollkästchen **Quickinfo bei unzureichendem freien Speicherplatz anzeigen**.
- Wählen Sie im Feld **Größe** den Grenzwert oder tippen Sie ihn ein und bestimmten Sie dann eine Maßeinheit.

Acronis Cyber Protect Home Office kann freien Platz auf folgenden Speichergeräten überwachen:

- Lokale Festplatten (und ähnlichen Laufwerke)
- USB-Laufwerke (z.B. USB-Sticks)
- Netzwerkfreigaben (SMB)

**Hinweis**
Diese Meldung wird nicht angezeigt, wenn das Kontrollkästchen **Während der Durchführung keine Meldungen bzw. Dialoge zeigen (Stiller Modus)** im Bereich **Fehlerbehandlung** der Backup-Optionen aktiviert ist.

**Hinweis**
Für CD-/DVD-Laufwerke und FTP kann diese Option nicht aktiviert werden.

## E-Mail-Benachrichtigung

1. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen über Aktionsstatus senden**.
2. E-Mail-Einstellungen konfigurieren:
   - Geben Sie die E-Mail-Adresse in das Feld **An** ein. Sie können mehrere E-Mail-Adressen, per Semikolon getrennt, nacheinander eintragen.
   - Geben Sie die Adresse des Postausgangsservers (SMTP) in das Feld **Server-Einstellungen** ein.

- Tragen Sie die Port-Adresse des Postausgangsservers ein. Standardmäßig ist der Port auf 25 gesetzt.
- Aktivieren Sie bei Bedarf das Kontrollkästchen **SMTP-Authentifizierung** und geben Sie dann den Benutzernamen und das Kennwort in die entsprechenden Felder ein.

3. Klicken Sie auf die Schaltfläche **Testnachricht senden**, um zu überprüfen, ob Ihre Einstellungen korrekt sind.

***Wenn das Versenden der Testnachricht fehlschlägt***

1. Klicken Sie auf **Erweiterte Einstellungen anzeigen**.
2. Erweiterte E-Mail-Einstellungen konfigurieren:
   - Geben Sie die E-Mail-Adresse des Absenders das Feld **Von** ein. Falls Sie nicht sicher sind, welche Adresse Sie angeben sollen, dann geben Sie eine gewünschte Adresse im Standardformat vom Typ *aaa@bbb.com* ein.
   - Ändern Sie bei Bedarf den Nachrichtenbetreff im Feld **Betreff**.
   - Aktivieren Sie das Kontrollkästchen **Anmeldung beim Posteingangsserver**.
   - Geben Sie die Adresse des Posteingangsservers (POP3) in das Feld **POP3-Server** ein.
   - Legen Sie die Port-Adresse des Posteingangsservers fest. Standardmäßig ist der Port auf 110 gesetzt.
3. Klicken Sie erneut auf die Schaltfläche **Testnachricht senden**.

***Erweiterte Benachrichtigungseinstellungen***

- Um nach Fertigstellung eines Prozesses benachrichtigt zu werden, aktivieren Sie das Kontrollkästchen **Benachrichtigung bei erfolgreichem Abschluss einer Aktion**.
- Um über einen fehlgeschlagenen Prozess benachrichtigt zu werden, aktivieren Sie das Kontrollkästchen **Benachrichtigung bei Fehler einer Aktion**.
- Um benachrichtigt zu werden, wenn es während einer Aktion zu einer Ereignismeldung kommt, aktivieren Sie das Kontrollkästchen **Benachrichtigung, wenn Benutzereingriff erforderlich ist**.
- Um Benachrichtigungen inklusive eines vollständigen Ereignisberichts über die durchgeführten Aktionen zu verschicken, aktivieren Sie das Kontrollkästchen **Vollständiges Log zur Benachrichtigung hinzufügen**.

# Daten archivieren

## Was tut die Datenarchivierungsfunktion?

Bei der Datenarchivierungsfunktion handelt es sich um ein Tool, mit dem Sie bestimmte Daten (z.B. große oder selten verwendete) in die Acronis Cloud, auf ein NAS-Gerät, eine externe Festplatte oder einen USB-Stick verschieben können. Das Tool analysiert bei jeder Ausführung die Daten im ausgewählten Ordner und schlägt anschließend vor, die gefundenen Dateien in die Acronis Cloud oder auf einen lokalen Storage zu verschieben. Sie können die Dateien und Ordner auswählen, die Sie archivieren wollen. Nach dem Verschieben in ein Archiv werden die lokalen Kopien dieser Dateien dann gelöscht. Die Links zu diesen Dateien werden an einen speziellen Speicherort mit der Bezeichnung 'Acronis Drive' gespeichert. Sie können auf diesen Speicherort wie auf einen herkömmlichen Ordner im Windows Datei-Explorer zugreifen. Wenn Sie doppelt auf einen Datei-Link klicken, wird die Datei genauso geöffnet, als wäre in einem lokalen Ordner gespeichert. Sollte die Datei in die Acronis Cloud archiviert worden sein, so wird Sie zuerst wieder auf Ihren Computer heruntergeladen. Die Datei ist zudem auch direkt in der Acronis Cloud verfügbar und verwaltbar.

Die wichtigsten Fähigkeiten bzw. Möglichkeiten der Datenarchivierung sind:

- **Mehr freier Speicherplatz**

  Normalerweise wird der Speicherplatz auf modernen, großen Festplatten überwiegend durch Benutzerdaten (Fotos, Dokumente etc.) belegt – und nicht so sehr durch das Betriebssystem oder Software-Anwendungen. Da die Mehrzahl dieser Benutzerdaten nur selten verwendet wird, ist es nicht zwingend notwendig, diese auch ständig auf einem lokalen Laufwerk vorzuhalten. Die Datenarchivierungsfunktion hilft Ihnen, mehr Speicherplatz freizugeben, sodass dieser besser für häufig verwendete Dateien genutzt werden kann.
- **Cloud-Archivierung und lokale Archivierung**

  Sie können einen Zieltyp für Ihr Archiv bestimmen: die Acronis Cloud oder einen lokalen Storage (wie beispielsweise eine interne oder externe Festplatte, ein NAS-Gerät oder einen USB-Stick). Wenn Sie die Acronis Cloud als Ziel auswählen, werden die ausgewählten Daten immer in demselben Cloud-Archiv gespeichert. Lokale Archive sind unabhängig von einander und können daher (bei Bedarf) unterschiedliche Namen, Zielorte, Verschlüsselungseinstellungen usw. haben. Sie können jedoch auch hier immer ein vorhandenes Archiv als Ziel auswählen (statt ein neues zu erstellen). Die Anzahl der lokalen Archive ist nicht begrenzt.
- **Einfacher Zugriff auf Cloud-Archive von beliebigen Geräten**

  Wenn Sie Ihre Dateien in die Acronis Cloud archiviert haben, können Sie auf diese anschließend leicht über Acronis Cyber Protect Home Office, über die Acronis Cyber Protect Home Office Mobile App (für Mobilgeräte) und zudem über die Acronis Cloud-Webapplikation zugreifen. Also mit allen Geräten (einschließlich Smartphones und Tablets), auf denen entweder Windows, macOS, iOS oder Android als Betriebssystem läuft.
- **Schutz Ihrer Daten im Cloud-Archiv**

  Ihre in der Acronis Cloud gespeicherten Daten sind zuverlässig vor Beschädigungen oder einem Desaster (etwa ein Feuer, Wasserschaden oder Einbruch in Ihrer Wohnung) geschützt. Sollte

beispielsweise Ihre lokale Festplatte kaputtgehen, können Sie Ihre Dateien ganz einfach auf eine neue Festplatte herunterladen. Ihre Daten werden zudem verschlüsselt gespeichert. Daher haben Sie die Gewissheit, dass nur Sie (und sonst wirklich niemand, auch nicht Acronis) auf Ihre Daten zugreifen kann.

- **File-Sharing**

  Sobald Ihre Dateien in die Acronis Cloud hochgeladen wurden, können Sie öffentliche Links auf diese erstellen. Mit diesen Links können Sie die Dateien für bestimmte Personen (z.B. Freunde) oder in Foren und sozialen Netzwerken freigeben.
- **Dateiversionen**

  Bei Dateien, die geändert und dann entsprechend mehrfach in die Acronis Cloud hochgeladen werden, speichert Acronis Cyber Protect Home Office all diese durchgeführten Änderungen in Form von einzelnen Dateiversionen. Sie können daher jederzeit eine bestimmte, gewünschte Dateiversion auswählen und wieder auf Ihr Gerät herunterladen.

## Was wird von Archiven ausgeschlossen?

Standardmäßig werden von Acronis Cyber Protect Home Office folgende Daten/Dateien von den Archiven ausgeschlossen, um die Archivgröße zu senken und Risiken zur Beschädigung Ihres Systems zu vermeiden:

- pagefile.sys
- swapfile.sys
- Der temporäre Ordner ('Temp').
- Der Ordner 'System Volume Information'
- Der 'Papierkorb'
- Die temporären Daten des Webbrowsers:
  - Die temporären Internetdateien
  - Cache
- .tibx-Dateien
- .tib.metadata-Dateien
- .tmp-Dateien
- Dateien mit der Erweiterung .~

Eine vollständige Dateiliste finden Sie in diesem Knowledge Base-Artikel: https://kb.acronis.com/de/content/58297.

## Cloud-Archivierung vs. Online Backup

Wenn Sie Daten in die Acronis Cloud archivieren, gleicht dies zwar einem Online Backup, aber es gibt auch einige Unterschiede.

| | Online Backup | Cloud-Archivierung |
|---|---|---|
| Verwendungszweck | Schutz vor Beschädigung des Betriebssystems, Hardware-Fehlern und Verlust einzelner Dateien. | Bereinigung lokaler Speichergeräte und Datenverschiebung in die Acronis Cloud. |
| Data Protection | • Umfassende Sicherung all Ihrer Daten auf einem Computer (insbesondere des Betriebssystems).<br>• Sicherung von häufig verwendeten Dateien. | Sicherung von selten verwendeten oder alten Dateien (v.a. persönliche Dokumente, Fotos etc.). |
| Auswahl der Quelldaten | Manuelle Auswahl. | Manuelle Auswahl von automatisch gefundenen Dateien. |
| Handhabung der Quelldaten | Die Quelldaten bleiben am ursprünglichen Speicherort. | Die Quelldaten werden vom ursprünglichen Speicherort gelöscht. Dadurch erhalten Sie die Garantie, dass Ihre Daten nicht in falsche Hände geraten können (z.B. falls Ihr Computer oder Ihre Festplatte gestohlen werden sollten). |
| Häufigkeit von Datenänderungen | Die zu sichernden Daten werden häufig geändert. Zum Backup gehören viele, immer wieder aktualisierte Versionen. | Die zu archivierenden Daten werden selten geändert. Zu dieser Datei gibt es nur wenige Versionen. |

# Archivierung Ihrer Daten

Die Datenarchivierungsfunktion hilft Ihnen, lokalen Speicherplatz freizugeben, indem Sie alte oder selten verwendete Dateien in die Acronis Cloud oder auf einen lokalen Storage verschieben. Weitere Informationen finden Sie im Abschnitt 'Was tut die Datenarchivierungsfunktion'.

***So können Sie Ihre Daten archivieren***

1. Starten Sie Acronis Cyber Protect Home Office und wechseln Sie in den Programmbereich **Archivieren**.
2. [Optionaler Schritt] Wenn Sie die Grundlagen der Datenarchivierungsfunktion lernen wollen, schauen Sie sich die 'Erste Schritte'-Folien an.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um die Dateien Ihres Windows-Standardbenutzerordners (üblicherweise C:\Benutzer\[Benutzername]) analysieren zu lassen, müssen Sie auf **Benutzer-Basisordner analysieren** klicken.

- Um die Dateien eines benutzerdefinierten Ordners analysieren zu lassen, müssen Sie zuerst auf den nach unten zeigenden Pfeil klicken, dann auf **Anderen Ordner wählen** – und anschließend den zu analysierenden Ordner bestimmen.

  Acronis Cyber Protect Home Office analysiert die entsprechenden Dateien auf Ihrem Computer. Beachten Sie, dass dieser Prozess einige Minuten dauern kann.
4. Wählen Sie im linken Fensterbereich eine Datenkategorie aus. Wählen Sie anschließend im rechten Bereich die Dateien und Ordner aus, die Sie archivieren möchten.

   Zum Auswählen der gefundenen Dateien können Sie diese sortieren (beispielsweise nach Größe oder Alter, also dem letzten Änderungsdatum). Klicken Sie zum Sortieren der Dateien auf die entsprechenden Spaltenköpfe.
5. Klicken Sie auf **Ziel wählen** und bestimmen Sie, ob die Acronis Cloud oder ein benutzerdefinierter lokaler Zielspeicherort für die archivierten Dateien verwendet werden soll.
6. [Optionaler Schritt] Klicken Sie auf **Optionen**, um die Einstellungen für das Archiv festzulegen (wie das **Datacenter** oder die **Verschlüsselung**). Weitere Details finden Sie im Abschnitt 'Datenarchivierungsoptionen'.
7. Klicken Sie auf **Archivieren**.
8. Bestätigen Sie, dass Sie die Dateien in das Archiv verschieben und automatisch von Ihrem Computer löschen lassen wollen.

Zusätzlich können Sie sich englischsprachige Video-Anleitungen unter folgender Adresse anschauen: https://goo.gl/eEkNj2.

# Datenarchivierungsoptionen

## Datacenter

Wenn Sie Ihrer Dateien in die Acronis Cloud archivieren, werden Ihre Daten in eines der Acronis Datacenter hochgeladen, die jeweils in verschiedenen Ländern liegen. Beim Erstellen Ihres Acronis Kontos wird anfänglich dasjenige Datacenter für Sie festgelegt, welches Ihrem Standort am nächsten liegt. Anschließend werden Ihre archivierten Dateien standardmäßig in genau diesem Datacenter gespeichert.

Wir empfehlen, dass Sie dann ein anderes Datacenter für ein Archiv manuell festlegen, wenn Sie sich in einem anderen Land befinden – oder das standardmäßig ausgewählte Datacenter doch nicht das nächstliegende ist (bezogen auf Ihren Stand- bzw. Wohnort). Dies kann die Datenrate beim Upload deutlich steigern.

**Hinweis**
Sie können das Datacenter nicht mehr ändern, nachdem der Archivierungsprozess gestartet wurde.

***So können Sie ein Datacenter auswählen***

1. Klicken Sie beim Konfigurieren des ersten Archivierungsprozesses auf **Optionen**.
2. Wählen Sie dasjenige Land aus, das am nächsten zu Ihrem aktuellen Stand- bzw. Wohnort liegt.

## Verschlüsselung

Um die archivierten Daten gegen unberechtigte Zugriffe zu schützen, können Sie das Archiv mit dem AES-Algorithmus (Advanced Encryption Standard) verschlüsseln lassen, wobei eine Verschlüsselungstiefe von 256 Bit verwendet wird.

**Hinweis**
Die Option zur Archiv-Verschlüsselung kann nicht für bereits vorhandene Archive festgelegt oder geändert werden.

So können Sie ein Archiv verschlüsseln:

1. Klicken Sie beim Konfigurieren des ersten Archivierungsprozesses auf **Optionen**.
2. Aktivieren Sie das Kontrollkästchen **Archiv mit dem AES-256-Algorithmus verschlüsseln**.
3. Geben Sie das Kennwort für das Archiv in das entsprechende Feld ein. Wir empfehlen die Verwendung eines Kennworts, das aus mindestens acht Zeichen besteht und sowohl Buchstaben (am besten Groß- und Kleinbuchstaben) wie Zahlen enthält, damit es nicht leicht zu erraten ist.

   **Hinweis**
   Ein Kennwort kann nicht wieder abgerufen werden. Sie sollten Sie das zum Schutz des Archivs vergebene Kennwort daher sehr gut merken.

Acronis Cyber Protect Home Office wird Sie jedes Mal nach dem Kennwort fragen, wenn Sie versuchen, das Archiv zu ändern: Um auf das Archiv zugreifen zu können, müssen Sie das richtige Kennwort eingeben.

# Zugriff auf Ihre archivierten Dateien

Wenn Ihre Dateien erfolgreich archiviert sind, können Sie folgendermaßen auf diese zugreifen:

- **Windows Explorer**
  Starten Sie den Windows Explorer und klicken Sie unter Favoriten auf **Acronis Drive**.
  Die Dateien sind im Backup schreibgeschützt, Sie können mit ihnen im Nur-Lesen-Modus arbeiten (z.B. die Dateien anzeigen). Wenn Sie eine Datei richtig bearbeiten (ändern) wollen, müssen Sie diese zuerst in einen anderen Ordner kopieren.
- **Acronis Cloud** (nur für Cloud-Archive gültig)
  Gehen Sie folgendermaßen vor, um die Acronis Cloud-Webapplikation zu öffnen:
  - Starten Sie Acronis Cyber Protect Home Office, klicken Sie auf **Archivieren** und dann auf **In Ihrem Webbrowser anzeigen**.
  - Gehen Sie zu https://www.acronis.com/my/online-backup/webrestore/ und melden Sie sich an Ihrem Konto an.

# Daten freigeben

Sie können die Daten und Ordner, die in den Backups und Archiven vorliegen, die in der Acronis Cloud gespeichert sind, mit anderen Personen teilen bzw. für diese freigeben.

1. Klicken Sie in der Seitenleiste von Acronis Cyber Protect Home Office auf **Konto**.
2. Klicken Sie im Bereich **Acronis Cloud Storage** auf den Befehl **Meine Daten durchsuchen**. Sie werden zur Acronis Cloud-Webseite weitergeleitet.
3. Gehen Sie folgendermaßen vor, je nachdem, was Sie freigeben wollen:
   - Wenn Sie Dateien oder Ordner aus einem Backup freigeben wollen, klicken Sie in der linken Seitenleiste auf **BACKUPS**. Wählen Sie die gewünschte Datei oder den gewünschten Ordner über das entsprechende Kontrollkästchen aus.
   - Wenn Sie Dateien oder Ordner aus einem Archiv freigeben wollen, klicken Sie in der linken Seitenleiste auf **ARCHIVE**. Wählen Sie die gewünschte Datei oder den gewünschten Ordner über das entsprechende Kontrollkästchen aus.
4. Klicken Sie in der Seitenleiste auf **Link teilen**.
5. [Optional] Sie können Freigabe-Optionen konfigurieren. Klicken Sie dafür im entsprechenden Fenster auf **Link-Einstellungen**. Sie können ein Kennwort zuweisen, ein Ablaufdatum festlegen und die Anzahl der Downloads begrenzen.
6. Klicken Sie im Freigabe-Fenster auf den Befehl **Link kopieren** und schließen Sie das Fenster.

Sie können diesen Link jetzt mit anderen Personen teilen. Wenn Sie die freigegebenen Dateien einsehen wollen, müssen Sie in der linken Seitenleiste auf **FREIGEBEN** klicken. Sie können hier jede Datei auswählen und in der rechten Seitenleiste den entsprechenden Link kopieren, die Linkeinstellungen konfigurieren oder diese löschen.

# Die Daten der ganzen Familie sichern

## Was bedeutet 'Data Protection für die ganze Familie'?

'Data Protection für die ganze Familie' ist eine vereinheitlichte, plattformübergreifende Funktionalität, mit der Sie den Schutzstatus aller Computer, Smartphones und Tablets überwachen sowie steuern können, die sich alle zusammen ein gemeinsames Konto teilen. Da die Benutzer dieser Geräte alle am selben Konto angemeldet sein müssen, gehen wir davon aus, dass es sich hierbei üblicherweise um die Mitglieder einer Familie handelt. Grundsätzlich kann jedes Familienmitglied diese Funktion verwenden. Zumeist dürfte aber wohl ein Familienmitglied erfahrener im Umgang mit den entsprechenden modernen Technologien sein als die anderen. Es ist daher vernünftig, diese spezielle Person zum 'Datensicherungsverantwortlichen' bzw. 'Administrator' für die gesamten Familiendaten zu machen.

Sie verwenden das webbasierte Online Dashboard, um den Schutzstatus Ihrer Familiengeräte zu überwachen und zu kontrollieren. Sie können auf das Dashboard von jedem Computer zugreifen, der mit dem Internet verbunden ist. Dank der Webanwendung kann dieser 'Familien-IT-Administrator':

- Die Statuszustände aller Backups auf allen Familiengeräten steuern, die entweder Windows, macOS, iOS oder Android als Betriebssystem verwenden.
- Ein neues Gerät zur Liste hinzufügen.
- Ein beliebiges Backup auf jedem Computer manuell starten.
- Neue Backups jeden Typs (Backup des kompletten Maschine, Datei-Backup, Laufwerk-Backup) auf PCs und Macs erstellen.
- Die Einstellungen von bereits vorhandenen Backups ändern.
- Daten aus jedem in der Acronis Cloud gespeicherten Backup wiederherstellen (inkl. der Backups von PCs, Macs sowie von iOS- und Android-basierten Geräten wie Tablets und Smartphones).
- Einige produktbezogene Probleme lösen.

## Im Online Dashboard ein neues Gerät hinzufügen

Damit Sie alle Vorteile des Online Dashboards – einschließlich der Remote-Verwaltung Ihrer Backups – nutzen können, müssen Sie Ihre Geräte zuerst in die Geräte-Liste aufnehmen.

***So können Sie ein neues Gerät hinzufügen***

1. Installieren Sie Acronis Cyber Protect Home Office auf Ihrem Gerät.
   - Sie können die Installationsdateien für Windows und macOS von der Acronis Website herunterladen.
   - Wenn Sie Acronis Cyber Protect Home Office auf iOS- und Android-Geräten installieren wollen, befolgen Sie die Anweisungen im Abschnitt 'Acronis Cyber Protect Home Officefür

Mobilgeräte installieren'.

2. Starten Sie Acronis Cyber Protect Home Office und melden Sie sich an Ihrem Konto an.

Alternativ können Sie ein Gerät auch über die Benutzeroberfläche des Online Dashboards hinzufügen.

***So können Sie ein neues Gerät über das Online Dashboard hinzufügen***

1. Öffnen Sie auf dem Gerät, welches Sie hinzufügen wollen, das Online Dashboard über die Adresse: https://cloud.acronis.com.
2. Melden Sie sich mit Ihrem Konto an.
3. Klicken Sie in der Registerkarte **Ressourcen** auf den Befehl **Hinzufügen**.
4. Laden Sie Acronis Cyber Protect Home Office herunter und installieren Sie es.
5. Starten Sie Acronis Cyber Protect Home Office und melden Sie sich mit demselben Acronis Konto an.

# Daten aus der Ferne sichern (Remote-Backup)

Mit dem webbasierten Online Dashboard können Sie ein Backup auf jedem Computer (PC oder Mac) konfigurieren und ausführen, der das gleiche Konto verwendet.

***Stellen Sie vor der Backup-Ausführung sicher, dass Sie Zugriff auf den betreffenden Computer haben***

1. Öffnen Sie das Online Dashboard über die Adresse: https://cloud.acronis.com.
2. Melden Sie sich mit Ihrem Konto an.
3. Suchen Sie in der Registerkarte **Ressourcen** denjenigen Computer, dessen Daten Sie per Backup sichern wollen.
   - Falls Sie den Computer nicht finden können, müssen Sie ihn zuerst in die Geräteliste aufnehmen. Installieren Sie dafür Acronis Cyber Protect Home Office auf dem betreffenden Computer, starten Sie die Applikation und melden Sie sich an Ihrem Konto an. Ausführliche Informationen dazu finden Sie im Abschnitt 'Ein neues Gerät hinzufügen'.
   - Sollte der Computer gerade offline sein, dann sorgen Sie dafür, dass er eingeschaltet ist/wird und mit dem Internet verbunden ist.

***So können Sie das erste Backup auf einem Computer erstellen***

1. Öffnen Sie das Online Dashboard und suchen Sie dort nach dem Computer, auf dem die zu sichernden Daten vorliegen.
2. Klicken Sie auf **Backup aktivieren** und konfigurieren Sie anschließend die Einstellungen für das neue Backup, wie etwa:
   - Den Backup-Typ (komplette Maschine, Laufwerk-Backup oder Datei-Backup)
   - Die zu sichernde Daten (Backup-Quelle)
   - Das Backup-Ziel

- Planung
- Die Aufbewahrungsregeln
- Die Datenverschlüsselung

3. Klicken Sie nach Abschluss der Backup-Konfiguration auf **Anwenden** und anschließend auf den Befehl **Jetzt ausführen**.

***So können Sie eine neue Version von einem vorhandenen Backup erstellen:***

1. Öffnen Sie das Online Dashboard und suchen Sie dort nach dem Computer, auf dem die zu sichernden Daten vorliegen.
2. Klicken Sie auf **Backup jetzt** und wählen Sie das zu aktualisierende Backup aus.

***So können Sie die Einstellungen eines vorhandenen Backups ändern:***

1. Öffnen Sie das Online Dashboard und suchen Sie den Computer, von dem das betreffende Backup stammt.
2. Klicken Sie auf das Zahnradsymbol, dann auf **Backup** und suchen Sie dann das Backup, welches Sie rekonfigurieren wollen.
3. Klicken Sie neben dem Backup-Namen auf das Zahnradsymbol – und wählen Sie anschließend einen der nachfolgenden Befehle:
   - Wenn Sie die Haupteinstellungen ändern wollen, klicken Sie auf **Bearbeiten**.
   - Wenn Sie zusätzliche Optionen ändern wollen, klicken Sie auf **Backup-Optionen**.
4. Klicken Sie auf **Änderungen speichern**.

***So können Sie ein neues Backup erstellen***

1. Öffnen Sie das Online Dashboard und suchen Sie dort nach dem Computer, auf dem die zu sichernden Daten vorliegen.
2. Klicken Sie auf das Zahnradsymbol und anschließend auf **Backup**.
3. Klicken Sie auf **Backup-Plan hinzufügen**.
   - Wenn Sie ein Backup mit den vordefinierten Einstellungen erstellen wollen, klicken Sie auf **Anwenden**. Die komplette Maschine wird in die Acronis Cloud gesichert.
   - Wenn Sie ein Backup mit benutzerdefinierten Einstellungen erstellen wollen, klicken Sie zuerst auf **Neu erstellen**. Ändern Sie anschließend die vorgegebenen Einstellungen und klicken Sie dann auf **Anwenden**.
4. Klicken Sie zum Starten des Backups auf **Jetzt ausführen**.

# Daten über das Online Dashboard wiederherstellen

Mit dem webbasierten Online Dashboard können Sie Daten aus jedem Online Backup wiederherstellen, welches von einem Ihrer Familiengeräte (egal ob PCs, Macs, Smartphones oder Tablets) in die Cloud hochgeladen wurde.

***So können Sie Daten aus einem Online Backup wiederherstellen***

1. Öffnen Sie das Online Dashboard über die Adresse: https://cloud.acronis.com.
2. Melden Sie sich mit Ihrem Konto an.
3. Suchen Sie in der Registerkarte **Ressourcen** dasjenige Gerät, das als 'Recovery-Quelle' dienen soll (von dem aus also die gewünschten Daten wiederhergestellt werden sollen). Sollte das Gerät offline sein, dann überprüfen Sie, dass es eingeschaltet und mit dem Internet verbunden ist.
4. Wenn Sie Daten von folgenden Quellen herunterladen wollen:
   - Einem Computer – Klicken Sie auf **Recovery**. Die Acronis Cloud-Webapplikation wird geöffnet, wo Sie Ihre Daten durchsuchen und wiederherstellen können.
   - Einem Mobilgerät – Klicken Sie auf **Recovery**. Wählen Sie im linken Fensterbereich das gewünschte Backup anhand des jeweiligen Backup-Zeitpunkts aus. Wählen Sie im rechten Fensterbereich die wiederherzustellenden Elemente aus und klicken Sie dann auf **Download**.

# E-Mail-Benachrichtigungen

Manchmal kann eine Backup-Aktion eine längere Zeit in Anspruch nehmen. Um den Status Ihrer Backups und deren Fertigstellung zu verfolgen, können Sie E-Mail-Benachrichtigungen über das Online Dashboard konfigurieren.

***So können Sie die E-Mail-Benachrichtigungen konfigurieren***

1. Öffnen Sie die E-Mail-Benachrichtigungen auf dem Online Dashboard. Sie können dies auf zwei Arten tun:
   - Klicken Sie im Online Dashboard auf das Symbol für 'Konto' (in der rechten oberen Ecke) und wählen Sie **E-Mail-Benachrichtigungen**.
   - Klicken Sie in Ihrer Acronis Cyber Protect Home Office-Applikation auf **Einstellungen** und anschließend auf **Einstellungen für die E-Mail-Benachrichtigung ändern**.
2. Wählen Sie bei **Benachrichtigungen zu folgenden Ereignissen senden** diejenigen Informationen, die Sie interessieren:
   - Fehler
   - Warnungen
   - Erfolgreiche Backups
3. Geben Sie im Feld **E-Mail-Adressen der Empfänger** die Ziel-Adresse(n) ein. Sie können auch mehrere Adressen eingeben, müssen diese aber je per Semikolon trennen.
4. [Optional] Ändern Sie bei **Betreff** den Inhalt der Betreffzeile für die E-Mail-Benachrichtigungen. Sie können dafür folgende Variablen verwenden:
   - [computer_name] – Name des Computers
   - [operation_status] – Status, mit dem die Aktion abgeschlossen wurde
   - [backup_name] – Name des Backups

   Die Standardbetreffzeile ist: [computer_name] - [operation_status] - [backup_name].

Nach dem Speichern der Einstellungen werden Ihnen von den Acronis Servern entsprechende Informationen über alle Backups von all Ihren Familiengeräten zugesendet, die unter Windows und macOS laufen.

# Schutz

Acronis Cyber Protect Home Office bietet folgende Schutzfunktionen für Ihre Daten:

- Active Protection wird kontinuierlich im Hintergrund ausgeführt, um Ihre Maschinen in Echtzeit zu schützen, während Sie wie gewohnt arbeiten können.
- Antivirus-Scans werden bei Bedarf („On-Demand“) ausgeführt, um eine gründliche Suche nach Schadsoftware im gesamten System durchzuführen.
- Die Schwachstellenbewertung ist ein täglicher, im Hintergrund ausgeführter Scan, der Schwachstellen (wie Sicherheitslücken) in Ihrem System und Ihren Applikationen erkennen kann und dann deren Schweregrad bewerten.

**Hinweis**
Sie können den Schutz nur über die Benutzeroberfläche von Acronis Cyber Protect Home Office ein- bzw. ausschalten. Es ist dagegen nicht möglich, den Prozess manuell, über den Task Manager oder ein anderes, externes Tool zu stoppen.

Wenn Sie über eine Lizenz verfügen, bei der die Active Protection-Funktionalität enthalten ist, die entsprechende Komponente aber noch nicht installiert wurde, so können Sie diese auch nachträglich noch hinzufügen. Weitere Informationen dazu finden Sie im Abschnitt '"Active Protection konfigurieren" (S. 177)'.

Wenn Sie über eine Lizenz verfügen, bei der die Funktionalitäten Echtzeitschutz, Antivirus-Scans, Schutz für Videokonferenzen und Webfilterung enthalten sind, die entsprechende Komponenten aber noch nicht installiert wurden, so können Sie diese auch nachträglich noch hinzufügen. Weitere Informationen dazu finden Sie im Abschnitt '"Active Protection konfigurieren" (S. 177)'.

## Das Protection Dashboard

Das Protection Dashboard enthält statistische Daten über die **Active Protection**-, **Antivirus-Scan**- sowie **Schwachstellenbewertungs**-Prozesse und ermöglicht die Kontrolle über den Schutzstatus sowie den Zugriff auf die Schutzeinstellungen.

Wenn Sie auf das Protection Dashboard zugreifen wollen, klicken Sie in der Seitenleiste von auf **Schutz**.

In der Registerkarte **Überblick** des Dashboards können Sie Folgendes tun:

- Installieren Sie die fehlenden Schutzkomponenten. Klicken Sie dafür auf **Installieren** und befolgen Sie die Anweisungen auf dem Bildschirm.
- Statistiken über den aktiven Schutzstatus einsehen.
- Die Anzahl der erkannten Probleme, der unter Quarantäne gestellten Elemente und der Schutz-Ausschlüsse einsehen.
- Den letzten Bericht über den **Antivirus-Scan** einsehen. Wenn Sie diesen einsehen wollen, klicken Sie auf **Scan-Bericht**.

- Die nächste geplante Scanzeit einsehen.
- Manuell einen schnellen oder vollständigen **Antivirus-Scan** durchführen.Klicken Sie dafür entweder auf den Befehl **Vollständigen Scan ausführen** oder **Schnellscan ausführen**.
- Den jüngsten Bericht über erkannte Schwachstellen einsehen und einen neuen Scan ausführen. Wenn Sie diesen einsehen wollen, klicken Sie auf **Erkannte Schwachstellen**.
- Den gesamten Schutz für eine vordefinierte Zeitspanne (30 Minuten, 1 Stunde, 4 Stunden, bis zum Neustart) stoppen. Klicken Sie dafür auf **Schutz ausschalten** und wählen Sie den gewünschten Zeitraum aus.

**Hinweis**
Wenn Sie den Schutz ausschalten, deaktivieren Sie die Active Protection-Funktionalität. Geplante On-Demand-Scans werden nicht mehr gestartet.

Auf der Registerkarte **Aktivität** des Dashboards können Sie ein Protokoll derjenigen Änderungen einsehen, die Sie an Ihrem Schutzstatus und Ihren Einstellungen vorgenommen haben.

# Active Protection

Acronis Cyber Protect Home Office verwendet die Acronis Active Protection-Technologie, um Ihre Dateien vor Schadsoftware in Echtzeit zu schützen.

Active Protection überprüft Ihren Computer, während Sie wie gewohnt weiterarbeiten können. Zusätzlich zu Ihren Dateien schützt Acronis Active Protection außerdem die Applikationsdateien von Acronis Cyber Protect Home Office, Ihre Backups sowie die MBRs (Master Boot Records) Ihrer Festplattenlaufwerke.

Active Protection besteht aus mehreren Schutzstufen, die Sie unabhängig voneinander aktivieren können:

- Anti-Ransomware Protection
- Echtzeitschutz
- Webfilter

## Anti-Ransomware Protection

Ransomware verschlüsselt Dateien und verlangt ein Lösegeld für die Bereitstellung des Codierungsschlüssels. Cryptomining-Malware führt mathematische Berechnungen im Hintergrund durch, um digitale Crypto-Währungen zu 'schürfen', und stiehlt auf diese Weise Rechenleistung und Netzwerkressourcen von Ihrer Maschine.

Wenn der **Antiransomware Protection** Service eingeschaltet ist, überwacht er in Echtzeit die auf Ihrem Computer laufenden Prozesse. Wenn der Service erkennt, dass ein fremder Prozess versucht, Ihre Dateien zu verschlüsseln oder Ihren Computer zum Krypto-Mining zu verwenden (digitales Schürfen von Krypto-Währungen), werden Sie vom Service informiert und gefragt, ob der Prozess seine Aktivität fortsetzen darf oder Sie ihn blockieren möchten.

Klicken Sie auf **Vertrauen**, wenn Sie dem Prozess erlauben wollen, seine Aktivität fortzusetzen. Falls Sie sich nicht sicher sind, ob der Prozess sicher und zulässig ist, empfehlen wir, auf **Quarantäne** zu klicken. Danach wird der Prozess in die **Quarantäne** verschoben und jede seiner Aktivitäten blockiert.

Sollten Sie einen Prozess blockiert haben, so empfehlen wir, dass Sie anschließend Ihre Dateien darauf überprüfen, ob diese verschlüsselt oder irgendwie beschädigt wurden. Wenn sie das tatsächlich sind, können Sie auf **Geänderte Dateien wiederherstellen** klicken. Acronis Cyber Protect Home Office wird die nachfolgenden Speicherorte nach den neuesten Dateiversionen zur Wiederherstellung durchsuchen.

- Temporärer Dateikopien, die zuvor bei der Prozess-Verifizierung erstellt wurden
- Lokale Backups
- Cloud Backups

Wenn Acronis Cyber Protect Home Office eine gute temporäre Kopie findet, wird die ursprüngliche Datei mithilfe dieser Kopie wiederhergestellt. Wenn die temporäre Dateikopien für die Wiederherstellung nicht geeignet sein sollten, sucht Acronis Cyber Protect Home Office lokal und in der Cloud nach Backup-Kopien, vergleicht die Erstellungszeiten der an beiden Orten gefundenen Kopien und wird dann Ihre Datei von der letzten verfügbaren, unbeschädigten Kopie wiederherstellen.

**Hinweis**
Acronis Cyber Protect Home Office unterstützt keine Dateiwiederherstellung aus kennwortgeschützten Backups.

Wenn Sie Acronis Cyber Protect Home Office so konfigurieren wollen, dass Dateien nach dem Blockieren eines Prozesses automatisch wiederhergestellt werden, müssen Sie das Kontrollkästchen **Dateien automatisch wiederherstellen, wenn ein Prozess blockiert wurde** in den Active Protection-Einstellungen aktivieren. Siehe den Abschnitt 'Active Protection konfigurieren'.

## Echtzeitschutz

Wenn der **Echtzeitschutz** aktiviert ist, überprüft dieser kontinuierlich alle Dateien, mit denen Sie interagieren, um Ihre Maschine in Echtzeit vor verdächtigen Aktivitäten, Viren und anderen bösartigen Bedrohungen zu schützen.

Der Echtzeitschutz umfasst folgende zusätzliche Schutzoptionen:

- Verhaltensanalyse – Active Protection verwendet eine verhaltensbasierte Heuristik, um bösartige Prozesse zu erkennen. Die Funktion vergleicht die von einem Prozess ausgeführten Aktionsketten (z.B. Ereignisse im Dateisystem) mit Aktionsketten, die in einer Referenzdatenbank mit bekannten schädlichen Verhaltensmustern gespeichert sind. Mit diesem Ansatz kann Active Protection auch neue (bisher unbekannte) Malware anhand typischer Verhaltensmuster als Schadsoftware erkennen.

- Exploit-Prävention – Active Protection analysiert das Verhalten aller Prozesse, die auf einer Maschine laufen, und erkennt dabei nicht ordnungsgemäße Aktivitäten. Die Funktion verhindert, dass sich infizierte Prozesse ausbreiten und die Schwachstellen/Sicherheitslücken von anderen Programmen ausnutzen, die auf dem System installiert sind. Active Protection verwendet mehrere Methoden zur Exploit-Prävention:
  - Die Memory Protection erkennt und verhindert verdächtige Modifikationen der Ausführungsrechte von Arbeitsspeicherseiten (Memory Pages). Solche Modifikationen der Speicherseiten-Eigenschaften werden von schädlichen Prozessen vorgenommen, um die Ausführung von Shellcodes aus nicht ausführbaren Speicherbereichen (wie „Stack“ und „Heaps“) zu ermöglichen.
  - Die Privilege Escalation Protection erkennt und verhindert Versuche zur „Rechteausweitung“ (auch Privilegien-Erweiterung oder -Eskalation genannt), die von einem nicht autorisierten Code oder einer nicht autorisierten Applikation unternommen werden. Rechteausweitungstechniken werden von bösartigen Software-Codes verwendet, um vollen Zugriff auf eine angegriffene Maschine zu erhalten und dort dann kritische und sensible Tasks auszuführen. Nicht autorisierter Code darf normalerweise nicht auf kritische Systemressourcen zugreifen oder Systemeinstellungen ändern.
  - Die Code Injection Protection erkennt und verhindert, dass bösartiger Software-Code in Remote-Prozesse eingeschleust („injiziert“) wird. Code-Injektion-Techniken werden verwendet, um die böswillige Absicht einer Applikation hinter vermeintlich sauberen oder ungefährlichen Prozessen zu verbergen, um so der Erkennung durch Antimalware-Produkte zu entgehen.

Für Sie können folgende Scanning-Varianten wählen:

- Eine Erkennung **Bei Zugriff (intelligent)** (Smart On-Access Detection) bedeutet, dass das Programm im Hintergrund läuft und dabei das System Ihrer Maschine aktiv und kontinuierlich auf Viren und andere bösartige Bedrohungen scannt. Dies erfolgt während gesamten Betriebszeit Ihres Systems. Malware wird sowohl bei der Ausführung einer Datei als auch bei verschiedenen Aktionen mit einer Datei (etwa, wenn diese zum Lesen/Bearbeiten geöffnet wird) erkannt.
- Eine Erkennung **bei Ausführung** (On-Execution Detection) bedeutet, dass nur ausführbare Dateien gescannt werden – und zwar im Augenblick ihrer Ausführung. So wird sichergestellt, dass diese Dateien sauber sind und Ihre Maschine oder deren Daten nicht beschädigen können. Das Kopieren einer infizierten Datei wird jedoch nicht erkannt.

Sie können die Ergebnisse der Echtzeitschutz-Prüfungen auf der Registerkarte **Aktivität** des Protection Dashboard einsehen.

## Webfilter

Malware wird häufig über bösartige oder infizierte Websites verbreitet und verwendet dafür eine Angriffsmethode, die auch Drive-by-Download-Infektion genannt wird.

Die Webfilterung ermöglicht Ihnen, sich vor potenziell schädlichen Websites und nicht vertrauenswürdigen Webressourcen zu schützen. Dafür wird der Zugriff auf die entsprechenden Websites blockiert, wenn Sie versuchen, diese zu öffnen. Um festzustellen, welche Websites

möglicherweise schädlich sind, verwendet die Webfilterung die Schutz-Update-Datenbank. Die Webfilter-Datenbank enthält auch Informationen über Websites, die Scam- und Phishing-URLs enthalten. Sie können die in dieser Datenbank definierten Regeln ändern, indem Sie Ausnahmen für die Webfilterliste konfigurieren.

Die Webfilterung hat zwei Betriebsmodi:

- **Vollständig blockieren** – der Zugriff auf die Website wird komplett gesperrt.
- **Nur benachrichtigen** – es wird eine Benachrichtigung angezeigt, aber die Benutzer können dennoch auf die Website zugreifen.

## Active Protection konfigurieren

***So können Sie auf die Active Protection-Einstellungen zugreifen***

1. Klicken Sie zuerst in der Seitenleiste auf **Schutz**, dann auf **Einstellungen** und gehen Sie anschließend zur Registerkarte **Active Protection**.
2. [Optionaler Schritt] Wenn die Active Protection-Funktionalität noch nicht installiert ist, klicken Sie unter **Active Protection und Antivirus-Scan abrufen** auf **Installieren** und befolgen Sie die Anweisungen auf dem Bildschirm.

***So können Sie die Antiransomware Protection konfigurieren***

1. Aktivieren Sie den Schalter für **Antiransomware Protection**, um die Antiransomware Protection-Funktionalität zu aktivieren.
   Sobald der Schalter aktiviert wurde, schützt die Funktion Ihren Computer vor potenziell schädlichen Applikationen und Hintergrund-Prozessen.
2. Wählen Sie die Optionen, die Sie aktivieren wollen.
   - **Dateien nach Blockieren eines Prozesses automatisch wiederherstellen** – Auch wenn Sie einen Prozess blockiert haben, besteht die Möglichkeit, dass Ihre Dateien geändert wurden. Wenn dieses Kontrollkästchen aktiviert ist, stellt Acronis Cyber Protect Home Office die Dateien folgendermaßen wieder her.
     Acronis Cyber Protect Home Office durchsucht die nachfolgenden Speicherorte nach den neuesten Dateiversionen zur Wiederherstellung.
     - Temporärer Dateikopien, die zuvor bei der Prozess-Verifizierung erstellt wurden
     - Lokale Backups
     - Cloud Backups

     Wenn Acronis Cyber Protect Home Office eine gute temporäre Kopie findet, wird die ursprüngliche Datei mithilfe dieser Kopie wiederhergestellt. Wenn die temporäre Dateikopien für die Wiederherstellung nicht geeignet sein sollten, sucht Acronis Cyber Protect Home Office lokal und in der Cloud nach Backup-Kopien, vergleicht die Erstellungszeiten der an beiden Orten gefundenen Kopien und wird dann Ihre Datei von der letzten verfügbaren, unveränderte Kopie wiederherstellen.

**Hinweis**
Acronis Cyber Protect Home Office unterstützt keine Dateiwiederherstellung aus kennwortgeschützten Backups.

- **Backup-Dateien vor Ransomware schützen** – Wenn diese Option aktiviert ist, wird Acronis Cyber Protect Home Office seine eigenen Prozesse sowie Ihre Backups vor Ransomware schützen. Auch Ihre Archive werden geschützt.
- **Netzwerkfreigaben und NAS-Geräte schützen** – Acronis Cyber Protect Home Office wird die Netzwerkfreigaben und NAS-Geräte überwachen, auf die Sie zugreifen können. Sie können auch einen Speicherort spezifizieren, wo solche Dateien wiederhergestellt werden, die durch einen Ransomware-Angriff betroffen wurden.
- **Schützen Sie Ihren Computer vor illegalem Cryptomining** – Aktivieren Sie dieses Kontrollkästchen, um Ihren Computer vor Cryptomining-Malware zu schützen.

3. Klicken Sie auf **OK**.

***So können Sie den Echtzeitschutz konfigurieren***

1. [Optionaler Schritt] Wenn die Echtzeitschutz-Funktionalität noch nicht installiert ist, klicken Sie unter **Vollständigen Schutz abrufen** auf **Installieren** und befolgen Sie die Anweisungen auf dem Bildschirm.
2. Aktivieren Sie den Schalter für **Echtzeitschutz**, um Real-time Protection-Funktion einzuschalten. Wenn die Funktion aktiviert wird, überprüft der Echtzeitschutz alle Dateien, mit denen Sie interagieren, auf Malware.
3. Wählen Sie aus, wann die Dateien überprüft werden sollen.
   - **Bei Zugriff (intelligent)** – alle Systemaktivitäten werden überwacht und die Dateien werden gescannt, sobald Sie auf diese zugreifen.
   - **Bei Ausführung** – es werden nur ausführbare Dateien gescannt – und zwar, wenn diese gestartet werden. Dadurch wird sichergestellt, dass diese Dateien Ihre Maschine nicht beschädigen können.
4. Wählen Sie aus dem Listenfeld aus, was mit den erkannten Objekten geschehen soll.
   - **Blockieren und benachrichtigen** – Der Prozess, bei dem der Verdacht auf Malware-Aktivität besteht, wird blockiert und Sie erhalten eine Benachrichtigung darüber.
   - **Quarantäne** – Der Prozess, bei dem der Verdacht auf Malware-Aktivität besteht, wird blockiert und die ausführbare Datei wird in den Quarantäne-Ordner verschoben.
5. Aktivieren Sie die zusätzlichen Schutzoptionen.
   - **Schädliche Verhaltensmuster in Prozessen erkennen** – ermöglicht Active Protection, auch neue (bisher unbekannte) Malware anhand typischer Verhaltensmuster als Schadsoftware zu erkennen und zu blockieren.
   - **Erkennen und verhindern, dass bösartige Prozesse vorhandene Software-Schwachstellen in einem System ausnutzen (experimentell)** – ermöglicht es der Active Protection, Prozesse zu erkennen und zu blockieren, die versuchen, die Sicherheitslücken und Schwachstellen anderer Prozesse auf dem System auszunutzen.

**Hinweis**
Alle erkannten Objekte werden sofort blockiert. Sie werden weder in die Quarantäne verschoben noch in die Liste der erkannten Probleme aufgenommen.

***So können Sie die Webfilterung konfigurieren***

1. [Optionaler Schritt] Wenn die Webfilterungsfunktionalität noch nicht installiert ist, klicken Sie unter **Vollständigen Schutz abrufen** auf **Installieren** und befolgen Sie die Anweisungen auf dem Bildschirm.
2. Aktivieren Sie den Schalter **Webfilterung**, um sich vor potenziell schädlichen Websites und nicht vertrauenswürdigen Webressourcen zu schützen.
3. Wählen Sie im Listenfeld (Dropdown-Menü) **Aktion bei Erkennung einer schädlichen URL** was mit erkannten schädlichen URLs passieren soll.
   - **Vollständig blockieren** – Der Zugriff auf die Website wird komplett gesperrt.
   - **Blockieren und benachrichtigen** – Die Website wird blockiert, aber Sie haben die Möglichkeit, mit dem Aufrufen fortzufahren.
4. Wenn Sie die Liste der als vertrauenswürdig eingestuften oder blockierten Websites konfigurieren wollen, klicken Sie auf **Ausnahmen verwalten**.
   a. Wenn Sie der Liste eine neue URL hinzufügen wollen, klicken Sie auf **URL hinzufügen**.
   b. Geben Sie einen gültigen URL-Namen ein. Deren Domain wird zu den Ausnahmen hinzugefügt.

      **Hinweis**
      Alle Adressen aus der Domain, die Sie eingegeben haben, werden als vertrauenswürdig oder blockiert (gesperrt) behandelt. Wenn Sie z.B. 'xyz.com' als vertrauenswürdige Domain eingegeben haben, werden auch alle Pfade bzw. Subdomains unterhalb von xyz.com als vertrauenswürdig behandelt.

   c. Wählen Sie im Listenfeld **Erlaubt** oder **Blockiert**. Die erlaubten Websites werden nicht nach Bedrohungen gescannt. Die geblockten Websites werden nicht geöffnet oder Sie werden benachrichtigt, wenn ein entsprechender Versuch erfolgt.
   d. Klicken Sie auf **URL hinzufügen**.
   e. Klicken Sie auf **Anwenden**.

# Antivirus-Scans

Die **Antivirus-Scan**-Funktionalität ist eine der Komponenten der Acronis Cyber Protect Home Office Antivirus & Antimalware Protection. Sie schützt Ihren Computer, indem sie bei Bedarf („On-Demand“) nach Malware sucht – manuell oder in vordefinierten Zeitintervallen, die Sie konfigurieren können.

Sie können zwischen zwei Scan-Varianten wählen.

- Ein **Vollständiger** Scan durchsucht die komplette Maschine nach Viren. Ein vollständiger Scan erkennt Malware, indem alle Dateien und Prozesse (oder eine Teilmenge von diesen) untersucht werden – mit Ausnahme solcher Dateien oder Ordner, die Sie in Form von Ausschlusslisten definieren können.
- Ein **Schnellscan** untersucht nur bestimmte Dateien und Ordner. Ein Schnellscan erkennt Malware, indem er bestimmte Ordner untersucht, die als gängige Speicherorte für Viren bekannt sind.

Sie können auch bestimmen, was gescannt werden soll: Archivdateien, externe Laufwerke oder nur neue sowie geänderte Dateien.

**Hinweis**
Sie können Acronis Cyber Protect Home Office so konfigurieren, dass Ihr Computer nicht in den Standby- oder Ruhezustandsmodus wechselt, wenn eine Scan-Aktion läuft. Beachten Sie, dass diese Option standardmäßig aktiviert ist.

Die Priorität eines Antivirus-Scans wird standardmäßig herabgesetzt, wenn es während seiner Ausführung zu einer hohen CPU-Last kommt, damit alle anderen Applikationen ungestört weiterarbeiten können. Dies kann jedoch wiederum die Scan-Geschwindigkeit herabsetzen. Sie können diese Option aber auch deaktivieren, wenn Sie das Scannen unter diesen Umständen beschleunigen wollen.

Wenn Sie das Fenster **Scan-Details-Bericht** mit ausführlichen Informationen zum Antivirus-Scan einsehen wollen, klicken Sie auf die Schaltfläche **Scan-Bericht**.

## Antivirus-Scans konfigurieren

Wenn Sie auf die **Antivirus**-Einstellungen zugreifen wollen, müssen Sie zuerst in der Seitenleiste auf **Schutz** klicken, dann auf **Einstellungen** und anschließend zur Registerkarte **Antivirus** gehen.

***So können Sie die 'Aktion bei Erkennung' konfigurieren:***

Wählen Sie die Optionen, die Sie aktivieren wollen.

- **Quarantäne** – Diese Option ist standardmäßig festgelegt. Wenn Acronis Cyber Protect Home Office eine potenzielle Malware-Bedrohung erkennt, stoppt es den entsprechenden Prozess und verschiebt dann die verdächtige Datei in den Quarantäne-Ordner.
- **Nur benachrichtigen** – Wenn ein verdächtiger Prozess erkannt wird, erhalten Sie eine Benachrichtigung über die potenzielle Malware-Bedrohung.

***So können Sie den Scan-Typ konfigurieren:***

Bestimmen Sie, auf welche Weise der Scan durchgeführt werden soll:

- **Vollständig** – Diese Option ist standardmäßig festgelegt. Acronis Cyber Protect Home Office wird den kompletten PC überprüfen.
- **Schnell** – Acronis Cyber Protect Home Office wird nur solche Ordner prüfen, die als gängige Speicherorte für Bedrohungen gelten.

***So können Sie eine Planung für die Antivirus-Scans festlegen:***

Aktivieren Sie eines passenden Kontrollkästchen, um den Zeitpunkt zu konfigurieren, an dem der Scan-Prozess gestartet werden soll.

- **Täglich** – der Scan wird jeden Tag am spezifizierten Zeitpunkt durchgeführt.
- **Wöchentlich** – der Scan wird an einem bestimmten Wochentag ausgeführt. Legen Sie den gewünschten Wochentag und die Uhrzeit fest.
- **Monatlich** – der Scan wird an einem bestimmten Tag des Monats ausgeführt.
- **Beim Systemstart** – der Scan wird bei jedem Start Ihres Betriebssystems ausgeführt.
- **Ohne Planung** – für die Scan-Ausführung wird kein bestimmter Zeitpunkt geplant.

***So können Sie konfigurieren, was gescannt werden soll:***

Aktivieren Sie die folgenden Kontrollkästchen:

- **Keine Archivdateien scannen, die größer sind als**. Wählen Sie mithilfe der Pfeile einen Wert aus.
- **Externe Laufwerke scannen**
- **Netzwerkfreigaben und NAS-Geräte scannen**
- **Nur neue und geänderte Dateien scannen**

***So können Sie das Systemverhalten während der Antivirus-Scans konfigurieren:***

Manchmal kann es vorkommen, dass das System heruntergefahren wird, bevor ein Antivirus-Scan abgeschlossen wurde. Aktivieren Sie für solche Fälle das Kontrollkästchen **Verpasste Tasks bei Neustart ausführen**, um Acronis Cyber Protect Home Office so zu konfigurieren, dass der Scan wieder aufgenommen wird, wenn das System neu gestartet wurde.

Sie können außerdem die Option **Standby- oder Ruhezustandsmodus verhindern** aktivieren, wenn Sie verhindern wollen, dass Ihr Computer während einer Scan-Ausführung zum Energiesparen heruntergefahren wird.

Für den Fall, dass die CPU bei einem Scan mal überlastet sein sollte, kann zudem die Priorität der Antivirus-Scans heruntergestuft werden, damit andere Applikationen in so einer Situation weiter korrekt arbeiten können. Diese Option ist standardmäßig aktiviert, was Scanvorgänge jedoch verlangsamen kann. Wenn Sie die Scans in solchen Situationen beschleunigen wollen, müssen Sie das Kontrollkästchen **Anderen Applikationen Priorität geben** deaktivieren.

Klicken Sie nach der Konfiguration der Antivirus-Scans auf **OK**.

# Schwachstellenbewertung

Die Schwachstellenbewertung ist eine (von mehreren) Komponenten der Acronis Cyber Protect Home Office Antivirus & Antimalware Protection. Es handelt sich um einen täglichen, im Hintergrund ausgeführten Scan, der Schwachstellen (wie Sicherheitslücken) in Ihrem System und

Ihren Applikationen erkennen kann und dann deren Schweregrad bewerten. Sie können den Scan bei Bedarf auch manuell ausführen.

**Hinweis**
Um die Schwachstellendatenbank aktualisieren zu können, ist eine stabile Internetverbindung erforderlich.

***So können Sie sich die Schwachstellen anzeigen lassen:***

1. Klicken Sie in der linken Seitenleiste auf **SCHUTZ**.
2. Klicken Sie in der Registerkarte **Überblick** unter **Schwachstellenbewertung** auf **Erkannte Schwachstellen**. Der entsprechende Bericht wird angezeigt.
3. Wenn Sie einen neuen Scan ausführen wollen, müssen Sie auf **Scan ausführen** klicken.
4. [optional] Wenn Sie das Fenster **Ausführliche Informationen** einsehen wollen, klicken Sie auf das Info-Symbol neben dem Namen der Schwachstelle.
5. [optional] Wenn Sie eine ausführliche Beschreibung der Schwachstelle einsehen wollen, klicken Sie neben dem Namen der betreffenden Schwachstelle auf den Pfeil. Es wird eine Webseite mit den entsprechenden Informationen angezeigt.
6. Wenn Sie die erkannten Probleme beheben wollen, müssen Sie die neuesten Updates für die betroffenen Applikationen installieren. Danach sollten Sie einen erneuten Scan durchführen, um zu überprüfen, dass die Schwachstellen auch wirklich behoben wurden. Wenn diese weiterhin bestehen, bedeutet dies, dass Ihr System immer noch durch einige Applikationen gefährdet ist. Wenn Sie Ihre Daten umfassend schützen wollen, sollten Sie das Betriebssystem per Backup sichern und die Antimalware Protection einschalten.

***So können Sie die Schwachstellenbewertung konfigurieren:***

1. Klicken Sie in der linken Seitenleiste auf **SCHUTZ** und anschließend auf **Einstellungen**.
2. Gehen Sie zur Registerkarte **Schwachstellenbewertung** und verwenden Sie den entsprechenden Schalter, um den Schwachstellen-Scan je nach Bedarf zu aktivieren oder zu deaktivieren.

# Erkannte Probleme verwalten

Wenn die Antivirus-Scans so konfiguriert sind, dass als 'Aktion bei Erkennung' **Blockieren und benachrichtigen** ausgewählt wurde, wird eine Liste mit erkannten Problemen erstellt. Sie sollten diese Liste regelmäßig überprüfen und entscheiden, ob Sie den erkannten Elementen vertrauen wollen oder diese in die Quarantäne verschieben wollen.

***So können Sie die erkannten Probleme überprüfen und verwalten:***

1. Sie können auf zwei Arten auf die gefundenen Probleme zugreifen:
   - Klicken Sie im **Protection** Dashboard auf **Erkannte Probleme**.
   - Klicken Sie zuerst im **Protection** Dashboard auf **Einstellungen** und gehen Sie dann zur Registerkarte **Erweitert**.

a. [Optionaler Schritt] Falls die Komponente für Echtzeitschutz, Antivirus-Scans, Videokonferenz-Schutz und Webfilterung noch fehlt, klicken Sie auf **Installieren** und befolgen Sie dann die Anweisungen auf dem Bildschirm.
b. Klicken Sie unter **Erkannte Probleme** auf den Befehl **Verwalten**.

2. Aktivieren Sie das Kontrollkästchen eines Problems in der Liste und wählen Sie aus, wie dieses behandelt werden soll.
   - Wenn Sie die Datei oder den Prozess in die Liste der 'Ausschlüsse für den Schutz' aufnehmen wollen, klicken auf **Vertrauen**.

     **Hinweis**
     Wenn Sie entschließen, dass eine Datei/ein Prozess vertrauenswürdig ist, wird diese/dieser von zukünftigen Antivirus-Scans ausgeschlossen.

   - Wenn Sie eine Datei oder einen Prozess unter Quarantäne stellen wollen, klicken Sie auf **Quarantäne**.
3. Klicken Sie auf **Schließen**.

# In Quarantäne befindliche Dateien verwalten

Auf Basis Ihrer Einstellungen können die Active Protection-Funktion und die Antivirus-Scans blockierte Dateien unter Quarantäne stellen. Die Quarantäne ist ein spezieller Speicherort, der verwendet wird, um infizierte oder verdächtige Applikationen gegenüber Ihrem Computer und seinen Daten zu isolieren. Indem Sie eine Applikationsdatei unter Quarantäne stellen, senken Sie das Risiko, dass die derartig blockierte Applikation noch potenziell schädliche Aktionen ausführen kann.

Standardmäßig werden die entsprechenden Dateien für 30 Tage in Quarantäne gehalten und dann von Ihrem PC gelöscht. Sie können sich die Dateien in der Quarantäne anzeigen lassen und entscheiden, ob Sie diese doch auf dem Computer behalten oder schon vor Ablauf der vorgegebenen Frist löschen wollen. Sie können zudem den Standardzeitraum ändern, den die entsprechenden Dateien in der Quarantäne aufbewahrt werden.

***So können Sie Dateien aus der Quarantäne wiederherstellen oder stattdessen löschen:***

1. Klicken Sie im **Protection** Dashboard auf **Quarantäne**.
2. Wählen Sie ein Element in der Quarantäne-Liste aus.
   - Klicken Sie auf **Wiederherstellen**, wenn das Element wieder zurück zu seinem ursprünglichen Speicherort verschoben werden soll.
   - Klicken Sie auf **Vom PC löschen**, wenn das Element dauerhaft gelöscht werden soll.
3. Klicken Sie auf **Schließen**.

***So können Sie den Zeitraum festlegen, nach dem die Dateien automatisch aus der Quarantäne gelöscht werden sollen:***

1. Klicken Sie im **Protection** Dashboard auf **Einstellungen** und anschließend auf die Registerkarte **Erweitert**.
2. Bestimmen Sie im Bereich **Quarantäne** die Anzahl der Tage, die die Elemente in Quarantäne aufbewahrt bleiben sollen.
3. Klicken Sie auf **OK**.

# Schutz-Ausschlüsse konfigurieren

Die Active Protection-Funktion und Antivirus-Scans verwenden Definitionen aus der Schutzdatenbank, um potenzielle Bedrohungen zu erkennen. Wenn Sie bestimmten Ausführungsdateien und Ordnern vertrauen wollen, können Sie diese in eine Liste von Schutz-Ausschlüssen aufnehmen, damit Acronis Cyber Protect Home Office diese Dateien/Ordner beim Scannen überspringt.

**Hinweis**
Wenn die Komponente für Echtzeitschutz, Antivirus-Scans, Videokonferenz-Schutz und Webfilterung noch nicht installiert ist, können Sie nur ausführbare Dateien zu den Schutz-Ausschlüssen hinzufügen, jedoch keine Ordner.

Nachdem Sie diese Komponente installiert haben, werden die vorhandenen Active Protection-Ausschlüsse auch auf die Antivirus-Scans angewendet.

***So können Sie Dateien oder Ordner in die Liste der Schutz-Ausschlüsse aufnehmen***

1. Klicken Sie im **Protection** Dashboard auf **Schutz-Ausschlüsse**.
2. Wählen Sie im Menü **Ausschluss hinzufügen** aus, welches Element Sie ausschließen wollen.
   - **Datei hinzufügen** – verwenden Sie diesen Befehl, um ausführbare oder andere Dateien vom Scannen und der Active Protection-Funktionalität auszuschließen.
   - **Ordner hinzufügen** – [optional, falls die Komponente für Echtzeitschutz, Antivirus-Scans, Videokonferenz-Schutz und Webfilterung nicht installiert ist] verwenden Sie diesen Befehl, um Ordner vom Scannen und der Active Protection-Funktionalität auszuschließen.
3. Durchsuchen Sie das Dateisystem nach dem auszuschließenden Element und klicken Sie dann auf **Öffnen**.
4. Sie können entweder noch ein anderes Element in die Ausschlussliste aufnehmen oder dann auf **Speichern** klicken, damit die Liste aktualisiert wird.

***So können Sie Dateien oder Ordner wieder aus der Liste der Schutz-Ausschlüsse entfernen***

1. Klicken Sie im **Protection** Dashboard auf **Schutz-Ausschlüsse**.
2. Aktivieren Sie in der Ausschlussliste das/die Kontrollkästchen für das/die Element(e), welche(s) Sie aus der Liste löschen wollen und klicken Sie dann auf **Entfernen**.
3. Wählen Sie **Speichern**, damit die Liste aktualisiert wird.

Wie Sie die Ausschlussliste für die Webfilterung konfigurieren können, finden Sie im Abschnitt Active Protection konfigurieren.

# Schutz für Videokonferenz-Applikationen

Die Applikationen Zoom, Cisco Webex Meetings und Microsoft Teams werden häufig für Webkonferenzen bzw. zur Kommunikation verwendet. Die Antiransomware-Funktion von Acronis Cyber Protect Home Office kann diese sogenannten Kollaborationsapplikationen standardmäßig durch diese Funktionen schützen.

- Applikationsprozesse vor Schadcode-Einschleusung schützen
- Verdächtige Aktionen durch Applikationsprozesse verhindern

# Schutz-Updates herunterladen

Acronis Cyber Protect Home Office lädt die Schutz-Updates standardmäßig automatisch herunter. Sie können den Status der Schutz-Datenbanken und -Komponenten entweder manuell überprüfen oder den automatischen Download der Schutz-Updates deaktivieren.

***So können Sie den Status der Schutz-Updates überprüfen:***

1. Klicken Sie im **Protection** Dashboard auf **Einstellungen** und anschließend auf die Registerkarte **Erweitert**.
2. Suchen Sie im unteren Bereich den Abschnitt **Schutz-Updates**.
   Die neueste Version der Datenbank und das Download-Datum werden im unteren Bereich des Abschnitts angezeigt.

***So können Sie das automatische Herunterladen der Schutz-Updates deaktivieren:***

**Hinweis**
Um den maximalen Schutz zu gewährleisten, empfehlen wir, die automatischen Schutz-Updates nicht zu deaktivieren.

1. Klicken Sie im **Protection** Dashboard auf **Einstellungen** und anschließend auf die Registerkarte **Erweitert**.
2. Suchen Sie im unteren Bereich den Abschnitt **Schutz-Updates**.
3. Deaktivieren Sie das Kontrollkästchen **Schutz-Updates automatisch herunterladen**.

***So können Sie die neuesten Schutz-Updates herunterladen:***

Auch wenn der automatische Download der Schutz-Updates deaktiviert ist, können Sie noch nach Updates suchen lassen und diese manuell herunterladen.

1. Klicken Sie im **Protection** Dashboard auf **Einstellungen** und anschließend auf die Registerkarte **Erweitert**.
2. Suchen Sie im unteren Bereich den Abschnitt **Schutz-Updates**.
3. Klicken Sie auf den Befehl **Auf Updates prüfen**. Diese Option ist nur verfügbar, wenn das

Kontrollkästchen **Schutz-Updates automatisch herunterladen** nicht aktiviert ist.

4. Wenn Ihre vorhandenen Schutz-Updates nicht mehr aktuell sind, klicken Sie auf **Update**.

# Daten synchronisieren

## Über die Synchronisierungsfunktion (Sync)

Die wichtigsten Highlights der Sync-Funktion:

- Sie können dieselben Daten – Dokumente, Fotos, Videos etc. – auf all Ihren Computern identisch vorhalten. Ihre Daten sind damit überall und jederzeit leicht verfügbar. Keine Notwendigkeit mehr, Dateien per E-Mail an sich selbst zu schicken oder dauernd einen USB-Stick mit sich herumzutragen.
- Sie können so viele 'Syncs' (Synchronisierungen) erstellen, wie Sie benötigen.
- Ihre synchronisierten Dateien und Versionen dieser Dateien werden in der Acronis Cloud aufbewahrt. Das ermöglicht Ihnen, bei Bedarf auch eine frühere Dateiversion wiederherzustellen.

  **Hinweis**
  Sie benötigen ein Acronis Cloud Storage-Abonnement, um diese Funktion nutzen zu können. Weitere Details dazu finden Sie im Abschnitt 'Abonnementinformationen'.

- Außerdem können Sie auch per Webbrowser auf die Cloud zugreifen, ohne dass Sie unsere Anwendung installieren müssen.
- Wenn Sie eine direkte Synchronisierung zwischen zwei oder mehr Computern erstellen, benötigen Sie kein Acronis Cloud-Abonnement.

## Was Sie synchronisieren können und was nicht

Sie können Daten synchronisieren, die in zwei oder mehreren Ordern gespeichert sind. Betrachten wir, wo diese Ordner sich befinden und welche Daten sie enthalten können.

### Storage-Typen

Sie können einen Synchronisierungsprozess einrichten zwischen:

- Zwei oder mehreren Ordnern auf zwei oder mehreren Computern.
- Einem oder mehreren Computern und der Acronis Cloud Cloud.
  Die Acronis Cloud enthält immer die letzten (neuesten) Versionen der synchronisierten Dateien. Sie können nicht zur selben Zeit einen Ordner in der Acronis Cloud auswählen, an einer Synchronisierung teilzunehmen. Ein solcher Ordner wird automatisch erstellt.

Sie können innerhalb eines Synchronisierungsprozesses nur einen Sync-Ordner auf jedem Computer zuweisen.

**Hinweis**
Sie können keine einzelne Datei zur Synchronisierung auswählen. Um eine Datei zu synchronisieren, wählen Sie für die Synchronisierung den Ordner, der diese Datei enthält.

## Datentypen

**Folgende Daten können Sie synchronisieren:**

- Dateien (Fotos, Musik, Videos, Dokumente usw.), mit unten aufgeführten Ausnahmen.

  **Hinweis**
  Es werden nur die ursprünglichen FAT32- und NTFS-Dateiattribute synchronisiert. Falls die synchronisierten Ordner einem anderen Dateisystem angehören, synchronisiert das Programm nur die Attribute, die von beiden Dateisystemen unterstützt werden.

- Andere Ordner innerhalb des Synchronisierungsordners (d.h. Synchronisierungsunterordner) und ihr Inhalt.

**Folgende Daten können Sie nicht synchronisieren:**

- Laufwerke und Volumes
- Systemdateien und Systemordner
- Versteckte Dateien und Ordner
- Temporäre Dateien und Ordner
- System-Registry
- Datenbanken
- Daten von E-Mail-Programmen (Microsoft Outlook und andere)
- Andere Daten, die nicht als separate Datei oder Ordner vorliegen (zum Beispiel 'Kontakte' aus Ihrem Adressbuch)
- Windows-Bibliotheken (Dokumente, Musik, etc.)

# Synchronisierungssymbole

Während Sie mit Synchronisierungen arbeiten, werden besondere Symbole angezeigt. Diese Symbole entsprechen folgenden Informationen:

- Typ und aktueller Status Ihrer Synchronisierungen (die entsprechenden Symbole werden im Infobereich der Taskleiste angezeigt).
- Aktueller Status von synchronisierten Dateien und Ordnern (die Symbole werden im Windows Datei-Explorer angezeigt).

## Der Infobereich

Symbole für den Status der Synchronisierungen:

| Symbol | Beschreibung |
|---|---|
|  | Die Synchronisierung arbeitet im Modus 'Normal'. |
|  | Die Synchronisierung wurde pausiert. |
|  | Während der letzten Synchronisierung trat ein Fehler auf. |

## Windows Explorer

Symbole für den Synchronisierungsstatus von Dateien und Ordnern:

| Symbol | Beschreibung |
|---|---|
|  | Die Datei oder der Ordner ist synchronisiert. |
|  | Die Datei oder der Ordner wird gerade synchronisiert. |
|  | Die Datei oder der Ordner wurde nicht synchronisiert, weil ein Fehler auftrat. |

Symbole für den Synchronisierungstyp von synchronisierten Ordnern:

| Symbol | Beschreibung |
|---|---|
|  | Mit der Acronis Cloud synchronisieren |
|  | Synchronisierung zwischen Computern, die über ein LAN (lokales Netzwerk) synchronisiert werden. |

# Eine Synchronisierung erstellen

Bevor Sie mit dem Erstellen einer neuen Synchronisierung beginnen, sollten Sie sicherstellen, dass folgende Bedingungen erfüllt sind:

- Sie haben ein Acronis Konto.
- Wenn Sie die Acronis Cloud in Ihre Synchronisierung einbeziehen wollen, benötigen Sie ein Acronis Cloud Storage-Abonnement. Ausführlichere Informationen finden Sie im Abschnitt '"Abonnementinformationen" (S. 37)'.
- Acronis Cyber Protect Home Office oder Acronis True Image (2012 oder höher) ist auf jedem Computer installiert.
- Falls Sie Ihre Computer über ein lokales Netzwerk verbinden, dann vergewissern Sie sich, dass die LAN-Verbindung auch verfügbar ist.
- Alle Computer sind mit dem Internet verbunden.

***So können Sie Dateien und Ordner synchronisieren***

1. Klicken Sie in der Seitenleiste auf **Sync**.
2. Sollten Sie noch nicht angemeldet sein, dann geben Sie jetzt die Anmeldedaten Ihres Acronis Kontos ein.
3. Klicken Sie auf **Sync hinzufügen**.
4. Entscheiden Sie, ob Sie die Acronis Cloud in Ihre neue Synchronisierung einschließen wollen – und wählen Sie dann den gewünschten Synchronisierungstyp.
5. Wählen Sie den zu synchronisierenden Ordner und klicken Sie dann auf **OK**.
6. Um dieser Synchronisierung beizutreten, müssen Sie Acronis Cyber Protect Home Office auf Ihrem Computer starten, diese Synchronisierung im Bereich 'Sync' auswählen, auf **Sync beitreten** klicken und anschließend den zu synchronisierenden Ordner auswählen.

# Versionen von synchronisierten Dateien

Mit Acronis Cyber Protect Home Office können Sie Änderungen, die aufgrund einer Synchronisierung an Ihren Dateien vorgenommen wurden, rückgängig machen. Wenn Sie bemerken, dass eine Ihrer Dateien eine unerwünschte Änderung enthält, können Sie vorherige Versionen dieser Datei ansehen und sie dann auf eine korrekte Version zurücksetzen. Details finden Sie unter Wiederherstellen einer vorherigen Dateiversion.

Alle Versionen werden in der Acronis Cloud gespeichert, auf die Sie über das Internet zugreifen können. Wenn Sie die Acronis Cloud verwenden wollen, müssen Sie ein Abonnement für den Acronis Cloud Service haben. Details finden Sie unter 'Abonnementinformationen'.

Wenn Sie veraltete Versionen löschen wollen, dann starten Sie die Bereinigungsaktion in der Acronis Cloud-Webapplikation. Weitere Details finden Sie unter 'So können Sie Ihren Speicherplatz in der Acronis Cloud bereinigen'.

**Warnung!**
Wenn Sie eine Testversion von Acronis Cyber Protect Home Office verwenden, werden bei Ablauf des Testzeitraums alle gespeicherten Versionen, einschließlich der letzten, aus der Cloud gelöscht.

## Wiederherstellen einer vorherigen Dateiversion

Wenn Sie den Synchronisierungsverlauf in der Acronis Cloud speichern, können Sie die aktuelle Version einer synchronisierten Datei auf eine vorherige zurücksetzen. Das ist nützlich, wenn Sie unerwünschte Synchronisierungsaktionen rückgängig machen wollen.

***So können Sie eine vorherige Dateiversion wiederherstellen***

1. Suchen Sie im Bereich **Sync** die Sync-Box mit der benötigten Datei. Klicken Sie dann auf den Link '**Acronis Cloud**'.
2. Nachdem die Liste der synchronisierten Elemente in Ihrem Webbrowser geöffnet wurde, wählen Sie die Datei, die Sie zu einer frühere Version wiederherstellen wollen. Klicken Sie dann auf der rechten Seite auf das Zahnradsymbol. Wählen Sie im geöffneten Menü den Befehl **Versionen anzeigen**.

3. Wählen Sie die Version, auf die die Datei zurückgesetzt werden soll. Zu der Version werden genaue Zeitangaben (Datum, Uhrzeit) angezeigt. Ihre aktuelle Version wird genau zu dem Zustand wiederhergestellt, der an diesem Zeitpunkt vorlag.
4. Klicken Sie auf **Recovery**, um fortzufahren. Die gewählte Version wird zur neuesten Version in der Cloud. Danach wird Sie zu dem Computer heruntergeladen, der die Synchronisierung besitzt.

## So stellen Sie eine gelöschte Datei wieder her

Es kann manchmal vorkommen, dass Sie versehentlich eine Datei von einer Synchronisierung löschen. In dem Fall müssen Sie die gelöschte Datei wiederherstellen. Das ist bei solchen Synchronisierung möglich, die Dateiversionen in der Acronis Cloud speichern.

Jedoch nur unter der Bedingung, dass die gelöschte Datei nicht während einer Cloud-Bereinigung gelöscht wurde.

So stellen Sie eine gelöschte Datei wieder her:

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Sync**, wählen Sie die Synchronisierung mit der wiederherzustellenden Datei aus und klicken Sie dann auf den Link **Acronis Cloud**.
3. Klicken Sie auf die Registerkarte **Dateien** und wählen Sie dann die Synchronisierung, aus der Sie die Datei gelöscht haben.
4. Nach Auswahl der Synchronisierung erscheint eine Liste von Dateien und Ordnern.
5. Aktivieren Sie das Kontrollkästchen **Gelöschte anzeigen** und wählen Sie dann die gelöschte und wiederherzustellende Datei.
6. Klicken Sie auf die Schaltfläche **Recovery**, um die gelöschte Datei zu ihrem Ordner wiederherzustellen.

## Eine Synchronisierung löschen

1. Klicken Sie in der Seitenleiste auf **Sync**.
2. Sollten Sie noch nicht angemeldet sein, dann geben Sie jetzt die Anmeldedaten Ihres Acronis Kontos ein.
3. Wählen Sie die gewünschte Sync aus der Synchronisierungsliste, klicken Sie auf das Pfeilsymbol und dann auf den Befehl **Löschen**.

Bei dieser Aktion werden nur die Verknüpfungen zwischen den synchronisierten Ordnern aufgehoben. Die eigentlichen synchronisierten Dateien verbleiben an ihren jeweiligen Speicherorten und werden nicht geändert oder gelöscht.

# Laufwerk klonen und Migration

Diese Aktion kopiert den gesamten Inhalt eines Laufwerks auf ein anderes. Das kann beispielsweise notwendig werden, wenn Sie Ihr Betriebssystem (inkl. Anwendungen und Daten) auf ein neues Laufwerk mit größerer Kapazität klonen wollen. Sie können dies auf zwei Arten tun:

- Verwenden Sie das Werkzeug 'Laufwerk klonen'.
- Erstellen Sie ein Backup Ihres alten Laufwerks und stellen Sie dieses dann auf dem neuen Laufwerk wieder her.

**Siehe auch**: Der Unterschied zwischen dem Backup und Klonen eines Laufwerks

## Das Werkzeug 'Laufwerk klonen'

Mit dem Werkzeug zum Klonen von Laufwerken können Sie alle Volumes eines Festplattenlaufwerks auf ein anderes übertragen.

Bevor Sie beginnen:

- Wenn Sie Ihr System auf ein Laufwerk mit einer höheren Kapazität klonen wollen, empfehlen wir folgenden Vorgehensweise: Installieren Sie das (neue) Ziellaufwerk dort, wo Sie es später verwenden wollen – und das Quelllaufwerk an einem anderen Ort, z.B. in einem externen USB-Gehäuse. Diese ist besonders bei Notebooks wichtig.

  **Hinweis**
  Es wird empfohlen, dass das alte und neue Laufwerk im selben 'Controller-Modus' (beispielsweise 'IDE' oder 'AHCI') arbeiten. Anderenfalls wird Ihr Computer möglicherweise nicht von dem neuen Laufwerk booten können.

  **Hinweis**
  Sie können ein Laufwerk mit Windows zwar auf eine externe USB-Festplatte klonen, jedoch können Sie möglicherweise nicht von dieser booten. Wir empfehlen, dass Sie als Ziel für die Klonen-Aktion stattdessen eine interne SSD- oder HDD-Festplatte verwenden.

- Das Werkzeug 'Laufwerk klonen' unterstützt keine Multiboot-Systeme.
- In der Programmanzeige werden beschädigte Volumes in der oberen linken Ecke mit einem weißen Kreuz auf rotem Kreis gekennzeichnet. Bevor Sie mit dem Klonen beginnen, sollten Sie mit den passenden Tools des Betriebssystems (wie chkdsk.exe) nach Laufwerksfehlern suchen und gefundene Fehler korrigieren lassen.
- Es wird außerdem dringend empfohlen, zur Sicherheit ein Backup des gesamten ursprünglichen Laufwerks zu erstellen. Das könnte die Rettung für Ihre Daten bedeuten, falls mit dem ursprünglichen Laufwerk beim Klonen etwas schief geht. Informationen zur Erstellung eines solchen Backups finden Sie im Abschnitt 'Backups von Laufwerken und Volumes'. Denken Sie unbedingt daran, das Backup nach dem Erstellen zu validieren.

## 'Laufwerk klonen'-Assistent

Bevor Sie beginnen, empfehlen wir Ihnen, die allgemeinen Informationen über das Werkzeug 'Laufwerk klonen' durchzulesen. Wenn Sie einen UEFI-Computer verwenden und die Aktion 'Laufwerk klonen' mit einem Boot-Medium durchführen wollen, sollten Sie darauf achten, welcher Boot-Modus für das Boot-Medium im UEFI-BIOS eingestellt ist. Der Boot-Modus sollte normalerweise mit dem Typ des Systems im Backup übereinstimmen. Wenn das Backup ein BIOS-System enthält, sollten Sie das Boot-Medium im BIOS-Modus starten. Wenn es sich um ein UEFI-System handelt, sollten Sie das Medium im UEFI-Modus booten.

***So können Sie ein Laufwerk klonen***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Tools** und dann auf **Laufwerk klonen**.
3. Wählen Sie im Schritt **Modus für das Klonen** einen Übertragungsmodus.
   - **Automatisch** – Wird in den meisten Fällen empfohlen.
   - **Manuell** – Der manuelle Modus bietet mehr Flexibilität beim Datentransfer. Der manuelle Modus ist vor allem dann nützlich, wenn die Partitionsstruktur des neuen Laufwerks geändert werden soll.

   **Hinweis**
   Wenn das Programm zwei Laufwerke findet, eins partitioniert (also mit Volumes) und das andere nicht, erkennt es automatisch das partitionierte Laufwerk als Quelle und das unpartitionierte Laufwerk als Ziel. In diesem Fall werden die nächsten Schritte übersprungen und Sie gelangen zum Fenster **Zusammenfassung**.
4. Wählen Sie im Schritt **Quelllaufwerk** dasjenige Laufwerk aus, das Sie klonen wollen.

   **Hinweis**
   Das Klonen von dynamischen Laufwerken wird von Acronis Cyber Protect Home Office nicht unterstützt.
5. Wählen Sie im Schritt **Ziellaufwerk** dasjenige Laufwerk aus, das als Ziel für die zu klonenden Daten dienen soll.

   Falls auf dem Ziellaufwerk Volumes (Partitionen) vorliegen, müssen Sie deren Löschung bestätigen. Beachten Sie, dass die Daten erst dann tatsächlich gelöscht werden, wenn Sie im letzten Schritt des Assistenten auf **Fertigstellen** klicken.

   **Hinweis**
   Wenn ein vorhandenes Laufwerk unpartitioniert ist, erkennt das Programm dieses automatisch als Ziellaufwerk und überspringt den nächsten Schritt.
6. [Dieser Schritt ist nur verfügbar, wenn auf dem Quelllaufwerk ein Betriebssystem installiert ist.] Bestimmen Sie im Schritt **Speicherplatznutzung**, welchen Verwendungszweck das geklonte

Laufwerk haben soll.

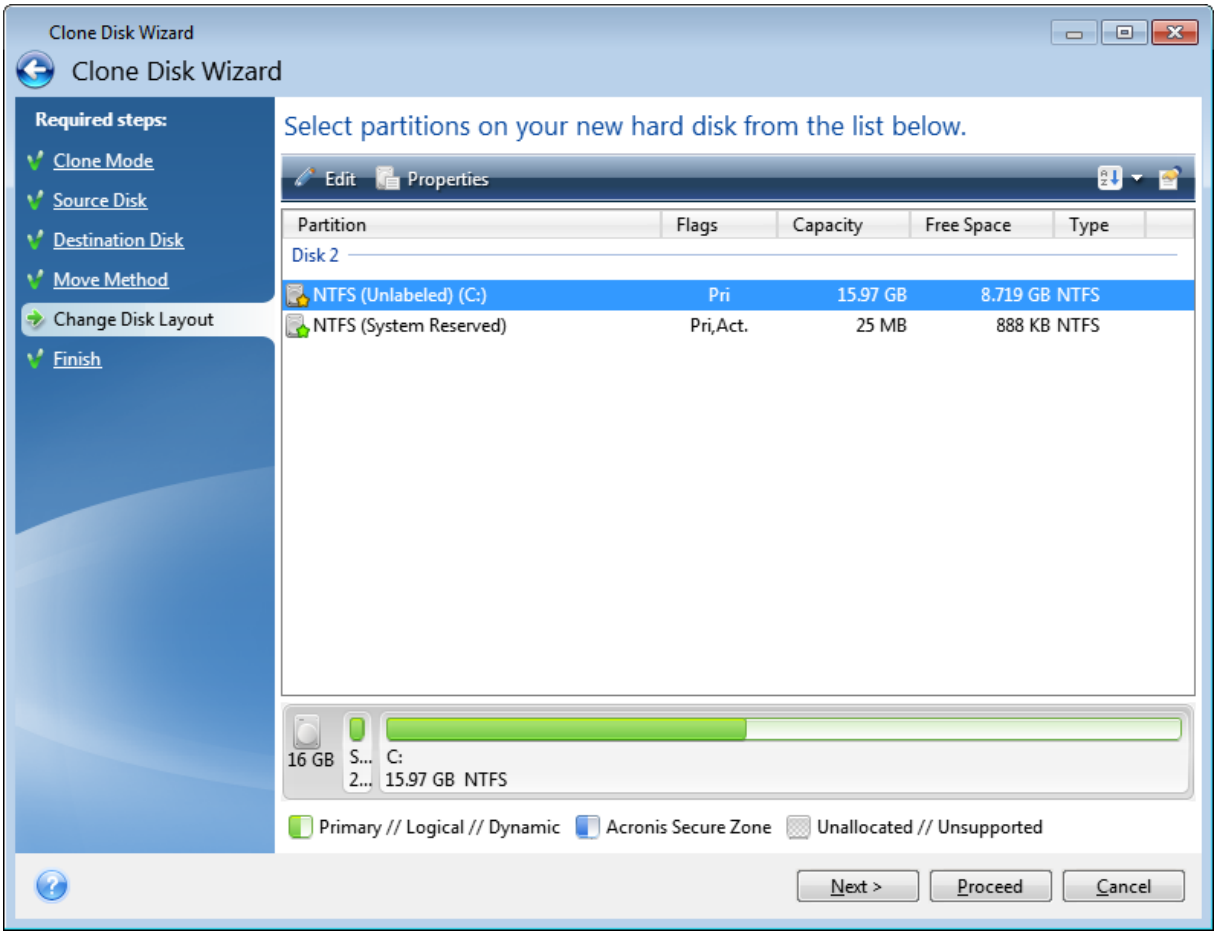
- **Zum Ersetzen eines Laufwerks auf dieser Maschine** – die Daten des Systemlaufwerks werden kopiert und das geklonte Laufwerk wird bootfähig gemacht. Verwenden Sie diesen Klon, um das Systemlaufwerk des PCs durch ein neues Laufwerk zu ersetzen.
- **Zur Verwendung mit einer anderen Maschine** – die Daten des Systemlaufwerks werden kopiert und das geklonte Laufwerk wird bootfähig gemacht. Verwenden Sie diesen Klon, um alle Daten des Quelllaufwerks über ein bootfähiges Laufwerk zu einem anderen PC zu übertragen.
- **Zur Verwendung als Datenlaufwerk** – die Daten des entsprechenden Laufwerks werden kopiert. Verwenden Sie diesen Klon als nicht bootfähiges Datenlaufwerk.

7. [Dieser Schritt ist nur im Klon-Modus 'Manuell' verfügbar]. Bestimmen Sie im Schritt **Methode zum Verschieben**, auf welche Art die Daten verschoben werden sollen.
   - **Wie vorliegend** – für jedes alte Volume wird ein neues Volume erstellt (identisch in Bezug auf Größe, Volume-Typ, Dateisystem und Volume-Bezeichnung). Der ungenutzte Speicherplatz wird zu 'nicht zugeordnet'.
   - **Proportional** – der neue Speicherplatz des Laufwerks wird proportional zwischen den geklonten Volumes aufgeteilt.
   - **Manuell** – Sie können die Größe und andere Parameter des neuen Laufwerks selbst bestimmen.
8. [Dieser Schritt ist nur im Klon-Modus 'Manuell' verfügbar]. Sie können im Schritt **Laufwerkslayout ändern** die Einstellungen der Volumes ändern, die auf dem Ziellaufwerk erstellt werden. Weitere Informationen finden Sie im Abschnitt 'Manuelle Partitionierung'.
9. [Optionaler Schritt] Sie können im Schritt **Ausschlusskriterien** Dateien und Ordner spezifizieren, die nicht mitgeklont werden sollen. Weitere Informationen finden Sie im Abschnitt 'Elemente vom Klonen ausschließen'.
10. Stellen Sie im Schritt **Abschluss** sicher, dass die konfigurierten Einstellungen Ihren Vorstellungen entsprechen – und klicken Sie dann auf **Fertigstellen**.

Sollte die Klonen-Aktion aus irgendeinem Grund gestoppt werden, müssen Sie die Prozedur erneut konfigurieren und starten. Sie werden keine Daten verlieren, weil Acronis Cyber Protect Home Office das ursprüngliche Laufwerk und darauf gespeicherte Daten während des Klonens nicht verändert.

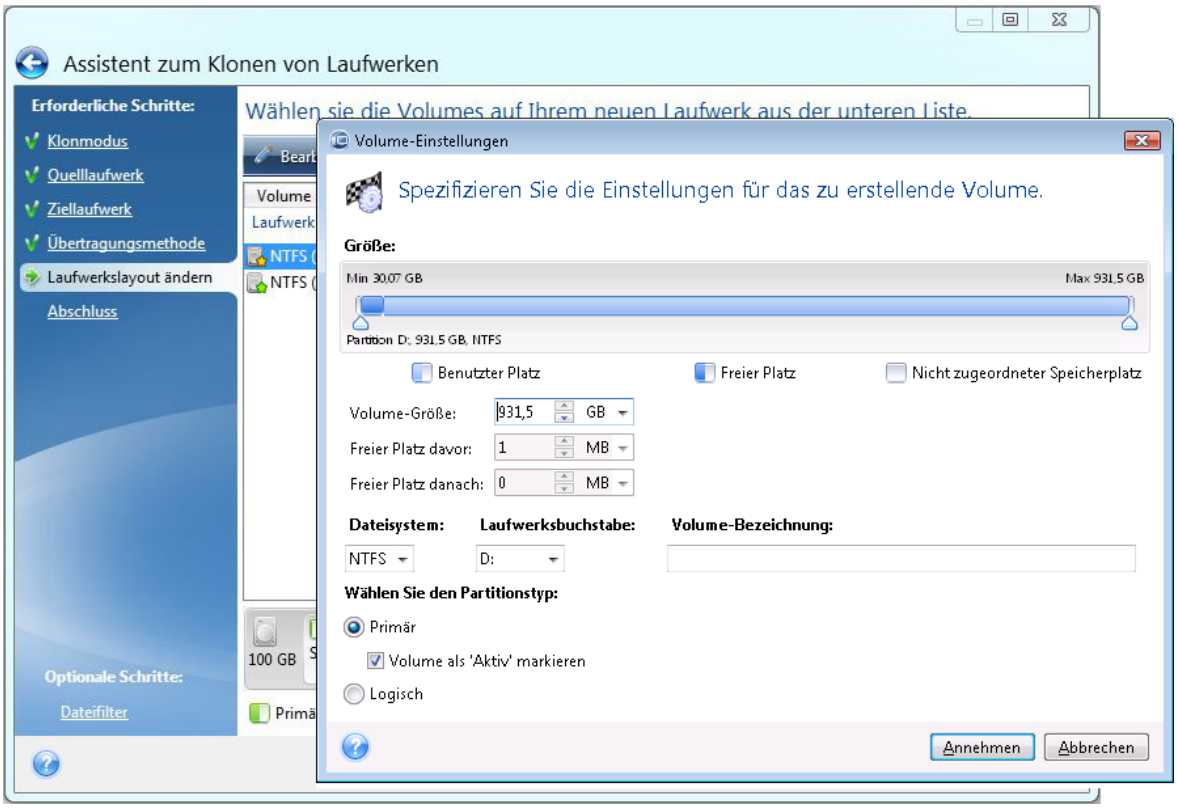
## Manuelle Partitionierung

Die manuelle Übertragungsmethode ermöglicht Ihnen, die Volumes (Partitionen) des neuen Laufwerks in der Größe anzupassen. Standardmäßig ändert das Programm die Größen proportional.




***So können Sie ein Volume (eine Partition) bearbeiten***

1. Wählen Sie das Volume und klicken Sie dann auf **Bearbeiten**. Daraufhin öffnet sich das Fenster 'Volume-Einstellungen'.




2. Spezifizieren Sie folgende Einstellungen für das Volume:
   - Größe und Position
   - Dateisystem
   - Volume-Typ (nur für MBR-Laufwerke verfügbar)
   - Laufwerksbuchstabe und Volume-Bezeichnung

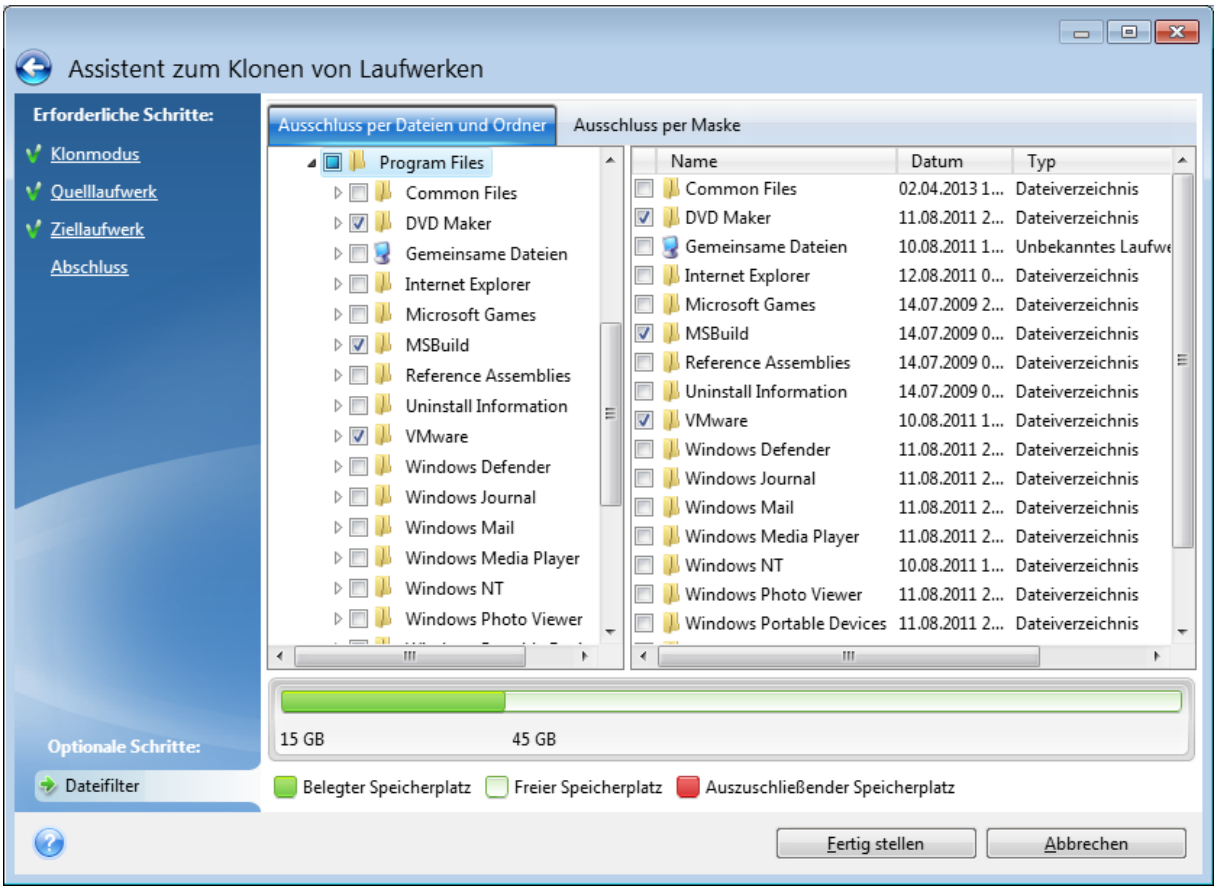
   Weitere Details finden Sie im Abschnitt 'Volume-Einstellungen'.
3. Klicken Sie auf **Übernehmen**.

**Warnung!**
Sollten Sie an dieser Stelle in der Seitenleiste auf einen vorherigen Assistentenschritt klicken, werden alle vorgenommenen Änderungen zu Größe und Position zurückgesetzt, sodass Sie diese bei Bedarf neu vornehmen müssen.

## Elemente vom Klonen ausschließen

Falls Sie bestimmte Dateien eines Quelllaufwerks nicht mitklonen wollen (beispielsweise, weil Ihr Ziellaufwerk kleiner als das Quelllaufwerk ist), können Sie diese auf Wunsch im Schritt **Ausschlusskriterien** ausschließen.

**Hinweis**
Wir raten davon ab, versteckte Dateien und Systemdateien beim Klonen Ihres System-Volumes auszuschließen.




**Sie haben zwei Möglichkeiten, Dateien und Ordner auszuschließen:**

- **Ausschluss per Dateien und Ordner** – diese Registerkarte ermöglicht es Ihnen, bestimmte Dateien und Ordner über den Verzeichnisbaum auszuschließen.
- **Per Maske ausschließen** – diese Registerkarte ermöglicht es Ihnen, eine Gruppe von Dateien per Maske auszuschließen oder einzelne Dateien per Name bzw. Pfad.

  Klicken Sie zum Hinzufügen eines Ausschlusskriteriums auf den Befehl **Hinzufügen**, geben Sie dann einen Dateinamen, einen Pfad oder eine Maske ein – und klicken Sie abschließend auf **OK**. Sie können so viele Dateien und Masken hinzufügen, wie Sie möchten.

**Beispiele für Ausschlusskriterien:**

- Sie können eindeutige Dateinamen eingeben:
  - *file.ext* – alle Dateien mit diesem Namen werden vom Klonen ausgeschlossen.
  - *C:\file.ext* – die Datei 'file.ext' auf Laufwerk C: wird ausgeschlossen.
- Sie können Platzhalterzeichen (* und ?) verwenden:
  - **.ext* – Alle Dateien mit der Erweiterung '.ext' werden ausgeschlossen.
  - *??name.ext* – Dateien mit der Erweiterung .ext, deren Namen aus sechs Buchstaben bestehen (beginnend mit zwei beliebigen Zeichen (??) und mit *name* endend), werden ausgeschlossen.
- Sie können einen Pfad oder einen Ordner eingeben:
  - *C:\Meine Bilder* – der Ordner '*Meine Bilder*' auf dem Laufwerk C: wird ausgeschlossen.

Sie können Ausschlusskriterien mit den entsprechenden Schaltflächen im rechten Fensterbereich bearbeiten und entfernen.

## Migrationsmethode

Acronis Cyber Protect Home Office ermöglicht Ihnen, nach Abschluss einer Klon-Aktion für ein Ziellaufwerk das Partitionierungsschema zu wählen:

- **MBR (Master Boot Record)** – ein 512 Byte großer Boot-Sektor, der als erster Sektor auf dem entsprechenden Laufwerk liegt und dessen primäre Partitionstabelle enthält.
- **GPT (GUID-Partitionstabelle)** – ein Standard für das Partitionstabellenlayout (auch Partitionierungsschema genannt) von Festplatten und verwandten Laufwerken. GPT ermöglicht Laufwerke/Volumes mit einer Größe bis zu 9,4 ZB (9,4 x 10^21 Byte).

Durch Verwendung dieses Assistenten können Sie während einer Klon-Aktion das Partitionierungsschema konvertieren oder wie vorliegend belassen.

- **Partitionen ohne Änderungen kopieren** – wählen Sie diese Option, um Ihr System wie vorliegend (also ohne Änderung des Partitionierungsschemas) zu migrieren. Beachten Sie, dass in diesem Fall der Speicherplatz oberhalb von 2 TB nicht verfügbar ist. Sie können den Acronis Extended Capacity Manager verwenden, um den Speicherplatz oberhalb von 2 TB zuzuweisen.
- **Volumes kopieren und ein Laufwerk als 'Nicht-System' (GPT-Schema) verwenden** – wählen Sie diese Option, um Ihre Partition (Volume) zum GPT-Layout zu konvertieren.

Sie können mit Acronis Cyber Protect Home Office zudem **BIOS**- zu **UEFI**-Systemen konvertieren. Zu weiteren Informationen siehe Unified Extensible Firmware Interface.

### Per BIOS gebootetes System, MBR, UEFI nicht unterstützt

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

#### Aktuell enthält Ihr System:

**System**: Per BIOS gebootet

**Quell-Partitionierungsschema**: MBR

**Betriebssystem auf dem Quelllaufwerk**: Windows, Booten per UEFI wird nicht unterstützt

**Größe des Ziellaufwerks**: weniger als 2 TB

#### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: Per BIOS gebootet

**Partitionierungsschema**: MBR

**Betriebssystem**: Windows, Booten per UEFI wird nicht unterstützt

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per BIOS gebootetes System, MBR, UEFI unterstützt

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

### Aktuell enthält Ihr System:

**System**: Per BIOS gebootet

**Quell-Partitionierungsschema**: MBR

**Betriebssystem auf dem Quelllaufwerk**: Windows, Booten per UEFI wird unterstützt

**Größe des Ziellaufwerks**: weniger als 2 TB

### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: Per BIOS gebootet

**Partitionierungsschema**: MBR

**Betriebssystem**: Windows, Booten per UEFI wird unterstützt

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per BIOS gebootetes System, MBR, 'Nicht-Windows'

Acronis Cyber Protect Home Office ermöglicht Ihnen, nach Abschluss einer Aktion das Partitionslayout für ein Ziellaufwerk zu bestimmen.

### Aktuell enthält Ihr System:

**System**: Per BIOS gebootet

**Quell-Partitionierungsschema**: MBR

**Betriebssystem auf dem Quelllaufwerk**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Größe des Ziellaufwerks**: weniger als 2 TB

### Mit diesen Systemparametern können Sie Folgendes wählen:

1. **Volumes ohne Änderungen kopieren**

Sie können das MBR-Partitionierungsschema auf dem Ziellaufwerk belassen.

**Ziellaufwerk nach Migration:**

**System**: Per BIOS gebootet

**Partitionierungsschema**: MBR

**Betriebssystem**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

2. **Volumes kopieren und ein Laufwerk als 'Nicht-System' (GPT-Schema) verwenden**

Sie können das Partitionierungsschema zu GPT konvertieren.

**Ziellaufwerk nach Migration:**

**System**: nicht bootfähig per BIOS

**Partitionierungsschema**: GPT

**Betriebssystem**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

**Warnung!**
Das Ziellaufwerk kann nach der Migration nur als 'Nicht-System'-Laufwerk genutzt werden. Diese Option ist nicht verfügbar, falls Acronis Cyber Protect Home Office unter Windows XP x86 (32-Bit) als Betriebssystem ausgeführt wird.

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per BIOS gebootetes System, GPT, UEFI unterstützt

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

### Aktuell enthält Ihr System:

**System**: Per BIOS gebootet

**Quell-Partitionierungsschema**: GPT

**Betriebssystem auf dem Quelllaufwerk**: Windows, Booten per UEFI wird unterstützt

### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: nicht bootfähig per BIOS

**Partitionierungsschema**: GPT

**Betriebssystem**: Windows, Booten per UEFI wird unterstützt

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

**Warnung!**
Das Betriebssystem kann nach der Migration nicht mehr per BIOS vom Ziellaufwerk booten. Wenn Sie nach der Migration vom Ziellaufwerk booten wollen, müssen Sie in Ihrem System das Booten per UEFI aktivieren (siehe den Abschnitt zu 'Unified Extensible Firmware Interface'). Starten Sie die Aktion anschließend neu.

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per BIOS gebootetes System, GPT, 'Nicht-Windows'

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

### Aktuell enthält Ihr System:

**System**: Per BIOS gebootet

**Quell-Partitionierungsschema**: GPT

**Betriebssystem auf dem Quelllaufwerk**: 'Nicht-Windows' oder 'Kein Betriebssystem'

### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: Per BIOS gebootet

**Partitionierungsschema**: GPT

**Betriebssystem**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per UEFI gebootetes System, MBR, UEFI nicht unterstützt

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

### Aktuell enthält Ihr System:

**System**: Per UEFI gebootet

**Quell-Partitionierungsschema**: MBR

**Betriebssystem auf dem Quelllaufwerk**: Windows, Booten per UEFI wird nicht unterstützt

**Größe des Ziellaufwerks**: weniger als 2 TB

### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: nicht bootfähig per UEFI

**Partitionierungsschema**: MBR

**Betriebssystem**: Windows, Booten per UEFI wird nicht unterstützt

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

**Warnung!**

Das Betriebssystem kann möglicherweise nicht per UEFI vom Ziellaufwerk booten.

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per UEFI gebootetes System, MBR, UEFI wird unterstützt

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

### Aktuell enthält Ihr System:

**System**: Per UEFI gebootet

**Quell-Partitionierungsschema**: MBR

**Betriebssystem auf dem Quelllaufwerk**: Windows, Booten per UEFI wird unterstützt

### Falls Sie das System auf das gewählte Laufwerk migrieren:

Das Partitionierungsschema des Ziellaufwerks wird nach der Migration zu GPT konvertiert und Sie können dann von diesem booten.

**Ziellaufwerk nach Migration:**

**System**: Per UEFI gebootet

**Partitionierungsschema**: GPT

**Betriebssystem**: Windows, Booten per UEFI wird unterstützt

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per UEFI gebootetes System, MBR, 'Nicht-Windows'

Acronis Cyber Protect Home Office ermöglicht Ihnen, nach Abschluss einer Aktion das Partitionslayout für ein Ziellaufwerk zu bestimmen.

### Aktuell enthält Ihr System:

**System**: Per UEFI gebootet

**Quell-Partitionierungsschema**: MBR

**Betriebssystem auf dem Quelllaufwerk**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Größe des Ziellaufwerks**: weniger als 2 TB

### Mit diesen Systemparametern können Sie Folgendes wählen:

1. **Volumes ohne Änderungen kopieren**

Sie können das MBR-Partitionierungsschema auf dem Ziellaufwerk belassen.

**Ziellaufwerk nach Migration:**

**System**: Per UEFI gebootet

**Partitionierungsschema**: MBR

**Betriebssystem**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

2. **Volumes kopieren und ein Laufwerk als 'Nicht-System' (GPT-Schema) verwenden**

Sie können das Partitionierungsschema zu GPT konvertieren.

**Ziellaufwerk nach Migration:**

**System**: nicht bootfähig per UEFI

**Partitionierungsschema**: GPT

**Betriebssystem**: 'Nicht-Windows' oder 'Kein Betriebssystem'

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

**Warnung!**
Das Ziellaufwerk kann nach der Migration nur als 'Nicht-System'-Laufwerk genutzt werden.

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per UEFI gebootetes System, GPT, UEFI wird unterstützt

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

### Aktuell enthält Ihr System:

**System**: Per UEFI gebootet

**Quell-Partitionierungsschema**: GPT

**Betriebssystem:** Windows, Booten per UEFI wird unterstützt

### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: Per UEFI gebootet

**Partitionierungsschema**: GPT

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

## Per UEFI gebootetes System, GPT, 'Nicht-Windows'

In diesem Schritt des Assistenten müssen Sie das Ziellaufwerk wählen.

### Aktuell enthält Ihr System:

**System**: Per UEFI gebootet

**Quell-Partitionierungsschema**: GPT

**Betriebssystem**: 'Nicht-Windows' oder 'Kein Betriebssystem'

### Falls Sie das System auf das gewählte Laufwerk migrieren:

**System**: Per UEFI gebootet

**Partitionierungsschema**: GPT

**Laufwerksgröße**: der komplette Speicherplatz ist verfügbar

Weitere Informationen zur Migrationsprozedur finden Sie im Abschnitt Migrationsmethode.

# Migration Ihres Systems von einer Festplatte auf SSD

Stellen Sie zuerst sicher, dass Acronis Cyber Protect Home Office Ihre neue SSD sowohl unter Windows als auch mit einem Acronis Boot-Medium erkennt. Im Falle eines Problems siehe 'Vorgehensweise, falls Acronis Cyber Protect Home Office Ihre SSD nicht erkennt'.

## SSD-Größe

Da SSDs üblicherweise eine geringere Kapazität als Festplatten (HDDs) haben, kann der belegte Speicherplatz auf Ihrem alten Festplattenlaufwerk die Größe Ihrer SSD möglicherweise überschreiten. In diesem Fall ist eine Migration nicht möglich.

Gehen Sie folgendermaßen vor, um die Datenmenge auf Ihrem Systemlaufwerk zu reduzieren:

- Verschieben Sie Ihre Datendateien von Ihrem alten Laufwerk zu einem anderen Speicherort, beispielsweise auf ein anderes (internes oder externes) Festplattenlaufwerk.
- Erstellen Sie .zip-Archive von Ihren Datendateien (beispielsweise Ihre Dokumente, Bilder, Audiodateien etc.) und löschen Sie dann die Originaldateien.
- Bereinigen Sie das Laufwerk mit dem Windows-Werkzeug 'Datenträgerbereinigung'.

Beachten Sie, dass zum stabilen Betrieb von Windows auf dem System-Volume mehrere GB freier Speicherplatz erforderlich sind.

## Die Wahl der Migrationsmethode

Sollte Ihr Systemlaufwerk aus einem einzigen Volume bestehen (das versteckte Volume 'System-reserviert' nicht mitgezählt), dann können Sie versuchen, mit der Funktion 'Laufwerk klonen' auf die neue SSD zu migrieren. Weitere Informationen finden Sie unter 'Ein Laufwerk klonen'.

Wir empfehlen jedoch in den meisten Fällen, die 'Backup und Recovery'-Methode zu verwenden. Diese Methode ermöglicht gegenüber der Migration mehr Flexibilität und Kontrolle. Siehe 'Migration auf eine SSD mit der 'Backup und Recovery'-Methode'.

# Was Sie tun können, wenn Acronis Cyber Protect Home Office Ihre SSD nicht erkennt

Es kann manchmal vorkommen, dass Acronis Cyber Protect Home Office eine SSD nicht richtig erkennt.

Überprüfen Sie in diesem Fall, ob die SSD korrekt im BIOS erkannt wird.

Sollte das BIOS Ihres Computers die SSD nicht anzeigen, dann überprüfen Sie, ob die Strom- und Datenkabel des Laufwerks richtig angeschlossen sind. Sie können außerdem versuchen, das BIOS und die SATA-Treiber zu aktualisieren. Falls diese Vorschläge nicht helfen, dann kontaktieren Sie den Support Ihres SSD-Herstellers (um beispielsweise ein Firmware-Update für die SSD zu erhalten).

***Wenn das BIOS Ihres Computers die SSD anzeigt***

1. Geben Sie (abhängig von Ihrem Betriebssystem) in das Feld 'Suchen' oder 'Ausführen' den Befehl `cmd` ein und drücken Sie dann auf die **Eingabetaste** (Enter).
2. Geben Sie Folgendes in die Eingabeaufforderung ein:

   ```
   diskpart
   list disk
   ```

   Der Bildschirm zeigt die an Ihren Computer angeschlossenen Laufwerke an. Ermitteln Sie die Laufwerksnummer für Ihre SSD. Verwenden Sie deren Größe als Referenz.
3. Führen Sie folgenden Befehl aus, um das Laufwerk auszuwählen:

   ```
   select disk N
   ```

   Wobei N die Laufwerksnummer Ihrer SSD ist.
4. Führen Sie folgenden Befehl aus, um alle Informationen von der SSD zu löschen und deren MBR mit dem Standard-MBR zu überschreiben:

   ```
   clean
   exit
   exit
   ```

Starten Sie Acronis Cyber Protect Home Office und überprüfen Sie, ob das Programm die SSD erkennt. Falls es die SSD erkennt, dann verwenden Sie das Werkzeug 'Neues Laufwerk hinzufügen', um ein einziges Volume (Partition) auf dem Laufwerk zu erstellen, welche den kompletten Laufwerksspeicherplatz belegt. Überprüfen Sie beim Erstellen eines Volumes, dass der freie Speicherplatz davor 1 MB beträgt. Weitere Informationen finden Sie unter 'Ein neues Laufwerk hinzufügen'.

***So können Sie überprüfen, ob Ihr Acronis Boot-Medium die SSD erkennt***

1. Starten Sie den Computer mit dem Acronis Boot-Medium.
2. Wählen Sie im Hauptmenü die Befehle **Extras und Werkzeuge –> Neues Laufwerk hinzufügen** – worauf in der Anzeige **Laufwerksauswahl** entsprechende Informationen über alle in Ihrem System verfügbaren Laufwerke anzeigt werden. Verwenden Sie diese, um zu überprüfen, ob die SSD in der Notfallumgebung erkannt wird.
3. Falls Ihre SSD angezeigt wird, klicken Sie einfach auf **Abbrechen**.

Sollte das Boot-Medium die SSD nicht erkennen und der SSD-Controller zudem im AHCI-Modus laufen, dann können Sie versuchen, den Modus auf 'IDE' (von manchen BIOS-Typen auch 'ATA' genannt) umzustellen – und anschließend schauen, ob dies das Problem gelöst hat.

**Warnung!**
Achtung! Sie sollten nach Änderung des Controller-Modus nicht Windows starten, da dies zu ernsten Systemproblemen führen kann. Sie müssen den Modus zurück auf AHCI stellen, bevor Sie Windows starten.

Falls das Boot-Medium nach Umstellung des Controller-Modus die SSD erkennt, dann können Sie folgende Prozedur verwenden, um Recovery- oder Klon-Aktionen mit einem Boot-Medium durchzuführen:

1. Fahren Sie den Computer herunter.
2. Booten Sie und gehen Sie direkt ins BIOS, wo Sie den Controller-Modus von AHCI auf IDE ändern (von manchen BIOS-Typen auch ATA genannt).
3. Starten Sie den Computer mit dem Acronis Boot-Medium.
4. Führen Sie eine Recovery- oder Klon-Aktion mit dem Laufwerk durch.
5. Booten Sie wieder, gehen Sie direkt in das BIOS und wechseln Sie den Controller-Modus zurück von IDE auf AHCI.
6. Starten Sie Windows.

### Vorgehensweise, falls die oberen Vorschläge nicht helfen

Sie können versuchen, ein WinPE-basiertes Boot-Medium zu erstellen. Dieses Medium stellt vermutlich die notwendigen Treiber bereit. Weitere Informationen finden Sie unter 'Ein Acronis Boot-Medium erstellen'.

## Migration auf eine SSD mit der 'Backup und Recovery'-Methode

Sie können für alle unterstützten Betriebssysteme folgende Prozedur verwenden. Betrachten wir zuerst einen einfachen Fall: Ihr Systemlaufwerk besteht aus einem einzelnen Volume (einer Partition). Beachten Sie, dass bei Windows 7 (und höher) das Systemlaufwerk ein zusätzliches, verstecktes Volume namens 'System-reserviert' enthalten kann, in dem Windows wichtige Boot-Dateien hinterlegt hat.

Wir empfehlen, dass Sie Ihr System auf eine leere SSD migrieren, welche noch keine Volumes (Partitionen) enthält (deren Laufwerkspeicherplatz also als 'nicht zugeordnet' gekennzeichnet sind). Beachten Sie, dass Ihre SSD keine Volumes enthält, falls Sie neu ist und noch niemals verwendet wurde.

***So können Sie Ihr System auf eine SSD migrieren***

1. Acronis Cyber Protect Home Office starten.
2. Sollten Sie noch kein Acronis Boot-Medium haben, dann erstellen Sie eins. Klicken Sie dazu im Bereich **Extras** auf **Boot-Medium erstellen** und folgen Sie den Bildschirmanweisungen.
3. Sichern Sie Ihr komplettes Systemlaufwerk (im Modus 'Laufwerk-Backup') auf ein weiteres Festplattenlaufwerk, welches weder Ihr Systemlaufwerk noch die SSD ist.
4. Schalten Sie den Computer aus und entfernen Sie Ihr Systemlaufwerk.
5. Schließen Sie die SSD in dem Anschluss bzw. Einbauschacht an, wo zuvor die Festplatte war.

**Hinweis**
Bei einigen SSD-Typen müssen Sie die SSD in einen PCI-Express-Steckplatz einbauen.

6. Starten Sie den Computer mit Ihrem Acronis Boot-Medium.
7. Validieren Sie das Backup, um sicherzustellen, dass es für die Wiederherstellung verwendbar ist. Klicken Sie dazu im linken Fensterbereich auf **Recovery** und wählen Sie das Backup aus. Klicken Sie mit der rechten Maustaste darauf, wählen Sie den Befehl **Archiv validieren** aus dem Kontextmenü und klicken Sie auf **Fertigstellen**.
8. Klicken Sie nach Abschluss der Validierung mit der rechten Maustaste auf das Backup und wählen Sie den Befehl **Recovery** aus dem Kontextmenü.
9. Wählen Sie im Schritt 'Recovery-Methode' die Option **Recovery kompletter Laufwerke und Volumes** und klicken Sie dann auf **Weiter**.
10. Wählen Sie im Schritt 'Recovery-Quelle' das Systemlaufwerk aus.
11. Klicken Sie auf **Neuer Speicherort** und wählen Sie die SSD als Ziel für Ihr Systemlaufwerk aus; klicken Sie anschließend auf **Übernehmen**.
12. Klicken Sie im nächsten Schritt auf **Fertigstellen**, um die Wiederherstellung zu starten.
13. Beenden Sie nach Abschluss der Wiederherstellung die autonome Notfallversion von Acronis Cyber Protect Home Office.
14. Versuchen Sie, von der SSD zu booten und überprüfen Sie, ob Windows und alle Anwendungen korrekt laufen.

Sollte Ihre Systemfestplatte außerdem ein verstecktes Recovery- oder Diagnose-Volume enthalten (wie es häufig bei Notebooks der Fall ist), dann ist die Prozedur etwas anders. Sie müssen die Größe der Volumes bei der Wiederherstellung auf die SSD üblicherweise manuell anpassen. Weitere Anweisungen finden Sie unter 'Ein Laufwerk mit einem versteckten Volume wiederherstellen'.

# Extras

***Schutzwerkzeuge***

- "Acronis Universal Restore" (S. 261)
- "Acronis Startup Recovery Manager" (S. 223)
- "Acronis Media Builder" (S. 210)
- "Acronis Secure Zone" (S. 232)
- "Try&Decide" (S. 225)

***Laufwerk klonen***

- "Das Werkzeug 'Laufwerk klonen'" (S. 192)

***Sicherheit und Schutz der Privatsphäre***

- "Acronis DriveCleanser" (S. 242)
- "Systembereinigung" (S. 249)

***Laufwerksverwaltung***

- "Ein neues Laufwerk hinzufügen" (S. 237)

***Image mounten***

- "Ein Backup-Image mounten" (S. 257)
- "Ein gemountetes Image trennen" (S. 258)

## Acronis Cloud Backup Download

Acronis Cloud Backup Download ist ein Tool, mit dem Sie Cloud Backups sicher herunterladen können – und das selbst dann, wenn die Internetverbindung instabil ist. Der Download wird nicht mitten drin einfach abgebrochen, wenn die Verbindung ausfallen sollten, sondern er wird nur pausiert und kann später wieder fortgesetzt werden. Außerdem ist eine Wiederherstellung aus einem heruntergeladenen Backup wesentlich schneller als eine Wiederherstellung aus der Cloud.

***So können Sie Acronis Cloud Backup Download installieren***

1. Sie können das Tool auf eine der folgenden Arten herunterladen:
   - Gehen Sie in Acronis Cyber Protect Home Office zum Bereich **Extras**. Klicken Sie auf **Acronis Cloud Backup Download**, um zur Download-Seite zu gehen. Wählen Sie dann die gewünschte Version des Tools und laden Sie dieses herunter.
   - Gehen Sie zu https://www.acronis.com/my/online-backup/webrestore/ und melden Sie sich an Ihrem Acronis Konto an. Klicken Sie in der Seitenleiste auf **Backups** und wählen Sie dann das Backup aus, dessen Dateien Sie wiederherstellen wollen. Klicken Sie in der Detailansicht auf **Download**. Klicken Sie anschließend im Fenster **Cloud Backups herunterladen** auf **Das Tool**

**herunterladen**. Wählen Sie dann die gewünschte Version des Tools und laden Sie dieses herunter.

- Gehen Sie zur Download-Seite unter https://go.acronis.com/cloud-backup-download. Wählen Sie dann die gewünschte Version des Tools und laden Sie dieses herunter.

**Hinweis**
Das Tool wird auch heruntergeladen, wenn Sie es bereits zuvor installiert haben sollten.

2. Extrahieren Sie die ausführbare Datei und führen Sie diese aus.
3. Akzeptieren Sie die Lizenzvereinbarung und melden Sie sich an.

***So können Sie ein Cloud Backup herunterladen***

**Wichtig**
Sie können nur Backups von Laufwerken, Volumes oder der kompletten Maschine im TIBX-Format herunterladen. Datei- oder Ordner-Backups können nicht mit Acronis Cloud Backup Download heruntergeladen werden.

1. Starten Sie Acronis Cloud Backup Download und melden Sie sich an.
2. Wählen Sie im Fenster '**Acronis Cloud Backup Download**' das Backup aus, das Sie herunterladen wollen.
3. Wählen Sie im Fenster **Backup zum Download auswählen** entweder das gewünschte einzelne Backup oder das komplette Backup-Set aus.
4. [Optionaler Schritt] Wenn das Backup verschlüsselt ist, müssen Sie das entsprechende Kennwort eingeben.
5. Wählen Sie das Download-Ziel aus und klicken Sie dann auf **Speichern**.

Der Download der .tibx-Datei wird gestartet. Sie können ihn jederzeit pausieren oder bei Bedarf auch abbrechen.

***So können Sie das heruntergeladene Backup verwenden***

- Wenn Sie die Sicherung der entsprechenden Daten fortsetzen wollen, fügen Sie das Backup zu Acronis Cyber Protect Home Office hinzu (wie im Abschnitt '"Ein vorhandenes Backup der Liste hinzufügen" (S. 102)' beschrieben).
- Stellen Sie die Daten aus dem Backup wieder her, wie im Abschnitt '"Laufwerke und Volumes wiederherstellen" (S. 114)' beschrieben.
- Erstellen Sie ein Boot-Medium wie im Abschnitt '"Ein Acronis Boot-Medium erstellen" (S. 211)' beschrieben.
- Erstellen Sie ein Acronis Survival Kit, wie im Abschnitt '"Ein Acronis Survival Kit erstellen" (S. 27)' beschrieben..
- Mounten Sie das heruntergeladene Backup wie in Abschnitt '"Ein Backup-Image mounten" (S. 257)' beschrieben.

# Acronis Media Builder

Der Acronis Media Builder ermöglicht Ihnen, einen USB-Stick, eine externe Festplatte oder eine leere CD/DVD bootfähig zu machen. Wenn Windows nicht mehr starten kann, können Sie das Boot-Medium verwenden, um eine autonome Notfallversion von Acronis Cyber Protect Home Office auszuführen und Ihren Computer damit wiederherzustellen.

**Sie können verschiedene Arten von Boot-Medien erstellen:**

- **Acronis Boot-Medium**

  Dieser Typ wird für die meisten Benutzer empfohlen.
- **WinPE-basiertes Boot-Medium mit dem Acronis Plug-in**

  Indem Sie Acronis Cyber Protect Home Office unter einer solchen 'Preinstallation'-Umgebung (PE) ausführen, erreichen Sie möglicherweise eine größere Kompatibilität mit der Hardware Ihres Computers, da PE-Medien mit Windows-Treibern arbeiten.

  Die Erstellung dieses Boot-Medium-Variante empfiehlt sich, wenn Sie Ihren Computer – beispielsweise wegen Treiber-Problemen – mit dem herkömmlichen, Linux-basierten Acronis Boot-Medium nicht starten können.

  Damit Sie diese Option nutzen können, muss eine der nachfolgenden Komponenten installiert sein:
  - Das Windows Automated Installation Kit (AIK).

    Diese Komponente wird zur Erstellung von WinPE 3.0 benötigt.
  - Das Windows Assessment and Deployment Kit (ADK).

    Diese Komponente wird zur Erstellung von WinPE 4.0, WinPE 5.0 und WinPE 10.0 benötigt.
- **WinRE-basiertes Boot-Medium mit dem Acronis Plug-in**

  Diese Art von Boot-Medium ist einem WinPE-basierten Medium sehr ähnlich, hat jedoch einen entscheidenden Vorteil – es ist nicht notwendig, das WADK oder WAIK von der Microsoft-Website herunterzuladen. Denn die 'WinRE' (Windows Recovery Environment, Windows-Wiederherstellungsumgebung) ist seit Windows Vista in allen Windows-Versionen direkt enthalten. Acronis Cyber Protect Home Office verwendet diese Dateien von Ihrem System, um ein WinRE-basiertes Boot-Medium zu erstellen. Genau wie bei einem WinPE-basierten Boot-Medium können Sie auch hier notwendige Treiber hinzufügen, um die Kompatibilität mit Ihrer Hardware zu gewährleisten. Sie können ein WinRE-basiertes Medium jedoch nur auf dem Computer verwendet werden, auf dem dieses erstellt wurde – oder auf einem Computer mit dem gleichen Betriebssystem.

**Hinweise**

- Wir empfehlen, nach jedem Update von Acronis Cyber Protect Home Office auch ein neues Boot-Medium zu erstellen.
- Wenn Sie ein Medium verwenden, welches kein optisches Medium ist, muss dieses FAT16 oder FAT32 als Dateisystem verwenden.

- Der Acronis Media Builder unterstützt nur die x64-Versionen von WinPE 3.0, WinPE 4.0, WinPE 5.0 und WinPE 10.0.
- Ihr Computer muss folgende Anforderungen erfüllen:
  - Für WinPE 3.0 – mindestens 256 MB RAM
  - Für WinPE 4.0 – mindestens 512 MB RAM
  - Für WinPE 5.0 – mindestens 1 GB RAM
  - Für WinPE 10.0 – mindestens 512 MB RAM
- Sollte der Acronis Media Builder Ihren USB-Stick nicht erkennen, dann gehen Sie so vor, wie in diesem Artikel der Acronis Knowledge Base beschrieben: https://kb.acronis.com/content/1526.
- Wenn Sie mit einem Boot-Medium booten, können Sie keine Backups auf Laufwerke bzw. Volumes mit Ext2-/Ext3-/Ext4-, ReiserFS- und Linux SWAP-Dateisystemen ausführen.
- Wenn Sie das System mit einem Boot-Medium starten und dessen autonome Notfallversion von Acronis Cyber Protect Home Office verwenden, können Sie keine Dateien oder Ordner wiederherstellen, die mit der Verschlüsselungsfunktion von Windows XP (und späteren Windows-Versionen) geschützt wurden. Weitere Informationen finden Sie unter Dateisicherheitseinstellungen für Backups. Backups, die von Acronis Cyber Protect Home Office selbst verschlüsselt wurden, können jedoch wiederhergestellt werden.
- Wenn Sie versuchen, ein Boot-Medium auf einem Laufwerk zu erstellen, auf dem bereits ein Survival Kit ist, wird der Acronis Media Builder versuchen, nur das versteckte Volume zu überschreiben und mit dem Boot-Medium zu aktualisieren – und nicht das ganze Laufwerk zu formatieren.

## Ein Acronis Boot-Medium erstellen

1. Schließen Sie einen USB-Stick oder eine externe Festplatte (HDD/SDD) an oder legen Sie eine leere CD bzw. DVD ein.
2. Acronis Cyber Protect Home Office starten.
3. Klicken Sie im Bereich **Extras** auf **Bootable Rescue Media Builder**.
4. Wählen Sie eine Erstellungsmethode.
   - **Einfach** – Das ist die einfachste Methode. Acronis Cyber Protect Home Office wird den optimalen Medientyp für Ihren Computer auswählen. Falls Sie Windows 7 oder eine neuere Windows-Version verwenden, wird ein WinRE-basiertes Medium erstellt.
   - **Advanced** – Mit dieser Option können Sie einen Medientyp wählen. Das bedeutet, dass Sie das Boot-Medium nicht nur für diesen Computer erstellen können, sondern auch für einen Computer mit einer anderen Windows-Version. Ausführlichere Informationen finden Sie im Abschnitt 'Acronis Media Builder'.

     Wenn Sie die Erstellung eines Linux-basierten Mediums ausgewählt haben, müssen Sie noch die Acronis Cyber Protect Home Office Komponenten bestimmen, die auf dem Medium eingerichtet werden sollen. Überprüfen Sie, dass die von Ihnen ausgewählten Komponenten mit der Hardware-Architektur des Zielcomputers kompatibel sind. Weitere Informationen finden Sie im Abschnitt 'Einstellungen für Wechselmedien'.

Falls Sie die Erstellung eines WinRE- oder WinPE-Mediums ausgewählt haben, müssen Sie folgendermaßen vorgehen:

- Bestimmen Sie die Hardware-Architektur für das Medium – 32 oder 64 Bit. Beachten Sie dabei, dass ein 32-Bit-Boot-Medium nur mit 32-Bit-Computern funktioniert, während ein 64-Bit-Boot-Medium mit 32- und 64-Bit-Computern funktioniert.
- Wählen Sie ein Toolkit aus, welches für die Erstellung des Boot-Mediums verwendet werden soll. Wenn Sie 'WAIK' oder 'WADK' auswählen und das entsprechende Kit aber nicht auf Ihrem Computer installiert ist, müssen Sie dieses zuerst von der Microsoft-Website herunterladen und dann die erforderlichen Komponenten (die Bereitstellungstools und Windows-Vorinstallationsumgebung (Windows PE)) installieren.

  Falls die WinPE-Dateien auf Ihrem Computer bereits vorliegen, aber nicht im Standard-Ordner gespeichert sind, müssen Sie den tatsächlichen Speicherort der Dateien erst noch spezifizieren. Anschließend wird das Acronis Plug-in dem vorhandenen WinPE-Image hinzugefügt.
- Um eine optimale Kompatibilität mit Ihrer Hardware zu gewährleisten, können Sie Treiber auswählen, die dem Medium hinzugefügt werden sollen.

5. Bestimmen Sie das Ziel für das Medium:
   - **CD**
   - **DVD**
   - **Externes Laufwerk**
   - **USB-Stick**

     Falls Ihr Laufwerk ein nicht unterstütztes Dateisystem verwendet, wird Acronis Cyber Protect Home Office vorschlagen, dieses mit dem FAT-Dateisystem zu formatieren.

     **Warnung!**
     Durch eine Formatierung werden alle Daten auf dem Laufwerk gelöscht.

   - **ISO-Image-Datei**

     Sie müssen den Namen für die .iso-Datei und den Zielordner spezifizieren.

     Wenn die .iso-Datei erstellt wurde, können Sie diese anschließend auf CD bzw. DVD brennen. Unter Windows 7 (und höher) können Sie dies beispielsweise auch mit der integrierten Brennfunktion tun. Klicken Sie dazu im Windows Datei-Explorer doppelt auf die erstellte ISO-Image-Datei und dann auf **Brennen**.
   - **WIM-Image-Datei** (nur für WinPE-basierte Medien verfügbar)

     Acronis Cyber Protect Home Office kann das Acronis Plug-in einer (vom Windows AIK oder dem Windows ADK erstellten) .wim-Datei hinzufügen. Sie müssen einen Namen für die neue .wim-Datei und den Zielordner spezifizieren.

     Um ein Boot-Medium auf Basis einer .wim-Datei erstellen zu können, müssen Sie diese zuerst in eine .iso-Datei konvertieren. Weitere Informationen finden Sie im Abschnitt 'Eine .iso-Datei von einer .wim-Datei erstellen'.

**Hinweis**
Wenn der Acronis Media Builder auf diesem Laufwerk ein zuvor erstelltes Survival Kit erkennt, wird er versuchen, nur das versteckte Volume zu überschreiben und mit dem Boot-Medium zu aktualisieren – und nicht das ganze Laufwerk zu formatieren.

6. Klicken Sie auf **Fertigstellen**.

## Startparameter für das Acronis Boot-Medium

Sie können Startparameter für das Acronis Boot-Medium einrichten, um bestimmte Boot-Optionen für eine bessere Kompatibilität mit abweichender Hardware zu konfigurieren. Es sind verschieden Optionen verfügbar (nousb, nomouse, noapic usw.). Diese Parameter sind für erfahrene Benutzer gedacht. Wenn Sie beim Testen des Boot-Vorgangs von einem Acronis Boot-Medium Probleme mit der Hardware-Kompatibilität erleben, wenden Sie sich am besten an den Acronis Support.

***So können Sie Startparameter hinzufügen:***

1. Geben Sie einen Befehl in das Eingabefeld **Parameter** ein. Sie können mehrere Befehle eingeben, indem Sie diese per Komma trennen.
2. Klicken Sie auf **Weiter**, um fortzufahren.

Vor dem Booten des Linux-Kernels können zusätzliche Parameter zugewiesen werden

### Beschreibung

Die folgenden Parameter können verwendet werden, um den Linux-Kernel in einen speziellen Modus zu laden:

- **acpi=off**

Deaktiviert ACPI und kann bei bestimmten Hardware-Konfigurationen hilfreich sein.

- **noapic**

Deaktiviert APIC (Advanced Programmable Interrupt Controller) und kann bei bestimmten Hardware-Konfigurationen hilfreich sein.

- **nousb**

Deaktiviert, dass USB-Module geladen werden.

- **nousb2**

Deaktiviert die USB 2.0-Unterstützung. USB 1.1-Geräte arbeiten mit dieser Option weiterhin. Mit dieser Einstellung können einige USB-Laufwerke im USB 1.1-Modus verwendet werden, wenn sie im USB 2.0-Modus nicht arbeiten.

- **quiet**

Dieser Parameter ist standardmäßig aktiviert und daher werden beim Start keine Meldungen angezeigt. Wird er gelöscht, so werden während des Ladevorgangs des Linux-Kernels Startmeldungen angezeigt und die Befehlszeilenoberfläche vor Ausführung des Acronis Cyber Protect Home Office Programms angeboten.

- **nodma**

Deaktiviert DMA für alle IDE-Laufwerke. Verhindert auf mancher Hardware ein Einfrieren des Kernels.

- **nofw**

Deaktiviert die Unterstützung für FireWire (IEEE1394).

- **nopcmcia**

Deaktiviert die Erkennung von PCMCIA-Hardware.

- **nomouse**

Deaktiviert die Maus-Unterstützung.

- **[module name]=off**

Deaktiviert das betreffende Modul (z.B. **sata_sis=off**).

- **pci=bios**

Erzwingt die Verwendung des PCI BIOS und dass auf Hardware-Geräte nicht direkt zugegriffen wird. Dieser Parameter kann z.B. verwendet werden, wenn die Maschine eine nicht standardgemäße PCI Host-Bridge hat.

- **pci=nobios**

Verbietet die Verwendung des PCI BIOS; nur direkte Hardware-Zugriffsmethoden sind erlaubt. Dieser Parameter kann z.B. hilfreich sein, wenn Sie erleben, dass es während des Boot-Vorgangs zu wahrscheinlich durch das BIOS verursachten Abstürzen kommt.

- **pci=biosirq**

Verwendet PCI BIOS-Aufrufe, um die Interrupt Routing-Tabelle zu erhalten. Von solchen Aufrufen ist bekannt, dass sie auf diversen Maschinen fehlerhaft sind und die Maschine sich durch ihre Verwendung aufhängen kann, auf anderen Computern kann es aber der einzige Weg sein, die Interrupt Routing-Tabelle zu erhalten. Versuchen Sie diese Option, wenn es dem Kernel nicht möglich ist, IRQs zuzuteilen oder den sekundären PCI-Bus auf dem Mainboard zu entdecken.

- **vga=ask**

Zeigt eine Liste der für Ihre Grafikkarte verfügbaren Videomodi an und ermöglicht den für Ihre Grafikkarte und Ihren Monitor am besten passenden Darstellungsmodus zu wählen. Testen Sie diese Option, falls der automatisch gewählte Videomodus mit Ihrer Hardware nicht funktioniert.

## Treiber zu einem vorhandenen .wim-Image hinzufügen

Manchmal verfügt ein einfaches WinPE-Medium mit Acronis Plug-in nicht über die für Ihre Hardware notwendigen Treiber (beispielsweise für Massenspeicher-Controller). Treiber lassen sich am leichtesten im 'Erweiterten Modus' des Acronis Media Builder auswählen und hinzufügen. Sie können die Treiber manuell zu einer vorhandenen .wim-Datei hinzufügen, bevor Sie eine ISO-Datei mit dem Acronis Plug-in erstellen.

**Warnung!**
Achtung! Sie können nur Treiber hinzufügen, die die Dateinamenserweiterung '.inf' haben.

Die folgende Prozedur basiert auf einem (englischsprachigen) MSDN-Artikel, den Sie unter https://technet.microsoft.com/ finden können.

***So können Sie ein benutzerdefiniertes Windows PE-Image erstellen***

1. Sollten Sie noch keine .wim-Datei mit dem Acronis Plug-in haben, so können Sie diese erstellen, indem Sie den Acronis Media Builder starten und dann die Option **WIM-Datei** als Ziel für das WinPE-basierte Medium bestimmen. Weitere Informationen finden Sie im Abschnitt 'Ein Acronis Boot-Medium erstellen'.
2. Gehen Sie – in Abhängigkeit von Ihrer Version des Windows AIK oder Windows ADK – folgendermaßen vor:
   - Klicken Sie im **Start**-Menü auf **Microsoft Windows AIK**, klicken Sie dann mit der rechten Maustaste auf **Windows PE Tools-Eingabeaufforderung** und wählen Sie anschließend den Befehl **Als Administrator ausführen**.
   - Klicken Sie im **Start**-Menü auf **Microsoft Windows AIK**, klicken Sie dann mit der rechten Maustaste auf **Deployment-Tools-Eingabeaufforderung** und wählen Sie anschließend die Option **Als Administrator ausführen**.
   - Klicken Sie im **Start**-Menü zuerst auf **Windows-Kits**, dann auf **Windows ADK**, dann mit der rechten Maustaste auf **Umgebung für Bereitstellungs- und Imageerstellungstools** und wählen Sie abschließend den Befehl **Als Administrator ausführen**.
3. Starten Sie das Skript 'copype.cmd', um einen Ordner mit den Windows PE-Dateien zu erstellen. Geben Sie z.B. auf der Kommandozeilen-Ebene ein:

   ```
   copype amd64 C:\winpe_x64
   ```

4. Kopieren Sie Ihre Wim-Datei in einen Ordner – beispielsweise 'C:\winpe_x64\'. Der vorgegebene Standardname für die Datei ist 'AcronisBootablePEMedia.wim'.
5. Mounten Sie das Basisabbild (Image) unter Verwendung des DISM-Tools an ein lokales Verzeichnis. Geben Sie dazu Folgendes ein:

   ```
   Dism /Mount-Wim /WimFile:C:\winpe_x64\AcronisBootablePEMedia.wim /index:1
   /MountDir:C:\winpe_x64\mount
   ```

6. Fügen Sie Ihre Hardware-Treiber unter Verwendung des 'DISM'-Befehls mit der Option 'Add-Driver' hinzu. Beispiel: um den Treiber 'Mydriver.inf' hinzuzufügen, der sich im Ordner 'C:\drivers\' befindet, geben Sie folgenden Befehl ein:

```
Dism /image:C:\winpe_x64\mount /Add-Driver /driver:C:\drivers\mydriver.inf
```

7. Wiederholen Sie den vorherigen Schritt für jeden noch zusätzlich benötigten Treiber.
8. Übernehmen Sie die Änderungen per DISM-Befehl:

```
Dism /Unmount-Wim /MountDir:C:\winpe_x64\mount /Commit
```

9. Erstellen Sie dann ein PE-Image (.iso-Datei) von der resultierenden .wim-Datei. Weitere Informationen finden Sie im Abschnitt 'Eine .iso-Datei von einer .wim-Datei erstellen'.

## Eine .iso-Datei von einer .wim-Datei erstellen

Um ein Boot-Medium auf Basis einer .wim-Datei erstellen zu können, müssen Sie diese zuerst in eine .iso-Datei konvertieren.

***So können Sie ein PE-Image (.iso-Datei) von der resultierenden .wim-Datei erstellen***

1. Gehen Sie – in Abhängigkeit von Ihrer Version des Windows AIK oder Windows ADK – folgendermaßen vor:
   - Klicken Sie im **Start**-Menü auf **Microsoft Windows AIK**, klicken Sie dann mit der rechten Maustaste auf **Windows PE Tools-Eingabeaufforderung** und wählen Sie anschließend den Befehl **Als Administrator ausführen**.
   - Klicken Sie im **Start**-Menü auf **Microsoft Windows AIK**, klicken Sie dann mit der rechten Maustaste auf **Deployment-Tools-Eingabeaufforderung** und wählen Sie anschließend die Option **Als Administrator ausführen**.
   - Klicken Sie im **Start**-Menü zuerst auf **Windows-Kits**, dann auf **Windows ADK**, dann mit der rechten Maustaste auf **Umgebung für Bereitstellungs- und Imageerstellungstools** und wählen Sie abschließend den Befehl **Als Administrator ausführen**.
2. Starten Sie das Skript 'copype.cmd', um einen Ordner mit den Windows PE-Dateien zu erstellen. Geben Sie z.B. auf der Kommandozeilen-Ebene ein:

```
copype amd64 C:\winpe_x64
```

3. Überschreiben Sie die vorgegebene Datei 'boot.wim' (im Windows PE-Ordner) mit der neu erstellten .wim-Datei (beispielsweise 'AcronisBootablePEMedia.wim'). Falls sich die Datei 'AcronisBootablePEMedia.wim' auf 'c:\' befindet, gilt:
   Geben Sie für WinPE 3.0 Folgendes ein:

```
copy c:\AcronisBootablePEMedia.wim c:\winpe_x64\ISO\sources\boot.wim
```

   Geben Sie für WinPE 4.0, WinPE 5.0 oder WinPE 10.0 Folgendes ein:

```
copy "c:\AcronisBootablePEMedia.wim" c:\winpe_x64\media\sources\boot.wim
```

4. Verwenden Sie das Tool **Oscdimg**. Geben Sie zur Erstellung einer .iso-Datei Folgendes ein:

   ```
   oscdimg -n -bc:\winpe_x64\etfsboot.com c:\winpe_x64\ISO c:\winpe_x64\winpe_x64.iso
   ```

   Geben Sie alternativ Folgendes ein, um das Medium auf BIOS- und UEFI-Computern booten zu können:

   ```
   oscdimg -m -o -u2 -udfver102 -bootdata:2#p0,e,bc:\winpe_
   x64\fwfiles\etfsboot.com#pEF,e,bc:\winpe_x64\fwfiles\efisys.bin c:\winpe_x64\media
   c:\winpe_x64\winpe_x64.iso
   ```

5. Brennen Sie die .iso-Datei auf CD/DVD (mit dem Brennprogramm eines Drittanbieters). Sie verfügen anschließend über ein bootfähiges Windows PE-Medium mit integriertem Acronis Cyber Protect Home Office.

# So stellen Sie sicher, dass Ihr Boot-Medium bei Bedarf auch funktioniert

Um die Chance zur Wiederherstellung Ihres Computers zu maximieren, sollten Sie überprüfen, ob sich Ihr Computer mit dem Boot-Medium starten lässt. Sie sollten zudem überprüfen, dass das Boot-Medium auch alle notwendigen Geräte Ihres Computers erkennt, wie etwa Festplatten, Maus, Tastatur und Netzwerkadapter.

Falls Sie eine über den Handel vertriebene Paketversion haben, die eine bootfähige CD enthält – und Sie Acronis Cyber Protect Home Office noch nicht per Update aktualisiert haben – dann können Sie auch diese CD für den Test verwenden. Ansonsten sollten Sie möglichst ein neues Boot-Medium erstellen. Weitere Informationen finden Sie im Abschnitt 'Ein Acronis Boot-Medium erstellen'.

***So können Sie das Boot-Medium testen***

**Hinweis**
Externe Laufwerke, die Sie zum Speichern von Backups verwenden, müssen bereits vor der Ausführung des Boot-Mediums angeschlossen und eingeschaltet sein. Anderenfalls erkennt das Programm sie möglicherweise nicht.

1. Konfigurieren Sie Ihren Computer so, dass er das Booten von einem solchen Boot-Medium zulässt. Legen Sie dann das Gerät für das Boot-Medium (CD-/DVD-Laufwerk oder USB-Stick) als erstes Boot-Gerät fest. Weitere Informationen finden Sie im Abschnitt 'Boot-Reihenfolge im BIOS arrangieren'.
2. Wenn Sie eine bootfähige CD haben und von der CD booten möchten, drücken Sie eine beliebige Taste, wenn die Eingabeaufforderung 'Druecken Sie eine beliebige Taste, um von der CD zu starten' angezeigt wird. Wenn Sie nicht innerhalb von fünf Sekunden eine Taste drücken, müssen Sie den Computer neu starten.

3. Wählen Sie nach dem Erscheinen des Boot-Menüs den Eintrag **Acronis Cyber Protect Home Office**.

   **Hinweis**
   Sollte Ihre kabellose Maus nicht funktionieren, dann versuchen Sie sie mit einer kabelgebundenen zu ersetzen. Diese Empfehlung gilt auch für die Tastatur.

   **Hinweis**
   Wenden Sie sich an den Acronis Support, wenn Ihnen keine entsprechende Maus oder Tastatur zur Verfügung steht. Dort wird man für Sie eine bootfähigen CD mit den Treibern für Ihr Maus- und Tastaturmodell erstellen. Beachten Sie, dass die Suche nach passenden Treibern und das Erstellen einer benutzerdefinierten Boot-CD sehr zeitaufwendig sein kann. Bei manchen Modellen kann es unter Umständen auch nicht erfolgreich sein.

4. Wir empfehlen, bei Programmstart zu versuchen, einige Dateien aus Ihrem Backup wiederherzustellen. Mit einer probeweise durchgeführten Wiederherstellung können Sie sicherstellen, dass Ihre Boot-CD für die Wiederherstellung eingesetzt werden kann. Zusätzlich können Sie sicherstellen, dass das Programm alle in Ihrem System befindlichen Festplattenlaufwerke findet.

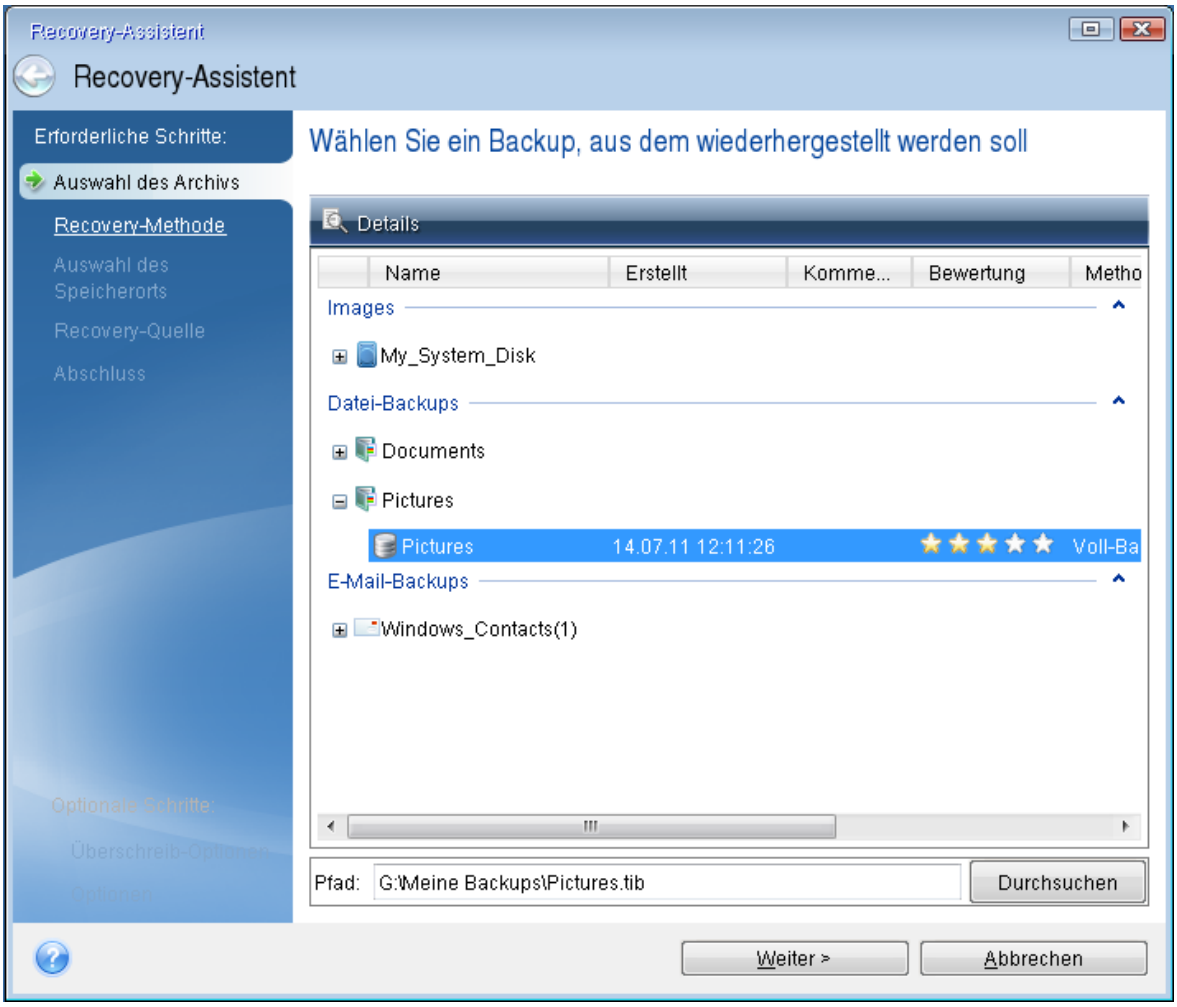
   **Hinweis**
   Wenn Sie über ein ungenutztes Laufwerk verfügen, empfehlen wir Ihnen, Ihr System-Volume testweise auf diesem Laufwerk wiederherzustellen.

***So können Sie die Wiederherstellung, Laufwerke und Netzwerkadapter überprüfen***

1. Wenn Sie Datei-Backups haben, starten Sie den Recovery-Assistenten, indem Sie in der Symbolleiste auf **Recovery** –> **Datei-Recovery** klicken.

   **Hinweis**
   Wenn Sie nur Laufwerk- und Volume-Backups haben, startet der Recovery-Assistent genauso, wie sich auch die Wiederherstellungsprozedur gleichen. Sie müssen in diesem Fall beim Schritt **Recovery-Methode** die Option **Recovery von Dateien und Verzeichnissen** auswählen.

2. Wählen Sie im Schritt **Archiv-Speicherort** ein Backup und klicken Sie dann auf **Weiter**.



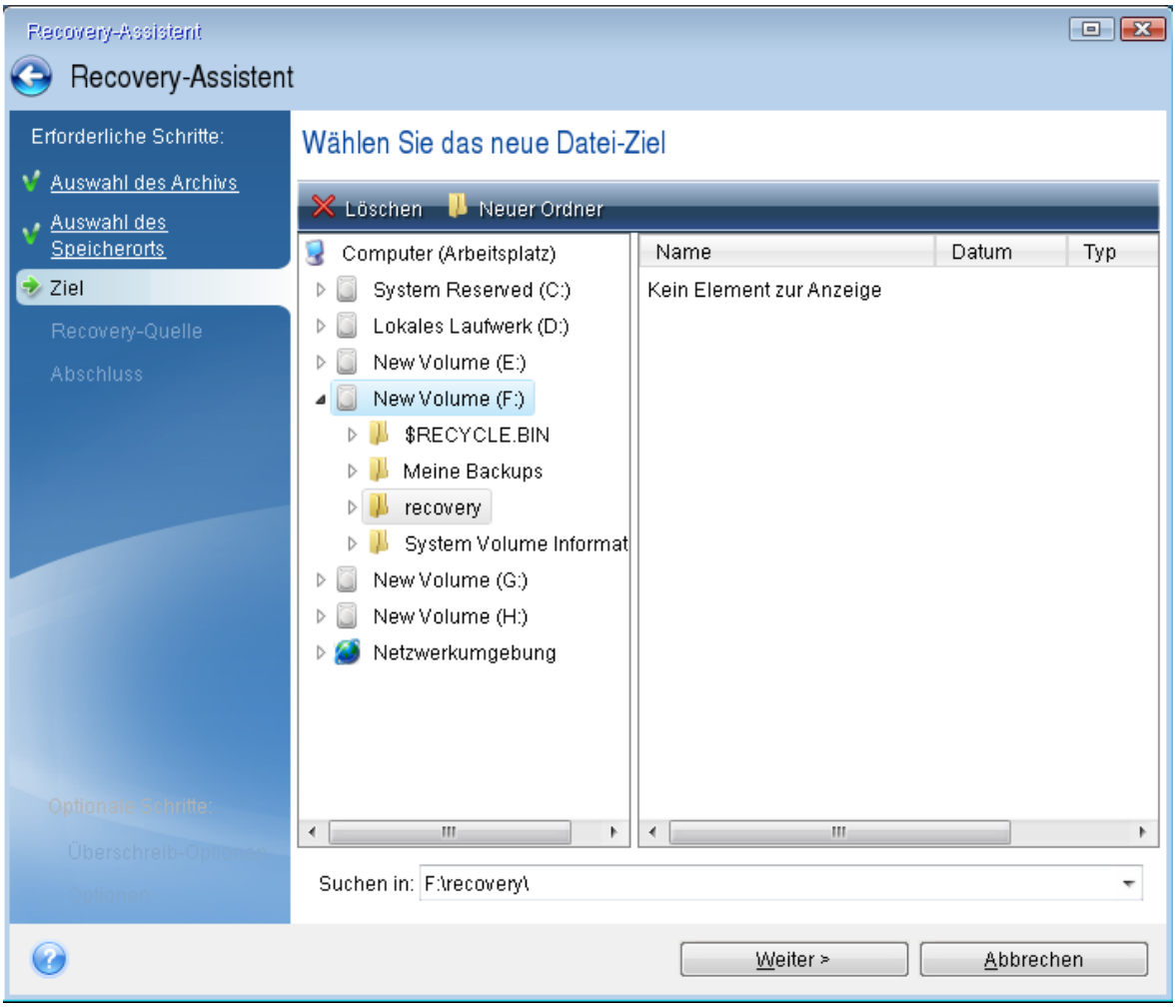

3. Wenn Sie Dateien mit der Boot-CD wiederherstellen, müssen Sie einen neuen Speicherort für die wiederhergestellten Dateien angeben. Klicken Sie daher beim Schritt **Auswahl des Speicherorts** einfach auf **Weiter**.
4. Überprüfen Sie, wenn sich das Fenster **Speicherort** öffnet, ob all Ihre Laufwerke unter **Computer** angezeigt werden.

**Hinweis**
Wenn Sie die Backups im Netzwerk speichern, sollten Sie auch überprüfen, ob Sie auf das Netzwerk zugreifen können.

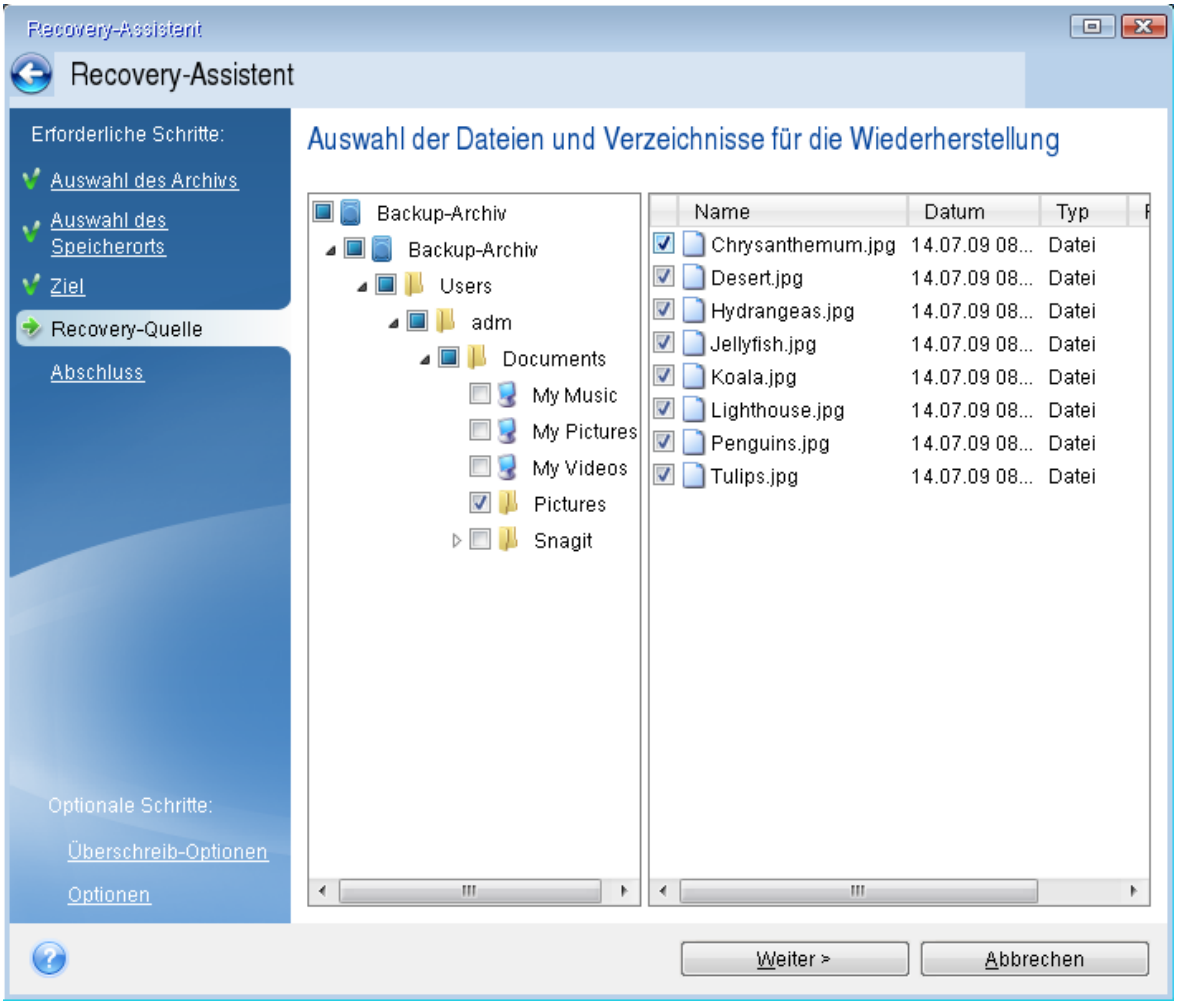
**Hinweis**
Wenn keine Computer im Netzwerk angezeigt werden, aber das Symbol **Netzwerkumgebung** unter unter **Computer** angezeigt wird, geben Sie die Netzwerkeinstellungen manuell ein. Öffnen Sie dazu das Fenster unter **Extras und Werkzeuge** –> **Options** –> **Netzwerkadapter**.

**Hinweis**

Wenn das Symbol **Netzwerkumgebung** nicht unter **Computer** angezeigt wird, gibt es möglicherweise Probleme mit Ihrer Netzwerkkarte oder mit dem Kartentreiber, der von Acronis Cyber Protect Home Office verwendet wird.




5. Wählen Sie den Zielort für die Dateien und klicken Sie dann auf **Weiter**.
6. Aktivieren Sie zur Auswahl mehrerer Dateien, die wiederhergestellt werden sollen, die entsprechenden Kontrollkästchen und klicken Sie dann auf **Weiter**.



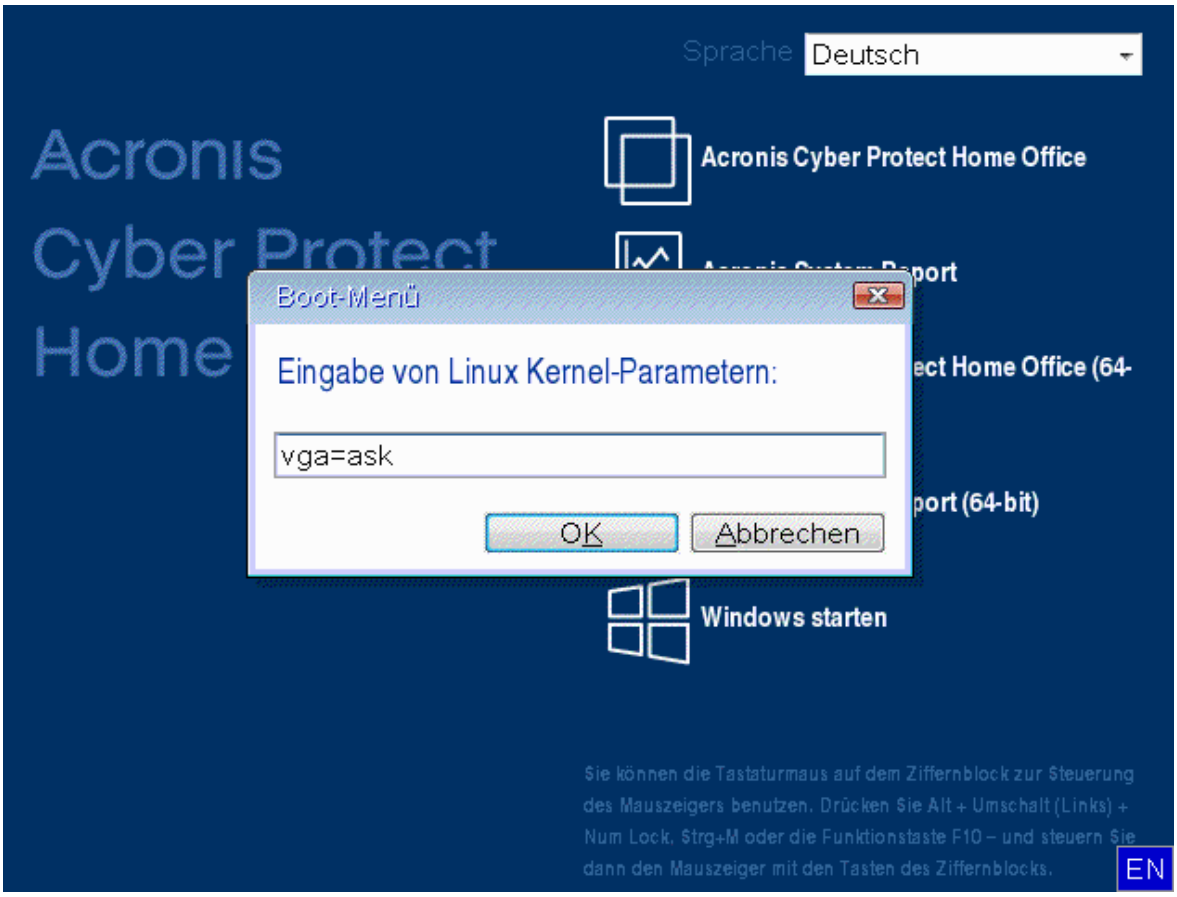

7. Klicken Sie im Fenster 'Zusammenfassung' auf **Fertigstellen**.
8. Beenden Sie nach Abschluss der Wiederherstellung die autonome Notfallversion von Acronis Cyber Protect Home Office.

So können Sie relativ sicher sein, dass Ihre Boot-CD bei Bedarf auch funktioniert.

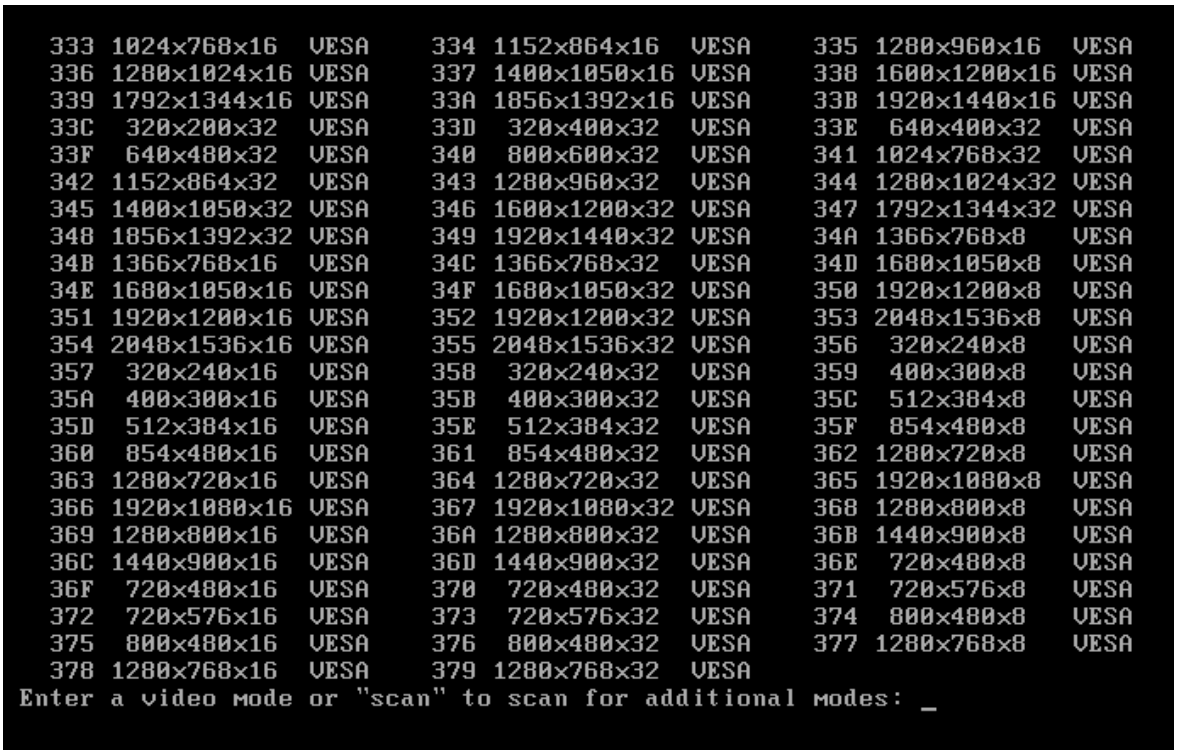
## Auswahl des Grafikkartenmodus beim Starten des Boot-Mediums

Beim Starten des Boot-Mediums wird – abhängig von den technischen Daten der Grafikkarte sowie des Monitors – automatisch der optimale Grafikkartenmodus ausgewählt. Es kann jedoch vorkommen, dass das Programm einen falschen Grafikmodus auswählt, der für die verwendete Hardware nicht geeignet ist. In einem solchen Fall können Sie einen geeigneten Grafikmodus folgendermaßen auswählen:

1. Beginnen Sie mit dem Start des Boot-Mediums. Wenn das Boot-Menü erscheint, bewegen Sie den Mauszeiger über den Eintrag **Acronis Cyber Protect Home Office** und drücken Sie dann die Taste F11.
2. Wenn die Befehlszeile erscheint, geben Sie **vga=ask** ein und klicken Sie auf **OK**.




3. Wählen Sie im Boot-Menü den Eintrag **Acronis Cyber Protect Home Office** aus, damit die entsprechende autonome Notfallversion des Produkts gestartet wird. Um die verfügbaren Grafikkartenmodi angezeigt zu bekommen, drücken Sie die Eingabetaste, wenn die entsprechende Meldung erscheint.
4. Wählen Sie einen Grafikmodus, der Ihrer Meinung nach am besten für Ihren Monitor geeignet ist und geben Sie dessen Nummer auf der Befehlszeile ein. Wenn Sie z.B. 338 eingeben, wird der Grafikkartenmodus 1600x1200x16 ausgewählt (siehe nachfolgende Abbildung).




5. Warten Sie, bis Acronis Cyber Protect Home Office geladen wurde und überprüfen Sie dann, ob die Darstellungsqualität der Willkommensseite auf dem Monitor Ihren Anforderungen entspricht.

Wenn Sie einen anderen Grafikkartenmodus testen möchten, beenden Sie Acronis Cyber Protect Home Office und wiederholen Sie die beschriebene Prozedur.

Nachdem Sie den optimalen Grafikkartenmodus für Ihre Hardware gefunden haben, können Sie ein neues Boot-Medium erstellen, das automatisch diesen Grafikkartenmodus auswählt.

Starten Sie dafür den Acronis Media Builder, wählen Sie die erforderlichen Medienkomponenten aus und geben Sie beim Schritt **Startparameter für das Boot-Medium** die Nummer für den Modus zusammen mit dem Präfix '0x' (in unserem Fall 0x338) in der Befehlszeile ein. Danach können Sie das Medium wie gewohnt erstellen.

# Acronis Startup Recovery Manager

Mit dem Acronis Startup Recovery Manager können Sie Acronis Cyber Protect Home Office starten, ohne dass das Betriebssystem des Computers geladen werden muss. Mit dieser Funktion können Sie Acronis Cyber Protect Home Office eigenständig zur Wiederherstellung beschädigter Volumes verwenden. Und das auch dann, wenn das eigentliche Betriebssystem nicht mehr starten kann. Anders als beim Starten mit einem Acronis Boot-Medium (auch Notfallmedium genannt), benötigen Sie kein separates Medium oder eine Netzwerkverbindung, um Acronis Cyber Protect Home Office starten zu können.

**Hinweis**
Der Acronis Startup Recovery Manager kann nicht auf Tablets verwendet werden, die Windows als Betriebssystem nutzen.

***So können Sie den Acronis Startup Recovery Manager aktivieren***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie im Programmbereich **Tools** auf **Alle Tools** und anschließend per Doppelklick auf **Acronis Startup Recovery Manager aktivieren**.
3. Klicken Sie im dann geöffneten Fenster auf **Aktivieren**.


Schalten Sie im Fall eines Fehlers den Computer ein und drücken Sie die Taste F11, sobald Sie die Meldung 'Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Managers' sehen. Auf diese Weise wird eine autonome, Linux-basierte Notfallversion von Acronis Cyber Protect Home Office gestartet, die sich nur wenig von der vollständigen Windows-Version unterscheidet.

***So können Sie den Acronis Startup Recovery Manager deaktivieren***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie im Programmbereich **Tools** auf **Alle Tools** und anschließend per Doppelklick auf **Acronis Startup Recovery Manager aktivieren**.
3. Klicken Sie im dann geöffneten Fenster auf **Deaktivieren**.

## Zusätzliche Informationen

Die Laufwerksbuchstaben in der autonomen Notfallversion von Acronis Cyber Protect Home Office können von der Zuordnung unter Windows abweichen. So könnte beispielsweise die Zuordnung des Laufwerks D: in der autonomen Notfallversion von Acronis Cyber Protect Home Office dem Laufwerk E: unter Windows entsprechen. Laufwerksbezeichnungen sowie Informationen zur

Volume-Größe, Dateisystem, Laufwerkskapazität, Hersteller und Modellnummer können Ihnen ebenfalls bei der korrekten Identifizierung gewünschter Laufwerke/Volumes helfen.

Sie können einen zuvor aktivierten Acronis Startup Recovery Manager nicht verwenden, wenn der Try&Decide-Modus angeschaltet ist. Wenn Sie den Computer im Probiermodus neu starten, können Sie den Acronis Startup Recovery Manager wieder verwenden.

**Beeinflusst der Acronis Startup Recovery Manager andere Boot-Loader?**

Wenn der Acronis Startup Recovery Manager aktiviert wird, überschreibt dieser den vorhandenen Master Boot Record (MBR) mit seinem eigenen Boot-Code. Falls Sie einen Boot-Manager aus anderer Quelle installiert haben, müssen Sie diesen nach Aktivierung des Startup Recovery Managers reaktivieren. Linux-Loader (z.B. LiLo oder GRUB) sollten Sie in den Boot-Record des Linux-Root- oder Boot-Volumes statt in den MBR verschieben, bevor Sie den Acronis Startup Recovery Manager aktivieren.

Der Boot-Mechanismus von UEFI-basierten Computern unterscheidet sich von BIOS-basierten. Jedes Ladeprogramm für ein Betriebssystem (OS Loader) oder anderes Boot-Programm hat seine eigene Boot-Variable, die einen Pfad zu dem entsprechenden Ladeprogramm (Loader) definiert. Alle Loader sind in einem speziellen Volume namens 'EFI-Systempartition' gespeichert. Wenn Sie den Acronis Startup Recovery Manager in einem per UEFI-gebooteten System aktivieren, ändert dieser die Boot-Sequenz, indem er seine eigene Boot-Variable schreibt. Diese Variable wird der Liste von Variablen hinzugefügt und ändert diese nicht. Da alle Loader unabhängig sind und sich nicht gegenseitig beeinflussen, muss weder vor noch nach Aktivierung des Acronis Startup Recovery Managers etwas geändert werden.

# Try&Decide

**Hinweis**
Wenn Sie Try&Decide installieren wollen, können Sie diese Komponente direkt bei der Installation von Acronis Cyber Protect Home Office auswählen oder sie auch später noch hinzufügen (wie in Abschnitt '"Acronis Cyber Protect Home Office installieren und deinstallieren" (S. 15)' beschrieben).

Wenn Sie Try&Decide einschalten, befindet sich der Rechner im 'Probiermodus' (auch 'Try&Decide'-Modus genannt). Sie können anschließend beliebige Computeraktionen ausführen, die möglicherweise gefährlich sind. Denn Sie müssen nun nicht mehr befürchten, möglicherweise Ihr Betriebssystem, Ihre Programme oder Daten zu beschädigen. Wenn Sie Try&Decide wieder ausschalten, können Sie entscheiden, ob Sie die an Ihrem Computer vorgenommene Änderungen hinzufügen oder verwerfen möchten.

## Szenarien, bei denen Try&Decide helfen kann

Wir empfehlen, Try&Decide vor der Durchführung folgender Aktionen einzuschalten:

- Der Änderung von Systemeinstellungen, wenn Sie sich nicht sicher sind, welchen Einfluss diese Änderungen auf Ihren Computer haben können.

- Dem Installieren von System-Updates, von Treibern etc.
- Dem Installieren unbekannter Anwendungen.
- Dem Öffnen von E-Mail-Anhängen, die von unbekannten Absendern kommen.
- Dem Besuch von Webseiten, die potenziell gefährliche Inhalte haben.

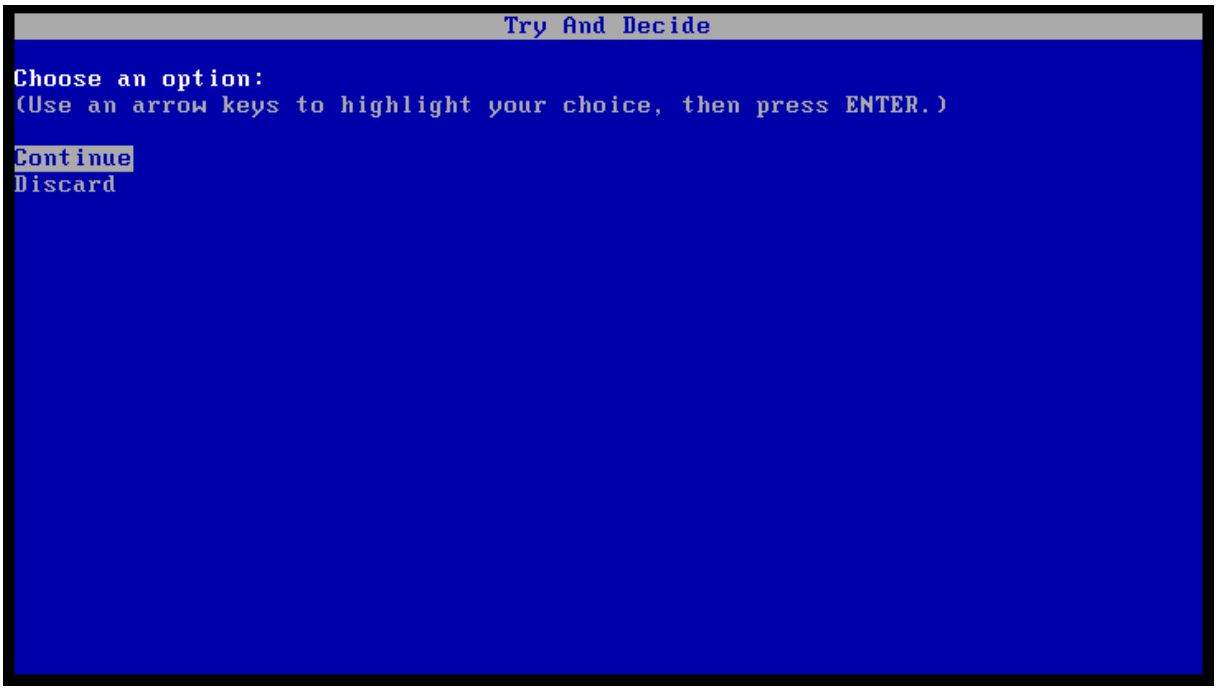
**Hinweis**
Beachten Sie: Wenn Sie im Probiermodus E-Mails von einem POP3-Mail-Server herunterladen, neue Dateien erstellen oder bestehende Dokumente ändern – und diese Änderungen dann verwerfen – gehen alle diese betreffenden Dateien und E-Mails samt der an ihnen vorgenommenen Änderungen verloren. Speichern Sie daher in diesem Fall die neuen Dateien und bearbeiteten Dokumente auf einem externen Laufwerk (beispielsweise einem USB-Stick) und trennen Sie dieses vom Computer, bevor Sie die vorgenommenen Änderungen mit Try&Decide verwerfen.

## Die Vorgehensweise von Try&Decide nach einem Computer-Neustart

Sie können Try&Decide so lange wie gewünscht eingeschaltet lassen, da dieser Modus die Neustarts Ihres Betriebssystems 'überlebt'.

Startet der Computer aus irgendeinem Grund neu, während Sie im Probiermodus arbeiten, dann wird vor dem Starten des Betriebssystems ein Dialogfeld mit zwei Optionen angezeigt – eine zum Beenden des Modus und zum Verwerfen der Änderungen sowie eine zum Weiterarbeiten im aktiven Modus. Auf diese Weise können Sie die Änderungen verwerfen, die zum Systemabsturz geführt haben. Wenn Sie andererseits nach Installation einer Anwendung das System neu booten, können Sie nach Start von Windows weiter im Probiermodus arbeiten.

Während Sie im Probiermodus sind, führt jeder normale (per Software ausgelöste) Neustart Ihres Computers dazu, dass dem Try&Decide-Storage, der zur Speicherung der virtuellen Änderungen festgelegt wurde, bis zu 500 MB organisatorische Daten hinzugefügt werden.



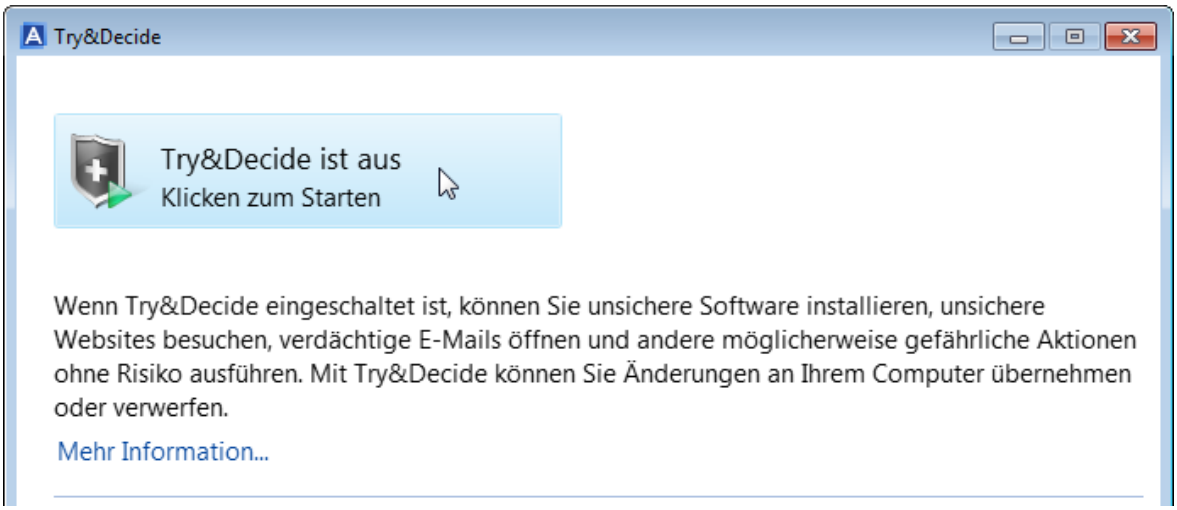

## Einschränkungen bei Verwendung von Try&Decide

- Try&Decide ist nicht mit der Funktion 'Speicher-Integrität' von Windows kompatibel (die in Windows 11 standardmäßig aktiviert ist). Wenn Sie Kompatibilitätsprobleme mit Try&Decide vermeiden wollen, können Sie die Funktion 'Speicher-Integrität' in den Sicherheitseinstellungen von Windows deaktivieren.
- Bedenken Sie bei einer Verwendung unter Windows 7, Windows 8 oder Windows 10, dass das Programm im Probiermodus den freien Speicherplatz intensiv nutzt, auch dann, wenn sich das System im Leerlaufbetrieb befindet. Der Grund dafür sind Aktionen wie etwa die Indexierung, die im Hintergrund ausgeführt werden.
- Beachten Sie, dass ein aktiviertes Try&Decide Ihr System verlangsamt. Zudem kann das Übernehmen der Änderungen lange dauern, vor allem wenn Sie den Probiermodus tagelang aktiviert lassen.
- Try&Decide kann keine Veränderungen an der Partitionierung von Laufwerken verfolgen. Daher sollten Sie im Probiermodus keine virtuellen Aktionen mit Volumes (Änderungen an Größe oder Struktur eines Volumes) durchführen. Darüber hinaus dürfen Sie Try&Decide nicht gleichzeitig mit einer Defragmentierung oder Fehlerprüfung von Laufwerken ausführen, da dies zu irreparablen Schäden am Dateisystem und Verlust der Bootfähigkeit des Systems führen kann.
- Sie können einen zuvor aktivierten Acronis Startup Recovery Manager nicht verwenden, wenn Try&Decide-Modus aktiviert wurde. Wenn Sie den Computer im Probiermodus neu starten, können Sie den Acronis Startup Recovery Manager wieder verwenden.
- Try&Decide und Nonstop Backup können nicht gleichzeitig arbeiten. Wenn Sie den Probiermodus aktivieren, wird Nonstop Backup unterbrochen. Die Nonstop Backup-Sicherung wird fortgesetzt, sobald Sie Try&Decide wieder deaktiviert haben.

- Sie können den Stromsparmodus 'Ruhezustand' nicht verwenden, wenn Try&Decide-Modus aktiviert wurde.
- Try&Decide kann nicht verwendet werden, um dynamische Datenträger zu schützen.
- Try&Decide kann nicht eingesetzt werden, wenn ein Volume in Ihrem System mit BitLocker verschlüsselt ist.
- Eine Acronis Secure Zone kann von Try&Decide weder geschützt noch als Storage für virtuelle Änderungen verwendet werden.

## Try&Decide verwenden

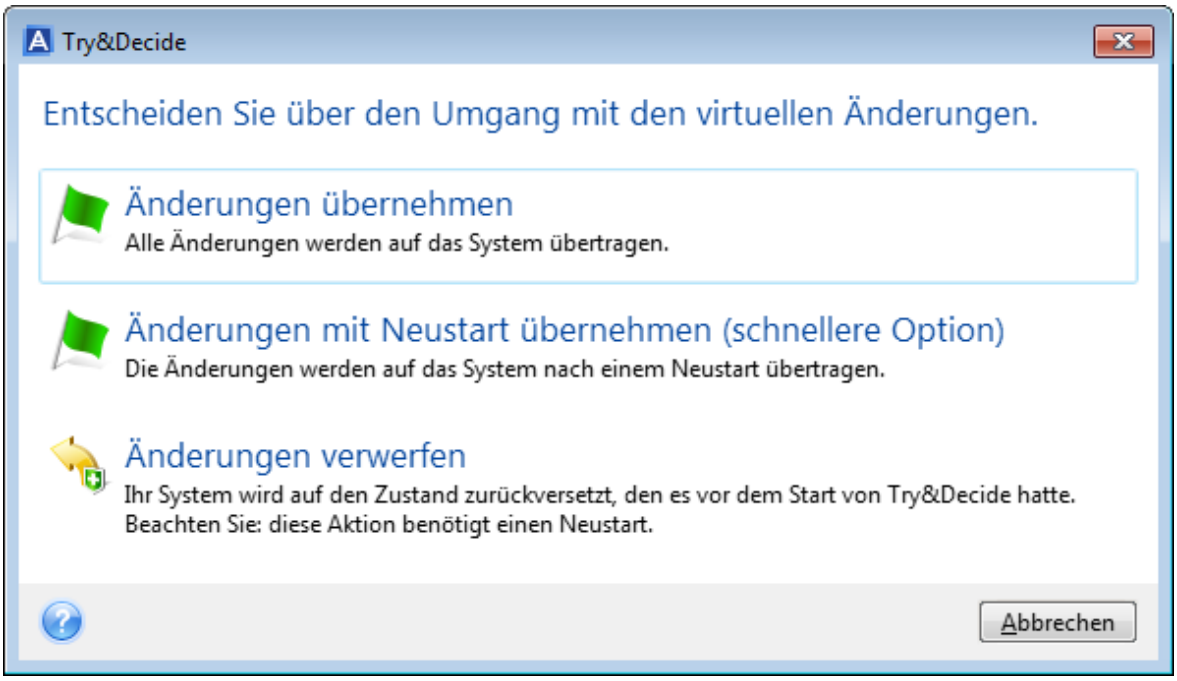
1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie im Bereich **Tools** auf **Try&Decide**.
3. Konfigurieren Sie (bei Bedarf) die Try&Decide-Optionen. Weitere Details finden Sie im Abschnitt 'Try&Decide-Optionen und -Benachrichtigungen'.
4. Klicken Sie auf das **Try&Decide**-Symbol, um den Probiermodus zu starten. Das Programm startet die Verfolgung aller Änderungen am Betriebssystem und den Dateien und speichert temporär alle Änderungen auf dem gewählten Laufwerk.




5. Führen Sie all die Änderungen durch, die Sie ausprobieren wollen.

**Hinweis**
Wenn der Speicherplatz des Speicherortes, den Sie zur Aufnahme der virtuellen Änderungen ausgewählt haben, zur Neige geht, werden Sie vom Programm gefragt, ob Sie die Änderungen übernehmen oder verwerfen wollen. Wenn Sie diese Alarmmeldung ignorieren, startet das Programm das System automatisch neu, sobald das betreffende Laufwerk voll ist. Alle Änderungen werden dabei verworfen.

6. Um den Probiermodus zu stoppen, können Sie auf das **Try&Decide**-Symbol im **Try&Decide**-Fenster klicken.




7. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie **Änderungen übernehmen**, wenn Sie die Änderungen am System übernehmen möchten.
   - Wählen Sie **Änderungen mit Neustart übernehmen**, um den Übernahmevorgang zu beschleunigen. Wenn Sie auf die Schaltfläche klicken, startet Try&Decide den Computer neu und übernimmt während des Neustarts die Änderungen.
   - Wählen Sie **Änderungen verwerfen**, wenn Ihr System auf den Zustand zurückgesetzt werden soll, in dem es sich vor Aktivierung des Probiermodus befand. Wenn Sie diese Option wählen, wird ein Pop-up-Fenster mit folgenden Optionen angezeigt: **Neustart, um die Änderungen zu verwerfen** und **Nicht neu starten**. Wenn Sie die Option **Nicht neu starten** wählen, bleibt die Try&Decide-Funktion aktiviert und die Änderungen werden nicht verworfen.

**Hinweis**
Wenn Sie **Änderungen verwerfen** auf einem Computer wählen, auf dem mehrere Betriebssysteme installiert sind, können Sie nach dem Neustart nur von dem Betriebssystem booten, unter dem Sie im Probiermodus gearbeitet haben. Erst bei einem zweiten Neustart wird der ursprüngliche MBR des Laufwerks wiederhergestellt und so auch die anderen Betriebssysteme wieder bootfähig gemacht.

## Try&Decide-Optionen und -Benachrichtigungen

Sie können die Try&Decide-Optionen im Try&Decide-Fenster ändern. Um alle Einstellungen auf die vorgegebenen Werte zurückzusetzen, klicken Sie auf den Befehl 'Auf Standard zurücksetzen'.

### Geschützte Volumes

So ändern Sie die Einstellung:

1. Klicken Sie auf den Laufwerksbuchstaben neben dem Einstellungsnamen. Das Fenster zur Volume-Auswahl wird geöffnet.
2. Wählen Sie die Volumes, die Sie schützen wollen, und klicken Sie dann auf **OK**.

   Die Standardeinstellung ist, dass Try&Decide das System-Volume (Laufwerk C) schützt. Sie können aber auch jedes andere Volume Ihres System zum Schützen auswählen.

### Storage für virtuelle Änderungen

So ändern Sie die Einstellung:

1. Klicken Sie auf den Laufwerksbuchstaben neben dem Einstellungsnamen. Das Fenster 'Storage für virtuelle Änderungen' wird geöffnet.
2. Bestimmen Sie das Volume, welches zum Speichern der virtuellen Änderungen verwendet werden soll, und klicken Sie anschließend auf **OK**.

   Standardmäßig speichert Try&Decide die Informationen in einem freien Speicherbereich auf Laufwerk C:.

**Hinweis**
Wollen Sie mehr als ein Volume schützen, dann können Sie keine der zu schützenden Volumes als Speicherplatz für die virtuellen Änderungen angeben. Außerdem können Sie kein externes Laufwerk verwenden.

### Benachrichtigungen

Klicken Sie auf **Alarmeinstellungen ändern**, um die Standardeinstellungen für Benachrichtigungen zu ändern. Das Fenster 'Einstellungen' wird geöffnet.

- Über verbleibenden freien Laufwerksspeicherplatz – Wenn der spezifizierte Wert für den freien Speicherplatz (im Storage für virtuelle Änderungen) unterschritten wird, zeigt das Programm eine Benachrichtigung an.
- Verstrichene Zeit seit dem Start von Try&Decide – Das Programm benachrichtigt Sie, wenn Try&Decide länger als die von Ihnen spezifizierte Zeit ausgeführt wird.

## Try&Decide: Typische Einsatzfälle

Die Try&Decide-Funktion kann in vielen Fällen hilfreich sein, beispielsweise:

### Software-Evaluierung

Es kann manchmal nützlich sein, den Probiermodus einschalten, bevor Sie eine neue Software installieren. Wir empfehlen seine Aktivierung, wenn Sie Folgendes tun wollen:

- Eine Antivirus-Software auswählen.

  Es sind viele Fälle bekannt, bei denen die Installation einer Antivirus-Software die Funktion von Anwendungen beeinträchtigt oder diese nach einer solchen Installation sogar den Start verweigern. Sie können eine Testversion des Antivirus-Programms ausprobieren. Falls

irgendwelche Probleme auftauchen, verwerfen Sie die Änderungen auf Ihrem System und testen dann die Antivirus-Software eines anderen Herstellers.

- Die Testversion eines Programms installieren.

  Es ist allgemein bekannt, dass die Komponente der Windows-Systemsteuerung, welche zum Hinzufügen und Entfernen von Programmen zuständig ist, eine saubere Deinstallation von Anwendungen nicht wirklich garantieren kann. Verwerfen Sie einfach die Änderungen an Ihrem System, wenn Sie das Programm nicht mögen. Sie können sicher sein, dass Try&Decide das Programm spurlos entfernt.
- Verdächtige Software installieren.

  Falls Sie dem Anbieter einer Software, die Sie installieren wollen, nicht trauen oder wenn Ihnen die Quelle der Software unbekannt ist, schalten Sie einfach vor der Installation dieser Software den Probiermodus ein. Geht irgendetwas schief, dann verwerfen Sie alle Änderungen, die während des Probiermodus aufgetreten sind.

## Datei-Recovery

Sie haben versehentlich einige Dateien gelöscht und dann noch den Papierkorb geleert. Dann haben Sie sich daran erinnert, dass die gelöschten Dateien wichtige Daten enthielten und nun wollen Sie ein Undelete mit einer entsprechenden Software versuchen. Manchmal können Sie einen Fehler machen, während Sie versuchen, Daten wiederherzustellen; als Folge ist die Situation noch schlechter als vor dem Wiederherstellungsversuch. Sie können dann folgendermaßen fortfahren:

- Aktivieren Sie Try&Decide.
- Starten Sie das Undelete-Programm.
- Nach dem Scan Ihrer Laufwerke auf der Suche nach gelöschten Dateien oder Verzeichniseinträgen wird das Undelete-Programm die gefundenen Elemente präsentieren (falls solche vorhanden sind), außerdem wird es für wiederherstellbare Dateien anbieten, diese zu rekonstruieren. Dabei besteht immer die Gefahr, dass Sie die falsche Datei wählen und bei der Wiederherstellung die Datei überschrieben wird, die Sie eigentlich retten wollten. Ohne Try&Decide hätte dieser Fehler fatale Konsequenzen, denn die Datei wäre unrettbar verloren.
- Nun aber können Sie die Änderungen verwerfen, die im Probiermodus erfolgt sind – und einen weiteren Versuch unternehmen, die Daten wiederherzustellen; wozu Sie Try&Decide nur erneut starten müssen. Solche Versuche können Sie wiederholen, bis Sie sicher sind, dass Sie zur Rettung der Daten alles unternommen haben, was möglich war.

## Schutz der Privatsphäre im Internet

Sie möchten vielleicht auch nicht, dass jemand erfährt, welche Internetseiten Sie besucht oder welche Webseiten Sie geöffnet haben – jeder hat das Recht auf seine Privatsphäre. Wenn Sie aber schnell und komfortabel im Internet surfen, speichert das System diese Informationen in versteckten Dateien: Cookies, die Sie erhalten haben, Einträge in Suchmaschinen, eingegebene URLs usw. Diese Informationen werden auch dann nicht komplett gelöscht, wenn Sie mit den eigenen Werkzeugen der Webbrowser die temporären Internet-Dateien löschen, Cookies entfernen oder den Verlauf löschen. Mit einer speziellen Software könnten diese Informationen aufgespürt werden.

Schalten Sie den Probiermodus ein und surfen Sie nach Belieben im Internet. Verwerfen Sie später, wenn Sie alle Spuren Ihrer Aktivitäten beseitigen wollen, die im Probiermodus erfolgten Änderungen.

# Acronis Secure Zone

Die Acronis Secure Zone ist ein spezielles, geschütztes Volume, welches Sie auf Ihrem Computer erstellen können, um Backups zu speichern. Die Acronis Secure Zone verwendet FAT32 als Dateisystem.

Wenn Sie eine Acronis Secure Zone erstellen, wird diese im Bereich **Andere** des Windows Datei-Explorers angezeigt. Sie können durch die Acronis Secure Zone wie durch ein gewöhnliches Volume (Partition) navigieren.

Wenn die Acronis Secure Zone durch ein Kennwort geschützt wird, müssen Sie bei jeder entsprechenden Aktion mit dieser das entsprechende Kennwort eingeben. Einzige Ausnahme ist die Anzeige von Details für eine Backup-Version.

## Bereinigung der Acronis Secure Zone

Wenn der Speicherplatz in der Acronis Secure Zone für neue Backups nicht mehr ausreicht, können Sie Folgendes tun:

- Brechen Sie eine aktuelle Backup-Aktion ab, vergrößern Sie den Speicherplatz der Acronis Secure Zone und führen Sie das Backup dann erneut aus.
- Brechen Sie eine aktuelle Backup-Aktion ab, löschen Sie (manuell) einige Backups in der Acronis Secure Zone und führen Sie das Backup dann erneut aus.
- Bestätigen Sie, dass Sie das älteste Backup vom selben Typ (Datei- oder Laufwerk-Backup) inkl. aller nachfolgenden inkrementellen und differentiellen Versionen automatisch löschen lassen wollen. Sollte der freie Speicherplatz danach immer noch nicht ausreichen, erfragt Acronis Cyber Protect Home Office Ihre Bestätigung und löscht dann das nächste Voll-Backup. Dies wird solange wiederholt, bis der freie Speicherplatz für das neue Backup wieder ausreicht. Sollte der freie Speicherplatz auch nach dem Löschen aller vorherigen Backups immer noch nicht ausreichen, dann wird das aktuelle Backup abgebrochen.

***So können Sie verhindern, dass die Zone überläuft:***

1. Wählen Sie ein geplantes Backup.
2. Klicken Sie auf **Optionen**.
3. Erweitern Sie auf der Registerkarte **Erweitert** den Bereich **Fehlerbehandlung**.
4. Aktivieren Sie das Kontrollkästchen **Ältestes Backup löschen, falls in der ASZ nicht genug Speicherplatz ist**.
5. Klicken Sie auf **OK**.

Weitere Informationen finden Sie im Abschnitt 'Fehlerbehandlung'.

Sie können die Acronis Secure Zone nicht als Storage für die virtuellen Systemänderungen des Try&Decide-Modus verwenden. Die Try&Decide-Daten werden automatisch bereinigt, sobald Sie eine Try&Decide-Sitzung stoppen.

Nonstop Backup-Versionen in der Acronis Secure Zone werden nicht automatisch von Acronis Cyber Protect Home Office gelöscht. Diese Versionen können nur manuell gelöscht werden. Weitere Informationen finden Sie im Abschnitt 'Acronis Nonstop Backup Storage'.

## Eine Acronis Secure Zone erstellen und verwalten

1. Klicken Sie auf die **Start**-Schaltfläche –> **Acronis** (Produktordner) –> **Acronis Secure Zone** .
   Der Assistent zum Verwalten der Acronis Secure Zone wird geöffnet.
2. Gehen Sie folgendermaßen vor:
   Wenn Sie eine Acronis Secure Zone erstellen wollen, spezifizieren Sie deren Speicherort und Größe.
   Wenn Sie eine vorhandene Acronis Secure Zone anpassen wollen, wählen Sie eine der nachfolgenden Aktionen:
   - Vergrößern oder verkleinern
   - Entfernen
   - Kennwort ändern
     Folgen Sie den Anweisungen des Assistenten.
3. Klicken Sie im Schritt **Abschluss** auf den Befehl **Fertigstellen**.

**Hinweis**
Für diese Aktion ist möglicherweise ein Neustart des Computers notwendig.

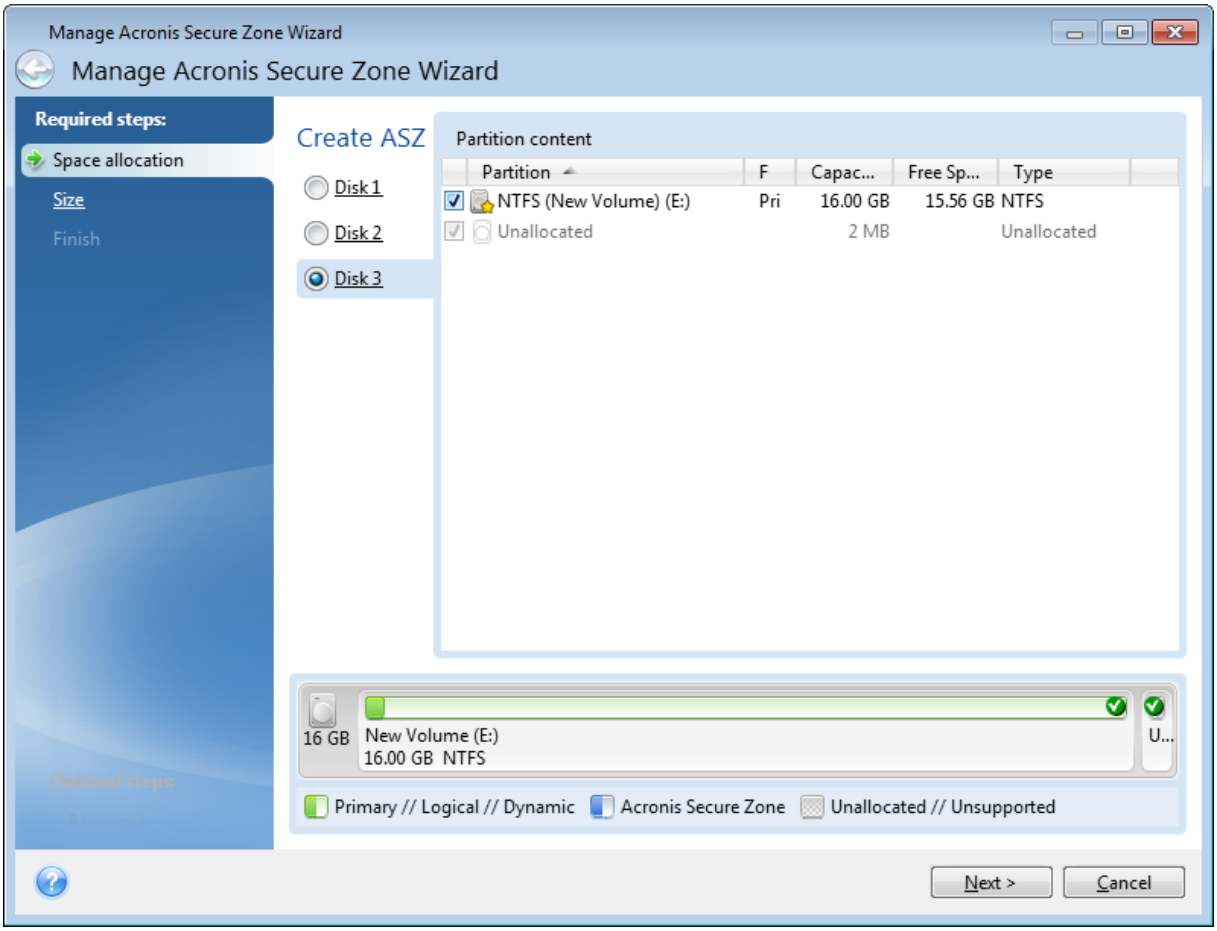
## Der Speicherort für die Acronis Secure Zone

***So können Sie einen Speicherort für die Acronis Secure Zone spezifizieren***

1. Wählen Sie auf ein Laufwerk aus, auf dem die Acronis Secure Zone erstellt werden soll.
2. Wählen Sie ein oder mehrere Volumes aus, deren nicht zugeordneter und/oder freier Speicherplatz für die Erstellung verwendet werden soll. Die Größe der markierten Volumes (Partitionen) wird bei Bedarf verkleinert und der freigegebene Speicherplatz für die Acronis Secure Zone verwendet.

   **Hinweis**
   Eine Acronis Secure Zone kann nicht auf dynamischen Datenträgern/Volumes erstellt werden.

3. Klicken Sie auf **Weiter**.

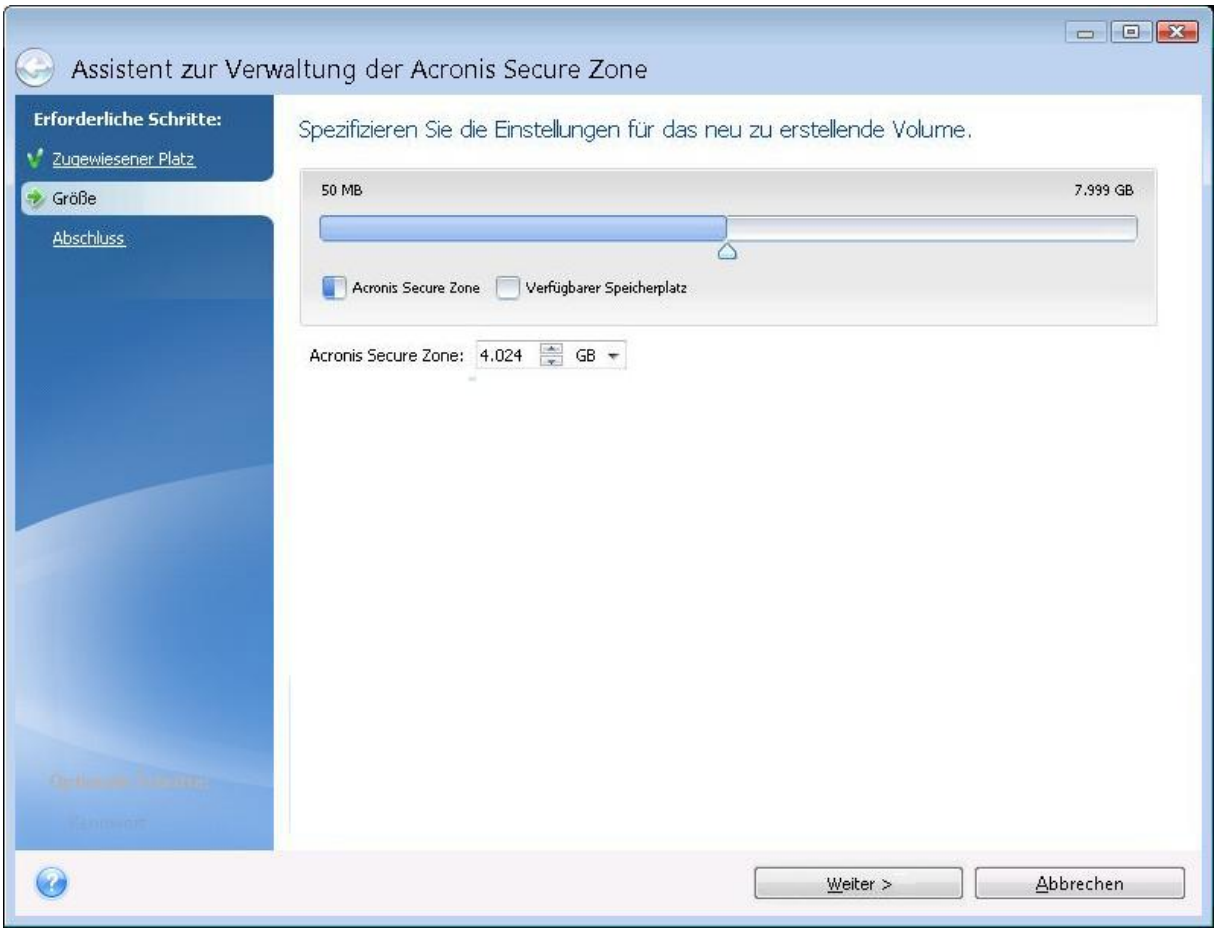



***So können Sie die Größe der Acronis Secure Zone anpassen***

1. Aktivieren Sie die Volumes, deren Speicherplatz zur Vergrößerung der Acronis Secure Zone verwendet werden soll – oder die bei einer Verkleinerung der Acronis Secure Zone den wieder frei werdenden Speicherplatz zugewiesen bekommen sollen. Sie können auch Volumes mit nicht zugeordnetem Speicherplatz wählen.
2. Klicken Sie auf **Weiter**.

## Die Größe der Acronis Secure Zone

Wenn Sie die Größe der Acronis Secure Zone spezifizieren wollen, bewegen Sie den grafischen Schieber in die gewünschte Position oder geben Sie den exakten Wert direkt ein.




Die minimale Größe einer Zone beträgt etwa 50 MB, abhängig von der Geometrie des Festplattenlaufwerks. Die maximale Größe ist identisch mit dem nicht zugeordneten Speicherplatz – zuzüglich der Größe des freien Speichers auf allen Volumes, die Sie im vorhergehenden Schritt gewählt haben.

Wenn Sie eine Acronis Secure Zone erstellen oder vergrößern, wird das Programm zuerst auf den verfügbaren nicht zugeordneten Speicherplatz zurückgreifen. Wenn nicht genug nicht zugeordneter Speicherplatz vorhanden ist, um die gewünschte Größe zu erreichen, werden die ausgewählten Volumes verkleinert. Die Größenänderung von Volumes kann einen Neustart erforderlich machen.

Wenn Sie eine Acronis Secure Zone verkleinern und auf dem Laufwerk noch weiterer 'nicht zugeordneter' Speicherplatz vorhanden ist, dann wird dieser gemeinsam mit dem Speicherplatz, der durch die Verkleinerung der Acronis Secure Zone frei wird, den zuvor ausgewählten Volumes zugewiesen. Durch dieses Verhalten bleibt auf dem Laufwerk kein nicht zugeordneter Speicherplatz übrig.

**Warnung!**
Wenn Sie ein System-Volume auf die kleinstmögliche Größe reduzieren, kann dies bewirken, dass das betreffende Betriebssystem nicht mehr booten kann.

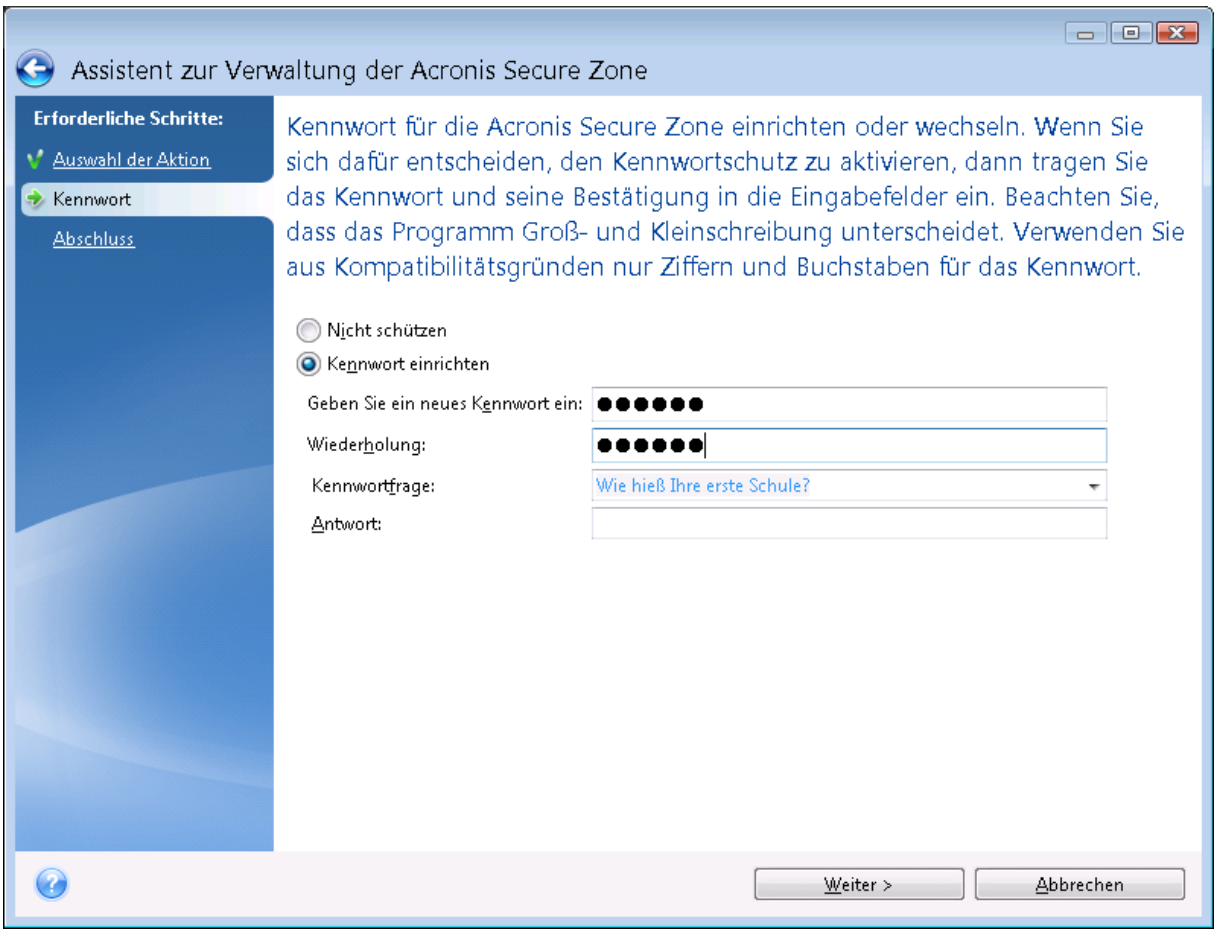
# Schutz für Acronis Secure Zone

Sie können einen Kennwortschutz für die Acronis Secure Zone einrichten, um sie vor unbefugtem Zugriff zu schützen.

Das Programm wird Sie bei jeder Aktion, die etwas mit der Acronis Secure Zone zu tun hat (wie etwa Backup-Erstellung oder Wiederherstellung; Images in der Acronis Secure Zone mounten oder Backups in dieser validieren; Größenveränderung und Löschung der Acronis Secure Zone) nach dem Kennwort fragen.

***So können Sie ein Kennwort für die Acronis Secure Zone festlegen***

1. Wählen Sie **Kennwort einrichten**.
2. Geben Sie das Kennwort in das Eingabefeld **Kennwort** ein.
3. Geben Sie das eben eingetippte Kennwort erneut in das Feld **Kennwort bestätigen** ein.
4. [Optionaler Schritt] Wählen Sie außerdem eine Geheimfrage, die Ihnen gestellt wird, falls Sie das Kennwort vergessen sollten. Wählen Sie eine Geheimfrage aus der Liste und geben Sie eine Antwort ein.
5. Klicken Sie auf **Weiter**, um fortzufahren.



**Hinweis**
Das Reparieren oder Updaten von Acronis Cyber Protect Home Office wird das Kennwort nicht beeinflussen. Wenn Sie das Programm jedoch deinstallieren, ohne vorher die Acronis Secure Zone zu entfernen, wird das Kennwort der Acronis Secure Zone bei einer erneuten Installation zurückgesetzt.

## Die Acronis Secure Zone entfernen

**Warnung!**
Acronis Wenn Sie die Secure Zone löschen, werden automatisch auch alle Backups in dieser Zone zerstört.

Bestimmen Sie die Volumes, denen Sie denjenigen Speicherplatz zuordnen wollen, der beim Entfernen der Acronis Secure Zone frei wird. Wenn Sie mehrere Volumes wählen, wird der Platz proportional zwischen diesen verteilt – und zwar auf Basis der jeweiligen Volume-Größen.

Sie können außerdem beim Deinstallieren des Programms wählen, dass auch eine vorhandene Acronis Secure Zone entfernt werden soll.

# Ein neues Laufwerk hinzufügen

Falls Sie nicht mehr genügend Speicherplatz für Ihre Daten haben, können Sie ein altes Laufwerk gegen ein neues, größeres austauschen. Oder Sie fügen ein neues Laufwerk nur zum Speichern von Daten hinzu, während Ihr Betriebssystem auf dem alten Laufwerk verbleibt.

***So können Sie ein neues Laufwerk hinzufügen***

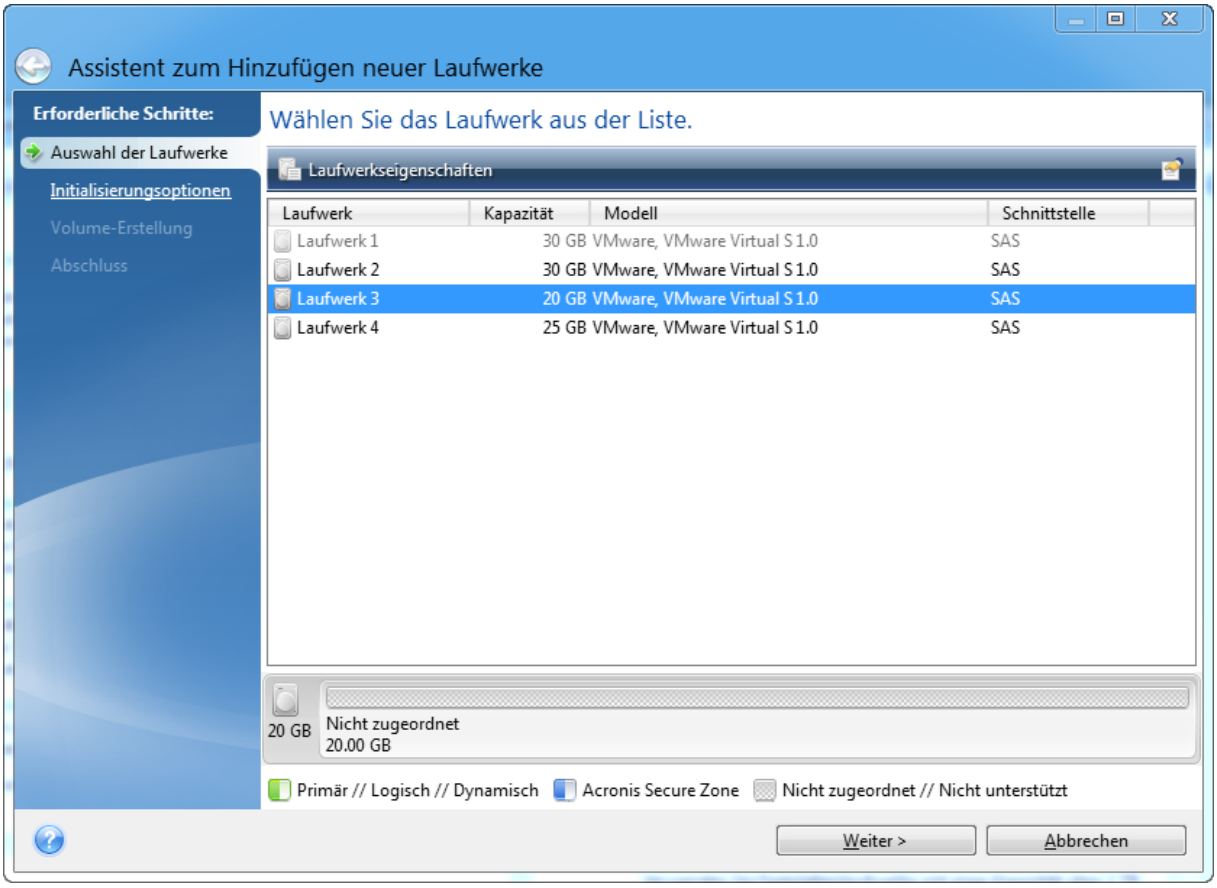
1. Fahren Sie Ihren Computer komplett herunter und bauen Sie das neue Laufwerk ein.
2. Schalten Sie Ihren Computer ein.
3. Klicken Sie auf die **Start**-Schaltfläche –> **Acronis** (Produktordner) –> **Neues Laufwerk hinzufügen**.
4. Folgen Sie den Anweisungen des Assistenten.
5. Stellen Sie im Schritt **Abschluss** sicher, dass das konfigurierte Laufwerkslayout Ihren Vorstellungen entspricht. Klicken Sie anschließend auf **Fertigstellen**.

## Ein Laufwerk auswählen

Wählen Sie die Festplatte (oder ein ähnliches Laufwerk), die Sie neu an den Computer angeschlossen haben. Wenn Sie mehrere Laufwerke neu angeschlossen haben, wählen Sie eins aus und klicken Sie dann auf **Weiter**, um fortzufahren. Die anderen Laufwerke können Sie später berücksichtigen, nach einem Neustart des 'Assistenten zum Hinzufügen neuer Laufwerke'.

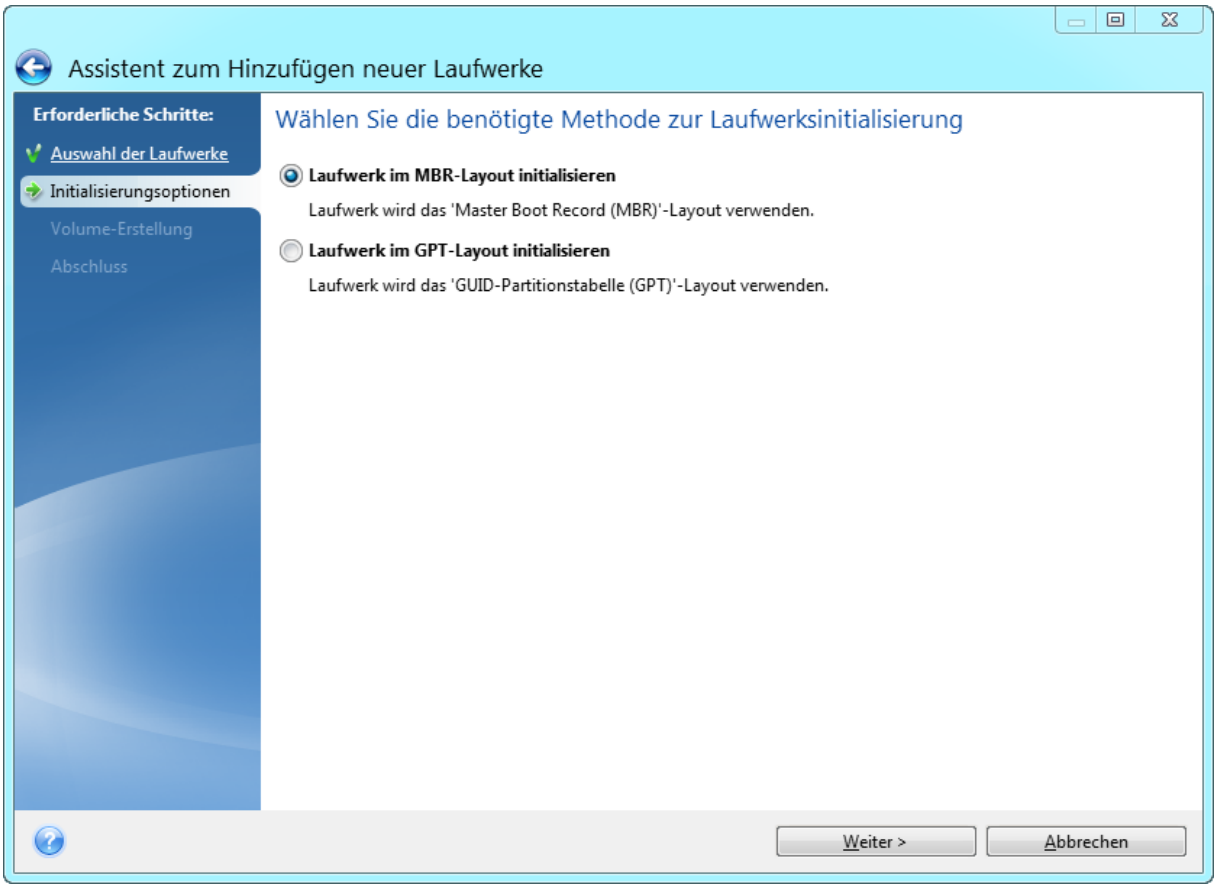
**Hinweis**

Sollten auf dem neuen Laufwerk irgendwelche Volumes (Partitionen) vorliegen, wird Acronis Cyber Protect Home Office Sie warnen, dass diese gelöscht werden.




## Wahl der Initialisierungsmethode

Acronis Cyber Protect Home Office unterstützt die Partitionierungsschemata MBR und GPT. Die GUID-Partitionstabelle (GPT) ist ein neues Laufwerk-Partitionsschema, das Vorteile gegenüber dem älteren MBR-Partitionsschema bringt. Wenn Ihr Betriebssystem GPT-Laufwerke unterstützt, können Sie das neue Laufwerk als ein GPT-Laufwerk initialisieren.




- Um ein GPT-Laufwerk hinzuzufügen, klicken Sie auf **Laufwerk im GPT-Layout initialisieren**.
- Um ein MBR-Laufwerk hinzuzufügen, klicken Sie auf **Laufwerk im MBR-Layout initialisieren**.

Klicken Sie nach Wahl der gewünschten Initialisierungsmethode auf **Weiter**.

## Neue Volumes erstellen

Ein neues Laufwerk muss partitioniert werden, damit sein Speicherplatz verwendet werden kann. Partitionieren ist ein Prozess, der den Speicherplatz eines Laufwerks in logische Abschnitte unterteilt. Diese Abschnitte werden Partitionen (älterer Begriff) oder Volumes (modernerer, universellerer Begriff) genannt. Jedes Volume (jede Partition) kann als separates Laufwerk fungieren, dem ein Laufwerksbuchstabe zugewiesen werden kann und in dem ein eigenes Dateisystem verwendet wird.

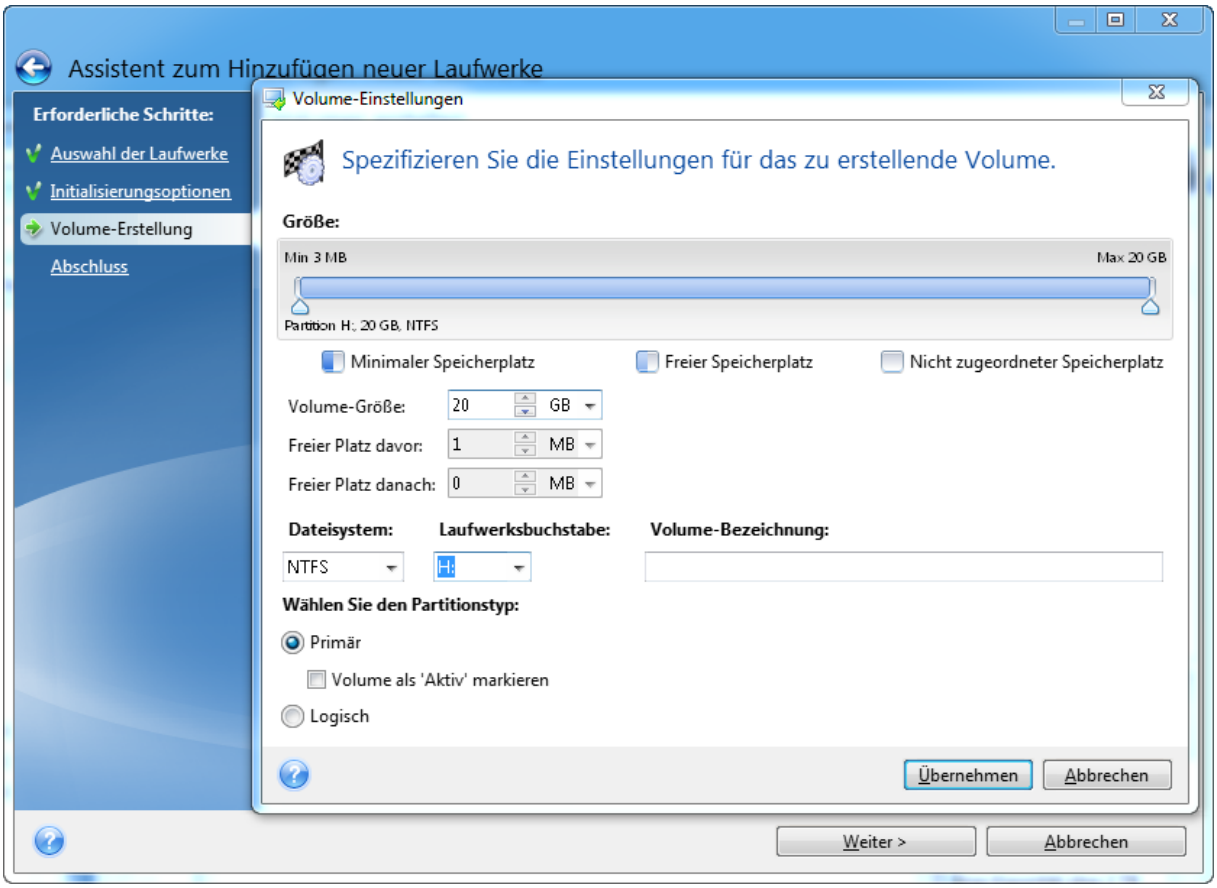
***So können Sie ein neues Volume erstellen***

1. Wählen Sie im Assistenten-Schritt **Volume-Erstellung** den gewünschten nicht zugeordneten Speicherplatz und klicken Sie dann auf **Neues Volume erstellen**.
2. Legen Sie folgende Einstellungen für das zu erstellende Volume fest:
   - Größe und Position
   - Dateisystem

- Volume-Typ (nur für MBR-Laufwerke verfügbar)
- Laufwerksbuchstabe und Volume-Bezeichnung

  Weitere Details finden Sie im Abschnitt 'Volume-Einstellungen'.

3. Klicken Sie auf **Übernehmen**.




## Volume-Einstellungen

### Größe

***Verwenden Sie eine der folgenden Aktionen, um die Größe eines Volumes zu ändern***

- Zeigen Sie mit der Maus auf die Begrenzungen des Volumes. Verschieben Sie die Begrenzungen mit dem Mauszeiger (sobald dieser als Pfeil mit zwei Spitzen angezeigt wird), um die Größe des Volumes zu vergrößern bzw. zu verkleinern.
- Oder geben Sie die gewünschte Größe des Volumes im Feld **Volume-Größe** als direkten Wert ein.

***Verwenden Sie eine der folgenden Aktionen, um die Position eines Volumes zu ändern***

- Verschieben Sie das Volume durch Ziehen mit der Maus an seine neue Position.
- Oder geben Sie die Werte für die gewünschte Zielgröße in den Feldern **Freier Speicherplatz davor** bzw. **Freier Speicherplatz danach** direkt ein.

**Hinweis**
Das Programm reserviert möglicherweise beim Erstellen von Volumes etwas nicht zugeordneten Speicherplatz direkt vor den erstellten Volumes, sofern dies für das System erforderlich ist.

## Dateisystem

Sie können das Volume entweder unformatiert belassen oder zwischen folgenden Dateisystemen wählen:

- **NTFS** – ist ein Dateisystem von Microsoft, welches seit Windows NT (und Nachfolgeversionen wie Windows XP, 7 etc.) zum Windows-Betriebssystem gehört. Wählen Sie diese Variante, wenn Sie einem dieser Windows-Betriebssysteme arbeiten. Beachten Sie, dass einige veraltete Microsoft-Betriebssysteme (wie DOS, Windows 95/98/ME) nicht auf NTFS-Partitionen zugreifen können.
- **FAT 32** – ist eine verbesserte 32-Bit-Version des Dateisystems FAT, welches Volumes bis zu einer Größe von 2 TB unterstützt.
- **FAT 16** – ist ein einfaches Dateisystem, welches ursprünglich für Microsoft DOS entwickelt wurde. Es wird von den meisten (auch aktuellen) Betriebssystemen erkannt. Wenn Ihr Laufwerk aber größer als 4 GB ist, können Sie dieses nicht mit FAT16 formatieren.
- **Ext2** – ist ein Dateisystem, welches ursprünglich für Linux entwickelt wurde. Es ist relativ schnell, jedoch kein Journaling-Dateisystem.
- **Ext3** – ist ein Journaling-Dateisystem von Linux und wurde offiziell mit Red Hat Linux Version 7.2 eingeführt. Es ist vorwärts und rückwärts kompatibel mit Linux Ext2. Es hat multiple Journaling-Modi sowie eine breite Cross-Plattform-Kompatibilität mit 32-Bit- und 64-Bit-Architekturen.
- **Ext4** – ist ein neueres Dateisystem von Linux. Gegenüber dem Ext3-Dateisystem weist es Verbesserungen auf. Es ist vollständig abwärtskompatibel zu Ext2 und Ext3. Allerdings ist Ext3 nur teilweise vorwärtskompatibel zu Ext4.
- **ReiserFS** – ist ein Journaling-Dateisystem von Linux. Es ist üblicherweise zuverlässiger und schneller als Ext2. Wählen Sie dieses System für Volumes, die unter Linux Daten (Dokumente usw.) aufnehmen sollen.
- **Linux Swap** – ist ein Dateisystem für das Auslagerungs-Volume von Linux. Verwenden Sie es, um mehr Platz für die Auslagerungsdateien von Linux bereitzustellen.

## Laufwerksbuchstabe

Bestimmen Sie einen Laufwerksbuchstaben, der dem Volume zugewiesen wird. Wenn Sie **Auto** auswählen, weist das Programm den ersten freien Laufwerksbuchstaben in alphabetischer Reihenfolge zu.

## Volume-Bezeichnung

Eine Volume-Bezeichnung (auch Laufwerksbezeichnung genannt) ist ein kurzer Name, den Sie einem Volume zur besseren Unterscheidung von anderen zuweisen können. Ein Volume mit einem Betriebssystem kann beispielsweise als 'System' bezeichnet werden und ein Volume mit Daten

'Daten' usw. Die Bezeichnung eines Volumes ist ein optionales Attribut (muss also nicht gesetzt werden).

### Volume-Typ (diese Einstellungen sind nur für MBR-Laufwerke verfügbar)

Sie können das neue Volume als primär oder logisch definieren.

- **Primär** – wählen Sie diese Option, wenn Sie von diesem Volume ein Betriebssystem booten möchten. Wenn nicht, ist es besser, das neue Volume als logisches Laufwerk einzurichten. Es sind nur vier primäre Volumes je Laufwerk möglich – oder drei primäre und ein erweitertes Volume.

  **Hinweis**
  Wenn Sie mehrere primäre Volumes haben, wird nur eines aktiv sein, die anderen primären Volumes werden versteckt und sind für das Betriebssystem unsichtbar.

  - **Volume als 'Aktiv' markieren** – aktivieren Sie dieses Kontrollkästchen, wenn Sie vorhaben, ein Betriebssystem auf diesem Volume zu installieren.
- **Logisch** – wählen Sie diesen Parameter, wenn Sie auf dem Laufwerk kein Betriebssystem installieren und davon starten möchten. Ein logisches Volume ist Teil eines physischen Laufwerks, der partitioniert und als unabhängiger Abschnitt eingerichtet wurde, sodass er wie ein eigenständiges Laufwerk verwendet werden kann.

# Werkzeuge für Sicherheit und zum Schutz Ihrer Privatsphäre

## Acronis DriveCleanser

Der Acronis DriveCleanser ermöglicht Ihnen, alle Daten auf ausgewählten Laufwerken bzw. Volumes dauerhaft zu zerstören (permanent zu löschen). Sie können vorinstallierte Algorithmen für diese Datenzerstörung verwenden oder auch eigene erstellen. Weitere Details finden Sie im Abschnitt 'Auswahl der Löschmethode'.

### Warum benötige ich das?

Wenn Sie ein altes Festplattenlaufwerk vor der Entsorgung einfach nur formatieren, werden darauf gespeicherte Informationen nicht permanent gelöscht und können daher wiederhergestellt werden. Ihre persönlichen Informationen können auf diese Weise leicht in falsche Hände geraten. Um dies zu verhindern, empfehlen wir den Acronis DriveCleanser zu verwenden, wenn Sie:

- Ein altes Festplattenlaufwerk gegen ein neues austauschen und das alte Laufwerk nicht mehr weiter verwenden wollen.
- Sie Ihr altes Festplattenlaufwerk andere Personen (z.B. Verwandte oder Freunde) weitergeben.
- Ihr altes Festplattenlaufwerk verkaufen.

## AnwendungAcronis DriveCleanser

***So können Sie die Daten auf Ihrem Laufwerk dauerhaft löschen***

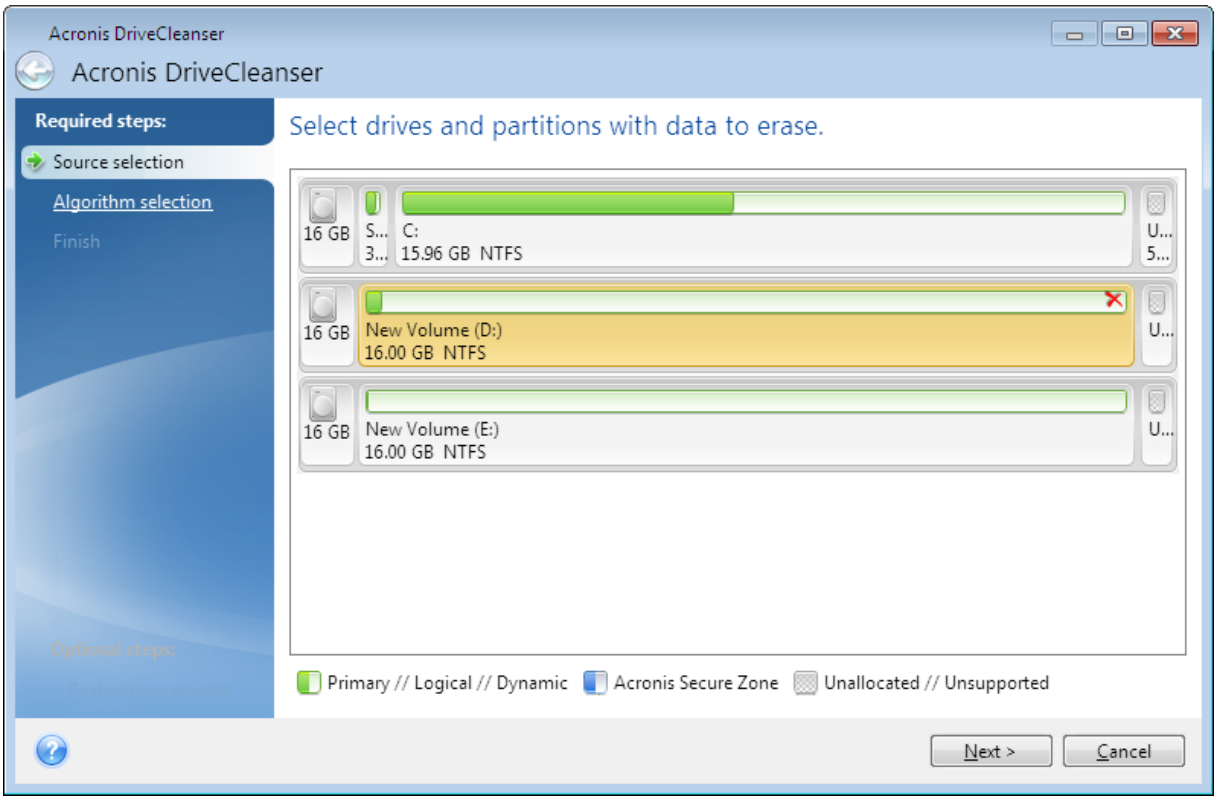
1. Klicken Sie auf die Schaltfläche **Start** –> **Acronis** (Produktordner) –> **Acronis DriveCleanser**. Der Acronis DriveCleanser-Assistent wird geöffnet.
2. Bestimmen Sie im Schritt **Auswahl der Daten** die Laufwerke bzw. Volumes, die Sie dauerhaft löschen wollen. Weitere Details finden Sie im Abschnitt 'Auswahl der Daten'.
3. Bestimmen Sie im Schritt **Auswahl der Löschmethode** den Algorithmus, den Sie für die Datenzerstörung verwenden wollen. Weitere Details finden Sie im Abschnitt 'Auswahl der Löschmethode'.
4. [Optionaler Schritt] Sie können auch Ihren eigenen Algorithmus erstellen. Weitere Details finden Sie im Abschnitt 'Einen benutzerdefinierten Algorithmus erstellen'.
5. [Optionaler Schritt] Wählen Sie im Schritt **Aktionen nach der Datenvernichtung**, was mit dem Laufwerk bzw. den Volumes geschehen soll, wenn die Löschaktion abgeschlossen ist. Weitere Details finden Sie im Abschnitt 'Aktionen nach der Datenvernichtung'.
6. Überprüfen Sie im Schritt **Abschluss**, dass die konfigurierten Einstellungen korrekt sind. Aktivieren Sie zum Starten des Prozesses das Kontrollkästchen **Ausgewählte Volumes unwiderruflich löschen** und klicken Sie dann auf **Fertigstellen**.

**Warnung!**
Beachten Sie, dass die Datenvernichtung abhängig von der Gesamtgröße der ausgewählten Volumes und des gewählten Algorithmus für die Datenvernichtung mehrere Stunden dauern kann.

## Auswahl der Daten

Bestimmen Sie im Schritt **Auswahl der Daten** die Laufwerke bzw. Volumes, deren Daten Sie dauerhaft löschen wollen:

- Sie können die Volumes auswählen, indem Sie die entsprechenden Rechtecke anklicken. Die erfolgte Auswahl eines Volumes wird mit einem roten Kreuz (  ) gekennzeichnet.
- Klicken Sie auf das Laufwerkssymbol (  ), um ein komplettes Laufwerk auszuwählen.

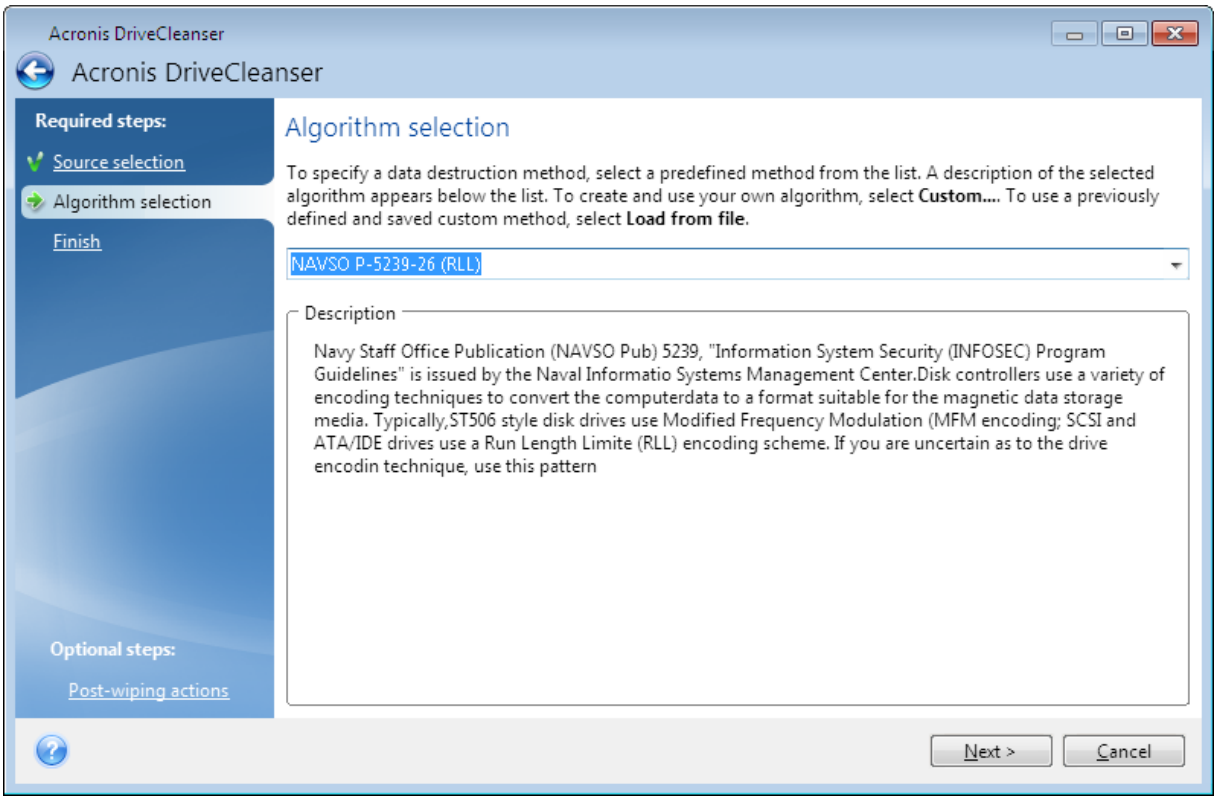



**Hinweis**
Der Acronis DriveCleanser kann keine Volumes auf dynamischen Datenträgern oder GPT-Laufwerken bereinigen. Diese werden daher auch nicht angezeigt.

## Wahl der Methode

Führen Sie im Schritt **Auswahl der Löschmethode** eine der folgenden Aktionen aus:

- Um einen der vorinstallierten Algorithmen zu verwenden, wählen Sie den gewünschten aus. Weitere Details finden Sie im Abschnitt 'Methoden zur Datenvernichtung auf Laufwerken'.
- [Nur für erfahrene Benutzer] Wählen Sie **Benutzerdefiniert**, wenn Sie einen eigenen Algorithmus definieren wollen. Fahren Sie dann mit dem Schritt **Definition der Löschmethode** fort. Sie können den erstellten Algorithmus später als Datei (mit der Erweiterung *.alg) speichern.
- Sie können einen solchen zuvor gespeicherten benutzerdefinierten Algorithmus verwenden, wenn Sie den Befehl **Von Datei laden** anklicken und die entsprechende Datei auswählen.




## Methoden zur Datenvernichtung auf Laufwerken

Informationen, die von einer Festplatte auf unsichere Art (z.B. durch die gewöhnliche Löschfunktion von Windows) entfernt werden, können einfach wiederhergestellt werden. Durch die Verwendung speziellen Equipments ist es sogar möglich, mehrfach überschriebene Informationen wiederherzustellen.

Daten werden auf einer Festplatte als eine binäre Sequenz von 1 und 0 (Einsen und Nullen) gespeichert, durch unterschiedlich magnetisierte Bereiche auf einer Festplatte repräsentiert. Allgemein gesprochen wird eine 1, die auf eine Festplatte geschrieben wurde, von ihrem Controller als 1 gelesen – eine 0 wird als 0 gelesen. Wenn Sie jedoch eine 1 über eine 0 schreiben, ergibt sich als Ergebnis bedingterweise 0,95 und umgekehrt – wenn eine 1 über eine 1 geschrieben wird, ist das Ergebnis 1,05. Für den Controller sind diese Unterschiede irrelevant. Durch die Verwendung speziellen Equipments ist es jedoch möglich, die 'zugrunde liegende' Sequenz von Einsen und Nullen auszulesen.

***Methoden zum permanenten Löschen von Informationen***

Die genaue Theorie zum garantierten Auslöschen von Informationen wird in einem Artikel von Peter Gutmann beschrieben. Siehe den englischsprachigen Artikel 'Secure Deletion of Data from Magnetic and Solid-State Memory' unter der Adresse https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

| Nr. | Algorithmus (Schreibmethode) | Durchgänge | Muster |
|---|---|---|---|
| 1. | United States Department of Defense 5220.22-M | 4 | 1. Durchgang – Zufallswert für jeden Sektor, 2. Durchgang – zum ersten Durchgang komplementärer Wert, 3. Durchgang – Zufallswert, 4. Durchgang – Prüfung. |
| 2. | USA (Vereinigte Staaten): NAVSO P-5239-26 (RLL) | 4 | 1. Durchgang – 0x01 für alle Sektoren, 2. Durchgang – 0x27FFFFFF, 3. Durchgang – Zufallswert, 4. Durchgang – Prüfung. |
| 3. | USA (Vereinigte Staaten): NAVSO P-5239-26 (MFM) | 4 | 1. Durchgang – 0x01 für alle Sektoren, 2. Durchgang – 0x7FFFFFFF, 3. Durchgang – Zufallswert, 4. Durchgang – Prüfung. |
| 4. | Deutsch: VSITR | 7 | 1. bis 6. Durchgang – alternierende Sequenz von: 0x00 und 0xFF; 7. Durchgang – 0xAA, d.h. 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA. |
| 5. | Russisch: GOST P50739-95 | 1 | Logische Nullen (0x00) für jedes Byte eines jeden Sektors für die 6. bis 4. Schutzklasse.<br>Zufallswerte (Ziffern) für jedes Byte in jedem Sektor für 3. bis 1. Schutzklasse. |
| 6. | Peter Gutmanns Methode | 35 | Peter Gutmanns Methode ist sehr ausgeklügelt. Sie basiert auf seiner Theorie zum Auslöschen von Informationen auf Festplatten (siehe Sichere Datenlöschung von magnetischem und 'Solid State'-Speicher). |
| 7. | Bruce Schneiers Methode | 7 | Bruce Schneier schlägt in seinem Buch 'Angewandte Kryptographie“ einen Überschreib-Algorithmus mit sieben Durchgängen vor. 1. Durchgang – 0xFF, 2. Durchgang – 0x00 – und dann fünfmal mit kryptographisch sicheren Pseudozufalls-Sequenzen. |
| 8. | Schnell | 1 | Logische Nullen (0x00) für alle auszulöschenden Sektoren. |

## Benutzerdefinierte Algorithmen erstellen

### Definition der Methode

Der Schritt **Definition der Löschmethode** zeigt Ihnen eine Vorlage für den zukünftigen Algorithmus.

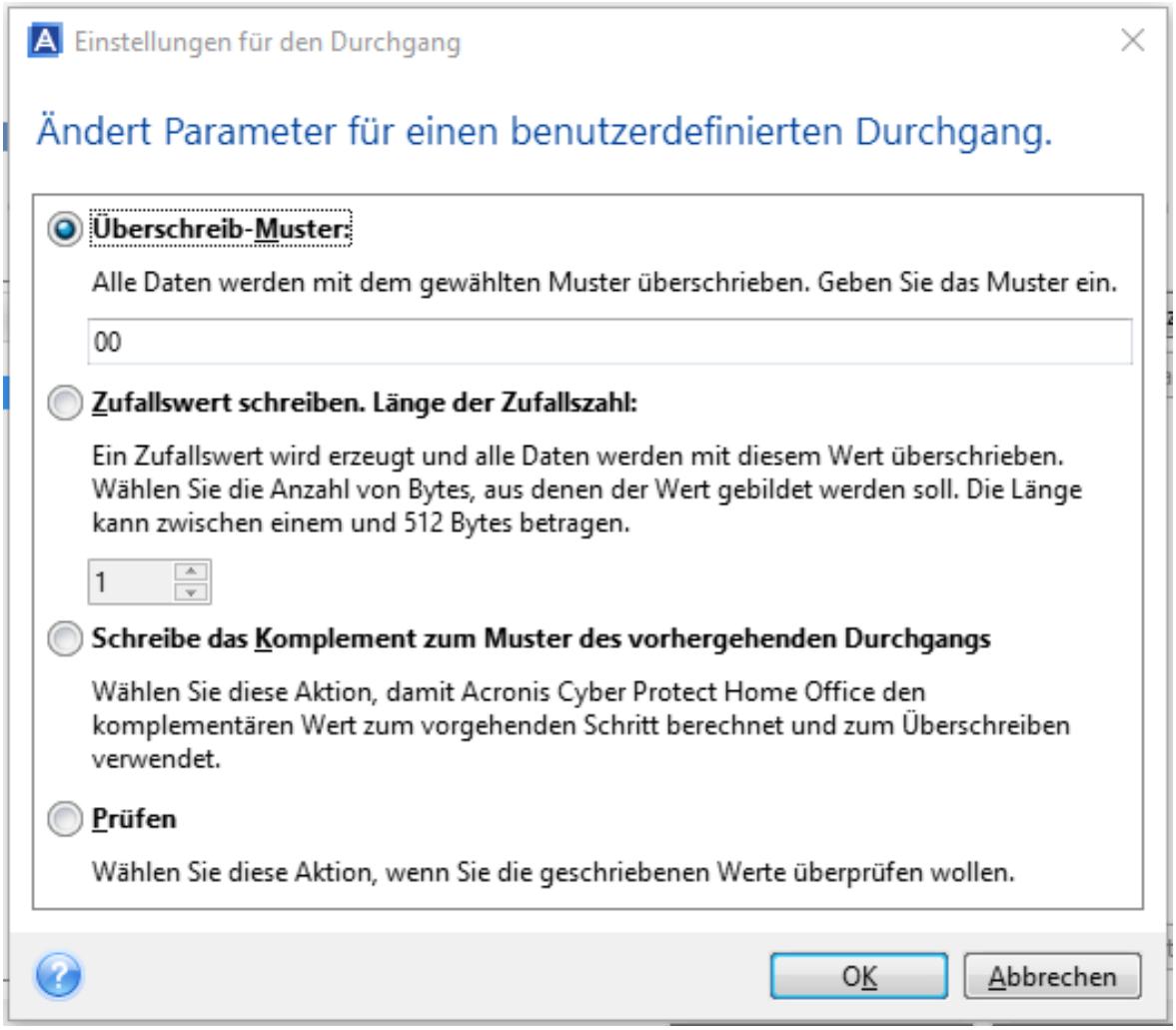
Die Tabelle ist folgendermaßen aufgebaut:

- Die erste Spalte enthält den Typ der Aktion (Schreiben eines Symbols auf das Laufwerk und Prüfen des geschriebenen Werts).
- Die zweite Spalte zeigt das Muster an, mit dem die Daten auf das Laufwerk geschrieben werden.

Jede Zeile definiert eine Aktion, die während eines Durchlaufs durchgeführt wird. Fügen Sie der Tabelle zur Erstellung Ihres Algorithmus so viele Zeilen hinzu, wie Sie es für eine sichere Datenzerstörung für ausreichend erachten.

***So können Sie einen neuen Durchlauf hinzufügen:***

1. Klicken Sie auf **Hinzufügen**. Das Fenster 'Einstellungen für den Durchgang' wird geöffnet.




2. Wählen Sie eine Option:
   - **Überschreibmuster**

     Geben Sie einen hexadezimalen Wert ein, beispielsweise in folgender Art: 0x00, 0xAA, or 0xCD, etc. Diese Werte sind normalerweise ein Byte lang, können aber auch bis zu 512 Byte betragen. Mit Ausnahme solcher Werte, können Sie einen Hexadezimalwert beliebiger Länge (bis zu 512 Byte) eingeben.

**Hinweis**
Wenn der Binärwert durch die Sequenz 10001010 (0x8A) repräsentiert wird, dann lautet das Komplement 01110101 (0x75).

- **Zufallswert schreiben**
  Spezifizieren Sie die Länge des Zufallswerts in Byte.
- **Schreibe das Komplement zum Muster des vorhergehenden Durchgangs**
  Acronis Cyber Protect Home Office fügt einen Komplement des Wertes hinzu, der im vorhergehenden Durchgang auf das Laufwerk geschrieben wurde.
- **Verifizieren**
  Acronis Cyber Protect Home Office überprüft die Werte, die während des vorhergehenden Durchgangs auf das Laufwerk geschrieben wurden.

3. Klicken Sie auf **OK**.

***So können Sie einen vorhandenen Durchgang bearbeiten:***

1. Wählen Sie die entsprechende Zeile aus und klicken Sie dann auf **Bearbeiten**.
   Das Fenster 'Einstellungen für den Durchgang' wird geöffnet.

   **Hinweis**
   Wenn Sie mehrere Zeilen auswählen, werden die neuen Einstellungen auf alle ausgewählten Durchgänge angewendet.

2. Ändern Sie die Einstellungen und klicken Sie dann auf **OK**.

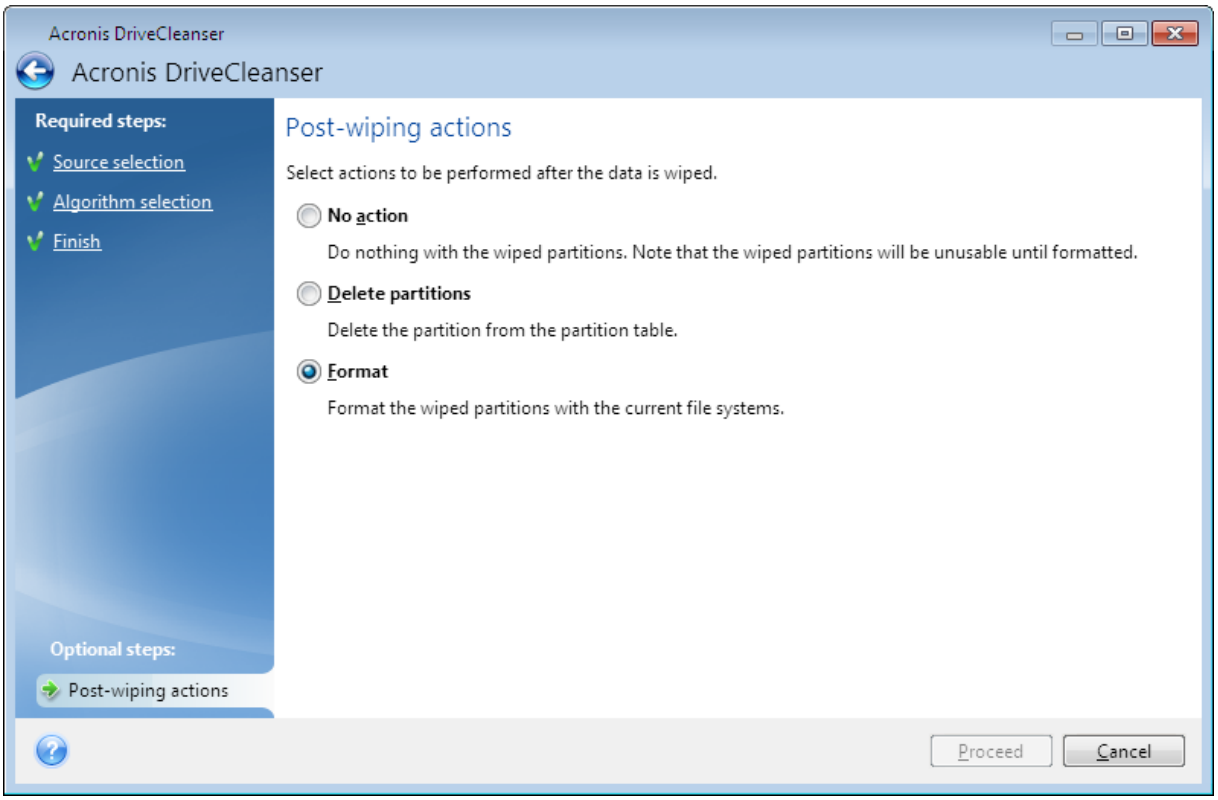
### Einen Algorithmus als Datei speichern

1. Wählen Sie im Schritt **Benutzerdefinierte Methode speichern** den Befehl **Als Datei speichern** und klicken Sie dann auf **Weiter**.
2. Spezifizieren Sie im geöffneten Fenster den Dateinamen und den Speicherort. Klicken Sie anschließend auf **OK**.

## Aktionen nach der Datenvernichtung

Im Fenster 'Aktionen nach der Datenvernichtung' können Sie einstellen, welche Aktionen nach der Datenvernichtung auf den Volumes ausgeführt werden sollen. Der Acronis DriveCleanser bietet Ihnen drei Optionen:

- **Keine Aktion** – führt lediglich eine Datenzerstörung (mit der gewählten Methode) aus
- **Volume löschen** – Daten zerstören und Volume löschen
- **Formatieren** — zerstört die Daten und formatiert das/die Volume(s) (voreingestellt)




## Systembereinigung

Sie können mit dem Assistenten zur Systembereinigung all jene Spuren sicher entfernen, die Ihre PC-Aktivitäten hinterlassen haben (inkl. Benutzernamen, Kennwörter und andere persönliche Informationen).

Sie können folgenden Aktionen ausführen:

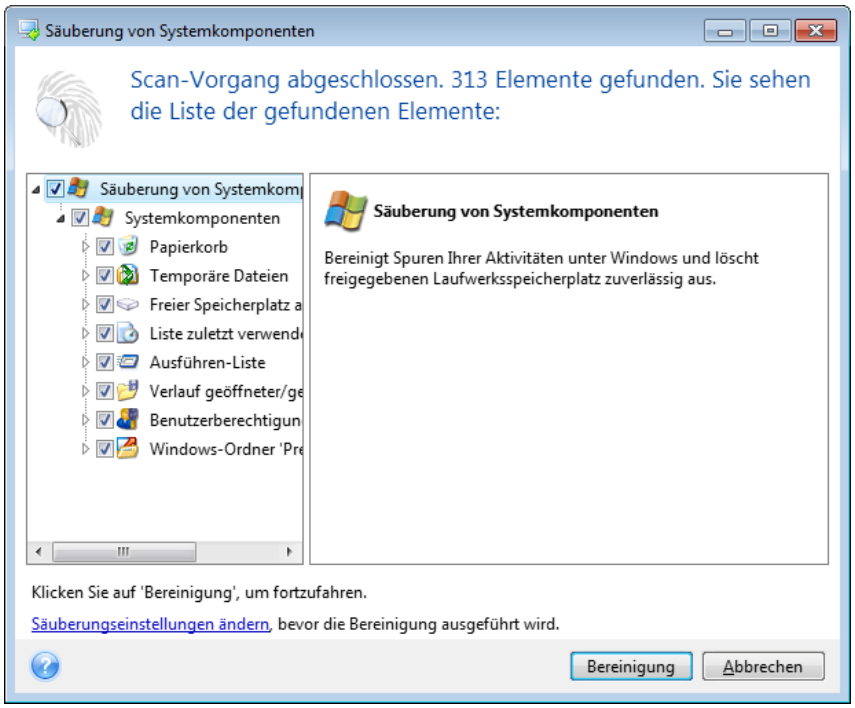
- Alle Daten im **Windows-Papierkorb** sicher löschen.
- Die **temporären Dateien** aus den entsprechenden Windows-Ordnern entfernen.
- Den **freien Speicherplatz von Festplattenlaufwerken** von allen Spuren dort gespeicherter Daten bereinigen.
- Spuren löschen, die bei der **Suche nach Dateien bzw. Computern** auf angeschlossenen Laufwerken bzw. nach Computern im lokalen Netzwerk hinterlassen wurden.
- Die Liste der **zuletzt verwendeten Dokumente** bereinigen.
- Die Liste des Befehls **Ausführen** von Windows bereinigen.
- Den Verlauf der **geöffneten/gespeicherter Dateien** bereinigen.
- Die Liste der Netzwerkressourcen bereinigen, mit denen sich der Anwender unter Verwendung von **Netzwerkanmeldedaten** verbunden hatte.
- Den **Windows-Ordner 'Prefetch'** bereinigen, in dem Windows Informationen über jene Programme speichert, die Sie kürzlich ausgeführt haben.

**Hinweis**
Windows 7 (und Nachfolgeversionen) speichert keine Informationen mehr über die Suche nach Dateien und Computern. Informationen über geöffnete und gespeicherte Dateien werden außerdem in der Registry unterschiedlich hinterlegt. Der Assistent zeigt diese Informationen daher auch unterschiedlich an.

**Hinweis**
Kennwörter werden von Windows bis zum Ende einer Sitzung gespeichert. Die Liste der Netzwerk-Anmeldedaten zu bereinigen, hat daher solange keine Auswirkung, bis Sie die aktuelle Windows-Sitzung durch Abmelden oder einen Computer-Neustart beenden.

Klicken Sie zum Starten des Systembereinigungsassistenten auf die **Start**-Schaltfläche und dann auf **Acronis** (Produktordner) —> **Systembereinigung**.

Nachdem Sie den Assistenten gestartet haben, sucht er nach sämtlichen Spuren von Benutzeraktivitäten, die in Windows gespeichert wurden. Das Ergebnis wird nach Abschluss der Suche im oberen Fensterbereich des Assistenten angezeigt.




Sie können das Suchergebnis einsehen und die zu löschenden Elemente manuell auswählen.

Klicken Sie auf den Hyperlink **Hier klicken**, um die Bereinigungseinstellungen zu ändern, bevor Sie fortfahren.

Klicken Sie auf **Bereinigung**, um mit dem Löschen der gefundenen Elemente zu starten.

## Einstellungen für die Bereinigung

Sie können die Bereinigungseinstellungen im entsprechenden Fenster für jede Systemkomponente ändern. Einige dieser Einstellungen gelten für alle Komponenten.

***So verändern Sie die Bereinigungseinstellungen einer Komponente***

- Erweitern Sie den Root-Eintrag **Systemkomponenten** im Baum und wählen Sie die Komponente, deren Bereinigungseinstellungen Sie ändern möchten. Auf der obersten Ebene können Sie die Analyse der Komponente ein- bzw. ausschalten. Dazu schalten Sie das Kontrollkästchen **Aktivieren** ein oder aus.

  Wenn erforderlich, können Sie die Komponente erweitern und Einstellungen vornehmen, wie etwa die Methode der Datenvernichtung wählen, die zu bereinigenden Dateien, die zu löschenden Registry-Such-Strings (zum Auffinden von Computern im lokalen Netzwerk) etc. Dazu klicken Sie auf das Dreieck neben der Komponente, wählen eine Option aus der Liste und spezifizieren Ihre Einstellung.
- Wenn Sie die gewünschten Eigenschaften der Komponenten konfiguriert haben, klicken Sie auf **OK**, um diese zu speichern. Diese Einstellungen werden als Standard benutzt, wenn Sie den Assistenten zur Systembereinigung das nächste Mal starten.

Wenn Sie die Bereinigungseinstellungen bereits verändert hatten, können Sie die Programmstandards durch einen Klick auf **Auf Standard zurücksetzen** erneut laden.

**Systemkomponenten:**

- Papierkorb
- Temporäre Dateien
- Freier Speicherplatz auf Laufwerk
- Computer-suchen-Liste
- Datei suchen-Liste
- Liste zuletzt verwendeter Dokumente
- Windows Ausführen-Liste
- Verlauf geöffneter/gespeicherter Dateien
- Anmeldedaten
- Windows-Ordner 'Prefetch'

## Standardoptionen für die Bereinigung

Sie erreichen die Standardoptionen für die Bereinigung, indem Sie auf der Optionsseite **Datenvernichtungsmethode** auf den Link **Standardmethode ändern...** klicken.

***So können Sie die Standardoptionen für die Bereinigung ändern:***

1. Wählen Sie die Option der Komponente, deren Bereinigungseinstellungen Sie ändern möchten.
2. Klicken Sie auf **OK**, um die geänderten Einstellungen zu speichern.

Wenn Sie die Bereinigungseinstellungen bereits verändert hatten, können Sie die Programmstandards durch einen Klick auf **Auf Standard zurücksetzen** erneut laden.

### Allgemein

Standardmäßig wird nach Abschluss jeder Bereinigungsprozedur ein zusammenfassender Dialog angezeigt (wenn das Kontrollkästchen **Zusammenfassung anzeigen** aktiviert wurde). Wenn Sie dieses Fenster in Zukunft nicht mehr sehen möchten, deaktivieren Sie das entsprechende Kontrollkästchen.

### Bereinigungsoptionen

Die Systembereinigung enthält einige der gängigsten Methoden zur Datenvernichtung. Hier können Sie die Datenvernichtungsmethode auswählen, die als Standard für alle anderen Komponenten verwendet wird.

Die Methoden zur Datenvernichtung sind in diesem Handbuch ausführlich unter Methoden zur Datenvernichtung auf Laufwerken beschrieben.

## Besondere Bereinigungsoptionen

Sie können folgende Optionen für die Bereinigung einstellen:

- Datenvernichtungsmethode
- Standardoptionen
- Dateien
- Freier Platz auf Laufwerk
- Computer
- Befehle
- Filter für Netzwerkressourcen

### Datenvernichtungsmethode

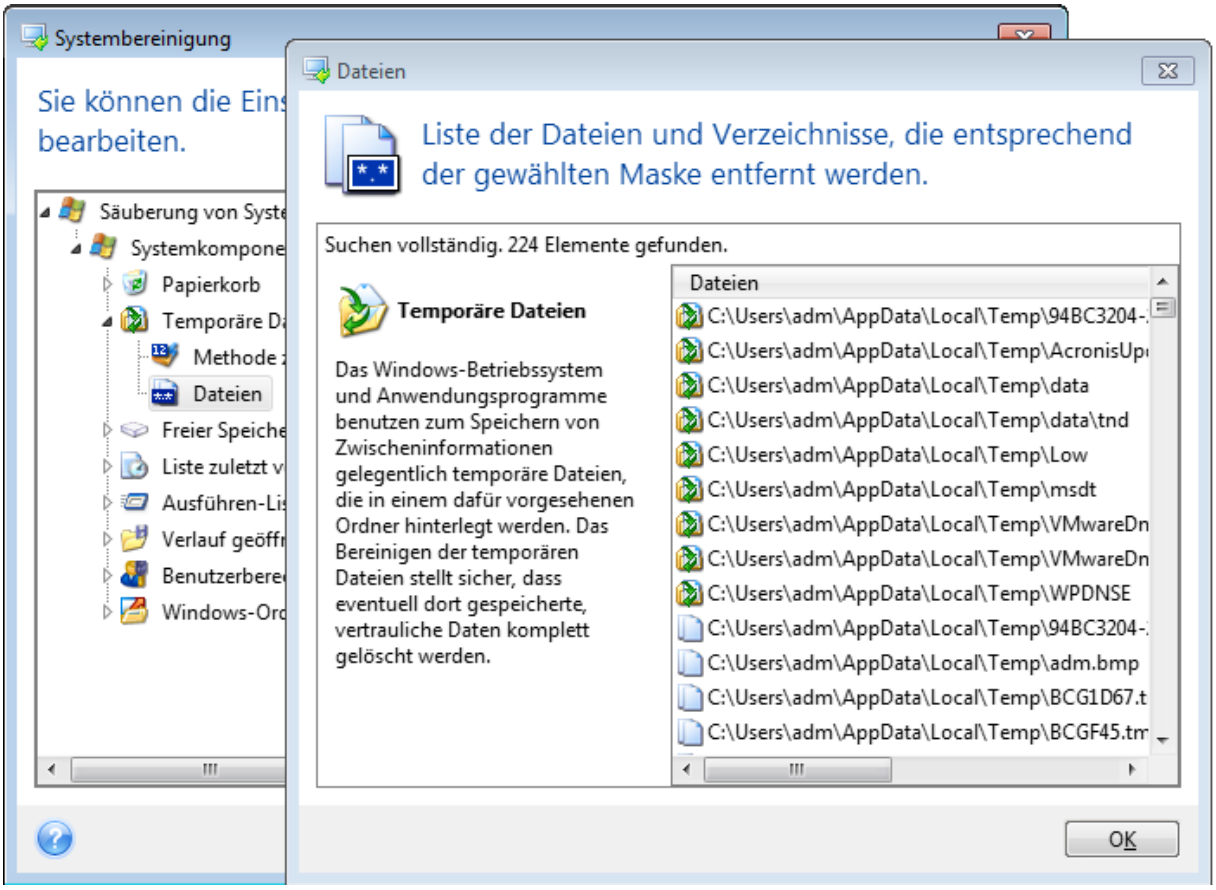
Die Systembereinigung enthält einige der gängigsten Methoden zur Datenvernichtung. Wählen Sie die gewünschte Methode zur Datenvernichtung.

- **Standardmethode verwenden** – wenn Sie diesen Parameter verwenden, wird das Programm die Standardmethode verwenden (die voreingestellte Methode ist 'Schnell').
  Wenn Sie eine andere Datenvernichtungsmethode als Standard einstellen möchten, klicken Sie auf den entsprechenden Link.
- **Benutzerdefinierte Methode für diese Komponente benutzen** – Diese Einstellung ermöglicht es, eine vorbereitete Methode zur Datenvernichtung aus der Liste zu wählen.

Die Methoden zur Datenvernichtung sind in diesem Handbuch ausführlich unter Methoden zur Datenvernichtung auf Laufwerken beschrieben.

## Dateien

Über die Einstellung 'Dateien' werden die Namen der Dateien zum Löschen mit dem Systembereinigungsassistenten bestimmt; Sie können dafür auch eine Suchmaske verwenden.




Suchmasken repräsentieren unter Windows ganze Dateinamen oder nur Teile davon. Eine Suchmaske kann jedes alphanumerische Zeichen, inklusive Kommas sowie Windows Wildcard-Symbole enthalten und ähnliche Werte wie folgt haben:

- *.* – um alle Dateien mit beliebigen Dateinamen und Erweiterungen zu löschen.
- *.doc – um alle Dateien mit einer bestimmten Erweiterung zu löschen (in diesem Fall Microsoft Word-Dokumente).
- read*.* – um alle Dateien mit beliebiger Erweiterung zu löschen, deren Name mit 'read' beginnt.
- read?.* – um alle Dateien mit beliebiger Erweiterung zu löschen, deren Name fünf Zeichen hat und mit 'read' beginnt, wobei das fünfte Zeichen beliebig ist.

  Resultat der Suche sind z.B. Dateien wie read1.txt oder ready.doc; Dagegen ist eine Datei mit dem Namen 'readyness.txt' ausgeschlossen, da sie unabhängig von der Endung einen Namen mit mehr als fünf Zeichen hat.

Sie können viele verschiedene Suchbegriffe per Semikolon getrennt eingeben, beispielsweise:

*.bak;*.tmp;*.~~~ (ohne Leerzeichen zwischen den Suchbegriffen)

Alle Dateien, deren Name mindestens eines der Kriterien erfüllt, werden gelöscht.

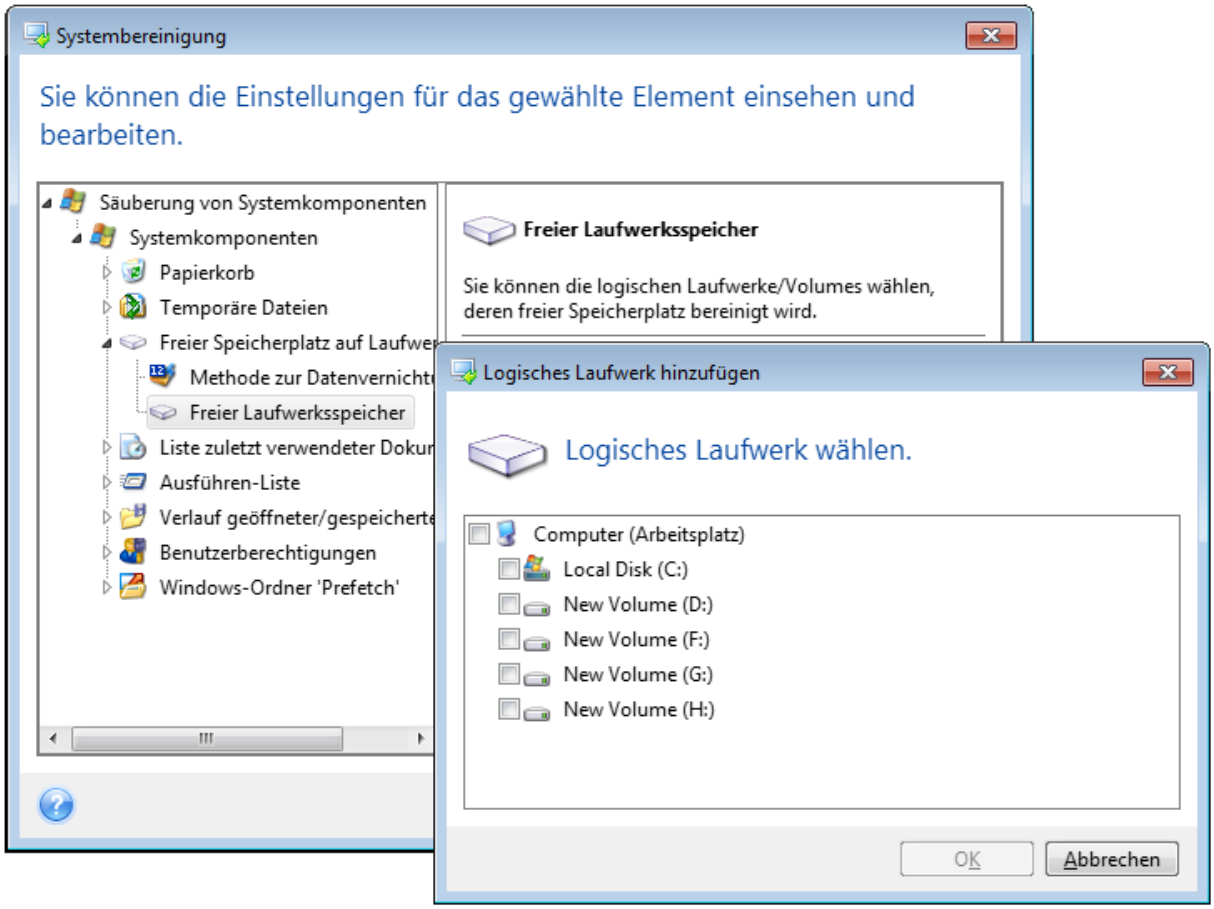
Nach Eingabe der Werte für die Dateieinstellungen können Sie diejenigen Dateien durchsuchen, die den Suchbegriffen entsprechen. Dazu klicken Sie auf **Dateien anzeigen**. Sie sehen ein Fenster mit den Namen der gefundenen Dateien. Diese Dateien werden bereinigt.

## Freier Platz auf Laufwerk

Hier können Sie spezifizieren, auf welchen physischen oder logischen Laufwerken der freie Platz bereinigt wird. In der Standardeinstellung wird die Systembereinigung den Platz auf allen verfügbaren Laufwerken bereinigen.

Wenn Sie die Einstellungen dieses Parameters verändern möchten, können Sie die Schaltfläche **Entfernen** verwenden, um die Laufwerke von der Liste zu entfernen, deren Speicherplatz Sie nicht bereinigen müssen.

Falls Sie diese Laufwerke wieder in die Liste aufnehmen möchten, benutzen Sie die Schaltfläche **Hinzufügen**.



## Computer

Die Einstellung **Computer** bereinigt die Windows-Registry von Computernamen, nach denen Sie im lokalen Netzwerk gesucht haben. Die Zeichenketten bewahren Informationen darüber auf, was Sie im Netzwerk interessiert hat. Zur Wahrung der Vertraulichkeit sollten daher auch diese Elemente gelöscht werden.

Die Einstellung **Computer** ist ähnlich zur Einstellung **Dateien**. Es handelt sich um eine Zeichenkette, die eine beliebige Zahl vollständiger oder partieller Computernamen enthalten kann, getrennt durch Semikolons. Die Löschung der 'Computer'-Suchbegriffe erfolgt nach üblichen Windows-Regeln und auf Basis eines Vergleichs mit den eingestellten Werten unter **Computer**.

Wenn Sie einfach nur die Suchbegriffe aller lokalen Netzwerkcomputer löschen müssen (in den meisten Fällen ausreichend), belassen Sie einfach die Standardvorgaben dieser Einstellung. So können Sie die Standardeinstellungen wiederherstellen:

- Wählen Sie Komponente **Computer suchen-Liste**.
- Stellen Sie sicher, dass das Kontrollkästchen **Aktivieren** eingeschaltet ist
- Wählen Sie die Einstellung **Computer**; stellen Sie sicher, dass die Textbox leer ist.

Als Ergebnis werden alle Suchbegriffe für Computer aus der Registry gelöscht.

Nachdem Sie den Wert für die Einstellung **Computer** eingegeben haben, können Sie die Zeichenketten durchsuchen, die der Systembereinigungsassistent in der Registry gefunden hat. Klicken Sie dafür auf **Computer anzeigen**. Sie sehen ein Fenster mit vollständigen und unvollständigen Computernamen, nach denen im Netzwerk gesucht wurde. Diese Einträge werden gelöscht.

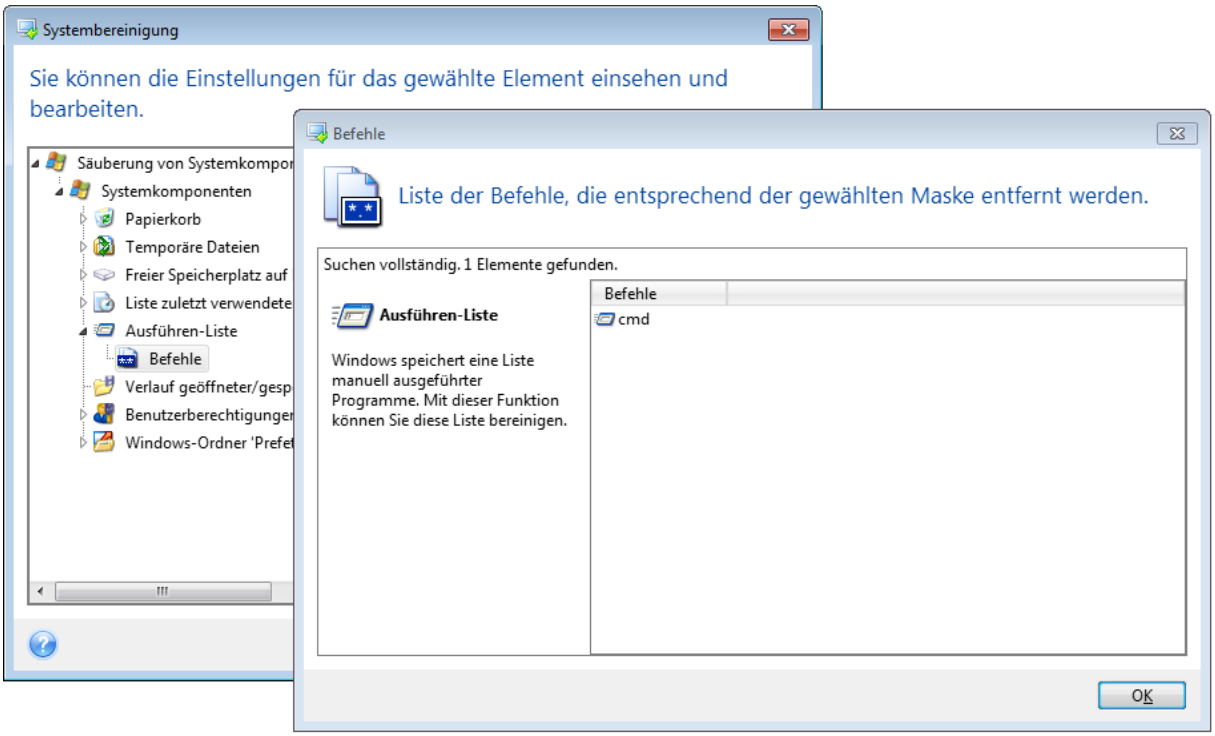
## Befehle einstellen

Hier können Sie festlegen, welche Befehle von der **Windows-Ausführen-Liste** entfernt werden.

Diese Vorlage kann vollständige Befehle oder nur Teile davon enthalten, jeweils getrennt durch ein Semikolon, z.B.:

*help; cmd; reg*

Diese Maske wird für das Entfernen aller Befehle sorgen, die dem Namen entsprechen oder einen Teil von dem enthalten, was Sie eingegeben haben.




## Filter für Netzwerkressourcen

Tragen Sie (durch Semikolon getrennt) die Host-Namen oder IP-Adressen der Netzwerkressourcen, Server, FTP-Server, Netzwerkfreigaben usw. ein, zu denen Sie unter Eingabe von Anmeldedaten (Benutzername und Kennwort) eine Verbindung hergestellt haben. Für die Eingabe von Host-Namen und IP-Adressen können Sie die Wildcards * und ? benutzen.

Klicken Sie auf **Netzwerkressourcen anzeigen**, um die Liste der von Ihnen besuchten Netzwerkressourcen einzusehen, deren Anmeldedaten Sie löschen wollen.

# Vorschau

Wenn die Suche beendet ist, erscheinen die Ergebnisse im oberen Teil des Assistentenfensters. Als Standard wurden alle Systemkomponenten für die Bereinigung gescannt. Wenn Sie einstellen möchten, welche der Systemkomponenten gescannt werden und welche nicht, dann ändern Sie die Standardoptionen für die Bereinigung.

Sie können die Suchergebnisse einsehen und manuell bestimmen, welche Elemente Sie behalten oder löschen wollen. Um Ihnen bei der richtigen Wahl zu helfen, sind alle Komponenten mit einer kurzen Beschreibung versehen. Klicken Sie einfach auf den Namen einer Komponente und die dazugehörige Beschreibung wird auf der rechten Seite des Fensters angezeigt.

**Um eine Komponente ein- bzw. auszuschalten, gehen Sie wie folgt vor:**

- Erweitern Sie das Element **Systemkomponenten** im Verzeichnisbaum der Systembereinigung und aktivieren Sie die Komponente, die Sie bereinigen wollen. Wenn Sie eine Komponente nicht bereinigen wollen, dann deaktivieren Sie einfach das entsprechende Kontrollkästchen.

- Wenn erforderlich, können Sie die Komponente selbst erweitern und einzelne Inhalte ein- bzw. ausschließen.

Wenn Sie die Komponenten für die Bereinigung gewählt haben, dann klicken Sie zum Fortfahren auf die Schaltfläche **Bereinigen**.

**Hinweis**
Windows 7 (und Nachfolgeversionen) speichert keine Informationen mehr über die Suche nach Dateien und Computern. Außerdem werden Informationen über geöffnete bzw. gespeicherte Dateien in der Registry anders hinterlegt, daher zeigt der Assistent diese Informationen anders an.

### Fortgang der Bereinigung

Das Statusfenster zeigt Informationen über den Fortgang der aktuellen Aktion.

Während die gewählte Aktion abläuft, wird der Grad der Vervollständigung per Fortschrittsbalken angezeigt.

In einigen Fällen kann die Fertigstellung der Aktion länger dauern. In diesen Fällen aktivieren Sie das Kontrollkästchen **Computer herunterfahren, wenn Aktion beendet ist.**. Wenn die Aktion abgeschlossen ist, wird Acronis Cyber Protect Home Office den Computer ausschalten.

## Ein Backup-Image mounten

Wenn Sie Images als virtuelle Laufwerke mounten, können Sie auf diese wie auf physische Festplattenlaufwerke zugreifen. Sie können ein lokales Backup mounten, welches Volumes (Partitionen) oder komplette Laufwerke enthält – und dann bestimmen, welche der enthaltenen Volumes gemountet werden sollen. Nach dem Mounten:

- Für jedes gemountete Volume wird in Ihrem System ein neues Laufwerk angezeigt.
- Sie können die Inhalte des Images direkt mit dem Windows Datei-Explorer (oder einem anderen Datei-Manager) im 'Nur Lesen'-Modus einsehen.

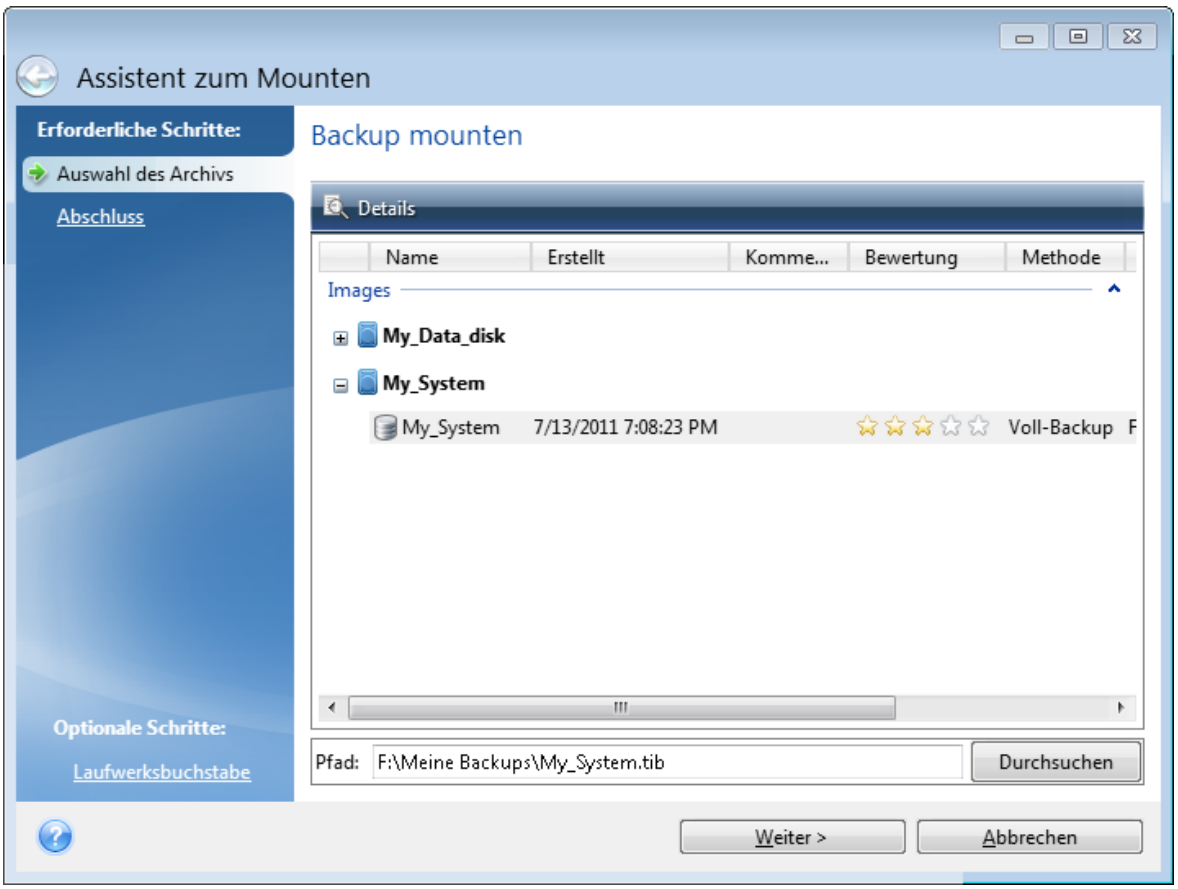
**Hinweis**
Die in diesem Abschnitt beschriebenen Aktionen werden nur für FAT- und NTFS-Dateisysteme unterstützt.

**Hinweis**
Ein Laufwerk-Backup kann nicht gemountet werden, falls es auf einem FTP-Server gespeichert ist.

### So können Sie ein Image mounten

1. Klicken Sie im Windows Datei-Explorer mit der rechten Maustaste auf diejenige Image-Datei, die Sie anbinden wollen, und klicken Sie dann auf **Mounten**.
   Der Assistent zum Mounten wird geöffnet.

2. Bestimmen Sie das zu mountende Backup anhand seines Erstelldatums (Zeitstempel). So können Sie den Datenzustand zu einem gewünschten Moment durchsuchen.




3. [Optionaler Schritt] Wählen Sie im Schritt **Laufwerksbuchstabe** denjenigen Buchstaben aus dem Listenfeld **Laufwerksbuchstabe** aus, der dem virtuellen Laufwerk zugewiesen werden soll. Wenn Sie ein Volume nicht mounten wollen, wählen Sie **Nicht mounten** aus der Liste oder deaktivieren Sie das Kontrollkästchen des Volumes.
4. Klicken Sie auf **Fertigstellen**.
5. Wenn das Image angeschlossen ist, startet der Windows Datei-Explorer und zeigt seinen Inhalt.

# Ein gemountetes Image trennen

Es wird empfohlen, ein gemountetes virtuelles Laufwerk wieder zu trennen, wenn alle gewünschten Aktionen beendet wurden, weil virtuelle Laufwerke einige Systemressourcen beanspruchen.

***So können Sie ein Image trennen („unmounten“)***

1. Klicken Sie im Windows Datei-Explorer mit der rechten Maustaste auf das Laufwerkssymbol und wählen Sie **Trennen**.
2. Starten Sie Ihren Computer neu oder fahren Sie ihn herunter.

# Mit .vhd(x)-Dateien arbeiten

Acronis Backups (.tibx-Dateien) von Laufwerken oder Volumes können in virtuelle Laufwerke (.vhd(x)-Dateien) konvertiert werden, die zudem auch das Dateiformat von Windows-Backups sind.

## So können Sie .vhd(x)-Dateien verwenden

- Sie können Ihren Computer von einer konvertierten .vhd(x)-Datei booten und so testen, ob das Backup gültig ist und als bootfähiges Betriebssystem wiederhergestellt werden kann.
- Sie können die .vhd(x)-Datei außerdem für Notsituationen aufbewahren. Sollte Ihr Computer beispielsweise nicht starten können und Sie ihn aber umgehend verwenden müssen, dann können Sie von einer solchen .vhd(x)-Datei booten.
- Sie können in Windows 7 eine .vhd(x)-Datei zudem als zusätzliches Laufwerk mounten. Die .vhd(x)-Datei kann beliebige Volumes (Partitionen) enthalten – egal ob vom Typ 'System' oder 'Nicht-System'.
- Sie können eine konvertierte .vhd(x)-Datei als virtuelle Maschine ausführen.

## Beschränkungen und zusätzliche Informationen

- Ein Datei-Backup kann nicht in eine .vhd(x)-Datei konvertiert werden.
- Um von einer konvertierten .vhd(x)-Datei booten zu können, muss diese Folgendes enthalten:
  - Das System-Volume desselben Computers. Sie können die .vhd(x)-Datei nicht verwenden, um andere Computer zu booten.
  - Windows 7 oder ein neueres Betriebssystem.
- Alle Änderungen, die Sie an einer gebooteten oder gemounteten .vhd(x)-Datei durchführen, werden in dieser gespeichert. Falls Sie von einer .vhd(x)-Datei booten und Änderungen an Daten durchführen, die nicht im Backup vorliegen, beeinflussen diese Änderungen Ihr aktuelles System ('Live-System').
- Die autonomen Notfallversionen von Acronis Cyber Protect Home Office, die Sie von einem Boot-Medium ausführen können, unterstützt keine Konvertierungsaktionen.
- Acronis Cyber Protect Home Office kann keine .tibx-Dateien konvertieren, die dynamische Volumes enthalten, welche usprünglich auf mehreren Laufwerken gelegen haben (beispielsweise dynamische Volumes vom Typ 'Übergreifend' oder 'Gespiegelt').

## Ein Acronis Backup konvertieren

Benutzer einer Enterprise oder Ultimate Edition von Windows 7 (und neueren Windows-Versionen) können das tibx-Image eines System-Volumes ins .vhd(x)-Format konvertieren, falls die konvertierte .vhd(x)-Datei zum Booten des Betriebssystems verwendet werden soll. Sie haben dann auch die Möglichkeit, Images ohne Acronis Cyber Protect Home Office zu mounten.

***So können Sie ein Acronis Laufwerk-Image (.tibx-Datei) in ein Windows-Backup (virtuelle .vhd(x)-Datei) konvertieren***

1. Acronis Cyber Protect Home Office starten.
2. Gehen Sie in den Programmbereich **Backup**.
3. Klicken Sie in der Backup-Liste auf den nach unten zeigenden Pfeil neben dem zu konvertierenden Backup – und klicken Sie dann auf **In VHD-Format konvertieren**.
   Falls das Backup kennwortgeschützt ist, wird Acronis Cyber Protect Home Office danach fragen. Beachten Sie, dass die .vhd(x)-Datei nach der Konvertierung nicht mehr kennwortgeschützt ist.
4. Wählen Sie die Backup-Version aus, die Sie konvertieren wollen.
   Zum Konvertieren eines inkrementellen Backups sind alle vorherigen inkrementellen Backups und das ursprüngliche Voll-Backup erforderlich. Zum Konvertieren eines differentiellen Backups ist das ursprüngliche vollständige Backup erforderlich. Das Ergebnis einer Konvertierung ist immer ein vollständiges Backup.
5. Geben Sie den Pfad zu der Datei an, die erstellt werden soll.
   Die Datei kann auf jedem lokalen Datenspeicher (Storage) gespeichert werden, der von Acronis Cyber Protect Home Office unterstützt wird (die Acronis Secure Zone und CDs/DVDs ausgenommen). Außerdem kann sie auf einem freigegebenen Netzlaufwerk gespeichert werden.
6. [Optionaler Schritt] Während das Backup konvertiert wird, können Sie das Kontrollkästchen **Virtuelle Maschine nach Fertigstellung starten** aktivieren. Wenn diese Einstellung aktiviert ist, wird Acronis Cyber Protect Home Office Ihren Computer neu starten und anschließend mithilfe der erstellten .vhd(x)-Datei die virtuelle Hyper-V-Maschine ausführen.

Wenn ein für die Konvertierung ausgewähltes .tibx-Image mehrere Volumes enthält (z.B. von zwei physischen Laufwerken), erstellt das Programm zwei .vhd(x)-Dateien, die den physischen Laufwerken entsprechen.

# Backup-Einstellungen importieren und exportieren

Acronis Cyber Protect Home Office ermöglicht Ihnen, die Einstellungen Ihrer Backups zu importieren oder zu exportieren. Das kann beispielsweise praktisch sein, um die Einstellungen auf einen neuen PC zu übertragen, nachdem Sie Acronis Cyber Protect Home Office auf diesem installiert haben. Die Einstellungen zu speichern kann zudem nützlich sein, wenn Sie vorhaben, später ein Upgrade auf eine neuere Version von Acronis Cyber Protect Home Office durchzuführen.

Durch Übertragung der Einstellungen wird die Konfiguration von Backups auf dem neuen PC deutlich erleichtert. Sie müssen die Einstellungen nur exportieren – und Sie dann auf dem anderen PC importieren. Die Einstellungen werden in Form von Skript-Dateien exportiert.

Der Inhalt der Einstellungen kann, abhängig vom Backup-Typ, unterschiedlich sein. Im Fall 'klassischer' Laufwerk- und Datei-Backups enthalten die Einstellungen folgende Elemente:

- Auflistung der zu sichernden Elemente
- Backup-Optionen
- Backup-Speicherort
- Planung

- Backup-Schema
- Automatische Bereinigungsregeln
- Regeln zur Benennung von Backup-Versionen

Es gibt folgende Einstellungen für Nonstop Backups:

- Liste der durch Nonstop Backup zu schützenden Elemente
- Speicherort des Nonstop Backup Storages (eine Liste von Speicherorten, falls es mehrere gibt)

**Hinweis**
Sie können jedoch keine Online Backup-Einstellungen von einem Computer zu einem anderen importieren.

***So können Sie Backup-Einstellungen exportieren***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie in der Seitenleiste auf **Einstellungen** –> **Übertragung von Backup-Einstellungen**. Klicken Sie anschließend auf **Einstellungen in Datei speichern** und bestimmen Sie dann den Zielort, an dem die Skript-Dateien mit den Einstellungen gespeichert werden sollen.

***So können Sie Backup-Einstellungen importieren***

1. Starten Sie Acronis Cyber Protect Home Office auf einem anderen Computer.
2. Klicken Sie in der Seitenleiste auf **Einstellungen** –> **Übertragung von Backup-Einstellungen**. Klicken Sie anschließend auf **Einstellungen aus Datei importieren** und geben Sie an, wo die Skript-Dateien mit den Einstellungen gespeichert sind.

Nach Import der Einstellungen kann es zudem angebracht sein, einige so anzupassen, dass sie für Ihre neue Arbeitsumgebung passend sind. Es kann beispielsweise notwendig sein, die Liste der zu sichernden Elemente, der Backup-Zielorte usw. anzupassen.

Falls Sie einige Backups auf einen anderen Computer kopieren wollen, ist es empfehlenswert auch die zu diesen Backups gehörenden Einstellungen zu exportieren. Auf diese Weise verlieren Sie keine zu den kopierten Backups gehörende Funktionalität.

# Acronis Universal Restore

Durch die Verwendung von Acronis Universal Restore können Sie einen bootfähigen Klon Ihres System auf bzw. für eine abweichende Hardware erstellen. Verwenden Sie dieses Werkzeug, um Ihr Systemlaufwerk auf einem Computer mit abweichender Hardware wiederherzustellen (wenn Prozessor, Mainboard oder Massenspeichergerät anders als im ursprünglich gesicherten System sind). Das kann beispielsweise nützlich werden, wenn Sie ein defektes Mainboard ersetzen oder Ihr System von einem Computer auf einen anderen Computer migrieren wollen.

## Welches Problem wird dabei gelöst?

Das Disk-Image eines Systems lässt sich leicht auf identischer Hardware bzw. auf dem Computer wiederherstellen, auf dem das Backup erstellt wurde. Wenn Sie jedoch versuchen, dies auf abweichender Hardware (als Ziel) durchzuführen, wird das wiederhergestellte System nicht bootfähig sein. Grund ist, dass die neue Hardware inkompatibel zu den wichtigsten, im Image enthaltenen Treibern ist. Das Werkzeug findet und installiert Treiber für solche Geräte, die für den Betriebssystemstart notwendig sind. Das sind insbesondere Treiber für Speicher-Controller (Festplatten-Controller) sowie für das Mainboard (die Hauptplatine) und dessen Chipsatz.

## Wie wird es verwendet?

Bevor Sie mit der Wiederherstellung auf einer abweichenden Hardware beginnen, sollten Sie überprüfen, dass Sie Folgendes haben:

- Ein Backup Ihres Systemlaufwerks oder ein Backup des kompletten PCs
- Acronis Boot-Medium
- Ein Acronis Universal Boot-Medium

**Hinweis**
Falls auf Ihrem Computer sowohl Acronis Cyber Protect Home Office als auch der Acronis Universal Boot Media Builder installiert sind, können Sie Acronis Cyber Protect Home Office und Acronis Universal Boot gemeinsam auf demselben Medium speichern lassen. Weitere Informationen finden Sie im Abschnitt 'Ein Acronis Universal Boot-Medium erstellen'.

So stellen Sie Ihr System auf einem Computer mit abweichender Hardware wieder her:

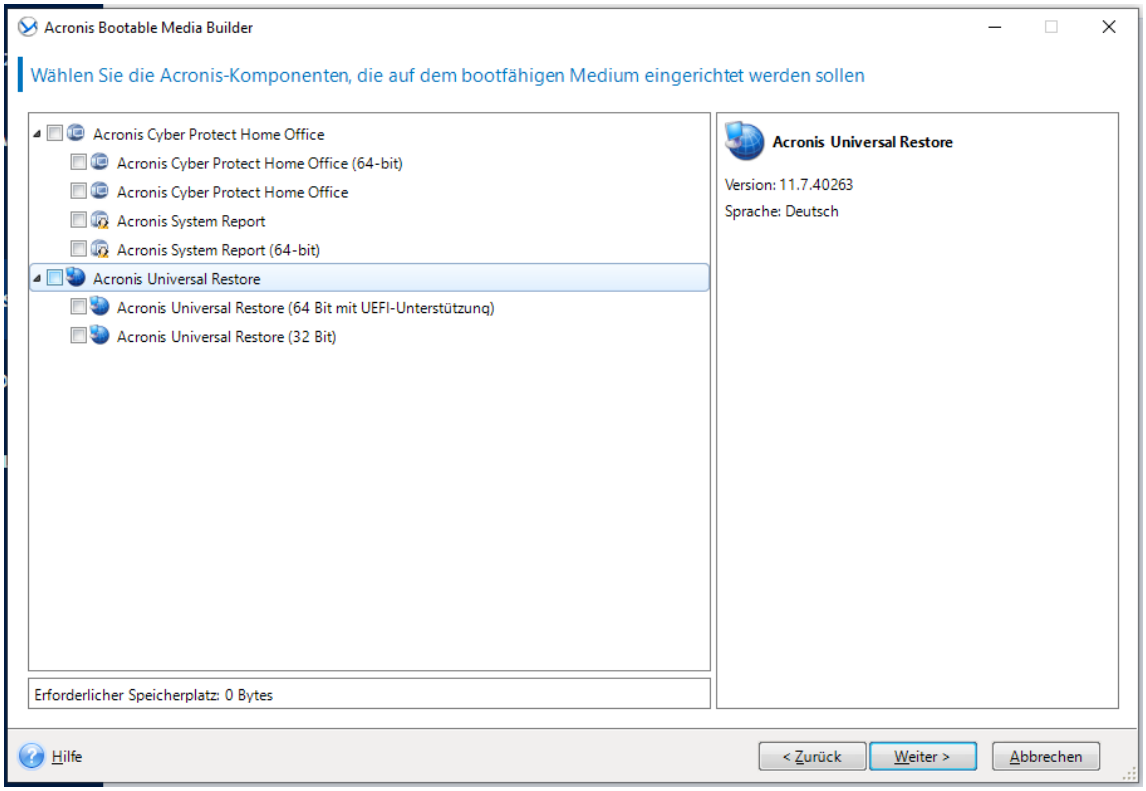
1. Starten Sie den Zielcomputer für die Wiederherstellung mit einem normalen Acronis Boot-Medium. Verwenden Sie ein vorliegendes 'System-Backup' oder ein 'Backup des kompletten PCs' und stellen Sie damit Ihr System auf dem Zielcomputer wieder her. Weitere Informationen finden Sie im Abschnitt 'Ein System mit einem Boot-Medium auf einem neuen Laufwerk wiederherstellen'.
2. Starten Sie den Zielcomputer mit einem Acronis Universal Boot-Medium und befolgen Sie die Bildschirmanweisungen, damit Ihr wiederhergestelltes System bootfähig gemacht werden kann. Weitere Details finden Sie im Abschnitt 'Acronis Universal Restore verwenden'.

## Ein Acronis Universal Boot-Medium erstellen

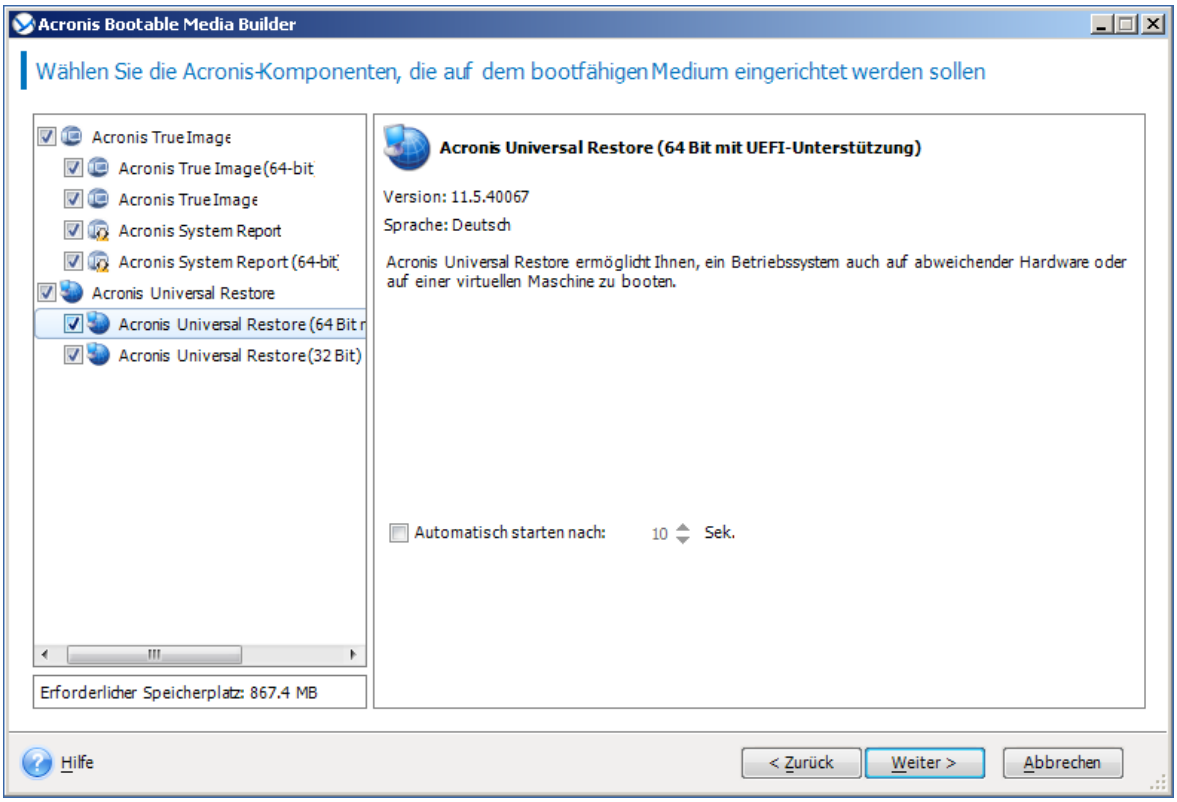
Ein Acronis Universal Boot-Medium wird verwendet, um einen Computer nach einer Wiederherstellung auf abweichender Hardware (z.B. einem ganz neuen PC) bootfähig zu machen. Weitere Details finden Sie im Abschnitt 'Acronis Universal Restore'.

***So können Sie ein Acronis Universal Boot-Medium erstellen:***

1. Acronis Cyber Protect Home Office starten.
2. Klicken Sie im Programmbereich **Extras** auf den Befehl **Acronis Universal Restore**.
3. Klicken Sie auf **Download**, um den Acronis Universal Boot Media Builder herunterzuladen.
4. Führen Sie die heruntergeladene Datei aus und installieren Sie den Media Builder.
5. Schließen Sie einen USB-Stick an oder legen Sie eine leere (beschreibbare) DVD ein, die Sie bootfähig machen wollen.
6. Führen Sie eine der nachfolgenden Aktionen aus, um den Acronis Universal Boot Media Builder zu starten:
   - Klicken Sie im Programmbereich **Extras** auf den Befehl **Acronis Universal Restore**.
   - Klicken Sie auf die Windows-Schaltfläche **Start**, gehen Sie in die Liste der installierten Programme und klicken Sie dort auf die Verknüpfung **Universal Boot Media Builder ausführen**.
7. Folgende Voraussetzungen müssen erfüllt sein:
   - Ein 'Linux-basiertes Medium' ist als Boot-Medium-Typ ausgewählt.
   - Die Laufwerke und Volumes werden mit der 'Windows-typischen Darstellung' angezeigt.




8. [Optional] Sie können Parameter für den Linux-Kernel spezifizieren. Weitere Details finden Sie im Abschnitt 'Startparameter für das Boot-Medium'.
9. Wählen Sie die Acronis Komponenten, die auf dem Medium eingerichtet werden sollen.




Sie können zwischen 32-Bit- und/oder 64-Bit-Komponenten wählen. Die 32-Bit-Komponenten funktionieren auch auf 64-Bit-Hardware. Sie benötigen jedoch 64-Bit-Komponenten, wenn Sie einen Computer booten möchten, dessen BIOS gemäß UEFI-Standard (Unified Extensible Firmware Interface) arbeitet.

Wählen Sie beide Komponententypen, wenn Sie das Medium auf verschiedenen Hardware-Varianten einsetzen wollen. Wenn Sie eine Maschine mit dem resultierenden Medium booten, können Sie die benötigten Komponenten (ob 32 Bit oder 64 Bit) dann aus dem Boot-Menü auswählen.

Falls auf Ihrem Computer Acronis Cyber Protect Home Office installiert ist, können Sie auch dieses auf dem Medium einrichten lassen. In diesem Fall erhalten Sie anschließend ein einziges Boot-Medium, welches beide Komponenten enthält, um Daten auf abweichende Hardware wiederherstellen zu können.

10. Bestimmen Sie das Ziel für das Medium:
    - **CD**
    - **DVD**
    - **USB-Stick**
    - **ISO-Image-Datei**

      Sie müssen den Namen für die .iso-Datei und den Zielordner spezifizieren.

      Wenn die .iso-Datei erstellt wurde, können Sie diese anschließend auf CD bzw. DVD brennen. Unter Windows 7 (und höher) können Sie dies beispielsweise auch mit der integrierten Brennfunktion tun. Klicken Sie dazu im Windows Datei-Explorer doppelt auf die erstellte ISO-Image-Datei und dann auf **Brennen**.

11. Spezifizieren Sie die benötigten Treiber für die Massenspeichergeräte (des Zielcomputers), die Acronis Universal Boot bei der Einrichtung verwenden soll, um das Zielbetriebssystem bootfähig zu machen.

    Sie müssen diese Treiber nicht schon hier hinzufügen. Sie können diese auch später noch tun, wenn Sie Acronis Universal Boot auf einen bestimmten Computer zum Einsatz bringen.
12. Klicken Sie auf **Fertigstellen**.

    Trennen Sie den USB-Stick vom Computer bzw. entnehmen Sie das gebrannte Medium aus dem Laufwerk. Dieser Datenträger ist nun Ihr fertiges Acronis Universal Boot-Medium.

# Acronis Universal Restore verwenden

## Vorbereitung

### Treiber vorbereiten

Bevor Sie Universal Restore auf ein Windows-Betriebssystem anwenden, sollten Sie sicherstellen, dass Sie über die passenden Treiber für den neuen Festplatten-Controller und den Chipsatz des Mainbords verfügen. Diese Treiber sind für den Start des Betriebssystem unerlässlich. Verwenden Sie (sofern vorhanden) die Treiber-CD/-DVD, die der Hardware-Hersteller Ihrem Computer/Mainboard beigelegt hat – oder laden Sie benötigten Treiber von der Website des Herstellers herunter. Die Treiber sollten die Erweiterungen *.inf, *.sys oder *.oem haben. Wenn Sie die Treiber im Format *.exe, *.cab oder *.zip herunterladen, extrahieren Sie diese mit einer entsprechenden Dritthersteller-Anwendung.

### Überprüfen Sie, dass auf die Treiber in der bootfähigen Umgebung zugegriffen werden kann.

Überprüfen Sie, dass Sie beim Arbeiten mit einem Boot-Medium auf das Gerät mit den Treibern zugreifen können. Ein WinPE-basiertes Medium sollte dann zum Einsatz kommen, wenn ein Gerät unter Windows verfügbar ist, von einem Linux-basierten Medium aber nicht erkannt wird.

## Universal Restore-Einstellungen

### Automatische Suche nach Treibern

Spezifizieren Sie, wo das Programm nach Treibern für die Hardware-Abstraktionsschicht (HAL, Hardware Abstraction Layer) sowie für Festplatten-Controller und Netzwerkkarten suchen soll:

- Befinden sich die Treiber auf einem Datenträger (CD/DVD) des Herstellers oder einem anderen Wechselmedium, dann aktivieren Sie **Wechselmedien durchsuchen**.
- Liegen die Treiber in einem Netzwerkordner oder auf einem Boot-Medium, so spezifizieren Sie den Pfad zu diesem Ordner durch Anklicken von **Ordner durchsuchen**.

Zusätzlich wird Universal Restore den Standardspeicherort (Ordner) für Treiber durchsuchen – normalerweise ist dies der Ordner 'C:\Windows/inf').

### Auf jeden Fall zu installierende Massenspeichertreiber

Sie benötigen diese Einstellung falls:

- Die Hardware einen speziellen Massenspeicher-Controller verwendet – z.B. einen RAID- (insbesondere NVIDIA RAID) oder Fibre Channel-Adapter.
- Falls die automatische Suche nach Treibern nicht hilft, das System zu booten.

Spezifizieren Sie die entsprechenden Treiber, indem Sie auf den Befehl **Treiber hinzufügen** klicken. Treiber, die hier definiert werden, werden auch dann (mit entsprechenden Warnmeldungen) installiert, wenn das Programm einen besseren Treiber findet.

## Der Universal Restore-Prozess

Klicken Sie auf **OK**, nachdem Sie die benötigten Einstellungen spezifiziert haben.

Nachdem der Prozess abgeschlossen wurde, können Sie die Netzwerk-Verbindung konfigurieren und weitere Treiber spezifizieren (beispielsweise für die Grafikkarte und USB-Geräte).

# Problembehebung (Troubleshooting)

## Lösungen für die häufigsten Probleme

Nachfolgend finden Sie eine Liste häufiger Probleme, auf die Anwender bei Acronis Cyber Protect Home Office stoßen können. Die entsprechenden Lösungen können Sie in der Acronis Knowledge Base nachlesen.

**Die Anmeldung beim Programmstart schlägt fehl**

**Fehlermeldung: 'Sie haben die maximale Anzahl an Aktivierungen für diese Seriennummer überschritten'**

**Fehlermeldung: 'Diese Seriennummer wurde bereits für ein anderes Konto registriert.'**

**Beim Durchsuchen von Backups mit einem Dateimanager werden keine Dateien und Ordner angezeigt**

**Fehlermeldung: 'Schließen Sie das externe Laufwerk an'**

**Ein Backup in die Acronis Cloud schlägt fehl und es wird die Fehlermeldung 'Schreibfehler', 'Fehler beim Schreiben der Datei' oder 'FES-Anforderung ist fehlgeschlagen' angezeigt**

**Nach Wiederherstellung auf neuer Hardware erscheint aufgrund fehlender Treiber ein Bluescreen (BSOD) mit der Fehlermeldung 'Stop 0x0000007B'**

Unter https://kb.acronis.com/true-image-known-solutions finden Sie eine vollständige Liste der häufigsten Probleme und dazugehöriger Lösungen.

Beachten Sie außerdem den Knowledge Base-Artikel 'https://kb.acronis.com/content/46340', der Troubleshooting-Informationen zu fehlschlagenden Wiederherstellungen enthält.

## Acronis System Report

Wenn Sie den Acronis Support kontaktieren, werden zur Lösung Ihres Problems zumeist auch Informationen über Ihr System benötigt. Manchmal können diese Informationen nur umständlich und zeitaufwendig beschafft werden.

Das Tool **Systembericht erstellen** generiert einen Systembericht, der alle notwendigen technischen Informationen enthält und von Ihnen in einer Datei gespeichert werden kann. Falls erforderlich, können Sie diese Datei an Ihre Problembeschreibung anhängen und an den Support senden. Das hilft, die Suche nach einer entsprechenden Lösung zu vereinfachen und zu beschleunigen.

***Führen Sie eine der folgenden Aktionen aus, um einen Systembericht zu generieren***

- Klicken Sie in der Seitenleiste auf **Hilfe** und dann auf **Systembericht erstellen**.
- Drücken Sie **Strg+F7**. Beachten Sie, dass Sie diese Tastenkombination auch dann verwenden können, wenn Acronis Cyber Protect Home Office gerade einen anderen Vorgang durchführt.

- Wenn Sie Windows 11 verwenden, klicken Sie auf **All Apps** –> **Acronis** –> **Acronis System Report**.
- Wenn Sie Windows 10 verwenden, klicken Sie im **Start**-Menü auf **Acronis** –> **Acronis System Report**.
- Wenn Sie Windows 7 oder 8 verwenden, klicken Sie auf **Start** –> **Alle Programme** –> **Acronis** –> **Acronis System Report**.

***Nachdem der Bericht erstellt wurde***

- Um den soeben erstellten Systembericht zu speichern, klicken Sie auf **Speichern** und geben im sich öffnenden Dialogfeld ein Speicherziel für die Datei an.
- Wenn Sie das Hauptfenster des Programms verlassen möchten, ohne den Bericht zu speichern, klicken Sie auf **Abbrechen**.

Sie können dieses Tool auch als separate Komponente auf einem Boot-Medium speichern, um einen Systembericht erstellen zu können, wenn Ihr Computer nicht mehr bootet. Nachdem Sie mit dem Boot-Medium gebootet haben, können Sie den Bericht generieren, ohne Acronis Cyber Protect Home Office auszuführen. Schließen Sie einfach einen USB-Stick an und klicken Sie auf das Symbol **Acronis System Report**. Der daraufhin erstellte Bericht wird auf dem USB-Stick gespeichert.

***So können Sie das Acronis System Report-Tool auf einem Boot-Medium speichern***

1. Aktivieren Sie das Kontrollkästchen **Acronis System Report** auf der Seite **Inhalt für das Boot-Medium wählen** im **Acronis Media Builder**-Assistenten.
2. Klicken Sie auf **Weiter**, um fortzufahren.

**Erstellung eines Systemberichts von der Eingabeaufforderung aus**

1. Führen Sie den Windows-Befehlsprozessor (cmd.exe) als Administrator aus.
2. Wechseln Sie vom aktuellen Verzeichnis zum Installationsordner von Acronis Cyber Protect Home Office. Geben Sie dazu Folgendes ein:

   ```
   cd C:\Program Files (x86)\Acronis\CyberProtectHomeOffice
   ```

3. Geben Sie zum Erstellen einer Systemberichtsdatei Folgendes ein:

   ```
   SystemReport
   ```

   Die Datei 'SystemReport.zip' wird im aktuellen Ordner erstellt.

   Falls Sie der Berichtsdatei einen benutzerdefinierten Namen zuweisen wollen, dann geben Sie diesen neuen Namen statt des Platzhalters '<file name>' ein:

   ```
   SystemReport.exe /filename:<file name>
   ```

***So können Sie einen Systembericht erstellen, wenn Sie unter einem Boot-Medium arbeiten***

1. Sollten Sie noch kein Acronis Boot-Medium haben, dann erstellen Sie eins. Ausführlichere Informationen finden Sie im Abschnitt 'Acronis Media Builder'.

2. Konfigurieren Sie die Boot-Reihenfolge in Ihrem BIOS so, dass das Gerät/Laufwerk Ihres Boot-Mediums (CD-/DVD-Laufwerk oder USB-Stick) das primäre Boot-Gerät ist. Weitere Informationen finden Sie im Abschnitt 'Boot-Reihenfolge im BIOS arrangieren'.
3. Starten Sie den Computer mit dem Acronis Boot-Medium und wählen Sie **Acronis Cyber Protect Home Office**.

   **Hinweis**
   Anstatt auf **Acronis Cyber Protect Home Office** zu klicken, können Sie auch einen USB-Stick einstecken und dann auf **Acronis System Report** klicken. In diesem Fall erstellt das Programm einen Bericht und speichert diesen automatisch auf dem USB-Stick.

4. Klicken Sie auf den Pfeil neben dem Help-Symbol (  ) und wählen Sie dann **Systembericht erstellen**.
5. Klicken Sie nach Erstellung des Reports auf **Speichern** und geben Sie im dann geöffneten Fenster einen Zielort für die Datei an.
   Das Programm archiviert den Bericht in einer zip-Datei.

# Acronis Smart Error Reporting

Wenn ein Fehler in einer Programmaktion zu einem Problem führt, zeigt Acronis Cyber Protect Home Office eine entsprechende Fehlermeldung an. Die Fehlermeldung enthält einen Ereigniscode und eine kurze Beschreibung des Fehlers.

## Wenn Sie eine Internetverbindung haben

Um einen Acronis Knowledge Base-Artikel einzusehen, der als mögliche Lösung zur Fehlerbehebung angegeben wurde, klicken Sie auf die Schaltfläche **Knowledge Base**.

Darauf öffnet sich ein Bestätigungsfenster, in dem die Informationen aufgelistet sind, die per Internet an die Acronis Knowledge Base geschickt werden. Klicken Sie auf **OK**, um die Übertragung der Informationen zu bestätigen.

Falls Sie solche Informationen zukünftig ohne Bestätigung übermitteln wollen, aktivieren Sie das Kontrollkästchen **Immer ohne Bestätigung versenden**.

## Wenn Sie keine Internetverbindung haben

1. Klicken Sie im Fehlermeldungsfenster auf **Mehr Details** und notieren Sie den Ereigniscode. Der Code kann so aussehen:
   0x000101F6 – Beispiel für einen gewöhnlichen Ereigniscode.
   0x00970007+0x00970016+0x00970002 – Beispiel für einen zusammengesetzten Ereigniscode. Ein Code dieser Art kann auftreten, wenn in einem Programmmodul niedriger Stufe (Low-Level-Modul) ein Fehler aufgetreten ist, dieser sich anschließend auf Module höherer Stufe (High-Level-Module) überträgt und damit in diesen Modulen ebenfalls zu Fehlern führt.

2. Wenn Sie über eine direkte Internetverbindung verfügen oder diese über einen anderen Computer nutzen können, dann geben Sie den Ereigniscode unter folgender Adresse ein: https://kb.acronis.com/errorcode/.

Sollte der Ereigniscode in der Knowledge Base nicht erkannt werden, dann liegt in dieser noch kein Artikel zur Lösung des Problems vor. Öffnen Sie in diesem Fall über den Acronis Support ein Ticket.

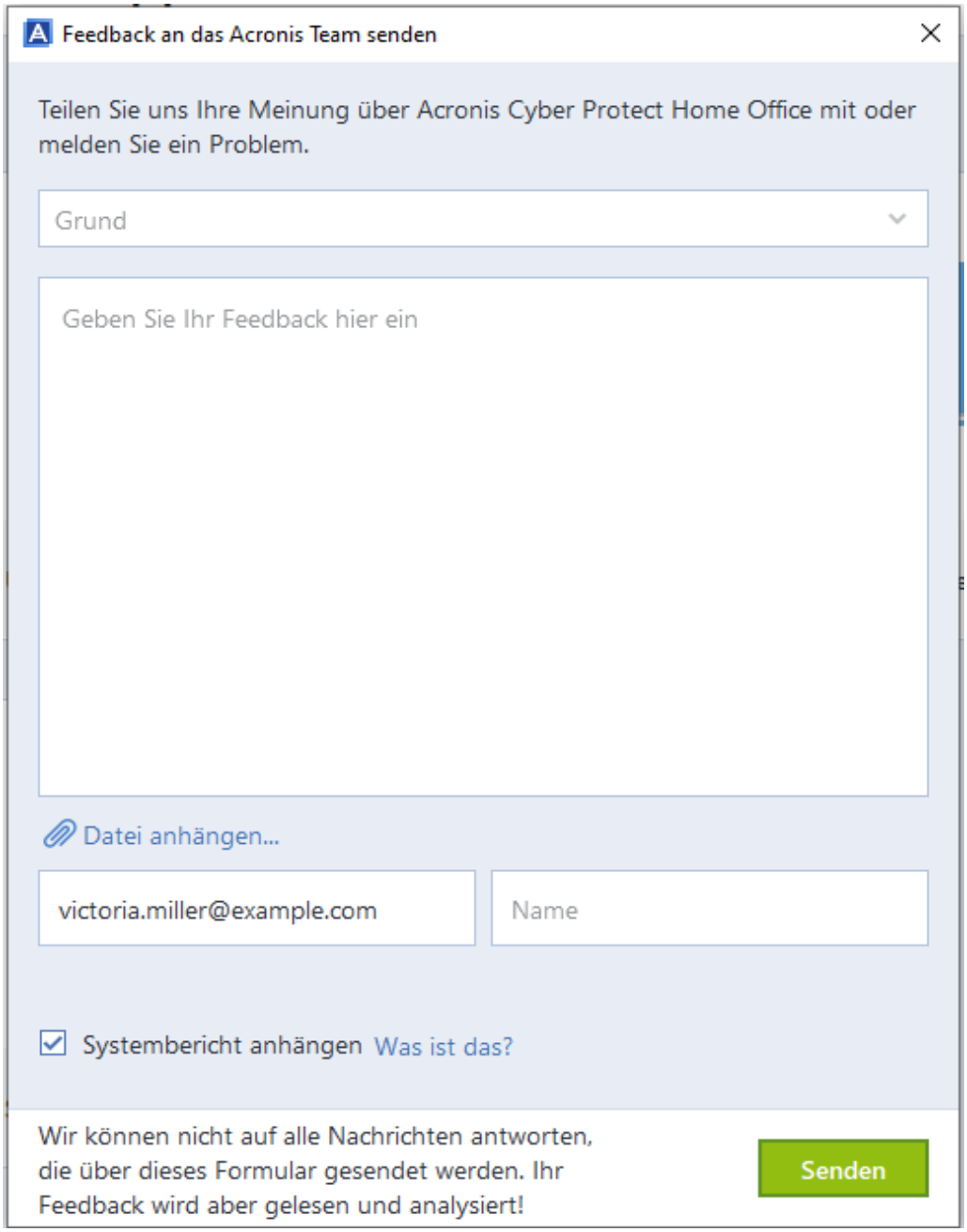
# Feedback an Acronis senden

Wir verbessern unsere Produkte und Dienste regelmäßig, indem wir sie funktioneller, zuverlässiger und schneller machen. Sie können uns über das Rückmeldungsformular Unannehmlichkeiten oder fehlerhafte Funktionen mitteilen, die wir zur Verbesserung von Acronis Cyber Protect Home Office beheben sollen. Bitte geben Sie uns einige Ihrer Minuten, um uns mitzuteilen, was Sie von unserem Produkt halten, um eine neue Funktion vorzuschlagen oder ein Problem zu melden. Alle Rückmeldungen werden von uns gelesen und analysiert.

**Hinweis**
Wir können jedoch nicht auf alle Rückmeldungen antworten. Sollten Sie Unterstützung für Acronis Cyber Protect Home Office benötigen, dann wenden Sie sich an den entsprechenden Support.

***So können Sie ein Feedback an Acronis senden***

1. Klicken Sie in der Seitenleiste auf **Hilfe** und dann auf **Feedback senden**. Daraufhin wird das Rückmeldungsformular geöffnet.




2. Wählen Sie einen Grund für Ihre Rückmeldung aus der Liste aus.
3. Geben Sie Ihre Nachricht ein.
4. Geben Sie Ihren Namen und Ihre E-Mail-Adresse an.
5. [Optionaler Schritt] Sie können eine Datei und einen Acronis Systembericht anhängen. Weitere Informationen finden Sie im Abschnitt 'Acronis System Report'.
   Wir empfehlen Ihnen, einen Systembericht anzuhängen, wenn Sie mit einem ernsthaften Problem konfrontiert wurden (beispielsweise, wenn Acronis Cyber Protect Home Office nicht mehr reagiert).
6. Klicken Sie auf **Senden**.

# So sammeln Sie Speicherabbilder (Crash Dumps)

Da Abstürze von Acronis Cyber Protect Home Office oder Windows unterschiedliche Gründe haben können, muss jeder Absturzfall getrennt untersucht werden. Der Acronis Support würde es begrüßen, wenn Sie folgende Informationen zur Verfügung stellen:

***Sollte Acronis Cyber Protect Home Office abstürzen, dann stellen Sie bitte folgende Informationen bereit:***

1. Eine Beschreibung mit einer genauen Abfolge aller von Ihnen durchgeführten Schritte, bevor das Problem eingetreten ist.
2. Ein Absturzdatei, auch Speicherabbild oder Crash Dump genannt. Informationen darüber, wie Sie solche Speicherabbilder einsammeln können, finden Sie im folgenden Artikel der Acronis Support Knowledge Base (KB) unter der Adresse 'https://kb.acronis.com/content/27931'.

***Falls Acronis Cyber Protect Home Office einen Windows-Absturz verursacht:***

1. Eine Beschreibung mit einer genauen Abfolge aller von Ihnen durchgeführten Schritte, bevor das Problem eingetreten ist.
2. Eine Windows-Speicherabbilddatei (Dump File). Informationen darüber, wie Sie solche Speicherabbilder einsammeln können, finden Sie im folgenden Artikel der Acronis Support Knowledge Base (KB) unter der Adresse 'https://kb.acronis.com/content/17639'.

***Falls sich Acronis Cyber Protect Home Office aufhängt***

1. Eine Beschreibung mit einer genauen Abfolge aller von Ihnen durchgeführten Schritte, bevor das Problem eingetreten ist.
2. Eine benutzerspezifische Speicherabbilddatei (userdump) des Prozesses. Siehe den Artikel der Acronis Support Knowledge Base (KB) unter der Adresse 'https://kb.acronis.com/content/6265'.
3. Das 'Procmon'-Log. Siehe den Artikel der Acronis Support Knowledge Base (KB) unter der Adresse 'https://kb.acronis.com/content/2295'.

Sollten Sie auf die Informationen nicht zugreifen können, dann kontaktieren Sie den Acronis Support, um einen FTP-Link zum Upload der Dateien zu erhalten.

Diese Informationen beschleunigen die Suche nach einer Lösung des Problems.

# Acronis Programm zur Kundenzufriedenheit (CEP)

Das Acronis Programm zur Kundenzufriedenheit (CEP) ermöglicht Acronis Kunden, Einfluss auf die Funktionen, das Design und die Entwicklung von Acronis Produkten zu nehmen. Das Programm ermöglicht Ihnen, uns mit verschiedenen Informationen zu versorgen, z.B. über die Hardware-Konfiguration physischer Computer oder virtueller Maschinen, über die am häufigsten (oder seltensten) verwendeten Funktionen und die Probleme, mit denen Sie sich konfrontiert sehen. Auf Basis dieser Informationen wollen wir die Produkte und Funktionen von Acronis verbessern, die Sie am häufigsten nutzen.

***So können Sie am Acronis Programm zur Kundenzufriedenheit (CEP) teilnehmen oder dieses wieder verlassen***

1. Klicken Sie in der Seitenleiste auf **Einstellungen**.
2. Deaktivieren Sie das Kontrollkästchen für **Am Acronis Programm zur Kundenzufriedenheit (CEP) teilnehmen**, um das Programm wieder zu verlassen.

Wenn Sie sich für eine Teilnahme entscheiden, werden alle 90 Tage entsprechende technische Informationen automatisch eingeholt. Es werden keine persönlichen Daten, wie z.B. Namen, Adressen, Telefonnummern oder Tastatureingaben gesammelt. Die Teilnahme am Programm zur Kundenzufriedenheit (CEP) ist freiwillig. Die Ergebnisse dieses Programms sind ausschließlich dazu gedacht, die Software zu verbessern, dessen Funktionalität zu erweitern und die Erwartungen unserer Kunden zukünftig noch besser erfüllen zu können.

# Glossar

## A

**Acronis Active Protection**

Eine Technologie zum Schutz vor Ransomware – eine bösartige Software, die den Zugriff auf ein komplettes System oder einzelne Dateien blockiert und anschließend für die Aufhebung dieser Sperrung ein Lösegeld verlangt. Die Technologie basiert auf einem heuritischen Ansatz, bei dem ein Computer in Echtzeit überwacht und der Benutzer benachrichtigt wird, wenn ein Prozess versucht, Daten auf dem Computer zu verschlüsseln. Falls dabei dennoch Dateien verschlüsselt werden, können diese direkt aus einem temporären Cache oder aus Backups wiederhergestellt werden.

**Acronis Drive**

Ein virtuelles Laufwerk, welches sowohl lokale wie auch Cloud-Archive enthält. Das Laufwerk ist per Datei-Manager (wie dem Windows Explorer) unter den Favoriten verfügbar und ermöglicht, auf die archivierten Dateien im 'Nur Lesen'-Modus zuzugreifen.

**Acronis Notary**

Eine Technologie, mit der ein Anwender überprüfen kann, ob eine per Notarized Backup gesicherte Datei seit ihrem Backup verändert wurde. Notary berechnet einen zusammenfassenden Hash-Wert (Prüfsumme, digitaler Fingerabdruck) aus den einzelnen Hash-Werten derjenigen Dateien, die für das Notarized Backup ausgewählt wurden, und sendet diesen Hash-Wert dann an eine Blockchain-basierte Datenbank. Die Blockchain-Technologie garantiert dabei, dass die dort gesicherten Hash-Werte nicht mehr verändert werden können. Daher kann die Authentizität der Datei leicht verifiziert werden, indem der Hash-Wert in der Datenbank und der Hash-Wert der zu überprüfenden Datei verglichen werden.

**Acronis Secure Zone**

Ein geschütztes Volume zum Speichern von Backups auf einem Festplattenlaufwerk. Vorteile: ermöglicht es, bei einer Laufwerkswiederherstellung dasselbe Laufwerk als Recovery-Ziel zu verwenden, auf dem das entsprechende Laufwerk-Backup selbst gespeichert ist. bietet eine kosteneffektive und handliche Methode zum Schutz vor Softwarefehlern, Virusangriffen, Bedienerfehlern eliminiert die Notwendigkeit, für Backup oder Wiederherstellung ein separates Medium oder eine Netzwerkverbindung bereitstellen zu müssen Beschränkungen: 1) Die Acronis Secure Zone kann nicht auf dynamischen Laufwerken erstellt werden. 2) Die Acronis Secure Zone steht in einer autonomen Notfallversion – also wenn Sie mit einem Boot-Medium, dem Startup Recovery Manager oder einem BartPE-basierten Boot-Medium starten – nicht als Speicherort für Backups zur Verfügung.

**Acronis Startup Recovery Manager**

Ein Schutztool mit dem Sie eine autonome Notfallversion des Produkts während des Bootens durch Drücken der F11-Taste starten können. Der Startup Recovery Manager macht es unnötig, ein Boot-Medium zu haben. Der Startup Recovery Manager ist besonders für Anwender mobiler Geräte (wie Notebooks) nützlich. Wenn ein schwerwiegender Fehler auftritt, kann der Benutzer die Maschine neu starten und auf die F11-Taste drücken, wenn

die Meldung „Druecken Sie F11 zum Ausfuehren des Startup Recovery Managers...“ erscheint. Anschließend kann er eine Datenwiederherstellung auf dieselbe Art durchführen, wie es Verwendung eines herkömmlichen Boot-Mediums der Fall wäre. Beschränkungen: kann nicht auf dynamischen Laufwerken organisiert werden; erfordert eine manuelle Konfiguration von Boot-Loadern (wie LILO und GRUB); benötigt eine Reaktivierung der Loader von Drittanbietern.

**Archiv**

Eine Datei, die als Ergebnis einer Archivierungsaktion erstellt wurde. Die Datei enthält einen Satz von komprimierten Dateien, die vom Anwender zur Archivierung ausgewählt wurden. Archive können in der Cloud oder auf einem lokalen Storage gespeichert werden. Bei letzterem kann es sich beispielsweise um eine externe Festplatte oder ein NAS-System handeln. Die Dateien in einem Archiv sind über das virtuelle Acronis Drive im 'Nur Lesen'-Modus verfügbar.

**Archivierungsaktion**

Eine Aktion, bei der ausgewählte Dateien komprimiert und dann in die Cloud oder zu einem lokalen Storage (wie eine externe Festplatte oder NAS-System) verschoben werden. Der Hauptzweck dieser Aktion ist es, Speicherplatz auf einem Laufwerk freizugeben, indem alte oder große Dateien zu einem anderen Storage verschoben werden. Mit Abschluss der Aktion werden die archivierten Dateien von ihrem ursprünglichen Speicherort gelöscht und sind anschließend über das Acronis Drive im 'Nur Lesen'-Modus verfügbar.

# B

**Backup**

Wird hier auch gleichbedeutend mit 'Backup-Aktion' verwendet. Eine Zusammenstellung von Backup-Versionen, unter Verwendung bestimmter Backup-Einstellungen erstellt und verwaltet. Ein Backup kann mehrere Backup-Versionen enthalten, erstellt unter Verwendung der Backup-Methoden vollständig und inkrementell. Backup-Versionen, die zum gleichen Backup gehören, werden üblicherweise am gleichen Ort gespeichert.

**Backup-Einstellungen**

Eine Zusammenstellung an Regeln, von einem Anwender bei Erstellung eines neuen Backups konfiguriert. Diese Regeln kontrollieren den Backup-Prozess. Sie können die Backup-Einstellungen auch später bearbeiten, um den Backup-Prozess zu verändern oder zu optimieren.

**Backup-Version**

Das Ergebnis einer einzelnen Backup-Aktion. Physisch handelt es sich um eine Datei oder eine Zusammenstellung von Dateien, die eine Kopie der gesicherten Daten zu einem spezifischen Zeitpunkt enthält. Backup-Versionen von Dateien, die von Acronis Cyber Protect Home Office erstellt werden, erhalten die Dateierweiterung '.tibx'. TIBX-Dateien, die sich aus einer Konsolidierung von Backup-Versionen ergeben, werden ebenfalls als Backup-Versionen bezeichnet.

**Backup (Aktion)**

Eine Aktion, die eine Kopie der Daten erstellt, die auf dem Laufwerk einer Maschine existieren, um diese wiederherzustellen oder in

den Zustand eines festgelegten Tags bzw. Zeitpunkts zurückzusetzen.

**Beglaubigte Datei**

Eine Datei, die mit Acronis Notary beglaubigt wurde. Eine Datei wird beglaubigt, indem sie einem Notarized Backup hinzugefügt und ihr Hash- Wert an eine Blockchain- basierte Datenbank gesendet wird.

**Beglaubigung (Notarization)**

Ein Prozess, um den Zustand einer Datei zu „erinnern“ (erfassen und speichern) und diesen Zustand dann als authentisch zu definieren. Acronis Notary berechnet bei einer digitalen Beglaubigung einen zusammenfassenden Hash- Wert (Prüfsumme, digitaler Fingerabdruck) aus den einzelnen Hash-Werten derjenigen Dateien, die für das Notarized Backup ausgewählt wurden, und sendet diesen Hash- Wert dann an eine Blockchain- basierte Datenbank.

**Boot-Medium**

Ein physisches Medium (CD, DVD, USB-Laufwerk oder ein anderes Medium, das vom BIOS der Maschine als Boot- Medium unterstützt wird), welches die autonome Notfallversion von Acronis Cyber Protect Home Office enthält. Ein Boot- Medium wird am häufigsten verwendet, um ein Betriebssystem wiederherzustellen, das nicht gestartet werden kann; um auf Daten zuzugreifen und zu sichern, die in einem beschädigten System „überlebt“ haben; um ein Betriebssystem auf einem fabrikneuen System bereitzustellen; um Volumes vom Typ 'Basis' oder 'Dynamisch' auf fabrikneuen Laufwerken einzurichten oder um Laufwerke mit nicht unterstütztem Dateisystem per Sektor- für- Sektor- Backup sichern zu können.

# D

**Datensynchronisierung**

Datensynchronisierung ist ein Prozess, der Daten in zwei oder mehreren synchronisierten Ordnern identisch hält. Diese Ordner können sich auf demselben Computer befinden oder auf verschiedenen Rechnern, die über ein lokales Netzwerk oder das Internet miteinander verbunden sind. Wenn Sie in Ihrem Synchronisierungsordner eine Datei oder ein Unterverzeichnis erstellen, kopieren, modifizieren oder löschen, wird dieselbe Aktion automatisch auch in den anderen Synchronisierungsordnern ausgeführt. Und umgekehrt – wenn sich etwas in den anderen Synchronisierungsordnern ändert, wird dieselbe Änderung auch in Ihrem Ordner vorgenommen.

**Differentielle Backup-Version**

Eine differentielle Backup- Version speichert Datenänderungen in Bezug auf die letzte, zugrundeliegende Voll- Backup- Version. Sie müssen auf die entsprechende Voll- Backup-Version zugreifen können, um Daten aus einer differentiellen Backup- Version wiederherstellen zu können.

**Differentielles Backup**

Eine Backup- Methode, die zur Sicherung von Datenänderungen verwendet wird, die innerhalb eines Backups seit der letzten Voll-Backup- Version aufgetreten sind. Ein Backup-Prozess, der eine differentielle Backup-Version erstellt.

# I

**Inkrementelle Backup-Version**

Eine Backup-Version, die Datenänderungen in Bezug zur letzten Backup-Version speichert. Sie müssen auf andere Backup- Versionen des gleichen Backups zugreifen können, um Daten aus einer inkrementellen Backup- Version wiederherstellen zu können.

**Inkrementelles Backup**

Eine Backup- Methode, die zur Sicherung von Datenänderungen verwendet wird, die innerhalb eines Backups seit der letzten Backup- Version (unabhängig vom Typ) aufgetreten sind. Ein Backup-Prozess, der eine inkrementelle Backup-Version erstellt.

# K

**Kette von Backup-Versionen**

Sequenz von mindestens zwei Backup-Versionen, bestehend aus dem ersten Voll-Backup- Version sowie einer oder mehreren nachfolgenden inkrementellen oder differentiellen Backup-Versionen. Eine Backup-Versionskette setzt sich fort, bis die nächste Voll- Backup- Version erstellt wird (sofern überhaupt erstellt).

**Kontinuierliche Sicherung**

Kontinuierliche Sicherung – Prozess, den die Nonstop Backup- Funktion ausführt, wenn sie eingeschaltet ist.

# L

**Laufwerk-Backup (Image)**

Ein Backup, welches eine Sektor-basierte Kopie eines Laufwerks oder Volumes in gepackter Form enthält. Normalerweise werden nur Sektoren kopiert, die Daten enthalten. Das Produkt bietet jedoch eine Option zum Erstellen von Raw-Images (d.h. eine Kopie aller Sektoren), mit der auch nicht unterstützte Dateisysteme per Image gesichert werden können.

# M

**Mobilgeräte-Backup**

Ein Backup, welches die Dateien eines Mobilgerätes (wie ein Smartphone oder Tablet) enthält.

# N

**Nonstop Backup**

Unter einem Nonstop Backup versteht man ein Backup von Laufwerken/Volumes oder Dateien, welches mit der Acronis Nonstop Backup-Funktion erstellt wurde. Es handelt sich um eine Zusammenstellung aus einer vollständigen Backup- Version und einer Sequenz inkrementeller Backup-Versionen, die in kurzen Zeitabständen erstellt werden. Die Funktion ermöglicht einen nahezu kontinuierlichen Schutz Ihrer Daten – oder anders ausgedrückt, dass Sie Ihre Daten auf den Zustand eines jeden von Ihnen gewünschten Zeitpunkts wiederherstellen können.

**Notarized Backup**

Ein Backup, welches Dateien enthält, die mit Acronis Notary beglaubigt wurden.

# O

**Online Backup**

Online Backup – eine Sicherung, die mit Acronis Online Backup erstellt wurde. Online Backups werden in einem speziellen, über das Internet zugänglichen Speicherort aufbewahrt, der verallgemeinernd als Cloud bezeichnet wird. Hauptvorteil des Online Backups ist, dass alle Sicherungen an einem entfernten Ort (remote) gespeichert werden. Das garantiert, dass alle gesicherten Daten unabhängig von den lokalen Speicherorten bzw. Storages des Anwenders geschützt sind.

# R

**Recovery**

Eine Wiederherstellung (Recovery) ist ein Prozess, bei dem beschädigte Daten mithilfe eines Backups zu einem früheren Zustandes wiederhergestellt werden.

# S

**Sync**

Gleichbedeutend mit Datensynchronisierung. Die Synchronisierungseinstellungen wurden auf dem Computer des Sync-Besitzers konfiguriert. Eine bestehende Synchronisierung wird über die entsprechende Sync-Box verwaltet. Das Erstellen einer Synchronisierung bedeutet nicht, dass der Synchronisierungsprozess gestartet wird. Andere Benutzer dürfen einer vorhandenen Synchronisierung beitreten.

# V

**Validierung**

Eine Aktion, die überprüft, ob Sie in der Lage sein werden, die Daten einer bestimmten Backup-Version, wiederherstellen zu können. Bei einer Voll-Backup-Version validiert das Programm nur diese Voll-Backup-Version. Bei einer differenziellen Backup-Version validiert das Programm die ursprüngliche Voll-Backup-Version und die gewählte differenzielle Backup-Version. Bei einer inkrementellen Backup-Version validiert das Programm die anfängliche vollständige Backup-Version, die gewählte inkrementelle Backup-Version und (sofern vorhanden) auch noch die gesamte Kette aller Backup-Versionen bis hin zur gewählten inkrementellen Backup-Version. Enthält die Kette eine oder mehrere differentielle Backup-Versionen, dann überprüft das Programm (zusätzlich zur anfänglichen vollständigen sowie gewählten inkrementellen Backup-Version) nur die jüngste differentielle Backup-Version in der Kette – und (sofern vorhanden) auch noch alle nachfolgenden inkrementellen Backup-Versionen (zwischen der differentiellen und der gewählten inkrementellen Backup-Version).

**Verdächtiger Prozess**

Acronis Active Protection verwendet eine verhaltensbasierte Heuristik und analysiert dazu die laufenden Programme auf Ihrem PC nach bestimmten Verhaltensmustern (Aktionsketten), die mit in einer Datenbank gespeicherten Aktionsketten von bekannten schädlichen Verhaltensmustern verglichen werden. Wenn ein laufendes Programm auf Ihrem System ein typisches Ransomware-Verhalten zeigt und versucht, Benutzerdateien zu modifizieren, wird das Programm als verdächtig eingestuft.

**Version einer synchronisierten Datei**

Das Stadium einer Datei, die sich in einem Synchronisierungsordner befindet, nach jeder an ihr durchgeführten Änderung. Dateiversionen können in der Acronis Cloud gespeichert werden.

**Voll-Backup**

Backup-Methode, welche verwendet wird, um alle für ein Backup ausgewählten Daten zu sichern. Ein Backup-Prozess, der eine vollständige Backup-Version erstellt.

**Voll-Backup-Version**

Eine selbstständige Backup-Version, die alle für ein Backup ausgewählten Daten enthält. Sie müssen auf keine andere Backup-Version zugreifen können, um Daten aus einer Voll-Backup-Version wiederherstellen zu können.

# Index


'

'Laufwerk klonen'-Assistent 193

1

1. Backup des kompletten PC – Zwei Vollversionen 74

2

2. Datei-Backup 'Tägliche inkrementelle Version und wöchentliche Vollversion' 75

3

3. Laufwerk-Backup 'Vollversion jeden 2. Monat und differentielle Version zweimal pro Monat' 76

32- oder 64-Bit-Komponenten 87

A

Abonnementinformationen 37

Acronis ASign 108

Acronis Cloud 19

Acronis Cloud Backup Download 208

Acronis Cyber Protect Home Office aktivieren 18

Acronis Cyber Protect Home Office installieren und deinstallieren 15

Acronis DriveCleanser 242

Acronis Konto 35

Acronis Media Builder 210

Acronis Mobile 63

Acronis Nonstop Backup 48

Acronis Nonstop Backup Storage 50

Acronis Programm zur Kundenzufriedenheit (CEP) 272

Acronis Secure Zone 232

Acronis Smart Error Reporting 269

Acronis Startup Recovery Manager 223

Acronis System Report 267

Acronis Universal Restore 126, 261

Acronis Universal Restore verwenden 265

Active Protection 174

Active Protection konfigurieren 177

Aktionen mit Backups 95

Aktionen nach der Datenvernichtung 248

Alle Daten auf Ihrem PC sichern 25

Allgemein 252

Allgemeine Beschränkungen 19

Andere Anforderungen 12

Anti-Ransomware Protection 174

Antivirus-Scans 179

Antivirus-Scans konfigurieren 180

AnwendungAcronis DriveCleanser 243

Archivierung Ihrer Daten 164

Assistenten 55

Auf jeden Fall zu installierende Massenspeichertreiber 266

Aufbewahrungsregeln 49

Auswahl der Daten 243

Auswahl des Grafikkartenmodus beim Starten des Boot-Mediums 221

Authentifizierungseinstellungen 48

Automatische Suche nach Treibern 265

**B**

Backup-Aktivität und -Statistiken 97

Backup-Aufteilung 84

Backup-Einstellungen importieren und exportieren 260

Backup-Inhalte durchsuchen 153

Backup-Optionen 65

Backup-Reservekopie 86

Backup-Schemata 11, 69

Backup-Schemata verwalten 74

Backup-Schutz 81

Backup-Versionen automatisch bereinigen 109

Backup-Versionen manuell bereinigen 110

Backup Ihres Computers 22

Backup von Dateien und Ordnern 60

Backups 'on-the-fly' aufteilen 102

Backups an verschiedene Plätze 101

Backups Ihrer Dateien 29

Backups im TIBX-Format bereinigen 11

Backups in der Liste sortieren 99

Backups in die Acronis Cloud replizieren 100

Backups validieren 101

Backups von Laufwerken und Volumes 58

Backups, Backup-Versionen und Replikate bereinigen 108

Backups, die in Acronis True Image (2020 oder 2021) oder Acronis Cyber Protect Home Office erstellt wurden 10

Befehle einstellen 255

Befehle vor bzw. nach dem Backup 83

Beispiel für eine Wiederherstellung auf UEFI-Systemen 143

Beispiele für benutzerdefinierte Schemata 74

Benachrichtigungen 230

Benachrichtigungen für Backup-Aktionen 77

Benachrichtigungen für Recovery-Aktionen 159

Benennung von Backup-Dateien 52

Benutzerbefehl für Backups bearbeiten 84

Benutzerbefehl für Wiederherstellung bearbeiten 157

Benutzerdefinierte Algorithmen erstellen 246

Benutzerdefinierte Schemata 72

Bereinigung der Acronis Secure Zone 232

Bereinigungsoptionen 252

Beschränkungen für Nonstop Backup 49

Beschränkungen und zusätzliche Informationen 259

Besondere Bereinigungsoptionen 252

Bevor Sie beginnen 31

Blockchain-Technologie verwenden 104

Boot-Reihenfolge im BIOS oder UEFI-BIOS arrangieren 144

**C**

Changed Block Tracker (CBT) 44

Cloud-Archivierung vs. Online Backup 163

Computer 255

Computer-Neustart 157

Computer herunterfahren 90

**D**

Das Menü 'Backup-Aktionen' 95

Das Partitionierungsschema nach der Wiederherstellung 142

Das Problem 'Zu viele Aktivierungen' 18

Das Protection Dashboard 173

Das Werkzeug 'Laufwerk klonen' 192

Datacenter 165

Datei-Recovery 231

Dateien 253

Dateien und Ordner wiederherstellen 151

Dateisicherheitseinstellungen für Backups 89

Dateisystem 241

Daten archivieren 162

Daten aus der Acronis Cloud entfernen 111

Daten aus der Ferne sichern (Remote-Backup) 169

Daten freigeben 167

Daten synchronisieren 187

Daten über das Online Dashboard wiederherstellen 170

Daten werden per Backup gesichert 58

Daten wiederherstellen 114

Datenarchivierungsoptionen 165

Datentypen 188

Datenvernichtungsmethode 252

Definition der Methode 246

Der Infobereich 188

Der Schutz von replizierten Daten 101

Der Speicherort für die Acronis Secure Zone 233

Der Universal Restore-Prozess 266

Die Acronis Secure Zone entfernen 237

Die Authentizität einer Datei manuell überprüfen 107

Die Authentizität von Dateien überprüfen 106

Die Daten der ganzen Familie sichern 168

Die Größe der Acronis Secure Zone 234

Die manuelle Bereinigung von lokalen Backups erfolgt nach folgendem Schema 11

Die Namenskonvention für Backup-Dateien, die mit Acronis True Image (2020 oder 2021) oder Acronis Cyber Protect Home Office erstellt wurden 52

Die Namenskonvention für Backup-Dateien, die mit einer Acronis True Image-Version vor 2020 erstellt wurden 53

Die Parameter für monatliche Backups 68

Die Parameter für tägliche Backups 68

Die Parameter für wöchentliche Backups 68

Die Performance von Backup-Aktionen 91

Die Performance von Recovery-Aktionen 159

Die Registerkarte 'Aktivität' 98

Die Registerkarte 'Backup' 99

Die Versionen eines Backup-Replikats in die Cloud löschen 112

Die Versionen eines Backups in die Cloud löschen 112

Die Vollversion kaufen 19

Die Vorgehensweise von Try&Decide nach einem Computer-Neustart 226

Die Wahl der Migrationsmethode 204

Differentielle Methode 43

**E**

E-Mail-Benachrichtigung 77, 160

E-Mail-Benachrichtigungen 171

Echtzeitschutz 175

Ein Acronis Backup konvertieren 259

Ein Acronis Boot-Medium erstellen 24, 211

Ein Acronis Survival Kit erstellen 27

Ein Acronis Universal Boot-Medium erstellen 262

Ein Backup-Image mounten 257

Ein Datacenter für Backups auswählen 93

Ein gemountetes Image trennen 258

Ein komplettes Backup-Replikat löschen 109

Ein komplettes Backup löschen 111

Ein komplettes Backup und dessen Replikat löschen 108

Ein Laufwerk auswählen 237

Ein Laufwerk klonen 31-32

Ein neues Laufwerk hinzufügen 237

Ein neues Laufwerk zur Nutzung für Backups vorbereiten 46

Ein System auf demselben Laufwerk wiederherstellen 116

Ein System mit einem Boot-Medium auf einem neuen Laufwerk wiederherstellen 119

Ein vorhandenes Backup der Liste hinzufügen 102

Eine .iso-Datei von einer .wim-Datei erstellen 216

Eine Acronis Secure Zone erstellen und verwalten 233

Eine Datei signieren 108

Eine Replikation aktivieren 100

Eine Synchronisierung erstellen 189

Eine Synchronisierung löschen 191

Einen Algorithmus als Datei speichern 248

Einführung 10

Einmalige Bereinigung 113

Einschränkungen bei Verwendung von Try&Decide 227

Einstellungen für die Bereinigung 251

Einstellungen für Wechselmedien 86

Elemente vom Backup ausschließen 79

Elemente vom Klonen ausschließen 196

Energieeinstellungen für Notebooks und Tablets 93

Erkannte Probleme verwalten 182

Erste Schritte 22

Erste Schritte mit der Acronis Cloud 36

Erweiterte Einstellungen 67

Extras 208

**F**

FAQ über Backup, Recovery und Klonen 56

Feedback an Acronis senden 270

Fehlerbehandlung 88

Fehlerbehandlung für Cloud Backups und Replikate 89

Filter für Netzwerkressourcen 256

Fortgang der Bereinigung 257

Freier Platz auf Laufwerk 254

FTP-Verbindung 47

**G**

Geschützte Volumes 229

Grenzwert für freien Speicherplatz 77, 160

Größe 240

Grundlegende Konzepte 38

**I**

Ihr System aus der Acronis Cloud wiederherstellen 147

Ihr System nach einem Absturz wiederherstellen 114

Ihr System schützen 22

Ihre Abonnementlizenzen manuell verwalten 18

Ihren Computer wiederherstellen 33

Im Online Dashboard ein neues Gerät hinzufügen 168

In Quarantäne befindliche Dateien verwalten 183

Informationen zur Testversion 19

Inkrementelle Methode 42

Integration in Windows 53

Integrierte Kaufmöglichkeit 21

**K**

Komprimierungsgrad 91

**L**

Laufwerk-Recovery aus der Cloud 146

Laufwerk klonen und Migration 192

Laufwerke und Volumes wiederherstellen 114

Laufwerksbuchstabe 241

Limitierungen bei Aktionen mit dynamischen Datenträgern 15

Lokaler Zielort für Backups von Mobilgeräten 64

Lösungen für die häufigsten Probleme 267

**M**

Manuelle Partitionierung 194

Methoden zur Datenvernichtung auf Laufwerken 245

Microsoft 365-Daten per Backup sichern 64-65

Microsoft 365-Daten wiederherstellen 154-155

Migration auf eine SSD mit der 'Backup und Recovery'-Methode 206

Migration Ihres Systems von einer Festplatte auf SSD 204

Migrationsmethode 135, 198

Minimale Systemanforderungen 12

Mit .vhd(x)-Dateien arbeiten 259

Mobilgeräte per Backup sichern 62

Modus zur Image-Erstellung 81

**N**

Nach Abschluss der Wiederherstellung 126

Neue Volumes erstellen 239

Nonstop Backup – Häufig gestellte Fragen (FAQs) 51

Notarized Backup 103

**O**

Online Backups schützen 83

Optionen für Backup-Validierung 85

Optionen für das Überschreiben von Dateien 158

Optionen für Datei-Recovery 158

Optionen für Validierung 157

**P**

Parameter zur Ausführung bei einem Ereignis 69

Partitionslayouts 130

Per BIOS gebootetes System, GPT, 'Nicht-Windows' 138, 200

Per BIOS gebootetes System, GPT, UEFI unterstützt 137, 200

Per BIOS gebootetes System, MBR, 'Nicht-Windows' 137, 199

Per BIOS gebootetes System, MBR, UEFI nicht unterstützt 136, 198

Per BIOS gebootetes System, MBR, UEFI unterstützt 136, 199

Per UEFI gebootetes System, GPT, 'Nicht-Windows' 141, 203

Per UEFI gebootetes System, GPT, UEFI wird unterstützt 140, 203

Per UEFI gebootetes System, MBR, 'Nicht-Windows' 139, 202

Per UEFI gebootetes System, MBR, UEFI nicht unterstützt 138, 201

Per UEFI gebootetes System, MBR, UEFI wird unterstützt 139, 201

Planung 66

Priorität für die Aktion 91, 159

Problembehebung (Troubleshooting) 48, 267

**R**

Recovery-Modus 'Laufwerk' 156

Recovery-Optionen 156

Recovery von dynamischen Volumes 141

Recovery von Laufwerken und Volumes vom Typ 'Dynamisch' oder 'GPT' 141

Remote-Storage 36

Replikat-Versionen automatisch bereinigen 109

**S**

Schema 'Eine Version' 71

Schema 'Versionskette' 71

Schutz 173

Schutz-Ausschlüsse konfigurieren 184

Schutz-Updates herunterladen 185

Schutz der Privatsphäre im Internet 231

Schutz für Acronis Secure Zone 236

Schutz für Videokonferenz-Applikationen 185

Schwachstellenbewertung 181

Snapshot für Backup 92

So entscheiden Sie, wo Sie Ihre Backups speichern 45

So erhalten Sie Zugriff auf ein kennwortgeschütztes Backup 82

So gewährleisten wir die Sicherheit Ihrer Daten 37

So können Sie .vhd(x)-Dateien verwenden 259

So können Sie ein Image mounten 257

So sammeln Sie Speicherabbilder (Crash Dumps) 272

So stellen Sie eine gelöschte Datei wieder her 191

So stellen Sie sicher, dass Ihr Boot-Medium bei Bedarf auch funktioniert 217

So verwenden Sie die Standardeinstellungen für die Ausschlusskriterien 79

So verwendet Acronis Cyber Protect Home Office die Blockchain-Technologie 105

Software-Evaluierung 230

Speicherplatz in der Acronis Cloud bereinigen 111

Sprache für die Benutzeroberfläche 22

SSD-Größe 204

Standardoptionen für die Bereinigung 251

Startparameter für das Acronis Boot-Medium 213

Storage-Typen 187

Storage für virtuelle Änderungen 230

Synchronisierung 19

Synchronisierungssymbole 188

Systemanforderungen und unterstützte Medien 12

Systembereinigung 249

Szenarien, bei denen Try&Decide helfen kann 225

**T**

Tabelle 1

Ziellaufwerk ist größer als 2 TB 131

Tabelle 2

Ziellaufwerk ist kleiner als 2 TB 134

Technischer Support 21

Treiber vorbereiten 265

Treiber zu einem vorhandenen .wim-Image hinzufügen 215

Try&Decide 225

Typische Einsatzfälle 230

Try&Decide-Optionen und -Benachrichtigungen 229

Try&Decide verwenden 228

**U**

Über die Synchronisierungsfunktion (Sync) 187

Überprüfen Sie, dass auf die Treiber in der bootfähigen Umgebung zugegriffen werden kann. 265

Übertragungsrate der Netzwerkverbindung 92

Und so funktioniert es 49, 146

Unified Extensible Firmware Interface (UEFI) 129

Universal Restore-Einstellungen 265

Unterschied zwischen dateibasierten Backups und Images von Laufwerken/Volumes 40

Unterstützte Betriebssysteme 12

Unterstützte Dateisysteme 13

Unterstützte Speichermedien 15

Unterstützte Typen von Internetverbindungen 14

Upgrade von Acronis Cyber Protect Home Office 20

Urheberrechtserklärung 9

**V**

Verschlüsselung 166

Versionen von synchronisierten Dateien 190

Versuche zur Bestimmung der Absturzursache 114

Vollständige Methode 41

Vollständige, inkrementelle und differentielle Backups 41

Volume-Bezeichnung 241

Volume-Eigenschaften 128

Volume-Einstellungen 240

Volume-Typ (diese Einstellungen sind nur für MBR-Laufwerke verfügbar) 242

Volumes und Laufwerke vom Typ 'Basis' wiederherstellen 142

Volumes und Laufwerke wiederherstellen 127

Von Acronis patentierte Technologien 9

Vor-/Nach-Befehle für Wiederherstellung 156

Vorbereitung 265

Vorgehensweise, falls die oberen Vorschläge nicht helfen 206

Vorschau 256

**W**

Wahl der Initialisierungsmethode 238

Wahl der Methode 244

Warum benötige ich das? 31, 242

Warum sollten Sie ein Backup replizieren? 100

Warum sollten Sie Microsoft 365-Daten per Backup sichern? 64

Warum UEFI? 129

Was bedeutet 'Data Protection für die ganze Familie'? 168

Was ist Acronis ASign? 108

Was ist Acronis Cyber Protect Home Office? 10

Was ist eine Blockchain? 105

Was ist UEFI? 129

Was passiert, wenn die Wiederherstellung unterbrochen wurde? 147

Was Sie ausschließen können und was nicht 80

Was Sie synchronisieren können und was nicht 187

Was Sie tun können, wenn Acronis Cyber Protect Home Office Ihre SSD nicht erkennt 204

Was tut die Datenarchivierungsfunktion? 162

Was wird von Archiven ausgeschlossen? 163

Webapplikation 36

Webfilter 176

Welche Elemente können wiederhergestellt werden? 154

Welches Backup behält das TIB-Format? 11

Welches Problem wird dabei gelöst? 262

Wenn Sie eine Internetverbindung haben 269

Wenn Sie keine Internetverbindung haben 269

Werkzeuge für Sicherheit und zum Schutz Ihrer Privatsphäre 242

Wie können Sie ein ursprüngliches System auf ein größeres Festplattenlaufwerk migrieren? 130

Wie können Sie UEFI im BIOS aktivieren? 129

Wie wird es verwendet? 262

Wiederherstellen einer vorherigen Dateiversion 190

Wiederherstellung vorbereiten 114

Windows Explorer 189

WLAN-Verbindungen für Backups in die Acronis Cloud 94

Wo finde ich diese Apps? 64

**Z**

Zugriff auf Ihre archivierten Dateien 166

Zusätzliche Informationen 224