# Acronis® Internet Security 2011

## Benutzerhandbuch

# Acronis Internet Security 2011
*Benutzerhandbuch*

Veröffentlicht 2011.01.24



## Rechtlicher Hinweis

# Inhaltsverzeichnis

Erste Schritte ..... 1

1. Übersicht ..... 2
1.1. Öffnen Sie Acronis Internet Security ..... 2
1.2. System Tray Icon ..... 2
1.3. Scanaktivitsänzeige ..... 3
1.3.1. Prüfe Dateien und Ordner ..... 3
1.3.2. Deaktiviern/Wiederherstellen der Aktivitätsanzeige ..... 4
1.4. Automatische Geräteerkennung ..... 4

2. Acronis Internet Security 2011 einrichten ..... 6

3. Hauptanwendungs-Fenster ..... 8
3.1. Basis-Ansicht ..... 8
3.1.1. Statusbereich ..... 9
3.1.2. Der Bereich "Ihren PC schützen" ..... 9
3.1.3. Hilfebereich ..... 10
3.2. Standard-Ansicht ..... 10
3.2.1. Dashboard ..... 11
3.2.2. Sicherheit ..... 12
3.2.3. Dateispeicherung ..... 13
3.2.4. Netzwerk ..... 14
3.3. Experten-Ansicht ..... 14

4. Meine Werkzeuge ..... 17

5. Warnhinweise und Pop-Ups ..... 20
5.1. Antivirus-Warnhinweise ..... 20
5.2. Active Virus Control-Warnungen ..... 21
5.3. Geräte-Entdeckungsbenachrichtigung ..... 21
5.4. Firewall Pop-Ups und Warnhinweise ..... 22
5.5. Antiphishing-Warnhinweise ..... 23
5.6. Warnhinweise Kindersicherung ..... 24
5.7. Warnhinweise Privatsphäre-Einstellungen ..... 24
5.7.1. Registry-Alarme. ..... 24
5.7.2. Skript-Alarme ..... 25
5.7.3. Cookie-Alarme ..... 25

6. Alle beheben ..... 26
6.1. Fehlersuche-Assistent ..... 26
6.2. Status-Warnmeldungen konfigurieren ..... 27

7. Konfiguration der Grundeinstellungen ..... 29
7.1. Sicherheitseinstellungen ..... 29
7.2. Alarmeinstellungen ..... 31
7.3. Allgemeine Einstellungen ..... 32

8. Verlauf und Ereignisse ..... 34

Konfiguration und Verwaltung ..... 35
9. Allgemeine Einstellungen ..... 36
10. Antivirus-Schutz ..... 40
10.1. Echtzeitschutz ..... 40
10.1.1. Anpassen der Sicherheitsstufe des Echtzeitschutzes ..... 41
10.1.2. Erstellen einer benutzerdefinierten Schutzeinstellung ..... 41
10.1.3. Ändern der Aktion, die bei verdächtigen Dateien durchgeführt wird .... 43
10.1.4. Wiederherstellen der Voreinstellungen ..... 44
10.1.5. Konfigurieren des Active Virus Control ..... 45
10.1.6. Konfiguration des Intrusion Detection Systems ..... 47
10.2. Prüfvorgang ..... 47
10.2.1. Dateien und Ordner prüfen ..... 48
10.2.2. Antivirus Prüfassistent ..... 49
10.2.3. Prüfberichte anzeigen ..... 52
10.2.4. Verwaltung der existierenden Scan-Aufgaben ..... 53
10.3. Konfiguration der Scan-Ausschlüsse ..... 59
10.3.1. Dateien oder Verzeichnisse vom Scan ausschließen ..... 60
10.3.2. Dateierweiterungen vom Scan ausschließen ..... 61
10.3.3. Verwaltung von Scan-Ausschlüssen ..... 62
10.4. Quarantäne ..... 63
11. Antiphishing-Schutz ..... 65
11.1. Konfiguration der Antiphishing White List ..... 65
11.2. Handhabung des Acronis Internet Security Antiphishing-Schutzes in Internet Explorer und Firefox ..... 66
12. Search Advisor ..... 68
12.1. Deaktivierung des Search Advisors ..... 68
13. Antispam ..... 69
13.1. Antispam Einblicke ..... 69
13.1.1. Antispam Filter ..... 69
13.1.2. Antispam Vorgang ..... 71
13.1.3. Antispam Updates ..... 72
13.1.4. Unterstützte E-Mail-Clients und Protokolle ..... 72
13.2. Antispam Optimierungs-Assistent ..... 73
13.3. Verwendung der Antispam-Symbolleiste im Fenster "Ihr Mail Client" ..... 74
13.3.1. Anzeige von Feststellungsfehler ..... 76
13.3.2. Anzeige unentdeckter Spam-Nachrichten ..... 76
13.3.3. Erneutes Trainieren des Bayes Filters ..... 76
13.3.4. Speichern und Laden der Bayes Datenbank ..... 77
13.3.5. Konfiguration der allgemeinen Einstellungen ..... 77
13.4. Anpassen der Sicherheitsstufe ..... 78
13.5. Freundesliste konfigurieren ..... 78
13.6. Konfigurieren der Spammerliste ..... 80
13.7. Konfiguration der Antispam-Filter und -Einstellungen. ..... 81
14. Kindersicherung ..... 83
14.1. Kindersicherung konfigurieren ..... 83

14.1.1. Tresor der Kindersicherungs-Einstellungen ... 85
14.1.2. Web Kontrolle ... 86
14.1.3. Programmkontrolle (Anwendungskontrolle) ... 87
14.1.4. Schlüsselwortkontrolle ... 89
14.1.5. Instant Messaging (IM) Kontrolle ... 90
14.2. Kinderaktivität überwachen ... 91
14.2.1. Überprüfen der Kindersicherungsprotokolle ... 92
14.2.2. E-Mail-Benachrichtigungen konfigurieren ... 93

15. Privatsphärekontrolle ... 95
15.1. Sicherheitsstufe einstellen ... 95
15.2. Antispyware/Identitätskontrolle ... 96
15.2.1. Über die Identitätskontrolle ... 96
15.2.2. Konfiguration der Identitätskontrolle ... 98
15.2.3. Regeln bearbeiten ... 100
15.3. Registry-Überprüfung ... 100
15.4. Cookie-Kontrolle ... 101
15.5. Skript-Kontrolle ... 103

16. Firewall ... 105
16.1. Tresoreinstellungen ... 105
16.1.1. Standardaktion einstellen ... 105
16.1.2. Weitere Einstellungen der Firewall konfigurieren ... 106
16.2. Zugriffsregel für Anwendungen ... 107
16.2.1. Aktuelle Regeln ansehen ... 107
16.2.2. Regeln automatisch hinzufügen ... 109
16.2.3. Regeln manuell hinzufügen ... 110
16.2.4. Erweiterte Regelverwaltung ... 113
16.2.5. Löschen und Zurücksetzen von Regeln ... 114
16.3. Netzwerk-Einstellungen ... 114
16.3.1. Netzwerk-Zonen ... 115
16.4. Geräte ... 116
16.5. Aktivitätsanzeige ... 116
16.6. Fehlersuche Firewall ... 117

17. Schwachstellen ... 119
17.1. Auf Schwachstellen scannen ... 119
17.2. Status ... 120
17.3. Einstellungen ... 121

18. Instant-Messaging-Verschlüsselung ... 122
18.1. Verschlüsselung für bestimmte Benutzer deaktivieren ... 123
18.2. Acronis Internet Security-Symbolleiste im Chat-Fenster ... 123

19. Dateiverschlüsselung ... 124
19.1. Verwaltung der Datentresore über die Acronis Internet Security-Benutzeroberfläche ... 124
19.1.1. Datentresor erstellen ... 124
19.1.2. Datentresor öffnen ... 125
19.1.3. Datentresor abschließen ... 126
19.1.4. Passwort für Datentresor ändern ... 127

19.1.5. Dateien dem Datentresor hinzufügen ... 128
19.1.6. Dateien entfernen ... 129
19.1.7. Tresor-Inhalte ansehen ... 130
19.1.8. Datentresor löschen ... 131
19.2. Verwaltung von Datentresors in Windows ... 131
19.2.1. Datentresor erstellen ... 132
19.2.2. Datentresor öffnen ... 133
19.2.3. Datentresor abschließen ... 133
19.2.4. Dem Datentresor hinzufügen ... 134
19.2.5. Aus dem Datentresor entfernen ... 134
19.2.6. Passwort für Datentresor ändern ... 135

20. Spiele-/Laptop-Modus ... 136
20.1. Spiele-Modus ... 136
20.1.1. Konfiguration des Automatischen Spiele-Modus ... 137
20.1.2. Spieleliste verwalten ... 137
20.1.3. Spiele hinzufügen oder bearbeiten ... 138
20.1.4. Konfiguration der Einstellungen des Spiele-Modus ... 138
20.1.5. Änderung der Tastenkombination des Spiele-Modus ... 139
20.2. Laptop-Modus ... 139
20.2.1. Einstellungen des Laptop-Modus konfigurieren ... 140
20.3. Stumm-Modus ... 140
20.3.1. Konfiguration Vollbildschirmaktion ... 141
20.3.2. Konfiguration der Einstellungen des Stumm-Modus ... 141

21. Heimnetzwerk ... 142
21.1. Aktivierung des Acronis Internet Security-Netzwerks ... 142
21.2. Computer dem Acronis Internet Security-Netzwerk hinzufügen ... 143
21.3. Verwaltung des Acronis Internet Security-Netzwerks ... 144

22. Aktualisierung ... 146
22.1. Durchführung eines Updates ... 146
22.2. Konfiguration der Update-Einstellungen ... 147
22.2.1. Update-Adresse ... 148
22.2.2. Automatisches Update konfigurieren ... 148
22.2.3. Manuelle Update Einstellungen ... 148
22.2.4. Weitere Einstellungen konfigurieren ... 149

Wie man ... 150

23. Wie kann ich Dateien und Verzeichnisse scannen? ... 151
23.1. Unter Verwendung des Windows Kontext Menus ... 151
23.2. Unter Verwendung von Prüfaufgaben ... 151
23.3. Aktivitätsanzeige ... 152

24. Wie erstelle ich eine benutzerdefinierte Scan-Aufgabe? ... 154

25. Wie plane ich einen Scan? ... 156

26. Wie benutze ich einen Datentresor? ... 158

27. Wie erstelle ich ein Windows Benutzerkonto? ... 160

28. Wie kann ich Acronis Internet Security über einen Proxy-Server aktualisieren? ..... 162

Fehlediagnose und Problemlösung ..... 163

29. Problemlösung ..... 164
29.1. Der Scan startet nicht ..... 164
29.2. Ich kann eine Anwendung nicht länger benutzen ..... 164
29.3. Ich kann keine Verbindung zum Internet herstellen. ..... 165
29.4. Ich kann den Drucker nicht benutzen ..... 166
29.5. Ich kann keine Dateien mit anderen Computern teilen ..... 168
29.6. Meine Internetverbindung ist langsam ..... 169
29.7. Wie Sie ein Acronis Internet Security-Update mit einer langsamen Internetverbindung durchführen. ..... 170
29.8. Acronis Internet Security-Dienste antworten nicht. ..... 170
29.9. Antispamfilter funkioniert nicht richtig ..... 171
29.9.1. Seriöse Nachrichten werden markiert als [spam] ..... 171
29.9.2. Viele Spam Nachrichten werden nicht entdeckt. ..... 174
29.9.3. Antispam-Filter entdeckt keine Spamnachrichten. ..... 177

30. Malware von Ihrem System entfernen ..... 179
30.1. Was ist zu tun, wenn Acronis Internet Security auf Ihrem Computer einen Virus findet? ..... 179
30.2. Wenn Ihr System nicht startet ..... 180
30.3. Wie entferne ich einen Virus aus einem Archiv? ..... 181
30.4. Wie entferne ich einen Virus aus einem Email-Archiv? ..... 182
30.5. Was ist zu tun, wenn Acronis Internet Security eine saubere Datei als infiziert klassifiziert? ..... 183
30.6. Wie säubern Sie infizierte Dateien in den System Volume Information ..... 184
30.7. Welches sind die passwortgeschützten Dateien im Scan-Protokoll? ..... 185
30.8. Was sind die übersprungenen Einträge im Scan-Protokoll? ..... 186
30.9. Was sind die überkomprimierten Dateien im Scan-Protokoll? ..... 186
30.10. Warum hat Acronis Internet Security eine infizierte Datei automatisch gelöscht? ..... 186

31. Support ..... 187

32. Nützliche Information ..... 188
32.1. Wie entferne ich andere Sicherheitsprogramme? ..... 188
32.2. Wie führe ich einen Neustart im abgesicherten Modus durch? ..... 189
32.3. Ist auf meinem System die 32- oder 64-bit-Version von Windows installiert? ..... 189
32.4. Wo finde ich "Meine Proxy-Einstellungen"? ..... 190
32.5. Wie aktiviere/deaktiviere ich den Echtzeitschutz? ..... 190
32.6. Wie kann ich verborgene Objekte in Windows anzeigen lassen? ..... 191

Glossar ..... 193

# Erste Schritte

# 1. Übersicht

Sobald Sie Acronis Internet Security 2011 installiert haben, ist Ihr Computer gegen jede Art von Malware (wie beispielsweise Viren, Spyware und Trojaner) und andere Internetbedrohungen (wie Hacker, Phishing und Spam) geschützt.

Sie können jedoch auch die Acronis Internet Security-Einstellungen für die Feineinstellung nutzen und Ihren Schutz verbessern.Darüber hinaus gibt es auch einige nützliche Extrafunktionen.Erstellen Sie zunächst ein Benutzerprofil wie unter *„Acronis Internet Security 2011 einrichten“ (S. 6)* beschrieben.

Von Zeit zu Zeit sollten Sie Acronis Internet Security öffnen und existierende Probleme beheben.Es ist möglich, dass-Sie, um Ihren Computer und Ihre Daten zu schützen, bestimmte Acronis Internet Security-Komponenten konfigurieren oder vorbeugende Maßnahmen durchführen müssen.Wenn Sie möchten, können Sie Acronis Internet Security so konfigurieren, dass Sie bei bestimmten Problemen nicht alarmiert werden.Für weitere Informationen lesen Sie bitte *„Alle beheben“ (S. 26)*.

## 1.1. Öffnen Sie Acronis Internet Security

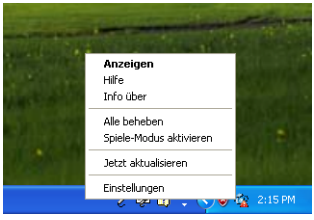
Zugriff auf die Hauptbenutzeroberfläche von Acronis Internet Security 2011 erhalten Sie über das Windows-Startmenü: **Start → Alle Programme → Acronis Backup and Security 2011 → Acronis Internet Security 2011 → Acronis Internet Security 2011** oder schneller per Doppelklick auf das Acronis Internet Security Symbol in der Systemleiste.

Weitere Informationen zum Haupt-Anwendungsfenster finden Sie unter *„Hauptanwendungs-Fenster“ (S. 8)*.

## 1.2. System Tray Icon

Um das gesamte Produkt schneller zu verwalten, können Sie das Acronis Internet Security-Symbol im System-Tray nutzen.Wenn Sie auf dieses Symbol doppelklicken öffnet sich Acronis Internet Security. Zudem öffnen Sie durch einen Rechtsklick ein Untermenü das Ihnen ein schnelles Verwalten des Acronis Internet Security-Produktes ermöglicht.

- **Anzeigen** - öffnet die Hauptbedienoberfläche von Acronis Internet Security.
- **Hilfe** - öffnet die Hilfedatei, die erklärt, wie man Acronis Internet Security 2011 konfiguriert und benutzt.
- **Über** - öffnet ein Fenster, in dem Sie Informationen über Acronis Internet Security erhalten und Hilfe finden, falls etwas Unvorhergesehenes geschieht.




Tray Icon

- **Alle Risiken beheben** - hilft bestehende Sicherheitsschwachstellen zu entfernen.Falls die Option nicht verfügbar ist, so gibt es keine zu behebenden Probleme.Für weitere Informationen lesen Sie bitte *„Alle beheben“ (S. 26)*.
- **Spiele-Modus An / Aus** - aktiviert / deaktiviert den Spiele-Modus.
- **Jetzt Aktualisieren** - startet ein sofortiges Update.Ein neues Fenster wird erscheinen, in dem Sie Status des Updates sehen können.
- **Einstellungen** - öffnet ein Fenster, in dem Sie die Haupteinstellungen des Produkts aktivieren und deaktivieren oder das Benutzerprofil neu konfigurieren können.Für weitere Informationen lesen Sie bitte *„Konfiguration der Grundeinstellungen“ (S. 29)*.

Das Acronis Internet Security-Symbol in der System Tray informiert Sie über spezielle Symbole, über mögliche Probleme:

**Rotes Dreieck mit einem Ausrufezeichen:** Kritische Probleme betreffen die Sicherheit Ihres Systems. Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.

**Buchstabe G:**Das Produkt arbeitet im Spiele-Modus.

Wenn Acronis Internet Security nicht funktioniert, ist das Symbol grau hinterlegt.Dies passiert normalerweise, wenn die Lizenz abgelaufen ist, aber auch, wenn die Acronis Internet Security Dienste nicht reagieren oder andere Fehler die normale Funktionsweise von Acronis Internet Security einschränken.

## 1.3. Scanaktivitsänzeige

Die **Scan Aktions-Anzeige** ist eine graphische Visualisierung der Prüfaktivität auf Ihrem System.Dieses kleine Fenster steht in der Voreinstellung nur in der Experten-Ansicht zur Verfügung.

Die grauen Balken (die **Datei-Zone**) zeigen die Anzahl der gescannten Dateien pro Sekunde, auf einer Skala von 0 bis 50.Die orangen Balken in der **Netz-Zone** zeigen die Anzahl der transferierten KBytes (gesendet und empfangen aus dem Internet) pro Sekunde auf einer Skala von 0 bis 100.

**Beachten Sie**
Die Aktivitätsanzeige informiert Sie mit einem roten „X“, wenn der Echtzeitschutz oder die Firewall deaktiviert ist (**Datei** oder **Netz**).

### 1.3.1. Prüfe Dateien und Ordner

Sie können die Aktivitätsanzeige verwenden um kurzerhand Dateien und Ordner zu prüfen. Ziehen Sie die gewünschte Datei auf den **Datei-/Netzprüfmonitor**, wie auf den folgenden Bildern dargestellt.


Herüberziehen der Datei


Ablegen der Datei

Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

**Scanoptionen.** Die Prüfoptionen sind für bestmögliche Enteckungsraten vorkonfiguriert.Falls infizierte Dateien entdeckt werden, wird Acronis Internet Security versuchen diese zu desinfizieren (den Malware-Code entfernen). Sollte die Desinfizierung fehlschlagen, wird Ihnen der Antivirus Scan-Assistent andere Möglichkeiten vorschlagen, wie mit den infizierten Dateien verfahren werden kann.Die Prüfoptionen sind standartisiert, sie können daher nicht geändert werden.

## 1.3.2. Deaktiviern/Wiederherstellen der Aktivitätsanzeige

Wenn Sie die graphische Visualisierung nicht länger sehen wollen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Ausblenden**.Um die Aktivitätsanzeige wiederherzustellen folgen Sie diesen Schritten:

1. Öffnen Sie Acronis Internet Security.
2. Klicken Sie in der oberen rechten Bildschirmecke auf **Optionen** und wählen Sie **Einstellungen**
3. Aktivieren Sie in der Kategorie "Allgemeine Einstellungen" das entsprechende Kästchen für die **Scan-Aktivitätsanzeige**.
4. Klicken Sie **OK**, um die Änderungen zu speichern und zu übernehmen.

# 1.4. Automatische Geräteerkennung

Wenn ein externes Speichergerät mit dem PC verbunden wird, erkennt Acronis Internet Security dies automatisch, und bietet an, es vor dem Zugriff zu zu überprüfen.Dies ist empfohlen um die Infizierung Ihres Systems durch Viren und andere Malware zu verhindern.

Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs

- USB-Speichergeräte, sowie Flashstifte und externe Festplatten
- verbundene (entfernte) Netzlaufwerke

Wenn solch ein Gerät entdeckt wird, erscheint ein Hinweis.

Um das Speichergerät zu prüfen, klicken Sie **Ja**.Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

Falls Sie das Gerät nicht prüfen möchten, klicken Sie **Nein**. In diesem Fall, könnte eine der folgenden Optionen helfen:

- **Bei diesem Gerätetyp nicht mehr nachfragen** - Acronis Internet Security wird für diesen Gerätetyp keine Prüfung vorschlagen, wenn dieser mir dem PC verbunden wird.
- **Automatische Geräteerkennung deaktivieren** - Sie werden nicht länger aufgefordert neue Speichergeräte zu prüfen, wenn diese mit dem PC verbunden werden.

Falls Sie die automatische Geräteerkennung versehentlich deaktivieren und sie reaktivieren, oder die Einstellungen anpassen möchten, folgen Sie diesen Schritten:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus>Virusprüfung**.
3. Suchen Sie in der Liste der Scan-Aufgaben die Aufgabe **Geräte-Scan**.
4. Rechtsklicken Sie auf die Aufgabe und wählen Sie **Eigenschaften**.Ein neues Fenster wird sich öffnen.
5. Im **Übersichts** Tab, konfigurieren Sie die Prüfoptionen nach Bedarf.Für weitere Informationen lesen Sie bitte *„Konfigurieren der Prüfoptionen“* (S. 56).
6. Im **Erkennungs** Tab, wählen Sie welche Art von Speichergerät erkannt werden soll.
7. Klicken Sie **OK**, um die Änderungen zu speichern und zu übernehmen.

# 2. Acronis Internet Security 2011 einrichten

Sie können die zentralen Einstellungen und die Benutzeroberfläche von Acronis Internet Security 2011 ganz leicht konfigurieren, indem Sie ein Benutzerprofil anlegen.Das Nutzungsprofil reflektiert die hauptsächlich durchgeführten Aktivitäten auf dem Computer. Abhängig von Nutzungsprofil, wird die Benutzeroberfläche sortiert, damit Sie bequem auf Ihre bevorzugten Aufgaben zugreifen können.

Nach erfolgter Installation wird ein Standard-Benutzerprofil angewendet.

Folgen Sie diesen Schritten, um das Benutzerprofil zu rekonfigurieren:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Präferenzen**.
2. Klicken Sie auf den Link **Neukonfiguration Benutzerprofil**.
3. Folgen Sie dem Konfigurationsassistenten.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

   a. **Wählen Sie Ihre Ansicht.**

      Wählen Sie Ihre bevorzugte Ansicht.

   b. **Konfiguration von Meine Werkzeuge**

      Falls Sie die Basis- oder Standard-Ansicht gewählt haben, wählen Sie die Funktionen, für die Sie Verknüpfungen erstellen möchten, auf dem Dashboard.

   c. **Einstellungen konfigurieren**

      Wenn Sie die Experten-Ansicht gewählt haben, konfigurieren Sie die Acronis Internet Security-Einstellungen nach Bedarf.Um eine Einstellung zu aktivieren bzw. zu deaktivieren, nutzen Sie den entsprechenden Button.

   d. **Aktivierung der Kindersicherung**

      Beachten Sie

      Dieser Schritt wird nur eingeblendet, wenn Sie die Kindersicherung dem Bereich "Meine Werkzeuge" hinzugefügt haben.

      Sie können aus drei Optionen auswählen:

      - **Kindersicherung für Kinder-Benutzerkonten einrichten**

        Aktivieren Sie diese Option, um die Kindersicherung für die Benutzerkonten Ihrer Kinder zu aktivieren und diese von Ihrem Administrations-Benutzerkonto aus zu verwalten.

      - **Kindersicherung für das aktuelle Benutzerkonto einrichten**

Wählen Sie diese Option, um die Kindersicherungsfunktion für das aktuelle Benutzerkonto zu aktivieren. Dies bedeutet, dass Sie nicht für jedes Kind ein separates Benutzerkonto anlegen müssen, sondern dass die Kindersicherungsregeln für jeden angewendet werden, der dieses Benutzerkonto verwendet.

In diesem Fall ist ein Passwort notwendig, um die Kindersicherungseinstellungen zu schützen.Sie können dieses jetzt oder zu einem späteren Zeitpunkt im Acronis Internet Security-Fenster festlegen.

- **Den Setup vorerst überspringen**

  Aktivieren Sie diese Option, um diese Funktion zu einem späteren Zeitpunkt von einem Acronis Internet Security-Fenster aus zu konfigurieren.

e. **Heimnetzwerk-Verwaltung**

Beachten Sie

Dieser Schritt wird nur eingeblendet, wenn Sie die Heimnetzwerk-Verwaltung dem Bereich "Meine Werkzeuge" hinzugefügt haben.

Sie können aus drei Optionen auswählen:

- **Diesen PC als "Server" festlegen**

  Aktivieren Sie diese Option, wenn Sie Acronis Internet Security-Produkte auf anderen Computern des Heimnetzwerks von diesem Rechner aus verwalten möchten.

  Für die Teilnahme am Netzwerk ist ein Passwort nötig.Geben Sie in der entsprechenden Textbox Ihr Passwort ein und klicken Sie auf **Übertragen**.

- **Diesen PC als "Client" festlegen**

  Wählen Sie diese Option, wenn Acronis Internet Security von einem anderen Computer im Heimnetzwerk, auf dem Acronis Internet Security ebenfalls installiert ist, verwaltet werden soll.

  Für die Teilnahme am Netzwerk ist ein Passwort nötig.Geben Sie in der entsprechenden Textbox Ihr Passwort ein und klicken Sie auf **Übertragen**.

- **Den Setup vorerst überspringen**

  Aktivieren Sie diese Option, um diese Funktion zu einem späteren Zeitpunkt von einem Acronis Internet Security-Fenster aus zu konfigurieren.

f. **Setup abgeschlossen**

Klicken Sie auf **Fertigstellen**.

# 3. Hauptanwendungs-Fenster

Acronis Internet Security 2011 ist sowohl für Profis als auch für Computer-Neulinge geeignet. Die grafische Benutzeroberfläche ist so konzipiert, dass Sie für jeden Benutzer anpassbar ist.

Sie können die Benutzeroberfläche in einem von 3 Modi darstellen lassen, abhängig von Ihrer Computer Erfahrung und Ihrer Erfahrung mit Acronis Internet Security.

Basis-Ansicht

Geeignet für Anfänger und für diejenigen, die Acronis Internet Security ohne Aufwand zum Schutz des Computers und der Daten nutzen wollen. Diese Ansicht ist einfach in der Handhabung und verlangt minimalen Aufwand Ihrerseits.

Sie müssen nur dann Probleme beheben, wenn Acronis Internet Security Sie dazu auffordert. Ein intuitiver Schritt-für-Schritt Assistent hilft Ihnen dabei.Zusätzlich können Sie normale Aufgaben, Vorgänge wie das Aktualisieren der Acronis Internet Security-Virensignaturen und Produktdateien oder den Scan Ihres Computers durchführen.

Standard-Ansicht

Diese Ansicht ist für Benutzer mit durchschnittlichen Computer-Kenntnissen gedacht und erweitert Basis-Ansicht.

Sie können offene Punkte separat beheben und wählen welche Punkte überwacht werden.Ferner können Sie die auf anderen Computern in Ihrem Haushaltinstallierten Acronis Internet Security-Produkte verwalten.

Experten-Ansicht

Gedacht für technisch fortgeschrittene Anwender, erlaubt diese Ansicht jede Funktion von Acronis Internet Security zu konfigurieren.Sie können auch alle Funktionen benutzen, um Ihren Computer und Ihre Daten zu schützen.

Änderung des Ansichtsmodus:

1. Öffnen Sie Acronis Internet Security.
2. Klicken Sie in der oberen rechten Bildschirmecke auf den Button **Optionen**.
3. Wählen Sie die gewünschte Ansicht im Menü aus.

## 3.1. Basis-Ansicht

Wenn Sie ein Computer-Anfänger sind, ist die Basis-Ansicht der Benutzeroberfläche vermutlich die beste Wahl für Sie.Dieser Modus ist einfach zu handhaben und erfordert nur minimale Interaktion Ihrereseits.

Das Fenster ist aufgeteilt in drei Hauptbereiche:

Statusbereich

Die Statusinformation wird auf der linken Bildschirmseite angezeigt.

Der Bereich "Ihren PC schützen"
: Hier können Sie die für die Verwaltung Ihres Schutzes notwendigen Aktionen durchführen.

Hilfebereich
: Hier können Sie herausfinden, wie Sie Acronis Internet Security 2011 benutzen und wie Sie Hilfe bekommen können.

Über den Button **Optionen** in der rechten oberen Bildschirmecke können Sie die Ansicht ändern und die Hauptprogramm-Einstellungen konfigurieren.

In der rechten unteren Ecke des Fensters findes Sie einige nützliche Links.

| Link | Beschreibung |
|---|---|
| Protokolle anzeigen | Zeigt Ihnen eine detaillierte Historie aller von Acronis Internet Security auf Ihrem System durchgeführten Aufgaben. |
| **Hilfe und Support** | Klicken Sie auf diesen Link, wenn Sie Hilfe zu Acronis Internet Security benötigen. |
| | Gibt Ihnen Zugriff auf eine Hilfedatei, die Sie bei der Verwendung von Acronis Internet Security unterstützt. |

## 3.1.1. Statusbereich

Die Statusinformation wird auf der linken Bildschirmseite angezeigt.

- **Sicherheitsstatus** informiert Sie über die Risiken die die Sicherheit Ihres Systems gefährden, und hilft diese zu beheben.Durch Klicken auf **Alles Risisken beheben** erscheint ein Assistent der Ihnen helfen wird Bedrohungen für PC und Daten zu entfernen.Für weitere Informationen lesen Sie bitte *„Alle beheben“ (S. 26)*.
- **Lizenzstatus** zeigt an, wie viele Tage noch verbleiben, bis die Lizenz ausläuft.Wenn Sie eine Testversion verwenden oder Ihre Lizenz bald ausläuft, können Sie auf **Jetzt kaufen** klicken, um so einen Lizenzschlüssel zu erwerben.

## 3.1.2. Der Bereich "Ihren PC schützen"

Hier können Sie die für die Verwaltung Ihres Schutzes notwendigen Aktionen durchführen.

Drei Schaltflächen sind verfügbar:

- **Sicherheit** bietet Ihnen Verknüpfungen zu Sicherheitsaufgaben und Einstellungen.
- **Jetzt aktualisieren** hilft Ihnen, die Virensignaturen und Produktdateien von Acronis Internet Security upzudaten.Ein neues Fenster wird erscheinen, in dem Sie Status des Updates sehen können.Wenn neue Updates erkannt werden, werden sie automatisch auf Ihren PC heruntergeladen und installiert.

- In **Meine Werkzeuge** können Sie Verknüpfungen für Ihre favorisierten Aufgaben und Einstellungen definieren.

Um eine Aufgabe auszuführen oder Einstellungen zu konfigurieren, klicken Sie im Menü auf den entsprechenden Button für das gewünschte Werkzeug.Um Verknüpfungen hinzuzufügen oder zu entfernen, klicken Sie auf den entsprechenden Button und wählen Sie **Weitere Optionen**.Für weitere Informationen lesen Sie bitte *„Meine Werkzeuge“* (S. 17).

### 3.1.3. Hilfebereich

Hier können Sie herausfinden, wie Sie Acronis Internet Security 2011 benutzen und wie Sie Hilfe bekommen können.

**Smart Tipps** sind ein einfacher und unterhaltsamer Weg, mehr über Computer-Sicherheitstechniken und wie Acronis Internet Security 2011 diese anwendet, herauszufinden.

Falls Sie Hilfe benötigen, tippen Sie im Feld **Hilfe und Support** ein Schlagwort oder eine Frage ein und klicken Sie auf **Suchen**.

## 3.2. Standard-Ansicht

Die Standard-Ansicht ist für Benutzer mit durchschnittlich guten PC-Kenntnissen ausgelegt, die Oberfläche gibt Ihnen Zugriff auf alle grundlegenden Module. Sie müssen Warnungen und kritische Alarme nachverfolgen und unerwünschte Probleme beheben.

Die Standard-Ansicht ist in mehrere Bereiche unterteilt.

Dashboard
: Das Dashboard hilft Ihnen, Ihren Schutz einfach zu überwachen und zu verwalten.

Sicherheit
: Zeigt den Status der Sicherheitseinstellungen an und hilft Ihnen, festgestellte Probleme zu beheben.Sie können Sicherheitsaufgaben ausführen oder Sicherheitseinstellungen konfigurieren.

Dateispeicherung
: Zeigt den Status der Dateiverschlüsselung und erlaubt die Verwaltung von Datentresoren.

Netzwerk
: Zeigt die Struktur des Acronis Internet Security Heimnetzwerks an.Hier können Sie verschiedene Aktionen durchführen, um die in Ihrem Heimnetzwerk installierten Acronis Internet Security Produkte, zu konfigurieren und zu verwalten.Auf diesem Wege können Sie die Sicherheit Ihres Heimnetzwerks von einem einzelnen Computer aus verwalten.

Über den Button **Optionen** in der rechten oberen Bildschirmecke können Sie die Ansicht ändern und die Hauptprogramm-Einstellungen konfigurieren.

In der rechten unteren Ecke des Fensters findes Sie einige nützliche Links.

| Link | Beschreibung |
|---|---|
| Protokolle anzeigen | Zeigt Ihnen eine detaillierte Historie aller von Acronis Internet Security auf Ihrem System durchgeführten Aufgaben. |
| **Kaufen/Verlängern** | Unterstützt Sie beim Kauf des Lizenzschlüssels für Ihr Acronis Internet Security 2011-Produkt. |
| **Hilfe und Support** | Klicken Sie auf diesen Link, wenn Sie Hilfe zu Acronis Internet Security benötigen. |
| ? | Gibt Ihnen Zugriff auf eine Hilfedatei, die Sie bei der Verwendung von Acronis Internet Security unterstützt. |

### 3.2.1. Dashboard

Das Dashboard hilft Ihnen, Ihren Schutz einfach zu überwachen und zu verwalten.

Das Dashboard besteht aus folgenden Bereichen:

- **Statusdetails** - zeigt den Status jedes Hauptmoduls, unter Verwendung eindeutiger Sätze und eines der folgenden Symbole:

  **Grüner Kreis mit einem Häkchen:** Keine Risiken beeinflussen den Sicherheitsstatus.Ihr Rechner und Ihre Daten sind geschützt.

  **Roter Kreis mit einem Ausrufezeichen:** Risiken beeinflussen die Sicherheit Ihres Systems.Kritische Risiken erfordern Ihre unmittelbare Aufmerksamkeit. Nicht-kritische Risiken sollte auch alsbald Beachtung zukommen.

  **Grauer Kreis mit X:** Die Aktivität dieser Modulkomponenten wird nicht überwacht. Daher liegen keine Informationen zum Sicherheitsstatus vor.Es könnten möglicherweise, spezifische Probleme mit diesen Modul existieren.

  Klicken Sie auf den Namen eines Moduls um Einzelheiten zum Status zu erhalten und die Statusüberwachung für diese Komponente zu konfigurieren.

- **Lizenzstatus** zeigt an, wie viele Tage noch verbleiben, bis die Lizenz ausläuft.Wenn Sie eine Testversion verwenden oder Ihre Lizenz bald ausläuft, können Sie auf **Jetzt kaufen** klicken, um so einen Lizenzschlüssel zu erwerben.

- In **Meine Werkzeuge** können Sie Verknüpfungen für Ihre favorisierten Aufgaben und Einstellungen definieren.Für weitere Informationen lesen Sie bitte *„Meine Werkzeuge“ (S. 17)*.

- **Smart Tipps** sind ein einfacher und unterhaltsamer Weg, mehr über Computer-Sicherheitstechniken und wie Acronis Internet Security 2011 diese anwendet, herauszufinden.

## 3.2.2. Sicherheit

Über den Reiter "Sicherheit" können Sie die Sicherheit Ihres Computers und Ihrer Daten verwalten.

„Statusbereich“ (S. 12)
„Schnellmaßnahmen“ (S. 12)

### Statusbereich

Im Status Bereich können Sie die vollständige Liste der überwachten Sicherheitskomponenten und deren aktuellen Status sehen.Durch die Überwachung jedes Sicherheitsmoduls wird Acronis Internet Security Sie nicht nur darüber informieren, wenn Sie Einstellungen vornehmen, die die Sicherheit Ihres Computers beeinträchtigenkönnen. Sondern auch, wenn wichtige Aufgaben vergessen wurden.

Der aktuelle Status einer Komponente wird angezeigt unter Verwendung eindeutiger Sätze und eines der folgenden Symbole:

**Grüner Kreis mit einem Häkchen:** Keine Risiken gefährden Ihren Computer.
**Roter Kreis mit einem Ausrufezeichen:** Risiken gefährden Ihren Computer.

Klicken Sie auf **Beheben** um das jeweilige Problem zu beheben.Sollte ein Problem nicht direkt behoben werden, dann folgen Sie den Assistent.

Um zu konfigurieren, welche Komponenten überwacht werden sollen:

1. Klicken Sie auf **Liste hinzufügen/bearbeiten**.
2. Um die Überwachung für einen bestimmten Eintrag ein- oder auszuschalten, verwenden Sie diesen Schalter.
3. Klicken Sie auf **Schließen**, um die Änderungen zu speichern und das Fenster zu schließen.

**Wichtig**
Um zu gewährleisten, dass Ihr System komplett gesichert ist, aktivieren Sie bitte das Tracking für alle Komponenten und alle gemeldeten Probleme reparieren

### Schnellmaßnahmen

Hier finden Sie Links zu den wichtigsten Sicherheitsaufgaben:

- **Jetzt Aktualisieren** - startet ein sofortiges Update.
- **Vollständiger Scan** - ermöglicht Ihnen einen System Scan zu starten und automatische Scans einzurichten.

- **Benutzerdefinierte Prüfung** - startet einen Assistenten, mit dem Sie eine individuelle Prüfung erstellen und starten können.
- **Schwachstellenprüfung** - startet einen Assistenten der Ihnen beim Finden und Beheben von Schwachstellen in Ihrem System behilflich ist.
- **Kindersicherung** - öffnet das Konfigurationsfenster für die Kindersicherung.Für weitere Informationen lesen Sie bitte *„Kindersicherung“* (S. 83).
- **Firewall konfigurieren** - öffnet ein Fenster, in dem Sie die Firewall-Einstellungen einsehen und konfigurieren können.Für weitere Informationen lesen Sie bitte *„Firewall“* (S. 105).

## 3.2.3. Dateispeicherung

Im Reiter Dateispeicherung können Sie Ihre vertraulichen Daten in verschlüsselten Datentresoren speichern, um sie vor dem Zugriff Anderer zu schützen.

„Statusbereich“ (S. 13)
„Schnellmaßnahmen“ (S. 13)

### Statusbereich

Der aktuelle Status einer Komponente wird angezeigt unter Verwendung eindeutiger Sätze und eines der folgenden Symbole:

**Grüner Kreis mit einem Häkchen:** Keine Risiken gefährden Ihren Computer.
**Roter Kreis mit einem Ausrufezeichen:** Risiken gefährden Ihren Computer.

Klicken Sie auf **Beheben** um das jeweilige Problem zu beheben.

Um zu konfigurieren, welche Komponenten überwacht werden sollen:

1. Klicken Sie auf **Liste hinzufügen/bearbeiten**.
2. Um die Überwachung für einen bestimmten Eintrag ein- oder auszuschalten, verwenden Sie diesen Schalter.
3. Klicken Sie auf **Schließen**, um die Änderungen zu speichern und das Fenster zu schließen.

### Schnellmaßnahmen

Folgende Aktionen stehen zur Verfügung:

- **Datei einem Datentresor hinzufügen** - startet den Assistenten zum Speichern Ihrer Dateien/Dokumente in einem Datentresor (verschlüsseltes Schutzlaufwerken).
- **Dateien aus Datentresor entfernen** - startet den Assistenten zum Löschen von Daten aus einem Datentresor.
- **Datentresor ansehen** - startet den Assistenten, mit dem Sie den Inhalt eines Datentresors einsehen können.

- **Datentresor schließen** - startet den Assistenten, mit dem Sie einen offenen Datentresor schließen können, um dessen Inhalt zu schützen.

Detaillierte Informationen, wie Sie Ihre Dateien mithilfe von Vaults schützen können, finden Sie unter *„Dateiverschlüsselung“ (S. 124)*.

### 3.2.4. Netzwerk

Hier können Sie verschiedene Aktionen durchführen, um die in Ihrem Heimnetzwerk installierten Acronis Internet Security Produkte, zu konfigurieren und zu verwalten.Auf diesem Wege können Sie die Sicherheit Ihres Heimnetzwerks von einem einzelnen Computer aus verwalten.

Für weitere Informationen lesen Sie bitte *„Heimnetzwerk“ (S. 142)*.

## 3.3. Experten-Ansicht

Die Experten-Ansicht gibt Ihnen Zugriff auf jede einzelne Komponente von Acronis Internet Security. Hier können Sie Acronis Internet Security im Einzelnen konfigurieren.

**Beachten Sie**

Die Experten-Ansicht ist für Anwender geeignet, die über sehr gute PC-Kenntnisse verfügen, die umfassende Kenntnisse über existierende PC-Bedrohungen haben und wissen, wie ein Sicherheitsprogramm arbeitet.

Auf der linken Seite des Fensters sehen Sie ein Menu, das alle Sicherheitsmodule beinhaltet:Jedes Modul verfügt über ein oder mehrere Tabs in welchem Sie die dazugehörigen Sicherheitseinstellungen konfigurieren oder Sicherheits- und administrative Aufgaben durchführen können. Die folgende Auflistung beschreibt in Kürze jedes Modul.Für weitere Informationen lesen Sie bitte „Konfiguration und Verwaltung“ (S. 35) diesen Teil des Benutzerhandbuchs.

Allgemein
: Hier haben Sie Zugriff zu den allgemeinen Einstellungen. Sie können hier auch das Dashboard und detaillierte Systeminformationen betrachten.

Antivirus
: Bietet Ihnen die Möglichkeit Ihr Virus-Schild und Prüfprozesse zu konfigurieren, Ausnahmen festzulegen und das Quarantäne-Modul zu konfigurieren.Hier können Sie auch die Funktionen Antiphishing-Schutz und Search Advisor konfigurieren.

Antispam
: Bietet Ihnen die Möglichkeit Ihr Postfach SPAM-frei zu halten und die Antispam-Einstellungen detailliert zu konfigurieren.

Kindersicherung
: Bietet Ihnen die Möglichkeit Ihre Kinder gegen jugendgefährdende Inhalte zu schützen. Nutzen Sie dabei Ihre selbst festgelegten Regeln.

Privatsphärekontrolle
: Bietet Ihnen die Möglichkeit Datendiebstahl von Ihrem Computer vorzubeugen und Ihre Privatsphäre zu schützen während Sie online sind.

Firewall
: Erlaubt es Ihnen Ihren Computer für unerlaubte Zugriffe von Aussen und Innen zu schützen. Ziemlich ähnlich dem Sicherheitsbeamten an einer Tür - wird es ein wachsames Auge auf Ihre Internetverbindung haben und beobachten wem der Zugriff zum Internet zu erlauben und wer zu blockieren ist.

Schwachstellen
: Bietet Ihnen die Möglichkeit wichtige Software auf Ihrem PC stets auf dem neusten Stand zu halten.

**Verschlüsseln**
: Bietet Ihnen die Möglichkeit, Unterhaltungen über Yahoo und Windows Live (MSN) Messenger zu verschlüsseln und Ihre wichtigen Dateien, Verzeichnisse und Partitionen lokal zu verschlüsseln.

Spiele/Laptop-Modus
: Bietet Ihnen die Möglichkeit, voreingestellte Scan Acronis Internet Security Aufgaben zu verschieben, wenn Ihr Laptop im Akkubetrieb ist. Zudem werden während des Spielbetriebs keine Pop-Up-Fenster und andere Benachrichtigungen eingeblendet.

Heimnetzwerk
: Bietet Ihnen die Möglichkeit mehrere Computer in Ihrem Haushalt zu verwalten und konfigurieren.

Aktualisierung
: Bietet Ihnen die Möglichkeit die neusten Updates zu erhalten, das Produkt zu aktualisieren und den Update-Prozess genau zu konfigurieren.

**Registrierung**
: So können Sie Ihr Produkt mit einem neuen Lizenzschlüssel registrieren.

Über den Button **Optionen** in der rechten oberen Bildschirmecke können Sie die Ansicht ändern und die Hauptprogramm-Einstellungen konfigurieren.

In der rechten unteren Ecke des Fensters findes Sie einige nützliche Links.

| Link | Beschreibung |
|---|---|
| Protokolle anzeigen | Zeigt Ihnen eine detaillierte Historie aller von Acronis Internet Security auf Ihrem System durchgeführten Aufgaben. |
| **Kaufen/Verlängern** | Unterstützt Sie beim Kauf des Lizenzschlüssels für Ihr Acronis Internet Security 2011-Produkt. |
| **Hilfe und Support** | Klicken Sie auf diesen Link, wenn Sie Hilfe zu Acronis Internet Security benötigen. |

| Link | Beschreibung |
| --- | --- |
|  | Gibt Ihnen Zugriff auf eine Hilfedatei, die Sie bei der Verwendung von Acronis Internet Security unterstützt. |

# 4. Meine Werkzeuge

Wenn Sie Acronis Internet Security in der Basis- oder Standard-Ansicht verwenden, können Sie Ihr Dashboard anpassen, indem Sie wichtigen Aufgaben und Einstellungen Verknüpfungen zuweisen.Auf diese Weise erhalten Sie schnell Zugriff auf die Funktionen, die Sie regelmäßig nutzen und auf die Erweiterten Einstellungen, ohne dabei in eine andere Ansicht wechseln zu müssen.

Abhängig von der gewählten Ansicht stehen die dem Bereich "Meine Werkzeuge" hinzugefügten Verknüpfungen wie folgt zur Verfügung:

Basis-Ansicht
: Klicken Sie im Bereich "Ihren PC schützen" auf **Meine Werkzeuge**.Ein neues Menü wird eingeblendet.Klicken Sie auf die Verknüpfung des entsprechenden Werkzeugs, um dieses aufzurufen.

Standard-Ansicht
: Die Verknüpfungen werden unter "Meine Werkzeuge" angezeigt.Klicken Sie auf die Verknüpfung des entsprechenden Werkzeugs, um dieses aufzurufen.

Um das Fenster zu öffnen, in dem Sie die Verknüpfungen auswählen können, die im Bereich "Meine Werkzeuge" angezeigt werden, gehen Sie folgendermaßen vor:

Basis-Ansicht
: Klicken Sie im Bereich "Ihren PC schützen" auf "Meine Werkzeuge" und dann auf **Weitere Optionen**.

Standard-Ansicht
: Klicken Sie im Bereich "Meine Werkzeuge" auf eine Schaltfläche oder auf den **Konfigurieren** Link.

Über die Schalter können Sie wählen, welche Werkzeuge dem Bereich "Meine Werkzeuge" hinzugefügt werden sollen.Sie können jede der folgenden Werkzeugkategorien auswählen.

- **Prüfaufgaben**

  Fügen Sie die Aufgaben, die Sie regelmäßig anwenden, um Ihr System auf Sicherheitsbedrohungen zu scannen, hinzu.

| Prüfaufgabe | Beschreibung |
|---|---|
| **Vollsystem-Scan** | Prüft alle Dateien mit Ausnahme von Archiven.In der standard Konfiguration, wird nach allen Arten von Malware geprüft, ausser rootkits. |
| **Meine Dokumente** | Verwenden Sie diese um die folgenden für den jeweiligen Benutzer wichtigen Ordner zu prüfen: `Eigene Dateien`, `Desktop` und `Autostart`. Dies stellt sicher das Ihre Eigenen Dateien, Ihr Desktop |

| Prüfaufgabe | Beschreibung |
|---|---|
| | und die beim Starten von Windows geladenen Programme schädlingsfrei sind. |
| **Angepasster Scan** | Startet einen Assistenten, mit dem Sie eine benutzerdefinierte Aufgabe erstellen können. |
| **Tiefe Systemprüfung** | Prüft das komplette SystemIn der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter. |
| **Quick Scan** | Beim Quick Scan wird das sog In-the-cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren.Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde. |
| **"Meine Aufgaben" planen** | Leitet Sie in das Fenster mit den Antiviren-Einstellungen weiter, in dem Sie die On-Demand Scan-Aufgaben anpassen können. |

Weitere Informationen über Scan-Aufgaben finden Sie unter *„Verwaltung der existierenden Scan-Aufgaben“* (S. 53).

- **Einstellungen**

  Weisen Sie den Acronis Internet Security-Einstellungen, die Sie konfigurieren möchten, Tastaturkürzel zu.

| Einstellungen | Beschreibung |
|---|---|
| **Jetzt aktualisieren** | Auslösen eines Updates von Acronis Internet Security. Weitere Informationen finden Sie unter *„Aktualisierung“* (S. 146). |
| **Kindersicherung** | Konfigurieren Sie die Kindersicherung. Weitere Informationen finden Sie unter *„Kindersicherung“* (S. 83). |
| **Firewall konfigurieren** | Konfigurieren Sie die Firewall-Modul. Weitere Informationen finden Sie unter *„Firewall“* (S. 105). |
| **Spiele-Modus** | Ein-/Ausschalten des Spiele-Modus. Weitere Informationen finden Sie unter *„Spiele-Modus“* (S. 136). |

| Einstellungen | Beschreibung |
|---|---|
| **Laptop-Modus** | Ein-/Ausschalten des Laptop-Modus. Weitere Informationen finden Sie unter *„Laptop-Modus“* (S. 139). |
| **Antivirus konfigurieren** | Konfigurieren Sie das Antiviren-Modul. Weitere Informationen finden Sie unter *„Antivirus-Schutz“* (S. 40). |
| **Anzeigen & Alle Probleme beheben** | Öffnen einen Assistenten, der Ihnen hilft, alle Sicherheitsprobleme, die Ihr System beeinträchtigen, zu beheben. Weitere Informationen finden Sie unter *„Alle beheben“* (S. 26). |

- **Hilfe & Support**

  Bietet Ihnen die Möglichkeit das Acronis Support Team zu kontaktieren.

# 5. Warnhinweise und Pop-Ups

Acronis Internet Security verwendet Pop-Ups-Fenster und Warnungen, um Sie über Aktionen oder besondere Vorkommnisse zu informieren und fordert Sie zu notwendigen Aktionen auf.In diesem Kapitel werden die Acronis Internet Security-Pop-Ups und Warnungen, die eingeblendet werden können, erläutert.

Pop-ups sind kleine Fenster, die hin und wieder auf dem Bildschirm erscheinen, um Sie über verschiedene Acronis Internet Security-Ereignisse zu informieren, so wie die Überprüfung von Emails, einen neuer Computer der sich in Ihr kabelloses Netzwerk einloggt, eine neue Firewall-Regel, usw.Wenn Pop-ups eingeblendet werden, werden Sie meistens aufgefordert, auf **OK** oder einen Link zu klicken.

Warnungen sind große Fenster, die Sie zu einer Handlung auffordern oder Sie über etwas Wichtiges (beispielsweise, dass ein Virus gefunden wurde) informieren.Neben Warnhinweisfenstern erhalten Sie unter Umständen Warnhinweise zu Emails, Instant Messages oder Internetseiten.

Die Acronis Internet Security Pop-Ups und Warnungen beinhalten:

- Antivirus-Warnhinweise
- Active Virus Control-Warnungen
- Geräte-Entdeckungsbenachrichtigung
- Firewall Pop-Ups und Warnhinweise
- Antiphishing Warn-seiten
- Warnhinweise Kindersicherung
- Warnhinweise Privatsphäre-Einstellungen

## 5.1. Antivirus-Warnhinweise

Acronis Internet Security schützt Sie vor allen Arten von Malware (wie Viren, Trojaner, Spyware, Rootkits usw.).Wenn Acronis Internet Security einen Virus oder andere Malware entdeckt, führt die Software mit der infizierten Datei spezifische Aktionen durch und informiert Sie darüber in einem Warnhinweisfenster.

Sie sehen den Namen des Virus, den Pfad der infizierten Datei und die Aktion, die Acronis Internet Security ausführt.

Klicken Sie auf **OK**, um dieses Fenster zu schließen.

### Wichtig

Wenn ein Virus gefunden wurde, ist es am sinnvollsten, den gesamten Computer zu scannen, um sicherzugehen, dass keine weitere Viren vorhanden sind.Für weitere Informationen lesen Sie bitte *„Wie kann ich Dateien und Verzeichnisse scannen?“* (S. 151).
Wurde der Virus nicht blockiert, siehe *„Malware von Ihrem System entfernen“* (S. 179).

## 5.2. Active Virus Control-Warnungen

Active Virus Control kann so konfiguriert werden, dass Sie informiert werden, wenn eine Anwendung versucht eine möglicherweise schädliche Aktion durchzuführen.

Wenn Sie die Basis- oder Standard-Ansicht verwenden, informiert Sie ein Pop-Up, wenn die Active Virus Control eine potentiell schädliche Anwendung blockiert hat.Wenn Sie die Experten-Ansicht nutzen, werden Sie über Warnhinweisfenster zu Aktionen aufgefordert, wenn eine Anwendung Anzeichen einer Malware-Infektion zeigt.

Wenn Sie die entdeckte Anwendung kennen und ihr vertrauen, klicken Sie auf **Erlauben**.

Wenn Sie die Anwendung unverzüglich beenden möchten, klicken Sie auf **OK**.

Wählen Sie **Diese Aktion für diese Anwendung merken** aus, bevor Sie Ihre Wahl treffen, und Acronis Internet Security wird die gleiche Aktion für die entdeckte Anwendung auch in Zukunft ausführen.Die Regel, die erstellt wird, wird in dem Active Virus Control Fenster gelistet.

## 5.3. Geräte-Entdeckungsbenachrichtigung

Wenn ein externes Speichergerät mit dem PC verbunden wird, erkennt Acronis Internet Security dies automatisch, und bietet an, es vor dem Zugriff zu zu überprüfen.Dies ist empfohlen um die Infizierung Ihres Systems durch Viren und andere Malware zu verhindern.

Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- USB-Speichergeräte, sowie Flashstifte und externe Festplatten
- verbundene (entfernte) Netzlaufwerke

Wenn solch ein Gerät entdeckt wird, erscheint ein Hinweis.

Um das Speichergerät zu prüfen, klicken Sie **Ja**.Der Antivirusprüfassistend wird erscheinen und Sie durch den Prüfprozess führen.

Falls Sie das Gerät nicht prüfen möchten, klicken Sie **Nein**. In diesem Fall, könnte eine der folgenden Optionen helfen:

- **Bei diesem Gerätetyp nicht mehr nachfragen** - Acronis Internet Security wird für diesen Gerätetyp keine Prüfung vorschlagen, wenn dieser mir dem PC verbunden wird.
- **Automatische Geräteerkennung deaktivieren** - Sie werden nicht länger aufgefordert neue Speichergeräte zu prüfen, wenn diese mit dem PC verbunden werden.

Falls Sie die automatische Geräteerkennung versehentlich deaktivieren und sie reaktivieren, oder die Einstellungen anpassen möchten, folgen Sie diesen Schritten:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus>Virusprüfung**.
3. Suchen Sie in der Liste der Scan-Aufgaben die Aufgabe **Geräte-Scan**.
4. Rechtsklicken Sie auf die Aufgabe und wählen Sie **Eigenschaften**.Ein neues Fenster wird sich öffnen.
5. Im **Übersichts** Tab, konfigurieren Sie die Prüfoptionen nach Bedarf.Für weitere Informationen lesen Sie bitte *„Konfigurieren der Prüfoptionen“ (S. 56)*.
6. Im **Erkennungs** Tab, wählen Sie welche Art von Speichergerät erkannt werden soll.
7. Klicken Sie **OK**, um die Änderungen zu speichern und zu übernehmen.

## 5.4. Firewall Pop-Ups und Warnhinweise

Die Firewall verwendet Pop-Ups, um Sie über die unterschiedlichen mit Ihrer Netzwerkverbindung zusammenhängenden Ereignisse zu informieren (beispielsweise, wenn sich ein neuer Computer in das WiFi-Netzwerk eingeloggt hat, wenn eine neue Anwendung auf das Internet zugreifen darf oder wenn ein Port-Scan blockiert ist).Diese Pop-Ups sind sehr nützlich, um Einbruchversuche aufzuspüren und sich gegen Netzwerkbedrohungen zu schützen.

Wenn Sie die Experten-Ansicht verwenden, werden Sie über Warnhinweisfenster zu Aktionen aufgefordert, wenn eine unbekannte Anwendung versucht, sich mit dem Internet zu verbinden.

Sie können folgendes sehen: Die Anwendung, die versucht, auf das Internet, den Pfad zur Anwendungsdatei, dem Bestimmungsort, das Protokoll verwendet und Port , auf dem die Anwendung versucht in Verbindung zu stehen.

Wählen Sie **Erlauben** um allen Datenverkehr für diese Anwendung über das eingestellt Protokol zu erlauben (eingehend und ausgehend). Wenn Sie **Verweigern**wählen, wird der Zugriff entsprechend blockiert.

Wichtig

Erlauben Sie nur eingehende Verbindungen von IP-Adressen oder Internet-Domänen, denen Sie wirklich vertrauen.

Bassierend auf Ihrer Wahl wird eine Regel erstellt. Das nächste Mal wenn die Anwendung versucht eine Verbindung herzustellen wird die Regeln direkt angewand.

Wenn Sie die Basis- oder Standard-Ansicht verwenden, wird der Verbindungsaufbau automatisch blockiert.

## 5.5. Antiphishing-Warnhinweise

Mit aktiviertem Antiphishing-Schutz alarmiert Acronis Internet Security Sie, wenn Sie versuchen, auf Webseiten zuzugreifen, die eingerichtet wurden, um persönliche Information zu stehlen.Bevor Sie auf solch eine Webseite zugreifen können, wird Acronis Internet Security diese Seite blockieren und ein allgemeines Webseiten-Alarmsignal zeigen:

Überprüfen Sie die Adresse der Webseite in der Adresszeile Ihres Browsers.Suchen Sie nach Hinweisen, die anzeigen könnten, dass die Webseite für Phishing verwendet wird.Wenn die Webseite verdächtigt ist, empfehlen wir diese nicht zu öffnen.

Anbei einige nützliche Tipps:

- Wenn Sie die Adresse einer legitimen Website eingetippt haben, überprüfen Sie, ob die Adresse richtig ist. Wenn die Adresse falsch ist, tippen Sie die Adresse erneut ein und greifen Sie erneut auf die Webseite zu.
- Wenn Sie auf einen Link in einer Email oder einer Instant Message geklickt haben, prüfen Sie nach, wer der Absender war. Wenn Ihnen der Absender unbekannt ist, handelt es sich möglicherweise um einen Phishing-Versuch. Wenn Sie den Absender kennen, sollten Sie überprüfen, ob diese Person Ihnen wirklich den Link gesendet hat.
- Falls Sie über eine Internetsuchanfragee Suche auf die Seite gelangt sind, überprüfen Sie die Webseite auf der Sie den Link gefunden haben (indem Sie im Browser auf „Zurück“ klicken).

Falls Sie sich die Webseite ansehen möchten, klicken Sie auf den entsprechenden Link, um eine dieser Aktion durchzuführen.

- **Internetseite einmalig betrachten.** Es existiert kein Risiko solange Sie auf der Webseite keine Informationen angeben.Falls die Seite seriös ist, können Sie diese der White List hinzufügen (klicken Sie auf die Acronis Internet Security Antiphishing-Symbolleiste und wählen Sie **Der White List hinzufügen**).
- **Fügen Sie die Internetseite der White List hinzu.** Die Seite wird sofort angezeigt und Acronis Internet Security wird sie nicht länger beanstanden.

Wichtig

Fügen Sie der White List ausschließlich Seiten hinzu, denen Sie vollkommen vertrauen (z.B.: der Homepage Ihrer Hausbank, Ihnen bekannte Online-shops, usw.)Acronis Internet Security wird die Seiten der White List nicht auf Phishing prüfen.

Der Antiphishing-Schutz und die White List können über die Acronis Internet Security-Toolbar Ihres Webbrowsers verwaltet werden.Für weitere Informationen lesen Sie bitte *„Handhabung des Acronis Internet Security Antiphishing-Schutzes in Internet Explorer und Firefox“* (S. 66).

## 5.6. Warnhinweise Kindersicherung

Sie können die Kindersicherung so konfigurieren, dass Folgendes blockiert wird:

- Unangemessene Webseiten.
- Den Internetzugang zu bestimmten Zeiten (beispielsweise während der Schule).
- Web-Seiten, Mails und Sofortnachrichten mit bestimmten Schlüsselwörtern.
- Anwendungen wie Spiele, Chat, Filesharing-Programme oder Andere.
- Sofortnachrichten, die von nicht erlaubten IM-Kontakten gesendet werden.

Der Benutzer wird mittels einer Warnmeldung (z. B. einer Standardwarn-Webseite, Email oder Instant Message)informiert, wenn eine Aktivität blockiert wurde.Detaillierte Informationen begründen, wieso die Aktivität geblockt wurde.

## 5.7. Warnhinweise Privatsphäre-Einstellungen

Die Privatsphärekontrolle bietet erfahrenen Benutzern einige Extrafunktionen, um die Privatsphäre zu schützen.Anhand von spezifischen Warnhinweisfenstern werden Sie zu Aktionen aufgefordert, falls Sie eine der folgenden Komponenten aktivieren:

- Registry-Kontrolle - fragt um Erlaubnis immer wenn ein Programm versucht die Registry zu ändern um beim Windows Neustart ausgeführt zu werden.
- Cookie-Kontrolle- fragt nach Ihrer Einwilligung, sobald eine neue Webseite einen Cookie auf Ihrem Rechner installieren will.
- Skript-Kontrolle- fragt nach Ihrer Einwilligung, sobald eine Webseite versucht, ein Skript oder andere aktive Inhalte zu aktivieren.

### 5.7.1. Registry-Alarme.

Wenn Sie die Registry Control aktivieren, werden Sie immer um Erlaubnis gefragt, wenn ein neues Programm versucht, einen Registry-Eintrag zu ändern, um beim Windows-Neustart ausgeführt zu werden.

Sie können das Programm sehen, das versucht die Windows-Registry zu modifizieren.

**Beachten Sie**

Acronis Internet Security wird Sie bei der Installation neuer Programme informieren, wenn ein automatisches Starten nach der Windows-Anmeldung erforderlich ist. In den meisten Fällen sind diese Programme legal und Sie können ihnen vertrauen.

Wenn Sie das Programm nicht kennen und es Ihnen verdächtig erscheint, klicken Sie auf **Blockieren** um es davon abzuhalten die Windows-Registry zu verändern.Klicken Sie andererseits auf **Erlauben** um die Veränderung zu erlauben.

Je nach Ihrer Auswahl wird eine Regel erstellt und in der Regeltabelle aufgelistet.Dieselbe Aktion wird immer ausgeführt wenn diese Anwendung versucht einen Registryeintrag zu ändern.

Für weitere Informationen lesen Sie bitte *„Registry-Überprüfung“* (S. 100).

### 5.7.2. Skript-Alarme

Wenn Sie die Funktion "Skript-Kontrolle" aktivieren, wird immer eine Anfrage an Sie gerichtet, wenn eine neue Webseite versucht, ein Skript oder einen anderen aktiven Inhalte zu verankern.

Der Namen der Quelle wird Ihnen angezeigt.

Klicken Sie **Ja** oder **Nein** und eine Regel wird erstellt werden, zugewiesen und gelistet in der Regeltabelle.Jedes Mal, wenn die entsprechende Seite versucht, aktive Inhalte auszuführen, wird automatisch dieselbe Aktion angewendet.

**Beachten Sie**
Einige Webseiten können nicht vollständig angezeigt werden, wenn Sie den aktiven Inhalt blockieren.

Für weitere Informationen lesen Sie bitte *„Skript-Kontrolle“* (S. 103).

### 5.7.3. Cookie-Alarme

Wenn Sie die Cookie-Kontrolle aktivieren, werden Sie jedes Mal, wenn eine neue Webseite versucht, einen Cookie zu speichern oder diesen abzufragen, um Ihre Erlaubnis gebeten.

Der Name des Programms, das versucht einen Cookie zu senden, wird Ihnen angezeigt.

Klicken Sie **Ja** oder **Nein** und eine Regel wird erstellt werden, zugewiesen und gelistet in der Regeltabelle.Wenn Sie auf die entsprechende Webseite zugreifen, wird immer dieselbe Aktion automatisch ausgeführt.

Für weitere Informationen lesen Sie bitte *„Cookie-Kontrolle“* (S. 101).

# 6. Alle beheben

Acronis Internet Security verwendet ein Problem-Tracking-System, um sicherheitsgefährdende Probleme festzustellen und Sie über diese zu informieren. Standardmäßig werden nur die wichtigsten Bereiche überwacht. Sie können es jedoch so konfigurieren, dass Sie über die von Ihnen gewählten Probleme benachrichtigt werden.

So werden Sie über noch ausstehende Risiken benachrichtigt:

- Ein besonderes Symbol wird über dem Acronis Internet Security-Symbol in der Systemleiste angezeigt, um auf latente Probleme hinzuweisen.Wenn Sie den Mauszeiger über das Symbol bewegen, wird Ihnen angezeigt, dass ein Porblem existiert.
- Wenn Sie Acronis Internet Security öffnen, wird im Bereich Sicherheitsstatus die Anzahl der offenen Probleme angezeigt.
  - ▶ In der Basis-Ansicht wird der Sicherheitsstatus auf der linken Bildschirmseite angezeigt.
  - ▶ Gehen Sie in der Experten-Ansicht auf **Allgemein > Dashboard**, um den Sicherheitsstatus zu überprüfen.

## 6.1. Fehlersuche-Assistent

Der einfachste Weg existierende Probleme zu beseitigen, ist Schritt für Schritt dem **Problemlösungs-Assistent** zu folgen.Befolgen Sie eine der folgenden Möglichkeiten, den Assistenten zu öffnen:

- Rechtsklicken Sie im System Tray auf das Acronis Internet Security-Symbol und wählen Sie **Basiseinstellungen**.
- Öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:
  - ▶ Klicken Sie in der Basis-Ansicht auf **Alle Probleme anzeigen**.
  - ▶ Gehen Sie in der Experten-Ansicht auf **Allgemein>Dashboard** und klicken Sie auf **Alle Probleme anzeigen**.

**Beachten Sie**
Im Bereich Meine Werkzeuge können Sie eine Verknüpfung hinzufügen.

Eine Liste von existierenden Sicherheitsbedrohungen wird angezeigt.

Alle aktuellen Probleme sind zum Beheben ausgewählt. Wenn es ein Problem gibt, dass nicht behoben werden soll, heben Sie einfach die entsprechende Markierung auf. Der Status wechselt dann auf **Überspringen**.

**Beachten Sie**

Falls Sie über bestimmte Probleme nicht benachrichtigt werden möchten, müssen Sie das Überwachungssystem wie im nächsten Abschnitt beschrieben, konfigurieren.

Um die ausgewählten Risiken zu beheben, klicken Sie auf **Beheben**. Einige Risiken werden sofort behoben.Für die anderen, hilft Ihnen ein Assistent diese zu beheben.

Die Risiken die Ihnen dieser Assistent hilft zu beheben, können in diese Hauptkategorien eingeordnet werden

- **Deaktivierte Sicherheitseinstellungen.** Solche Probleme werden sofort beseitigt, durch die entsprechenden Sicherheitseinstellungen.
- **Vorbeugende Sicherheitsaufgaben die Sie durchführen sollten.** Ein Beispiel für eine solche Aufgabe ist der Scan Ihres PCs. Es ist empfohlen, diesen scan mindestens einmal wöchentlich durchzuführen. In den meisten Fällen erledigt Acronis Internet Security dies automatisch. Falls Sie die Scan-Planung verändert haben oder diese nicht vollständig ist, so werden Sie darüber informiert.

  Bei der beseitigung solcher Probleme, hilft Ihnen ein Assistent.
- **System Schwachstellen.** Acronis Internet Security überprüft Ihr System automatisch auf Schwachstellen und informiert Sie über diese.Systemschwachstellen beinhalten das Folgende:

  ▶ Schwache Windows Benutzerkonten Passwörter.

  ▶ Nicht aktuelle Software auf Ihrem PC.

  ▶ fehlende Windows Updates.

  ▶ Automatisches Windows Update ist deaktiviert.

  Wenn solche Probleme beseitigt werden sollen, startet der Schwachstellen-Prüfungsassistent. Der Assistent hilft Ihnen bei der Beseitigung der entdeckten Schwachstellen.Weitere Informationen finden Sie unter *„Auf Schwachstellen scannen“* (S. 119).

## 6.2. Status-Warnmeldungen konfigurieren

Das Statuswarnsystem ist so vorkonfiguriert, dass die wichtigsten Sicherheitsrisiken für Ihr Systems und Ihre Daten überwacht und Sie darüber informiert werden.Neben den überwachten standard Problemen, gibt es weitere, über die Sie sich informieren lassen können.

Sie können das Warnsystem ganz nach Ihren individuellen Ansprüchen konfigurieren, indem Sie wählen, über welche Ereignisse Sie informiert werden möchten.Sie können dies sowohl in der Standard- als auch der Experten-Ansicht tun.

- In der Standard-Ansicht kann das Warnsystem von verschiedenen Stellen aus konfiguriert werden.Folgen Sie diesen Schritten:
  1. Gehen Sie auf den Reiter **Sicherheit**.

2. Klicken Sie im Statusbereich auf den Link **Liste hinzufügen/bearbeiten**.
3. Verwenden Sie den entsprechenden Schalter, um dessen Warnstatus zu ändern.

- In der Experten-Ansicht kann das Warnsystem zentral konfiguriert werden. Gehen Sie folgendermaßen vor:Folgen Sie diesen Schritten:
  1. Gehen Sie auf **Allgemein>Dashboard**.
  2. Klicken Sie auf **Warnungen hinzufügen/bearbeiten**.
  3. Verwenden Sie den entsprechenden Schalter, um dessen Warnstatus zu ändern.

# 7. Konfiguration der Grundeinstellungen

Sie können die Haupteinstellungen des Produkts (einschließlich der Benutzeransicht) im Fenster "Grundeinstellungen" konfigurieren. Um dieses zu öffnen, gehen Sie folgendermaßen vor:

- Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Präferenzen**.
- Rechtsklicken Sie in der Systemleiste auf das Acronis Internet Security-Symbol und wählen Sie **Präferenzen**.

### Beachten Sie

Um die Produkteinstellungen im Detail zu konfigurieren, benutzen Sie die Experten-Ansicht.Für weitere Informationen lesen Sie bitte „Konfiguration und Verwaltung“ (S. 35) diesen Teil des Benutzerhandbuchs.

Die Einstellungen sind in drei Gruppen unterteilt:

- Sicherheitseinstellungen
- Alarmeinstellungen
- Allgemeine Einstellungen

Um eine Einstellung zu aktivieren bzw. zu deaktivieren, nutzen Sie den entsprechenden Button.

Um die Änderungen anzuwenden und zu sichern, klicken Sie **OK**. Um das Fenster zu schliessen ohne die Änderungen zu übernehmen, wählen Sie **Abbrechen**.

Der Link **Neukonfiguration Benutzerprofil** in der linken oberen Bildschirmecke ermöglicht eine Neukonfiguration des Nutzungsprofils.Für weitere Informationen lesen Sie bitte *„Acronis Internet Security 2011 einrichten“* (S. 6).

## 7.1. Sicherheitseinstellungen

Hier können Sie Einstellungen aktivieren/deaktivieren, die verschiedene Bereiche von Computer und Datensicherheit betreffen.Um eine Einstellung zu aktivieren bzw. zu deaktivieren, nutzen Sie den entsprechenden Button.

### Warnung

Wir raten Ihnen zur Vorsicht wenn Sie den Echtzeitschutz, Firewall oder das automatische Update deaktivieren.Diese Funktionen zu deaktivieren kann die Sicherheit Ihres Computers gefährden. Falls sie wirklich einmal deaktiviert werden müssen, vergessen Sie nicht sie so bald als möglich zu reaktivieren.

Dieses sind die verfügbaren Einstellungen:

Antivirus

Der Echtzeit-Dateischutz gewährleistet, dass alle Dateien geprüft werden, sobald auf sie zugegriffen wird, sei es durch Sie oder eine ausgeführte Anwendung.

Automatisches Update

Durch das Automatische Update werden die aktuellsten Acronis Internet Security Produktdateien und Signaturen regelmäßig und automatisch heruntergeladen und installiert.Als Voreinstellungen werden die Updates stündlich durchgeführt.

Schwachstellen-Scan

Der Automatische Schwachstellen-Scan informiert Sie über eventuelleSystemschwachstellen und wie diese zu beheben sind. Zu solchen Schwachstellen gehören veraltete Software, unsichere Passwörter für Benutzerkonten oder fehlende Windows-Updates.

Antispam

Antispam filtert die eingehenden E-Mails und markiert unerwünschte und Junk-Mails als SPAM.

Antiphishing

Antiphishing entdeckt und alamiert sie umgehend in Echtzeit wenn eine Webseite dazu konfiguriert ist persönliche Informationen zu stehlen.

Search Advisor

Der Search Advisor scannt die Links Ihrer Suchergebnisse in Suchmaschinen und informiert Sie, welche Links sicher sind und welche nicht.

Antispyware/Identitätskontrolle

Die Indentitätskontrolle verhindert, dass persönliche Daten ohne Ihr Einverständnis ins Internet gesendet werden. Es blockiert IM Nachrichten, E-Mail oder online Mail die Daten an dritte senden wollen, die Sie als privat definiert haben.

Instant-Messaging-Verschlüsselung

Die IM-Verschlüsselung sichert Ihre Konversationen über Yahoo! Messenger und Windows Live Messenger, vorausgesetzt Ihr Chat-Partner verwendet ebenfalls ein Acronis Internet Security-kompatibles Produkt und IM-Software.

Kindersicherung (aktueller Benutzer)

Die Kindersicherung begrenzt die Rechner- und Online-Aktivitäten Ihrer Kinder, basierend auf den von Ihnen definierten Regeln.Beschränkungen können das Blockieren von unsachgemässen Web-Seiten beinhalten, sowie begrenzten Spiele- und Internet-Zugriff gemäss des festgelegten Zeitplans.

Firewall

Die Firewall schützt Ihren Computer vor Hackern und schädlichen Angriffen.

Dateiverschlüsselung

Über die Dateiverschlüsselung werden Ihre Dokumente geschützt, indem diese in besonders geschützten Laufwerken verschlüsselt abgespeichert werden.Wenn Sie Dateiverschlüsselung deaktivieren, wird jeder Tresor abgeschlossen und Sie haben keinen Zugriff mehr auf die sich darin befindenden Dateien.

Der Status von einigen dieser Einstellungen kann durch das Acronis Internet Security Tracking-System überwacht werden.Wenn Sie eine überwachte Einstellung deaktivieren, zeigt Acronis Internet Security dieses als Risiko an, das Sie beheben müssen.

Wenn Sie nicht wollen, dass eine überwachte Einstellung als ein Problem angezeigt wird, müssen Sie das Tracking System entsprechend konfigurieren. Dies können Sie sowohl in der Standard- als auch der Experten-Ansicht vornehmen.Für weitere Informationen lesen Sie bitte *„Status-Warnmeldungen konfigurieren“* (S. 27).

## 7.2. Alarmeinstellungen

Hier können Sie die Acronis Internet Security-Pop-Ups und Warnungen deaktivieren.Acronis Internet Security verwendet Warnungen, um Sie zu einer Aktion aufzufordern und Pop-Ups, um Sie über bereits automatisch durchgeführte Aktionen oder andere Ereignisse zu informieren.Um eine Warnhinweiskategorie ein- oder auszuschalten, verwenden Sie den entsprechenden Schalter.

Wichtig

Die Einblendung der meisten Warnungen und Pop-Ups sollte aktiviert sein, um so potentielle Probleme zu vermeiden.

Dieses sind die verfügbaren Einstellungen:

**Antivirus-Warnhinweise**

Antivirus-Warnungen informieren Sie, wenn Acronis Internet Security einen Virus gefunden und blockiert hat.Wenn ein Virus gefunden wurde, ist es am sinnvollsten, den gesamten Computer zu scannen, um sicherzugehen, dass keine weitere Viren vorhanden sind.

**Pop-Up Active Virus Control**

Wenn Sie die Basis- oder Standard-Ansicht verwenden, informiert Sie ein Pop-Up, wenn die Active Virus Control eine potentiell schädliche Anwendung blockiert hat.Wenn Sie die Experten-Ansicht nutzen, werden Sie über Warnhinweisfenster zu Aktionen aufgefordert, wenn eine Anwendung Anzeichen einer Malware-Infektion zeigt.

**Pop-Up Email-Scan**

Diese Pop-Ups werden angezeigt, um Sie darüber zu informieren, dass Acronis Internet Security Ihre Emails auf Malware scannt.

**Warnungen Heim-Netzwerkverwaltung**

Diese Warnungen informieren den Benutzer, wenn administrative Aktionen per Fernsteuerung durchgeführt werden.

**Firewall Pop-Ups**

Die Firewall verwendet Pop-Ups, um Sie über die unterschiedlichen mit Ihrer Netzwerkverbindung zusammenhängenden Ereignisse zu informieren (beispielsweise, wenn sich ein neuer Computer in das WiFi-Netzwerk eingeloggt hat, wenn eine neue Anwendung auf das Internet zugreifen darf oder wenn ein Port-Scan blockiert ist).Wenn Sie die Experten-Ansicht verwenden, werden Sie über Warnhinweisfenster zu Aktionen aufgefordert, wenn eine unbekannte Anwendung versucht, sich mit dem Internet zu verbinden.

Diese Pop-Ups sind sehr nützlich, um Einbruchversuche aufzuspüren und sich gegen Netzwerkbedrohungen zu schützen.

**Quarantäne-Warnungen**

Quarantäne-Warnungen informieren Sie, wenn alte Quarantänedateien gelöscht wurden.

**Kindersicherungs-Warnungen**

Wenn die Kindersicherung eine Aktivität blockiert, wird ein Warnhinweis eingeblendet, der Sie darüber informiert, wieso diese Aktivität blockiert wurde (z. B. wird eine Alarm-Webseite anstatt einer blockierten Webseite angezeigt).

**Registrierungs-Pop-Ups**

Registrierungs-Pop-Ups werden verwendet, um Sie daran zu erinnern, dass Sie Acronis Internet Security registrieren müssen oder um Sie zu informieren, dass der Lizenzschlüssel bald ablaufen wird oder schon abgelaufen ist.

## 7.3. Allgemeine Einstellungen

In diesem Berecih können Sie Einstellungen aktivieren/deaktivieren, die das Produktverhalten beeinflussen.Um eine Einstellung zu aktivieren bzw. zu deaktivieren, nutzen Sie den entsprechenden Button.

Dieses sind die verfügbaren Einstellungen:

Spiele-Modus

Der Spiele-Modus verändert temporär die Einstellungen so, dass sie die Systemleistung während des Spielens so wenig wie möglich beeinträchtigen.

Laptop-Modus Erkennung

Der Laptop-Modus verändert temporär die Einstellungen, so dass die Betriebsdauer des Laptopakkus so wenig wie möglich beeinträchtigt wird.

**Passworteinstellungen**

Um zu verhindern, dass jemand anderes die Acronis Internet Security-Einstellungen ändert, können Sie diese durch ein Passwort schützen.Wenn Sie diese Option aktivieren, werden SIe aufgefordert das

Einstellungspasswort zu erstellen.Geben Sie das Passwort in beide Felder ein und klicken Sie auf **OK** um das Passwort fest zu legen.

**Acronis Internet Security Neuigkeiten**

Wenn Sie diese Option aktivieren, erhalten Sie von Acronis Internet Security wichtige Firmenneuigkeiten, Produkt-Updates oder Informationen über die neusten Sicherheitsbedrohungen.

**Produktbenachrichtigungen**

Wenn Sie diese Option aktivieren, erhalten Sie Informationsbenachrichtigungen.

Scanaktivitsänzeige

Die Aktivitätsanzeige ist ein kleines, transparentes Fenster in dem der Fortschritt der Acronis Internet Security Scan-Aktivitäten wird.

**Virenbericht senden**

Wenn Sie diese Option aktivieren, werden Virenberichte zur weiteren Analyse an das Acronis Internet Security-Team gesendet. Bitte bachten Sie, dass diese Berichte keine vertraulichen Daten, wie Ihren Namen oder Ihre IP-Adresse enthalten und nicht für kommerzielle Zwecke verwendet werden.

**Outbreak Erkennung**

Wenn Sie diese Option aktivieren, werden Berichte über einen möglichen Virenausbruch an das Acronis Internet Security Labor zur weiteren Analysen weitergeleitet. Bitte beachten Sie, dass diese Berichte keine vertraulichen Daten, wie Ihren Namen oder Ihre IP-Adresse enthalten sollten und nicht für kommerzielle Zwecke verwendet werden.

# 8. Verlauf und Ereignisse

Der **Protokolle einsehen** Link im unteren Bereich des Acronis Internet Security Sicherheitscenters öffnet ein weiteres Fenster mit den Acronis Internet Security-Ereignissen und dem Verlauf. Dieses Fenster gibt Ihnen einen Überblick über alle sicherheitsrelevanten Ereignissen.So können Sie beispielsweise einfach überprüfen ob das Update erfolgreich durchgeführt wurde, ob Malware auf Ihrem entdeckt wurde usw.

Für eine Filterung des Verlaufs und der Ereignisse Acronis Internet Security werden auf der linken Seite die folgenden Kategorien eingeblendet:

- **Dashboard**
- **Antivirus**
- **Antispam**
- **Kindersicherung**
- **Privatsphärekontrolle**
- **Firewall**
- **Schwachstellen**
- **Instant-Messaging-Verschlüsselung**
- **Dateiverschlüsselung**
- **Spiele/Laptop-Modus**
- **Heimnetzwerk**
- **Aktualisierung**
- **Registrierung**

Für jede Kategorie steht eine Liste von Ereignissen zu Verfügung. Jedes Ereignis enthält folgende Informationen: Eine Kurzbeschreibung, die von Acronis Internet Security durchgeführte Aktion sowie Datum und Zeitpunkt des Auftretens. Wenn Sie nähere Informationen zu einem Ereignis erhalten möchten, doppelklicken Sie auf das entsprechende Ereignis.

Hier finden Sie auch Detailinformationen und Statistiken zu den Ereignissen der Kindersicherung, wie z. B. besuchte Webseiten oder durch Ihre Kinder genutzte Anwendungen.

Klicken Sie auf **Zurücksetzen** wenn Sie die Einträge entfernen möchten oder auf **Aktualisieren** um sicherzustellen das die Anzeige aktuell ist.

# Konfiguration und Verwaltung

# 9. Allgemeine Einstellungen

Das Allgemein-Modul bietet Informationen über die Acronis Internet Security-Aktivität und das System.Hier können Sie auch das allgemeine Verhalten von Acronis Internet Security ändern.

Konfiguration der allgemeinen Einstellungen:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Allgemein> Einstellungen**.

- **Passwortschutz für Programm-Einstellung aktivieren** - aktiviert die Festlegung eines Passwortes, um Ihre Acronis Internet Security-Einstellungen zu schützen.

  Beachten Sie

  Wenn Sie nicht der einzige Benutzer des Computers sind, empfehlen wir Ihnen, Ihre vorgenommenen Einstellungen mit einem Passwort zu schützen.

  Schreiben Sie ein Passwort in das **Passwort**-Feld und wiederholen Sie es in dem Feld **Wiederholung**. Danach klicken Sie auf **OK**.

  Wenn Sie das Passwort festgelegt haben, werden Sie immer danach gefragt, wenn Sie die Acronis Internet Security-Einstellungen ändern möchten.Ein anderer Systemadministrator (falls vorhanden) muss dieses Passwort ebenfalls angeben, um Acronis Internet Security-Einstellungen ändern zu können.

  Wenn Sie nur während der Konfiguration der Kindersicherung nach dem Passwort gefragt werden möchten, so aktivieren Sie die Option **Passwortschutz nur für Kindersicherungseinstellungen anwenden**.Wenn ein Passwort nur für die Kindersicherung festgelegt wurde, Sie diese Option jedoch deaktiviert haben wird das entsprechende Passwort bei der Einstellung jeder Acronis Internet Security-Option abgefragt werden.

  Wichtig

  Falls Sie Ihr Passwort vergessen haben sollten, müssen Sie das Produkt reparieren, um die Acronis Internet Security-Konfiguration zu ändern.

- **Bei Aktivierung der Kindersicherung fragen, ob ich ein Passwort konfigurieren möchte** - Sie werden bei Aktivierung der Kindersicherung aufgefordert, ein Passwort zu vergeben, falls dies noch nicht vergeben wurde.Wenn Sie ein Passwort festlegen, können andere Benutzer mit administrativen Rechten die Einstellungen der Kindersicherung nicht verändern.

- **Acronis Internet Security-News anzeigen** (sicherheitsrelevante Benachrichtigungen) - von Zeit zu Zeit erhalten Sie Sicherheitsmeldungen über Virenausbrüche, die von Acronis Internet Security-Servern versendet werden.
- **Pop-Ups und Hinweise anzeigen** - Pop-up-Fenster anzeigen, die über den Produktstatus informieren.Sie können Acronis Internet Security so konfigurieren, dass die Pop-Ups nur angezeigt werden, wenn Sie die Basis-, Standard- oder Experten-Ansicht gewählt haben.
- **Aktivitsänzeige aktivieren (grafische Bildschirmanzeige der Produktaktivität)** - zeigt die Leiste der Scanaktivität an wenn Windows läuft.Deaktivieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass die Scanaktivitätsleiste angezeigt wird.

## Virenbericht Einstellungen

- **Virenprotokolle senden** - sendet auf Ihrem Computer gefundene Viren an das Acronis Internet Security-Virenlabor. Diese Meldung hilft uns, Virenausbrüche im Auge zu behalten.

  Diese Meldungen beinhalten keine personifizierten Daten, wie Ihren Namen, IP-Adresse oder ähnliches. Diese werden nicht für kommerziele Zwecke verwendet. Die Meldungen beinhalten nur den Virennamen und werden für die Erstellung von Statistiken verwendet.
- **Acronis Internet Security Outbreak-Erkennung aktivieren** - sendet Protokolle über mögliche Virenausbrüche an das Acronis Internet Security-Labor.

  Diese Meldungen beinhalten keine personifizierten Daten, wie Ihren Namen, IP-Adresse oder ähnliches. Diese werden nicht für kommerziele Zwecke verwendet. Die Meldungen beinhalten nur den Virennamen und werden nur für die Erkennung von neuen Viren verwendet.

## Verbindungseinstellungen

Für viele Acronis Internet Security-Komponenten (Firewall, LiveUpdate, Echtzeit-Virenprotokoll und Echtzeit-Spambericht) ist ein Internetzugang notwendig. Acronis Internet Security ist mit einem Proxy-Manager ausgestattet, der Ihnen von einer Stelle aus die Konfiguration der Proxy-Einstellungen erlaubt, die die Acronis Internet Security Komponenten nutzen, um auf das Internet zuzugreifen.

Falls Ihre Firma für die Internetverbindungen einen Proxy-Server verwendet, müssen Sie dessen Proxy-Einstellungen konfigurieren um sicherzustellen, dass sich Acronis Internet Security selbst updaten kann. Anderenfalls werden die Proxy-Einstellungen des Administrators, der das Produkt installiert hat oder die momentanen Proxy-Einstellungen des Standard-Browsers verwendet.Für weitere Informationen lesen Sie bitte *„Wo finde ich "Meine Proxy-Einstellungen"?“* (S. 190).

**Beachten Sie**

Proxyeinstellungen können nur von Administratoren oder Hauptbenutzern (welche über das nötige Passwort verfügen) vorgenommen werden.

Um die Proxy-Einstellungen zu verwalten, klicken Sie auf **Proxy-Einstellungen**.

Es bestehen drei mögliche Proxyeinstellungen:

- **Proxy während Installation entdeckt** - während der Installation wurden Proxy-Einstellungen für das Administrator-Benutzerkonto gefunden. Diese können nur von diesem Administratorkonto aus geändert werden. Sollten ein Benutzername und Passwort nötig sein, so geben Sie diese in den dafür vorgesehenen Feldern ein.
- **Standard Browser Proxy** - Proxy-Einstellungen des aktuellen Benutzers, extrahiert vom Standard-Browser. Falls der Proxy einen Benutzernamen und Passwort voraussetzt, geben Sie diese in den entsprechenden Feldern an.

  **Beachten Sie**

  Die unterstützen Browser sind hierbei Internet Explorer, Mozilla Firefox und Opera. Sollten Sie einen anderen Browser verwenden kann Acronis Internet Security dessen Einstellungen nicht übernehmen.

- **Benutzerdefinierte Proxy-Einstellungen** - Hier können Sie selbst, als Administrator eingeloggt, Proxyeinstellungen vornehmen .

  Die folgenden Einstellungen müssen angegeben werden:
  - ▶ **Adresse** - Geben Sie die IP-Adresse des Proxy-Servers ein.
  - ▶ **Port** - Geben Sie den Port ein, über den Acronis Internet Security die Verbindung zum Proxy-Server herstellt.
  - ▶ **Name** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
  - ▶ **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.

Acronis Internet Security wird die Proxy-Einstellungs-Sets in der folgenden Reihenfolge anwenden, bis der Verbindungsaufbau zum Internet gelingt:

1. die spezifizierten Proxy-Einstellungen.
2. die bei der Installation gefundenen Proxy-Einstellungen.
3. die Proxy-Einstellungen des aktuellen Benutzers.

Bei einem Updateversuch werden alle Proxyeinstellung nacheinander verwendet bis ein Update möglich ist.

Zuerst wird versucht ein Update über die eigenen Proxyeinstellungen vorzunehmen. Als nächstes werden die Proxyeinstellungen des Administrators verwenden. Wenn auch dies nicht zum erfolgt führt wird ein Update über die Einstellungen des momentanen Benutzers durchgeführt.

Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Klicken Sie auf **Übernehmen** um die Einstellungen zu speichern. Wenn Sie auf **Standard** klicken werden die Werkseinstellungen geladen.

## System-Info

In Acronis Internet Security können Sie von einer Stelle aus alle Systemeinstellungen und die Programme, die beim Systemstart gestartet werden, einsehen. So können Sie die Aktivitäten des Systems und der installierten Anwendungen überwachen und mögliche Systeminfizierungen feststellen.

So finden Sie die Systeminformationen:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Allgemein > Systeminfo**.

Die Auflistung enthält alle Einstellungen die angewendet werden, sowohl wenn der Computer gestartet wird als auch wenn spezielle Anwendungen aufgerufen werden und gesonderte Regeln besitzen.

Drei Schaltflächen sind verfügbar:

- **Wiederherstellen** - stellt die ursprüngliche Dateiassoziation der aktuellen Datei wieder her.Nur für die Einstellungen **Dateiassoziationen** verfügbar!
- **Gehe zu** - öffnet ein Fenster mit der Pfadangabe für das Objekt (Zum Beispiel: **Eintragung**).

Beachten Sie

Je nach ausgewähltem Objekt wird die Schaltfläche **Gehe zu** nicht erscheinen.

- **Aktualisieren** - öffnet erneut die das Menü **System-Info**.

# 10. Antivirus-Schutz

Acronis Internet Security schützt Sie vor allen Arten von Malware (Viren, Trojaner, Spyware, Rootkits etc.).Der Virenschutz, den Acronis Internet Security bietet, lässt sich in zwei Kategorien einteilen:

- Echtzeitschutz - hält neue Malware-Bedrohungen davon ab, in Ihr System zu gelangen.Acronis Internet Security wird z.B. ein Worddokument auf Malware scannen, wenn Sie es öffnen oder eine Email-Nachricht, wenn Sie diese empfangen.

  Der Echtzeitschutz gilt auch für die Prüfung auf Zugriff (On-Access) - Dateien werden geprüft, sobald die Benutzer auf sie zugreifen.

  Wichtig
  Um zu verhindern, dass Viren Ihren Computer befallen, lassen Sie den **Echtzeitvirenschutz** immer aktiviert.

- On-demand Prüfung - erkennt und entfernt Malware die sich bereits auf dem System befindet.Hierbei handelt es sich um einen klassischen, durch den Benutzer gestarteten, Scan - Sie wählen das Laufwerk, Verzeichnis oder Datei, die Acronis Internet Security scannen soll und Acronis Internet Security scannt diese.Die Prüfaufgaben erlauben Ihnen die Prüfroutinen auf Ihre Bedürfnisse anzupassen und diese zu einem festgelegten Zeitpunkt zu starten.

Wenn Acronis Internet Security einen Virus oder andere Malware feststellt, versucht das Programm automatisch den Malware-Code der infizierten Datei zu entfernen und die Originaldatei wiederherzustellen.Diese Operation bezeichnet man als Desinfektion.Dateien, die nicht desinfiziert werden können, werden in das QuarantäneVerzeichnis verschoben, um so die Infizierung einzudämmen.Für weitere Informationen lesen Sie bitte *„Quarantäne“ (S. 63)*.

Wenn Ihr Computer mit Malware infiziert ist, siehe *„Malware von Ihrem System entfernen“ (S. 179)*.

Fortgeschrittene Anwender können Scan-Ausschlüsse festlegen, falls bestimmte Dateien vom Scan ausgeschlossen werden sollen.Für weitere Informationen lesen Sie bitte *„Konfiguration der Scan-Ausschlüsse“ (S. 59)*.

## 10.1. Echtzeitschutz

Acronis Internet Security bietet einen dauerhaften Echtzeitschutz gegen verschiedene Malware, indem alle Dateien auf die zugegriffen wird sowie Email-Nachrichten und die Kommunikationen per Instant Messaging Software (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) gescannt werden.

Die vorgegebenen Einstellungen zum Echtzeitschutz stellen einen guten Schutz gegen Malware bei nur minimaler Beeinträchtigung der Systemleistung sicher.Sie

können die Einstellungen zum Echtzeitschutz einfach Ihren Bedürfnissen anpassen, indem Sie eine der vordefinierten Schutzstufen wählen.Wenn Sie ein erfahrener Anwender sind, können Sie die Scan-Einstellungen auch selbst im Detail konfigurieren, indem Sie eine benutzerdefinierte Schutzstufe definieren.

Weitere Informationen zu folgenden Themen sind verfügbar:

- *„Anpassen der Sicherheitsstufe des Echtzeitschutzes“* (S. 41)
- *„Erstellen einer benutzerdefinierten Schutzeinstellung“* (S. 41)
- *„Ändern der Aktion, die bei verdächtigen Dateien durchgeführt wird“* (S. 43)
- *„Wiederherstellen der Voreinstellungen“* (S. 44)

Um Sie gegen unbekannte Malware-Anwendungen zu schützen, greift Acronis Internet Security auf eine fortschrittliche Heuristik-Technologie (Active Virus Control) und ein Intrusion Detection System, das Ihr System durchgehend überwacht, zurück.Weitere Informationen zu folgenden Themen sind verfügbar:

- *„Konfigurieren des Active Virus Control “* (S. 45)
- *„Konfiguration des Intrusion Detection Systems“* (S. 47)

## 10.1.1. Anpassen der Sicherheitsstufe des Echtzeitschutzes

Die Schutzstufe des Echzeitschutzes definiert die Scan-Einstellungen für den Echtzeitschutz.Sie können die Einstellungen zum Echtzeitschutz einfach Ihren Bedürfnissen anpassen, indem Sie eine der vordefinierten Schutzstufen wählen.

Um die Sicherheitsstufe für den Echtzeitschutz anzupassen:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Schieben Sie den Regler in die gewünschte Schutzstufenposition.Nutzen Sie die Beschreibung auf der rechten Seite, um die TresorSicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.

### Beachten Sie

In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Für weitere Informationen lesen Sie bitte *„Meine Werkzeuge“* (S. 17).

## 10.1.2. Erstellen einer benutzerdefinierten Schutzeinstellung

Erfahrene Anwender möchten sich eventuell näher mit den Scan-Einstellungen von Acronis Internet Security beschäftigen. Der Scanner kann so eingestellt werden, dass nur spezielle Dateiendungen oder spezielle Malware-Bedrohungen gescannt

oder Archive übersprungen werden. So werden die Scan-Zeit verringert und die Antwortzeiten Ihres Rechners während eines Scans verbessert.

Sie können die Einstellungen für den Echtzeitschutz im Detail konfigurieren, indem Sie eine benutzerdefinierte Schutzstufe festlegen.Schutzstsufe zu erstellen:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Benutzerdefinierte Einstufung**.
4. Konfigurieren Sie die Scan-Einstellungen nach Ihren Wünschen.Um herauszufinden was eine Option macht, halten Sie den Mauszeiger darüber und lesen die angezeigte Beschreibung im unteren Teil des Fensters.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach.Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Dateien in Echtzeit überprüfen.** Sie können Acronis Internet Security so programmieren, dass alle Dateien, nur Anwendungen (Programmdateien) oder nur bestimmte Dateitypen, die Sie als gefährlich einstufen, gescannt werden sollen.Das Scannen aller Dateien bietet den besten Schutz, während das ausschließliche Scannen der Anwendungen nur für die Verbesserung der Systemleistung verwendet werden kann.

  Anwendungen (oder Programmdateien) sind weitaus anfälliger gegen Malware-Angriffe als andere Typen oder Dateien.Diese Kategorie beinhaltet die folgenden Dateierweiterungen:`.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  Falls Sie sich für die Option **Anwenderdefinierte Erweiterungen scannen** entscheiden, empfehlen wir, dass Sie neben allen anderen Dateierweiterungen, die Sie als potentiell gefährlich einstufen, auch alle Anwendungserweiterungen mit einschließen.
- **Nur neue und veränderte Dateien prüfen.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Boot-Sektoren prüfen.** Sie können Acronis Internet Security einstellen, damit die Boot-Sektoren gescannt werden.Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten.Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte

Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.

- **Archive prüfen.** Das Scannen von Archiven ist ein langsamer und ressourcen-intensiver Vorgang, der aus diesem Grund nicht für den Echtzeitschutz empfohlen wird.Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit.Die Malware kann Ihr System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird.
- **Primäre Aktion.** Falls Sie die Aktionen, die auf verdächtige Dateien angewendet werden sollen, ändern möchten, finden Sie Tipps in *„Ändern der Aktion, die bei verdächtigen Dateien durchgeführt wird“* (S. 43).
- **Scan-Optionen für Email-,Internet- und Instant Messaging-Datenverkehr .** Um zu verhindern, dass Malware auf Ihren Computer geladen wird, scannt Acronis Internet Security automatisch die folgenden Malware Einfalltore:
  ▶ eingehende Emails
  ▶ Internet-Datenverkehr
  ▶ über Yahoo! Messenger und Windows Live Messenger empfangene Dateien
  Das Scannen des Web-Datenverkehrs kann Ihren Webbrowser geringfügig verlangsamen, dadurch können aber über das Internet übertragene Malware, einschließlich Drive-by-Downloads, blockiert werden.

  Obwohl wir dies nicht empfehlen, können Sie den Scan von Emails, Web- oder Instant Messaging deaktivieren, um die Systemleistung zu verbessern.Wenn Sie die entsprechenden Scan-Optionen deaktivieren, werden empfangene Emails und aus dem Internet geladene Dateien nicht gescannt. Dies bedeutet aber, dass infizierte Dateien auf Ihrem Computer gespeichert werden können.Dies ist keine bedeutende Bedrohung, da der Echtzeitschutz die Malware blockiert, wenn auf die infizierten Dateien zugegriffen wird (geöffnet, verschoben, kopiert oder ausgeführt).

### 10.1.3. Ändern der Aktion, die bei verdächtigen Dateien durchgeführt wird

Die vom Echtzeitschutz festgestellten Dateien werden in zwei Kategorien gruppiert:

- **Infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Acronis Internet Security Malware-Signaturen-Datenbank überein.Acronis Internet Security kann im Normalfall Malware-Codes aus einer infizierten Datei entfernen und die Originaldatei wiederherstellen. Diese Aktion wird Desinfektion genannt.

**Beachten Sie**

Malware-Signaturen sind Code-Bruchstücke, die aus aktuellen Malware-Beispielen extrahiert werden. Diese werden von Antiviren-Programmen zum Musterabgleich und zur Aufspürung von Malware verwendet.
Die Acronis Internet Security Malware-Signatur-Datenbank ist eine Sammlung von stündlich durch Acronis Internet Security-Mitarbeiter upgedateten Malware-Signaturen.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert.Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

Abhängig vom gefundenen Dateityp werden folgende Aktionen automatisch ausgeführt:

- Wird eine infizierte Datei gefunden, versucht Acronis Internet Security automatisch, diese zu desinfizieren.Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung in Schach zu halten.

**Wichtig**

Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- Wird eine verdächtige Datei gefunden, wird der Zugriff auf diese Datei verweigert, um so eine potentielle Infizierung auszuschließen.

Sie sollten die voreingestellten Aktionen für verdächtige Dateien nicht ändern, es sei denn, Sie haben einen guten Grund dafür.

Um die voreingestellten Aktionen für infizierte oder verdächtige Dateien zu ändern:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Benutzerdefinierte Einstufung**.
4. Konfigurieren Sie die Aktionen, die für jede Dateikategorie durchgeführt werden sollen.Die zweite Aktion wird ausgeführt, wenn die erste fehlschlägt (wenn beispielsweise die Desinfektion fehlschlägt, wird die infizierte Datei in die Quarantäne verschoben).

### 10.1.4. Wiederherstellen der Voreinstellungen

Die vorgegebenen Einstellungen zum Echtzeitschutz stellen einen guten Schutz gegen Malware bei nur minimaler Beeinträchtigung der Systemleistung sicher.

Um die vorgegebenen Echzeitschutz-Einstellungen wiederherzustellen:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Voreingestellter Level**.

### 10.1.5. Konfigurieren des Active Virus Control

Die Acronis Internet Security Active Virus Control kann potentiell gefährliche Anwendungen anhand ihrer speziellen Verhaltensweisen entdecken.

Die Active Virus Control überwacht kontinuierlich die auf Ihrem Computer laufenden Anwendungen auf Malware-ähnliche Aktionen. Jede dieser Aktionen wird eingestuft, für jeden Prozess wird zudem eine Allgemeineinstufung erstellt.Wenn die Allgemeineinstufung für einen Prozess einen bestimmten Schwellenwert erreicht, wird der Prozess als schädlich eingestuft. Abhängig von den Programmeinstellungen wird der Prozess entweder automatisch blockiert oder Sie werden aufgefordert, die auszuführende Aktion zu spezifizieren.

Active Virus Control kann so konfiguriert werden, dass Sie informiert werden, wenn eine Anwendung versucht eine möglicherweise schädliche Aktion durchzuführen.

Wenn Sie die entdeckte Anwendung kennen und ihr vertrauen, klicken Sie auf **Erlauben**.

Wenn Sie die Anwendung unverzüglich beenden möchten, klicken Sie auf **OK**.

Wählen Sie **Diese Aktion für diese Anwendung merken** aus, bevor Sie Ihre Wahl treffen, und Acronis Internet Security wird die gleiche Aktion für die entdeckte Anwendung auch in Zukunft ausführen.Die Regel, die erstellt wird, wird in dem Active Virus Control Fenster gelistet.

Konfiguration der Active Virus Control:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Weitere Einstellungen**.
4. Klicken Sie auf den Reiter **AVC** (Active Virus Control).
5. Markieren Sie das dazugehörige Kästchen um Active Virus Control zu ativieren.
6. Schieben Sie den Regler in die gewünschte Schutzstufenposition.Nutzen Sie die Beschreibung auf der rechten Seite, um die TresorSicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.

#### Anpassung des Schutzstufen-Levels

Konfiguration der Schutzstufe der Active Virus Control:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Weitere Einstellungen**.
4. Klicken Sie auf den Reiter **AVC** (Active Virus Control).
5. Schieben Sie den Regler in die gewünschte Schutzstufenposition.Nutzen Sie die Beschreibung auf der rechten Seite, um die TresorSicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.

## Konfiguration der Reaktion auf Malware-typisches Verhalten

Falls eine Anwendung Anzeichen einer Malware-Infektion zeigt, erhalten Sie eine Abfrage, ob diese zugelassen oder blockiert werden soll.

Konfiguration der Antwort auf Malware-typisches Verhalten:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Weitere Einstellungen**.
4. Klicken Sie auf den Reiter **AVC** (Active Virus Control).
5. Möchten Sie zu einer Aktion aufgefordert werden, wenn Active Virus Controll eine potentiell schädliche Anwendung findet, aktivieren Sie die Option **Warnen, bevor eine Aktion durchgeführt wird**.Soll eine Anwendung, die Zeichen einer Malware-Infizierung zeigt automatisch blockiert werden (ohne ein Warnhinweisfenster einzublenden), aktivieren Sie diese Option.

## Vertraute / Unzulässige Anwendungen verwalten.

Sie können Anwendungen die Sie kennen und denen Sie vertrauen, zur Liste der vertrauenswürdigen Anwendungen hinzufügen. Diese Anwendungen werden nicht länger von der Acronis Internet Security Active Virus Control gescannt, der Zugriff wird automatisch erlaubt.

Verwaltung der Anwendungen, die nicht von der Active Virus Control überwacht werden:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Weitere Einstellungen**.
4. Klicken Sie auf den Reiter **AVC** (Active Virus Control).
5. Klicken Sie auf den Reiter **Ausschlüsse**.

Die Anwendungen für die eine Regel erstellt wurde, wird in der nachfolgenden Tabelle **Ausnahmen** angezeigt.Der Pfad der Anwendung und die Aktion, die Sie dafür konfiguriert haben (erlaubt oder blockiert) wird für jede Regel angezeigt.

Um die Aktion für eine Anwendung zu ändern, klicken Sie die aktuelle Aktion und wählen eine andere Action.

Um die Liste zu verwalten, benutzen Sie die optionen unter der Tabelle.

- **Hinzufügen** - eine neue Anwendung zur Liste hinzufügen.
- **Entferne** - entfernen Sie eine Anwendung aus der Liste.
- **Editieren** - editiert eine Anwendungsregel.

### 10.1.6. Konfiguration des Intrusion Detection Systems

Das Intrusion Detection System von Acronis Internet Security überwacht das Netzwerk und die Systemaktivitäten auf Malware-Aktivitäten oder Richtlinienverletzungen.

Konfiguration des Intrusion Detection Systems:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Weitere Einstellungen**.
4. Klicken Sie auf den Reiter **IDS**.
5. Aktivieren Sie das entsprechende Kästchen, um das Intrusion Detection System zu aktivieren.
6. Schieben Sie den Regler in die gewünschte Schutzstufenposition.Nutzen Sie die Beschreibung auf der rechten Seite, um die Schutzstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.

## 10.2. Prüfvorgang

Die Hauptaufgabe der Acronis Internet Security-Software ist es sicherzustellen, dass Ihr virenfrei ist. Dies wird in erster Linie dadurch erreicht, dass neue Viren von Ihrem Computer ferngehalten werden und indem Ihre Email-Anhänge und Downloads gescannt und alle Aktionen, die auf Ihrem System stattfinden, überwacht werden.

Es besteht aber die Gefahr, dass sich bereits vor der Installation von Acronis Internet Security ein Virus in Ihrem System befand. Deshalb sollten Sie Ihren Computer nach der Installation von Acronis Internet Security auf residente Viren scannen. Und es ist definitiv eine gute Idee, auch in Zukunft Ihren Computer regelmäßig auf Viren zu scannen.

Der Prüfvorgang basiert auf Prüfaufgaben welche die Einstellungen zum Vorgang sowie die zu prüfenden Objekte beinhalten.Sie können den Computer scannen,

wann Sie wollen, indem Sie die voreingestellten Aufgaben, oder die von ihnen selbst definierten, starten. Sie können Sie auch einstellen, dass sie regelmässig laufen, oder wenn Ihr System im Leerlauf ist.Schnelle Hilfestellung finden Sie in folgenden Themenbereichen:

- *„Wie kann ich Dateien und Verzeichnisse scannen?“* (S. 151)
- *„Wie erstelle ich eine benutzerdefinierte Scan-Aufgabe?“* (S. 154)
- *„Wie plane ich einen Scan?“* (S. 156)

### 10.2.1. Dateien und Ordner prüfen

Wenn Sie den Verdacht hegen, dass Dateien und Verzeichnisse infiziert sein könnten, sollten Sie einen Scan durchführen.Rechtsklicken Sie auf die zu scannende Datei oder Verzeichnis und wählen Sie **Mit Acronis Internet Security scannen**.Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

Wenn Sie bestimmte Bereiche Ihres Computers scannen möchten, könnenSie eine benutzerdefinierte Scan-Aufgabe konfigurieren und ausführen.Für weitere Informationen lesen Sie bitte *„Wie erstelle ich eine benutzerdefinierte Scan-Aufgabe?“* (S. 154).

Um Ihren Computer oder Teile Ihres Computers zu prüfen können Sie die Standardeinstellungen nutzen oder Ihre eigenen Aufgaben einrichten.Um eine Scan-Aufgabe auszuführen, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Basis-Ansicht
: Klicken Sie auf den Button **Sicherheit** und wählen Sie eine der verfügbaren Scan-Aufgaben.

Standard-Ansicht
: Gehen Sie auf den Reiter **Sicherheit**.Klicken Sie im linken Quick Task-Bereich auf **Vollsystem-Scan** und wählen Sie eine der verfügbaren Scan-Aufgaben.

Experten-Ansicht
: Gehen Sie zu **Antivirus > Virusen-Scan**.Um einen System- oder Benutzerdefinierten Scan auszuführen, klicken Sie den entsprechenden **Aufgabe Ausführen** Button.

Dies sind die voreingestellten Aufgaben, die Sie für einen Scan Ihres Computers nutzen können:

**Vollsystem-Scan**
: Prüft alle Dateien mit Ausnahme von Archiven.In der standard Konfiguration, wird nach allen Arten von Malware geprüft, ausser rootkits.

**Quick Scan**
: Beim Quick Scan wird das sog In-the-cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren.Die Ausführung eines Quick Scans dauert

im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.

**Tiefe Systemprüfung**
Prüft das komplette SystemIn der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.

Bevor Sie einen Scan starten sollten Sie sich vergewissern, dass Acronis Internet Security auf dem neuesten Stand der Malware-Signaturen ist. Ihren Computer unter Verwendung einer veralteten Signaturendatenbank zu scannen, kann Acronis Internet Security daran hindern, neue seit dem letzten Update gefundene Malware zu erkennen.

Damit Sie einen vollständigen Scan mit Acronis Internet Security durchführen können, ist es wichtig, alle Programme zu beenden. Besonders wichtig ist, dass Sie Ihr Email Programm schließen (z. B. Outlook, Outlook Express oder Eudora).

### Prüftips

Hier sind noch einige Prüftips welche Sie vielleicht nützlich finden:

- Je nach Festplattengrösse kann das Durchführen einer umfassenden Systemprüfung (wie Systemprüfung oder Tiefe Systemprüfung) einige Zeit in Anspruch nehmen (bis zu einer Stunde oder mehr).Aus diesem Grund sollten Sie derartige Prüfungen nur durchführen wenn Sie den Computer für eine längere Zeit nicht nutzen (z.B. die Nacht über).

  Sie können die Prüfung planen zu einem günstigen Zeitpunkt zu starten.Stellen Sie sicher den Computer laufen zu lassen.Stellen Sie mit Windows Vista sicher, dass sich Ihr Rechner nicht im Schlafmodus befindet, wenn eine geplante Aufgabe ansteht.

- Falls Sie regelmässig Dateien aus dem Netz in einen bestimmten Ordner herunterladen, erstellen Sie eine neue Prüfaufgabe und legen den Ordner als Prüfziel fest..Planen sie die Aufgabe ein täglich oder häufiger zu laufen.

- Es gibt eine Malewareart welche sich, durch das Ändern der Windows-Einstellungen, konfiguriert beim Systemstart ausgeführt zu werden.Um Ihren Computer vor derartiger Maleware zu schützen, können Sie die **Autologon Prüfung** beim Systemstart laufen lassen.Bitte beachten Sie das Autologon prüfen die Systemleistung für kurze Zeit nach dem Starten beeinflussen kann.

## 10.2.2. Antivirus Prüfassistent

Wann immer Sie einen On-Demand Scan starten (z.B. indem Sie auf ein Verzeichnis rechtsklicken und dann **Mit Acronis Internet Security 2011 scannen wählen**), wird der Acronis Internet Security Antivirus Scan-Assistent eingeblendet.Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

### Beachten Sie

Falls der Prüfassistent nicht erscheint, ist die Prüfung möglicherweise konfiguriert still, im Hintergrund, zu laufen.Sehen Sie nach dem Prüffortschritticon im Systemtray.Sie können dieses Objekt anklicken um das Prüffenster zu öffnen und so den Prüffortschritt zu sehen.

## Schritt 1/3 - Prüfvorgang

Acronis Internet Security startet den Scan der aus gewählten Dateien und Verzeichnisse.

Sie können den Vorgangsstatus und die Statistiken hierzu sehen (Prüfgeschwindigkeit, vergangene Zeit, Anzahl der geprüften / infizierten / verdächtigen / versteckten Objekte).

Bitte warten Sie, bis Acronis Internet Security den Scan beendet hat.

### Beachten Sie

Der Prüfvorgang kann, abhängig von der Größe Ihrer Festplatte, einen Moment dauern.

**Passwortgeschützte Archive.** Wird ein passwortgeschütztes Archiv gefunden, werden Sie, abhängig von den Scan-Einstellungen, um die Eingabe des Passwortes gebeten.Mit Passwörtern geschützte Archive können nicht geprüft werden, außer wenn Sie das Passwort angeben.Die folgenden Optionen sind verfügbar:

- **Ich möchte für dieses Objekt das Passwort eingeben.** Wenn Sie möchten das Acronis Internet Security Archive scannt, wählen Sie diese Option aus und geben das Passwort an.Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.
- **Ich möchte für dieses Objekt kein Passwort angeben (dieses Objekt überspringen).** Wählen Sie diese Optione um das Prüfen diesen Archivs zu überspringen.
- **Ich möchte für kein Objekt ein Passwort angeben (alle passwortgeschützten Objekte überspringen).** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten.Acronis Internet Security kann diese Dateien und Objekte nicht scannen, erstellt aber einen Eintrag im Scan-Protokoll.

Klicken Sie auf **OK** um fortzufahren.

**Stoppen oder pausieren der Prüfung.** Sie können den Prüfvorgang jederzeit durch einen Klick auf **Stop&Ja** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten.Um den Prüfvorgang vorrübergehend zu stoppen klicken Sie einfach auf **Pause**. Um den Prüfvorgang fortzusetzen klicken Sie auf **Fortsetzen** .

## Schritt 2/3 - Aktionsauswahl

Wenn der Prüfvorgang beendet wurde wird Ihnen ein Fenster angezeigt in welchem Sie eine Zusammenfassung angezeigt bekommen.

Sind keine ungelösten Probleme vorhanden, klicken Sie auf **Weiter**.Andernfalls müssen Sie neue Aktionen konfigurieren, die auf die nicht beseitigten Bedrohungen angewandt werden sollen. Nur so ist Ihr System weiterhin geschützt.

Die infizierten Objekte werden in Gruppen angezeigt, je nach Malware, mit der sie infiziert sind.Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine umfassende Aktion für alle Probleme auswählen oder Sie können einzelne Aktionen für Problemgruppen auswählen.Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

**Keine Aktion durchführen**
Es wird keine Aktion für die infizierte Dateien ausgeführt.Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.

**Desinfiziert**
Den Malware-Code aus den entdeckten infizierten Dateien entfernen.

**Löschen**
Infizierte Dateien werden von der Festplatte entfernt.

**In Quarantäne verschieben**
Verschiebt die entdeckten Dateien in die Quarantäne.Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?Für weitere Informationen lesen Sie bitte *„Quarantäne“ (S. 63)*.

**Dateien umbenennen**
Die neue Erweiterung der versteckten Dateien wird `.bd.ren` sein.Infolgedessen werden Sie im Stande sein, zu suchen und solche Dateien auf Ihrem Computer zu finden, falls etwa.

Bitte beachten Sie das es sich bei den versteckten Dateien nicht um die absichtlich von Windows verborgenen Dateien handelt. Die relevanten sind die von speziellen Programmen versteckten, bekannt als Rootkits.Rootkits sind nicht grundsätzlich schädlich. Jedoch werden Sie allgemein dazu benutzt Viren oder Spyware vor normalen Antivirenprogrammen zu tarnen.

Klicken Sie auf **Fortfahren** um die festgelegten Aktionen anzuwenden.

## Schritt 3/3 - Zusammenfassung

Wenn Acronis Internet Security die Probleme gelöst hat, wird eine Zusammenfassung der Scan-Ergebnisse in einem neuen Fenster angezeigt.Falls Sie umfangreichere Informationen zum Scan-Prozess möchten, klicken Sie auf **Logdatei anzeigen**.

**Wichtig**
Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Säuberungsprozess abgeschlossen werden kann.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.

### Acronis Internet Security konnte einige Probleme nicht lösen

In den meisten Fällen desinfiziert Acronis Internet Security erfolgreich die aufgespürten infizierten Dateien oder er isoliert die Infektion.Dennoch gibt es Probleme, die nicht automatisch gelöst werden können.Weitere Informationen und Anweisungen, wie Sie Malware manuell entfernen können, finden Sie unter *„Malware von Ihrem System entfernen“* (S. 179).

### Acronis Internet Security hat verdächtige Dateien gefunden

Verdächtige Dateien sind Dateien, die von der heuristischen Analyse als potentiell infiziert erkannt werden, und deren Signaturen noch nicht bekannt sind.

Falls verdächtige Dateien während des Scanes erkannt werden, werden Sie aufgefordert, diese Dateien an das Acronis Internet Security-Labor zu senden.Klicken Sie auf **OK**, um diese Dateien zum Acronis Internet Security-Lab für weitere Analysen zu senden.

## 10.2.3. Prüfberichte anzeigen

Für jeden Scan wird ein Protokoll erstellt.Der Bericht enthält detaillierte Informationen über den Prüfprozess, so wie Prüfoptionen, das Prüfziel, die entdeckten Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **Protokoll anzeigen** klicken.

Um die Scan-Protokolle später anzusehen:

1. Öffnen Sie Acronis Internet Security.
2. Klicken Sie unten rechts im Fenster auf den Link **Protokolle ansehen**.
3. Klicken Sie auf **Antivirus** in dem Menü auf der linken Seite.
4. Im Bereich **On-Demand-Aufgaben** können Sie überprüfen, welche Scans kürzlich durchgeführt wurden.Doppelklicken Sie auf die Ereignisse in der Liste, um weitere Details zu erhalten.Um das Scan-Protokoll zu öffnen, klicken Sie auf **Scan-Protokoll ansehen**.Die Berichtdatei wird in Ihrem Webbrowser geöffnet.

Um einen Protokolleintrag zu löschen, rechtsklicken Sie auf ihn und wählen **Löschen**.

## 10.2.4. Verwaltung der existierenden Scan-Aufgaben

Acronis Internet Security verfügt über mehrere vordefinierte Aufgaben, die für die gängigsten Sicherheitsprobleme angewandt werden können.Für weitere Informationen lesen Sie bitte *„Wie erstelle ich eine benutzerdefinierte Scan-Aufgabe?“* (S. 154).

Verwaltung der existierenden Scan-Aufgaben:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Virusen-Scan**.

### Beachten Sie

In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Für weitere Informationen lesen Sie bitte *„Meine Werkzeuge“* (S. 17).

Es gibt drei verschiedene Einstellungen der Prüfoptionen:

- **Systemaufgaben** - Enthält eine Liste von standard Systemeinstellungen. Die folgenen Einstellungen sind möglich:

  **Vollsystem-Scan**
  Prüft alle Dateien mit Ausnahme von Archiven.In der standard Konfiguration, wird nach allen Arten von Malware geprüft, ausser rootkits.

  **Quick Scan**
  Beim Quick Scan wird das sog In-the-cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren.Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.

  **Prüfvorgang für Autologon**
  Prüft die Objekte, die ausgeführt werden, wenn ein Benutzer sich bei Windows anmeldet.Standardmäßig ist die Prüfung im Hintergrund deaktiviert.

  Um die Aufgabe zu benutzen, klicken Sie darauf mit der rechten Maustaste, wählen Sie **Planer** und setzen Sie die Ausführung der Aufgabe**beim Systemstart**.Geben Sie an wie lange nach dem Systemstart die Aufgabe gestartet sein wird.(Minuten)

  **Tiefe Systemprüfung**
  Prüft das komplette SystemIn der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.

### Beachten Sie

Dadurch das die Prüfvorgänge **Tiefgehende Systemprüfung** und **Systemprüfung** alle Dateien prüfen kann der Vorgang einige Zeit in Anspruch nehmen. Daher empfehlen wir Ihnen die Aufgabe mit niedriger Priotität durchzuführen oder wenn Sie das System nicht verwenden.

- **Benutzerdefinierte Aufgaben** - enthält die Anwender definierten Tasks.

  Eine Aufgabe `Meine Dokumente` steht ebenfalls zur Verfügung.Verwenden Sie diese um die folgenden für den jeweiligen Benutzer wichtigen Ordner zu prüfen: `Eigene Dateien`, `Desktop` und `Autostart`. Dies stellt sicher das Ihre Eigenen Dateien, Ihr Desktop und die beim Starten von Windows geladenen Programme schädlingsfrei sind.

- **Standardaufgaben** - enthält eine Liste verschiedener Prüfoptionen. Diese Optionen weisen auf andere Prüfoptionen hin, die in diesem Fenster nicht ausgeführt werden können. Sie können nur die Einstellungen ändern oder die Prüfberichte ansehen.Folgende Aufgaben stehen zur Verfügung:

  **Geräte-Scan**

  Acronis Internet Security stellt automatisch fest, wenn ein neues Speichergerät an den Computer geschlossen wird und scannt dieses.Nutzen Sie diese Aufgabe, um die Optionen der automatischen Erkennung und der Prüfung von Speichergeräten (CDs/DVDs, USB-Speicher oder Netzlaufwerke) zu konfigurieren.

  **Kontext Prüfung**

  Diese Aufgabe wird ausgeführt, wenn über das Kontextmenü von Windows oder über die Scan-Aktivitätsleiste gescannt wird.Sie können die Scan-Optionen an Ihre Situation anpassen.

- **Inaktive Skan-Aufgaben** - enthält eine Liste von voreingestellten System-Aufgaben, die so eingestellt werden können dass sie laufen, wenn Sie nicht am Computer sind. Bei komplexen Aufgaben kann der Scan-Prozess eine Weile dauern und er wird am besten funktionieren, wenn Sie Ihr System in dieser Zeit nicht nutzen. Deshalb sollten Sie solche Aufgaben für die Zeit terminieren, in denen Ihr Computer in den Ruhemodus gegangen ist.

Sie können die Scan-Aufgaben über die Buttons oder das Verknüpfungs-Menü verwalten.

Um einen System- oder Benutzerdefinierten Scan auszuführen, klicken Sie den entsprechenden **Aufgabe Ausführen** Button.Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

Um festzulegen, dass eine Scan-Aufgabe automatisch ausgeführt wird, klicken Sie auf den Button **Planer** und konfigurieren Sie die Aufgabe wie gewünscht.

Wenn sie eine erstellte Scan Aufgabe nicht mehr benötigen, können Sie diese löschen, indem Sie den **Löschen** Button, zur rechten der Aufgabe.Sie können system oder sonstige Aufgaben nicht entfernen.

Jede Scan-Aufgabe verfügt über ein Eigenschaftenfenster, in dem Sie die Einstellungen konfigurieren und sich die Scan-Protokolle ansehen können.Um das Fenster zu öffnen klicken Sie auf die **Eigenschaften** Schaltfläche, auf der linken Seite der Aufgabe (oder rechtsklicken Sie die Aufgabe und wählen Sie **Eigenschaften**).

Weitere Informationen zu folgenden Themen sind verfügbar:

- *„Konfigurieren der Prüfoptionen“* (S. 56)
- *„Festlegen der Zielobjekte“* (S. 58)
- *„Zeitgesteuerte Aufgaben festlegen“* (S. 59)

## Verwenden des Kontextmenüs

Für jede Aufgabe steht ein Shortcut Menü zur Verfügung. Mit einem rechten Mausklick könne Sie die ausgewählte Aufgabe öffnen.

Für System- und Benutzerdefinierte Aufgaben, sind die folgenden Befehle im Shortcut Menue verfügbar:

- **Jetzt prüfen** - führt die ausgewählte Aufgabe aus und startet eine sofortige Prüfung.
- **Pfad** - Öffnet das **Eigenschaften** Fenster, Reiter Pfad,wo Sie das Prüfziel für die ausgewählte Aufgabe ändern können.Im Falle von Systemaufgaben wird diese Option durch **Aufgabenpfade anzeigen** ersetzt.
- **Ablaufplan** - Öffnet das Fenster **Eigenschaften** , Planer, wo Sie die ausgewählten Aufgaben planen können.
- **Prüfberichte anzeigen** - Öffnet das Fenster **Eigenschaften** , Prüfberichte, in welchem Sie die Berichte sehen, die nach dem Prüfungvorgang erstellt wurden.
- **Aufgabe Klonen** - dupliziert die gewählte Aufgabe.Dies ist sinnvoll, wenn neue Aufgaben erstellt werden, weil die Einstellungen für die wiederholte Aufgabe geändert werden können.
- **Löschen** - löscht die ausgewählte Aufgabe.

  Beachten Sie
  Nur für benutzerdefinierte Aufgaben verfügbar. Voreingestellte Aufgaben können nicht gelöscht werden.

- **Eigenschaften** - Öffnet das Fenster **Eigenschaften**, Übersicht, wo Sie die Einstellungen für die ausgewählte Aufgabe ändern können.

Aufgrund ihrer speziellen Beschaffenheit können nur die Optionen **Eigenschaften** und **Berichtsdateien ansehen** unter dem Punkt **Verschiedene Aufgaben** ausgewählt werden.

## Konfigurieren der Prüfoptionen

Um die Prüfoptionen einer Prüfaufgabe festzulegen klicken Sie mit der rechten Maustaste auf die Aufgabe und wählen Sie **Eigenschaften**.

Sie können die Konfiguration einfach durch das Wählen der Scan-Tiefe festlegen. Ziehen Sie dazu den Zeiger an der Skala entlang, bis Sie den gewünschten Level erreicht haben.Nutzen Sie die Beschreibung auf der rechten Seite, um die Schutzstufe zu wählen, die für Ihre Bedürfnisse am besten geeignet ist.

Sie können auch folgende allgemeine Optionen konfigurieren:

- **Aufgaben mit niedriger Priorität ausführen.** Herabstufung der Priorität des Prüfvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfvorgang dauert damit aber entsprechend länger.
- **Prüfassistent ins System-tray minimieren. .** Das Scan-Fenster wird in die Symbolleiste minimiert. Wenn Sie auf das Acronis Internet Security-Symbol doppelklicken, wird es geöffnet.
- Wählen Sie die Aktion, die durchgeführt werden soll, wenn keine Bedrohungen gefunden wurden:

Erfahrene Anwender möchten sich eventuell näher mit den Scan-Einstellungen von Acronis Internet Security beschäftigen. Der Scanner kann so eingestellt werden, dass nur spezielle Dateiendungen oder spezielle Malware-Bedrohungen gescannt oder Archive übersprungen werden. So werden die Scan-Zeit verringert und die Antwortzeiten Ihres Rechners während eines Scans verbessert.

Konfiguration der Scan-Einstellungen im Detail:

1. Klicken Sie auf **Benutzerdefiniert**.
2. Konfigurieren Sie die Scan-Einstellungen nach Ihren Wünschen.Um herauszufinden was eine Option macht, halten Sie den Mauszeiger darüber und lesen die angezeigte Beschreibung im unteren Teil des Fensters.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach.Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Scan Level.** Definieren Sie die Art von Malware, die Acronis Internet Security scannen soll, indem Sie die passenden Optionen wählen.
- **Dateien prüfen.** Sie können Acronis Internet Security so programmieren, dass alle Dateien und Anwendungen (Programmdateien) oder nur bestimmte

Dateitypen, die Sie als gefährlich einstufen, gescannt werden sollen.Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

Anwendungen (oder Programmdateien) sind weitaus anfälliger gegen Malware-Angriffe als andere Typen oder Dateien.Diese Kategorie beinhaltet die folgenden Dateierweiterungen:`.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

Falls Sie sich für die Option **Anwenderdefinierte Erweiterungen scannen** entscheiden, empfehlen wir, dass Sie neben allen anderen Dateierweiterungen, die Sie als potentiell gefährlich einstufen, auch alle Anwendungserweiterungen mit einschließen.

- **Nur neue und veränderte Dateien prüfen.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Archive prüfen.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit.Die Malware kann Ihr System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird.Wir empfehlen jedoch, diese Option zu nutzen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.

  Beachten Sie

  Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Primäre Aktion.** Legen Sie die durchzuführende Aktion für jede Kategorie von entdeckten Dateien fest, indem Sie die Optionen in dieser Kategorie verwenden.Es gibt drei Kategorien von gefundenen Dateien:

  ▶ **Infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Acronis Internet Security Malware-Signaturen-Datenbank überein.Acronis Internet Security kann im Normalfall Malware-Codes aus einer infizierten Datei entfernen und die Originaldatei wiederherstellen. Diese Aktion wird Desinfektion genannt.

  Beachten Sie

  Malware-Signaturen sind Code-Bruchstücke, die aus aktuellen Malware-Beispielen extrahiert werden. Diese werden von Antiviren-Programmen zum Musterabgleich und zur Aufspürung von Malware verwendet.

Die Acronis Internet Security Malware-Signatur-Datenbank ist eine Sammlung von stündlich durch Acronis Internet Security-Mitarbeiter upgedateten Malware-Signaturen.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert.Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.
- **Verborgene Dateien (Rootkits).** Bitte beachten Sie das es sich bei den versteckten Dateien nicht um die absichtlich von Windows verborgenen Dateien handelt. Die relevanten sind die von speziellen Programmen versteckten, bekannt als Rootkits.Rootkits sind nicht grundsätzlich schädlich. Jedoch werden Sie allgemein dazu benutzt Viren oder Spyware vor normalen Antivirenprogrammen zu tarnen.

Sie sollten die voreingestellten Aktionen für verdächtige Dateien nicht ändern, es sei denn, Sie haben einen guten Grund dafür.

Um eine neue Aktion festzulegen, klicken Sie auf die aktuelle **Erste Aktion** und wählen die gewünschte Option aus dem Menü.Legen Sie eine **Zweite Aktion** fest, die durchgeführt wird, falls die Erste fehlschlägt.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

## Festlegen der Zielobjekte

Sie können das Prüfziel einer **Systemaufgabe** nicht ändern.Sie können nur ihr Prüfziel sehen.Um das Zielobjekt einer bestimmten Prüfaufgabe zu sehen, klicken Sie mit der rechten Maustaste auf die Aufgabe und wählen Sie **Aufgabenpfade anzeigen**.

Um das Prüfziel einer bestimmten Benutzerprüfaufgabe zu bestimmen, rechtsklicken Sie die Aufgabe und wählen **Pfade**. Alternativ, falls Sie bereits im Eigenschaftenfenster der Aufgabe sind, wählen Sie das **Pfade** Tab.

Sie können die Liste mit Lokalen, Netzwerk und Wechseldatenträgern sowie den Dateien und Ordnern einsehen. Alle markierten Objekte werden beim Prüfvorgang durchsucht.

Folgende Aktionen stehen zur Verfügung:

- **Ornder hinzufügen** - öffnet ein Fenster in dem Sie die zu prüfenden Dateien/Ordner auswählen können.

  Beachten Sie

  Ziehen Sie per Drag & Drop Dateien und Ordner auf die Prüfen-Sektion, um diese der Liste der zu prüfenden Objekte zuzufügen.

- **Entfernen** - Löscht die Datei/denOrdner, die/der zuvor ausgewählt wurde.

Ausser dieser Buttons, gibt es weitere Optionen, die das schnelle Auswählen der Scan-Ziele erlauben.

- **Lokale Laufwerke** - prüft die lokalen Laufwerke.
- **Netzlaufwerke** - prüft die verfügbaren Netzwerklaufwerke.
- **Wechseldatenträger** - prüft alle entfernbaren Laufwerke (CD-ROM-Laufwerke, Diskettenlaufwerke, USB-Sticks).
- **Alle Laufwerke** - prüft alle Laufwerke: lokale, entfernbare oder verfügbare Netzwerklaufwerke.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

### Zeitgesteuerte Aufgaben festlegen

Um die Planung einer bestimmten Aufgabe einzusehen oder zu modifizieren, wählen Sie eine Aufgabe und wählen **Planung**. Falls Sie sich bereits im den Eigenschaften der Aufgabe befinden, wählen Sie das **Planer** Register.

Hier können Sie die Einstellungen zum geplanten Prüfvorgang einsehen.

Wenn Sie Prüfvorgänge planen müssen Sie eine der folgenden Optionen auswählen:

- **Nein** - führt den Scan nur auf Anfrage des Nutzers hin durch.
- **Einmal** - führt den Scan nur einmal, zu einem bestimmten Zeitpunkt aus. Definieren Sie den Startzeitpunkt im Feld **Start Datum/Zeit**.
- **Regelmäßig** - führt die Prüfung regelmäßig, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Beginnend mit festgelegtem Datum und Uhrzeit.
- **Beim Systemstart** - führt den Scan nach einer festgelegten Anzahl von Minuten durch, nachdem der Benutzer sich bei Windows eingeloggt hat.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

## 10.3. Konfiguration der Scan-Ausschlüsse

In manchen Fällen wird es nötig sein bestimmte Dateien vom Prüfen auszunehmen. Zum Beispiel wenn Sie EICAR Testdateien von der Echtzeiprüfung ausschließen wollen, oder `.avi` Dateien nicht "on-demand" prüfen möchten.

Acronis Internet Security bietet die Möglichkeit, Objekte vom On-Access oder On-Deman-Scan oder von beidem auszuschließen. Dies soll der Erhöhung der Scan-Geschwindigkeit dienen und Wechselwirkungen mit Ihrer Arbeit vermeiden.

Zwei Arten von Objekten können vom Prüfen ausgenommen werden:

- **Pfade** - Die Datei oder der Ordner (inklusive der enthaltenen Objekte) werden nicht geprüft.

- **Erweiterungen** - alle Dateien mit einer bestimmten Erweiterung werden vom Scan ausgeschlossen, unabhängig von deren Speicherort auf der Festplatte.

Die ausgenommenen Objekte werden nicht geprüft, egal ob der Zugriff von Ihnen oder von einem Programm erfolgt.

**Beachten Sie**

Ausschlüsse werden bei Kontext-Scans NICHT berücksichtigt.Kontextprüfung ist eine Art von On-Demand-Scan: Rechtsklicken Sie auf die zu scannende Datei oder das Verzeichnis und wählen Sie **Mit Acronis Internet Security scannen**.

### 10.3.1. Dateien oder Verzeichnisse vom Scan ausschließen

Um Pfade vom Scan auszuschließen:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Ausschlüsse**.

**Beachten Sie**

In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Für weitere Informationen lesen Sie bitte *„Meine Werkzeuge“ (S. 17)*.

3. Markieren Sie das entsprechende Kästchen, um den Scan-Ausschluss zu ativieren.
4. So Starten Sie den Konfigurationsassistenten:
   - Rechtsklicken Sie auf die Tabelle mit den Dateien und Verzeichnissen und wählen Sie **Neuen Pfad hinzufügen**.
   - Klicken Sie auf den **Hinzufügen**-Button, dieser befindet sich am oberen Ende der Ausschluss Tabelle.
5. Folgen Sie dem Konfigurationsassistenten.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.
   a. Bitte wählen Sie welche Art von Ausnahme Sie erstellen möchten.Dieser Schritt wird nur eingeblendet, wenn Sie zum Starten des Assistenten auf den Button **Hinzufügen** geklickt haben.
   b. Um einen Pfad vom Prüfen auszuschliessen verwenden Sie eine von folgenden Methoden:
      - Klicken Sie auf **Durchsuchen** und wählen Sie den gewünschten Ordner bzw. Datei, klicken Sie dann auf **Hinzufügen**.
      - Geben Sie den Pfad welchen Sie vom Prüfen ausnehmen möchten direkt in das Eingabefeld ein und klicken Sie auf **Hinzufügen**.

Der Pfad erscheint in dem Moment in der Tabelle in welchem Sie ihn hinzufügen. Sie können so viele Pfade hinzufügen wie Sie wünschen.

c. Standardmässig sind die Pfade von beiden Prüftypen ausgenommen, Echtzeitschutz und Prüfvorgang. Um dies zu Ändern klicken Sie auf die entsprechende Anzeige und wählen Sie die gewünschte Option.

d. Es wird dringend empfohlen die Dateien unter den festgelegten Pfaden zu prüfen, um sicherzustellen, dass diese nicht infiziert sind.Bitte markieren Sie das Kontrollkästchen um diese Dateien zu prüfen, bevor Sie von der Prüfung ausgeschlossen werden.

Klicken Sie auf **Beenden**, um die Ausnahme hinzuzufügen.

6. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

## 10.3.2. Dateierweiterungen vom Scan ausschließen

Dateierweiterungen vom Scan ausschließen:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Ausschlüsse**.

### Beachten Sie

In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Für weitere Informationen lesen Sie bitte *„Meine Werkzeuge“ (S. 17)*.

3. Markieren Sie das entsprechende Kästchen, um den Scan-Ausschluss zu ativieren.
4. So Starten Sie den Konfigurationsassistenten:
   - Rechtsklicken Sie auf die Erweiterungen Tabelle und wählen Sie **Neue Erweiterungen hinzufügen**.
   - Klicken Sie auf den **Hinzufügen**-Button, dieser befindet sich am oberen Ende der Ausschluss Tabelle.
5. Folgen Sie dem Konfigurationsassistenten.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

   a. Wählen Sie die Option um eine Dateierweiterung vom Prüfen auszunehmen.Dieser Schritt wird nur eingeblendet, wenn Sie zum Starten des Assistenten auf den Button **Hinzufügen** geklickt haben.

   b. Um die auszunehmenden Erweiterungen festzulegen verwenden Sie eine der folgenden Methoden:

- Wählen Sie die gewünschte Erweiterung aus dem Menü aus und klicken Sie auf **Hinzufügen**.

  **Beachten Sie**
  Das Menü enthält eine Liste der auf Ihrem System vorhandenen Erweiterungen. Wenn Sie eine Erweiterung auswählen erhalten Sie, falls vorhanden, eine Beschreibung zu dieser.

- Geben Sie die gewünschte Erweiterung in das Eingabefeld ein und klicken Sie auf **Hinzufügen**.

  Die Erweiterungen erscheinen in der Tabelle sobald Sie diese hinzufügen. Sie können so viele Erweiterungen hinzufügen wie Sie wünschen.

c. Standardmässig werden die gewählten Erweiterungen von beiden Prüftypen ausgenommen (Echtzeitschutz und Prüfvorgang). Um dies zu klicken Sie auf die entsprechende Spalte und wählen Sie den gewünschten Eintrag.

d. Wir empfehlen dringend, die Dateien mit den festgelegten Erweiterungen zu scannen, um so sicherzustellen, dass sie nicht infiziert sind.

   Klicken Sie auf **Beenden**, um die Ausnahme hinzuzufügen.

6. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

### 10.3.3. Verwaltung von Scan-Ausschlüssen

Werden die konfigurierten Scan-Ausschlüsse nicht mehr benötigt, empfehlen wir, diese zu löschen oder die Scan-Ausschlüsse zu deaktivieren.

Verwaltung von Scan-Ausschlüssen:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Ausschlüsse**.

Um ein Objekt aus der Liste zu entfernen markieren Sie es und klicken Sie dann auf die **Entfernen**-Schaltfläche

Um ein Objekt aus der Liste zu bearbeiten, klicken Sie auf die **Bearbeiten**-Schaltfläche.Ein neues Fenster erscheint in welchem Sie die Erweiterung, den Pfad und den Prüftyp der Ausnahme festlegen können. Wenn Sie die Änderungen vorgenommen haben klicken Sie auf **OK**.

**Beachten Sie**
Sie können das Objekt auch mit der rechten Maustaste anklicken un es zu bearbeiten oder zu löschen.

Um die Scan-Ausschlüsse zu deaktivieren, löschen Sie die entsprechende Check-Box.

## 10.4. Quarantäne

Acronis Internet Security ermöglicht die Isolation von infizierten Dateien in einem sicheren Bereich, der so genannten Quarantäne. Durch die Isolation der infizierten Dateien in der Quarantäne reduziert sich das Risiko einer weiteren Infektion. Die infizierten Dateien können zur genaueren Analyse automatisch oder manuell an das Acronis Internet Security-Labor gesendet werden.

**Beachten Sie**

Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden.

Zudem scannt Acronis Internet Security nach jedem Update der Malware-Signaturen die Dateien der Quarantäne.Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

Anzeige und Verwaltung der Quarantänedateien und Konfiguration derQuarantäneeinstellungen.

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Quarantäne**.

**Beachten Sie**

In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Für weitere Informationen lesen Sie bitte *„Meine Werkzeuge“ (S. 17)*.

### Quarantäne-Dateien verwalten

Sie können jede ausgewählte Datei aus der Quarantäne an das Acronis Internet Security-Labor weiterleiten indem Sie auf **Senden** klicken.Voreingestellt überträgt Acronis Internet Security die Dateien in Quarantäne alle 60 Minuten.

Um eine Quarantäne-Datei zu löschen, markieren Sie diese und klicken dann auf den Button **Löschen**.

Wenn Sie eine Quarantäne-Datei am ursprünglichen Speicherort wiederherstellen möchten, klicken Sie zuerst auf die Datei und dann auf **Wiederherstellen**.

### Quarantäne-Einstellungen konfigurieren

Wenn Sie die Quarantäne-Einstellungen konfigurieren möchten klicken Sie auf **Einstellungen**.Über die Quarantäne-Einstellungen können Sie folgende Aktionen festlegen:

**Alte Dateien löschen.** Um alte Dateien in der Quarantäne automatisch zu löschen aktivieren Sie die entsprechende Option.Sie können festlegen, nach wie vielen Tagen alte Dateien gelöscht werden sollen und wie oft Acronis Internet Security diese überprüfen soll.

**Dateien automatisch senden.** Um Dateien automatisch an das AV Labor zu senden aktivieren Sie die entsprechende Option.Geben Sie an wie oft die Dateien gesendet werden sollen.

**Dateien in der Quarantäne nach einem Update nochmals prüfen.** Um Dateien in der Quarantäne nach einem Update nochmals prüfen zu lassen aktivieren Sie die entsprechende Option.Sie können gereinigte Dateien automatisch an ihrem ursprünglichen Speicherort wiederherstellen, indem Sie **Saubere Dateien wiederherstellen** wählen.

Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

# 11. Antiphishing-Schutz

Die Acronis Internet Security Antiphishing-Funktion schützt Sie davor, dass persönliche Daten während des Surfens ins Internet gelangen können. Der Benutzer wird über potentielle Phishing-Webseiten alarmiert.

Acronis Internet Security bietet den Antiphishing-Schutz in Echtzeit für:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

## 11.1. Konfiguration der Antiphishing White List

Sie können eine White List von Webseiten konfigurieren und verwalten. Die in dieser White Liste gelisteten Webseiten werden dann von der Antiphishing-Engine von Acronis Internet Security nicht gescannt.Die Whitelist sollte nur Webseiten enthalten, denen Sie vollständig vertrauen.Fügen Sie beispielsweise Webseiten hinzu, auf denen Sie häufig einkaufen.

### Beachten Sie

Mit Hilfe der Acronis Internet Security Antiphishing-Toolbar in Ihrem Webbrowser können Sie ganz einfach Webseiten zur White List hinzufügen.Für weitere Informationen lesen Sie bitte *„Handhabung des Acronis Internet Security Antiphishing-Schutzes in Internet Explorer und Firefox“* (S. 66).

Konfigurierung und Verwaltung der Antiphishing White List:

- Wenn Sie einen unterstützten Web Browser verwenden, klicken Sie auf die Acronis Internet Security-Symbolleiste und wählen Sie im Menü **White List**.
- Alternativ folgen Sie diesen drei Schritten:
  1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
  2. Gehen Sie zu **Antivirus > Schild**.
  3. Klicken Sie auf **White List**.

Um eine Seite zur Whitelist hinzuzufügen geben Sie die Adresse in das entsprechende Feld ein und klicken Sie dann auf **Hinzufügen**.

Um eine Webseite aus der Whitelist zu entfernen klicken Sie auf die entsprechende Schaltfläche **Entfernen**.

Klicken Sie auf **Speichern** um die Änderungen zu speichern und das Fenster zu schließen.

## 11.2. Handhabung des Acronis Internet Security Antiphishing-Schutzes in Internet Explorer und Firefox

Acronis Internet Security integriert sich über eine intuitive und einfach anzuwendende Toolbar in die folgenden Web-Browser:

- Internet Explorer
- Mozilla Firefox

Sie können die Antiphishing-Einstellungen und die White List leicht und effizient über die Acronis Internet Security Antiphishing-Leiste in den oben genannten Browsern verwalten.

Die Antiphishing-Leiste, dargestellt durch das Acronis Internet Security-Symbol, befindet sich im oberen Bereich des Browsers.Klicken Sie dieses an um die Leiste anzuzeigen.

**Beachten Sie**
Sollten Sie die Leiste nicht sehen, klicken Sie auf im Menü **Ansicht**, auf **Symbolleisten** und aktivieren Sie **Acronis Internet Security Symbolleiste**.

Folgende Aktionen stehen in der Leiste zur Verfügung:

- **Aktivieren/Deaktivieren** - aktiviert/deaktiviert die Acronis Internet Security Antiphishing-Leiste im aktuellen Browser.
- **Einstellungen** - Öffnet ein Fenster in welchem Sie Einstellungen zur Antiphishingleiste vornehmen können.Die folgenden Optionen sind verfügbar:
  - ▶ **Echtzeit Antiphishing Webschutz** - entdeckt und warnt Sie in Echtzeit wenn eine Webseite "fischt" (also persönliche Informationen stiehlt).Diese Optionen steuert den Acronis Internet Security Antiphishing-Schutz ausschließlich im aktuellen Browser.
  - ▶ **Vor dem Hinzufügen zur Whitelist fragen** - Frägt Sie bevor eine Webseite zur Whitelist hinzugefügt wird.
- **Zu Whitelist hinzufügen** - Fügt die momentane Webseite zur Whitelist hinzu.

**Wichtig**
Durch das Hinzufügen zur White List wird die Seite nicht mehr von Acronis Internet Security auf Phishing gescannt. Wir empfehlen Ihnen nur Seiten hinzuzufügen, denen Sie vollständig vertrauen.

- **White List zeigen** - Öffnet die White List.Für weitere Informationen lesen Sie bitte *„Konfiguration der Antiphishing White List“* (S. 65).
- **Als Phishing protokollieren** - informiert das Acronis Internet Security-Labor dass Sie die fragliche Webseite im Verdacht haben, Datendiebstahl zu

begehen.Durch berichten von phishing Webseiten helfen Sie andere leute gegen Datendiebstahl zu schützen.

- **Hilfe** - Öffnet die Hilfedatei.
- **Über** - öffnet ein Fenster, in dem Sie Informationen über Acronis Internet Security erhalten und Hilfe finden, falls etwas Unvorhergesehenes geschieht.

# 12. Search Advisor

Der Search Advisor erhöht Ihren Online-Schutz gegen Bedrohungen, indem Sie über Phishing-Versuche und nicht vertrauenswürdige Webseiten direkt auf der Ergebnisseite von Suchmaschinen informiert werden.

Der Suchberater funktioniert mit jedem Web Browser und scannt die angezeigten Suchergebnisse der gängigsten Suchmaschinen:

- Google
- Yahoo!
- Bing

Der Search Advisor zeigt an, ob ein Suchabfrageergebnis sicher ist oder nicht, indem vor dem Link ein kleines Statussymbol eingeblendet ist.

**Grüner Kreis mit einem Häkchen:** Sie können den Link sicher öffnen.

**Roter Kreis mit einem Ausrufezeichen:** Dies ist eine Phishing- oder nicht vertrauenswürdige Webseite.Sie sollten diesen Link nicht öffnen.Wenn Sie den Internet Explorer oder Firefox verwenden und versuchen, diesen Link zu öffnen, wird Acronis Internet Security diese Webseite automatisch blockieren und eine Warnseite anzeigen.Wenn Sie die Warnungen ignorieren und auf die Webseite zugreifen wollen, folgen Sie den Anweisungen der Warnseite.

## 12.1. Deaktivierung des Search Advisors

Deaktivierung des Search Advisors:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Präferenzen**.
2. Gehen Sie zu **Sicherheitseinstellungen**.
3. Nutzen Sie den Schalter, um den Search Advisor zu deaktivieren.

# 13. Antispam

Spam ist ein Begriff, den man für unaufgeforderte Emails verwendet.Spam ist ein wachsendes Problem für Heimanwender wie auch für Organisationen. Sie wollen wahrscheinlich nicht, dass Ihre Kinder die meisten dieser Spam-Mails mit häufig pornographischem Inhalt lesen oder dass Sie deswegen sogar in Unannehmlichkeiten geraten. Spam wird immer mehr zum Ärgernis. Daher ist es das Beste, diese Mails gar nicht mehr zu erhalten.

Acronis Internet Security Antispam greift auf außergewöhnliche technologische Innovationen und Standard-Antispam-Filter zurück, um Spams auszusortieren, bevor dieser im Posteingang landen.Für weitere Informationen lesen Sie bitte *„Antispam Einblicke“ (S. 69)*.

Der Acronis Internet Security Antispam-Schutz ist nur für Email Clients verfügbar, die Emails über das POP3-Protokoll zu empfangen.POP3 ist eines der am meisten benutzten Protokolle für das Downloaden der E-Mail-Nachrichten vom Mail-Server.

**Beachten Sie**

Acronis Internet Security bietet keinen Antispam-Schutz für Email-Konten, auf die Sie über einen web-basierten Email-Service zugreifen.

Von Acronis Internet Security aufgespürte Spams werden in der Betreffzeile mit dem `[spam]`-Marker gekennzeichnet.Acronis Internet Security legt Spam-Nachrichten automatisch in einem festgelegten Verzeichnis ab, wie folgt:

- In Microsoft Outlook, Spams werden verschoben in den **Spam** Ordner, zu finden unter **gelöschte Objekte**.Das **Spam**-Verzeichnis wurde während der Installation von Acronis Internet Security erstellt.
- In Outlook Express und Windows Mail, werden Spams direkt in **gelöschte Objekte** verschoben.
- Im Mozilla Thunderbird, werden Spams in den **Spam** Ordner verschoben, der unter **Trash** Ordner zu finden ist.Das **Spam**-Verzeichnis wurde während der Installation von Acronis Internet Security erstellt.

Wenn Sie andere Mail Clients verwenden, müssen Sie eine Regel erstellen, um Email-Nachrichten zu verschieben, die folgendermaßen markiert sind: `[spam]` von Acronis Internet Security in ein benutzerdefiniertes Quarantäne-Verzeichnis verschoben werden.

## 13.1. Antispam Einblicke

### 13.1.1. Antispam Filter

Die Acronis Internet Security Antispam Engine arbeitet mit verschiedenen Filtern, die sicherstellen, dass Ihr Posteingang spamfrei bleibt: Freundeliste, Spammerliste,

Charsetfilter, Bildfilter, URL-Filter, NeuNet (Heuristischer) Filter and Bayesianischer Filter.

## Liste der Freunde/Liste der Spammer

Viele Menschen kommunizieren normalerweise mit einer bestimmten Gruppe von Menschen oder aber erhalten Nachrichten von Firmen oder Organisationen mit derselben Domain. Wird eine **Liste der Freunde bzw. Spammer** geführt, so können Sie festlegen, welche E-Mails Sie erhalten wollen (die von Freunden) und welche Sie nicht erhalten möchten (die von Spammern).

### Beachten Sie

Wir empfehlen, dass Sie die Namen Ihrer Freunde und deren Email-Adressen der **Freundeliste** hinzufügen, damit sichergestellt ist, dass nur solche Emails an Sie weitergeleitet werden. Acronis Internet Security blockt keine Nachrichten von solchen Absendern.

## Zeichensatz-Filter

Viele der Spam-Mails sind in Kyrillisch und/oder Asiatisch geschrieben. Der Schriftsatz-Filter erkannt diese Art von Nachrichten und behandelt diese als SPAM.

## Grafik-Filter

Um die Erkennung von Spam E-Mails durch heuristische Filtermethoden zu erschweren gehen immer mehr Versender von Spam dazu, über nur noch Grafiken zu versenden. Um auch solche E-Mails zu erkennen nutzt der neue **Grafik-Filter** eine Liste mit bereits bekannten Grafiken aus Spam E-Mails und vergleicht diese mit Grafiken aus eingehenden E-Mails. Kommt eine Übereinstimmung zustande so wird die Nachricht als Spam markiert.

## URL-Filter

Viele Spam-Mails enthalten Links zu verschiedenen Webseiten (der Inhalt ist meist kommerziell). In der Acronis Internet Security-Datenbank sind diese Links aufgeführt.

Diese Datenbank wird von Acronis Internet Security ständig aktualisiert.Der URL-Filter prüft jede URL in einer Nachricht und vergleicht Sie mit der Datenbank. Sollten die URLs übereinstimmen wird die Nachricht als SPAM markiert.

## NeuNet-Filter (Heuristik)

Der **Heuristischer Filter** führt eine Reihe von Tests mit allen Nachrichtinhalten durch (z. B. wird nicht nur die Betreffzeile, sondern auch der Nachrichtentext auf HTML-Text überprüft), hält Ausschau nach Wörtern, Phrasen, Links oder anderen Charakteristiken von Spam.Basierend auf dem Resultat der Analyse wird ein SPAM Wert hinzugefügt.

Der Filter erkennt auch Nachrichten welche im Betreff als `Ausdrücklich Sexuel` markiert wurden und markiert diese als SPAM.

### Beachten Sie

Seit dem 19. Mai 2004 müssen E-Mails mit sexuellem Inhalt entsprechend markiert werden `Sexual ausdrücklich:` und in der Betreffzeile muss explizit auf den Inhalt hingewiesen werden.

### Bayesian-Filter

Der **Bayesian-Filter** klassifiziert Nachrichten an Hand von statistischen Informationen bezüglich spezieller Wörter, die in den Nachrichten auftauchen, als Spam oder Nicht-Spam (nach Ihren Vorgaben oder dem heuristischen Filter).

Das bedeutet zum Beispiel, dass es, wenn ein bestimmtes Wort mehrfach erscheint, sich mit hoher Wahrscheinlichkeit um Spam handelt. Alle relevanten Wörter innerhalb einer Nachricht werden einbezogen.

Dieser Filter bietet eine weitere interessante Charakteristik: Er ist lernfähig. Er speichert Informationen einer empfangenen Nachricht eines bestimmten Nutzers. Um korrekt zu funktionieren, benötigt der Filter Training, was bedeutet, dass er mit Mustern von legitimen Nachrichten gefüllt werden sollte. Ab und zu muss der Filter aktualisiert werden, besonders dann, wenn er eine falsche Entscheidung getroffen hat.

### Wichtig

Sie korrigieren den bayesianischen Filter, indem Sie die **Ist Spam** und **Kein Spam** -Schaltflächen in der Antispam Toolbar benutzen.

## 13.1.2. Antispam Vorgang

Die Acronis Internet Security Antispam Engine kombiniert alle Antispam-Filter um festzustellen, ob eine bestimmte Email in den **Posteingang** gelangen sollte, oder nicht.

Jede E-Mail, die aus dem Internet kommt, wird zuerst mit den Filtern Freundesliste/Spammerliste überprüft. Falls der Sender in der Freundesliste gefunden wird, wird diese Mail direkt in Ihren **Posteingang** gesendet.

Der Filter Spammerliste scannt, ob der Absender der Email auf der gleichnamigen Liste eingetragen ist. Falls dem so ist, wird die Email als Spam markiert und in den **Spam**-Verzeichnis verschoben.

Der Zeichensatz-Filter überprüft, ob die E-Mail in Kyrillisch oder mit asiatischen Buchstaben geschrieben worden ist. Falls dem so ist, wird die Mail markiert und in den **Spam**-Ordner verschoben.

Falls die E-Mail diese Merkmale nicht aufweist, wird sie mit dem Grafik-Filter überprüft. Die **Grafik-Filter** erkennt E-Mail-Nachrichten, die Bilder bzw. Grafiken und Spam-Inhalte beinhalten.

DerURL-Filter vergleicht die in Emails gefundenen Links mit den Links der Acronis Internet Security-Datenbank bekannter Spam-Links. Wird eine Übereinstimmung gefunden, wird die Email als SPAM eingestuft.

Der NeuNet/Heuristische Filter testet die Emails auf den Inhalt und sucht nach Wörtern, Phrasen, Links oder anderen Charakteristiken von SPAMs.Basierend auf den Analyseergebnissen erhält die Email eine Spam-Marke.

**Beachten Sie**
Wenn die email in der Betreffzeile als „ausdrücklich sexuell“ gekennzeichnet wurde, stuft Acronis Internet Security die Email als Spam ein.

Der Bayesian-Filter analysiert die Nachricht aufgrund statistischer Informationen in Bezug auf spezielle Wörter und vergleicht diese mit denen, die nicht als Spam klassifiziert sind. Das Ergebnis ist das Hinzufügen eines Spam-Score in die E-Mail.

Wenn das Gesamt-Spam-Ergebnis (heuristische Einstufung + Bayesianische Einstufung) den Schwellenwert übersteigt, wird die Email als SPAM eingestuft.Die Schwelleneinstellung hängt ab von der Antispam Schutzeinstellung.Für weitere Informationen lesen Sie bitte *„Anpassen der Sicherheitsstufe“* (S. 78).

## 13.1.3. Antispam Updates

Bei jedem durchgeführten Update werden:

- werden neue Bildsignaturen zum **Grafik-Filter** hinzugefügt.
- werden neue Links zum **URL-Filter** hinzugefügt.
- werden dem **Heuristik-Filter** neue Regeln hinzugefügt.

Somit wird die Effektivität des AntiSpam-Moduls laufend verbessert.

Für einen fortlaufenden Schutz führt Acronis Internet Security automatische Updates durchführen. Lassen Sie daher die Funktion **Automatische Update** aktiviert.

## 13.1.4. Unterstützte E-Mail-Clients und Protokolle

Der Antispam-Schutz steht für alle POP3/SMTP Email-Clients zur Verfügung.Die Acronis Internet Security Antispam-Toolbar wird integriert in:

- Microsoft Outlook 2003 / 2007 / 2010
- Microsoft Outlook Express
- Microsoft Windows Mail
- Mozilla Thunderbird 3.0.4

Beachten Sie
Acronis Internet Security 2011 scannt keine POP3-Übertragungen von Lotus Notes.

## 13.2. Antispam Optimierungs-Assistent

Beim ersten Start Ihres Mail-Clients nach der Installation von Acronis Internet Security öffnet sich ein Assistent, der Sie dabei unterstützt, den Bayesianischen-Filter zu trainieren, sowie die Freundeliste und die Spammerliste zu konfigurieren, um die Effektivität der Antispamfilter zu erhöhen.

Beachten Sie
Der Assistent kann jederzeit über die Schaltfläche **Assistent** in der Antispam-Toolbaraufgerufen werden.

Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Wenn Sie einen Konfigurationsschritt überspringen möchten, wählen Sie **Überspringen**.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Begrüßungsfenster**
2. **Kontakte zur Freundesliste hinzufügen**

   Hier sehen Sie alle Ihre Adressen aus Ihrem **Adressbuch**. Bitte wählen Sie all die Adressen aus, die Sie Ihrer **Freundesliste** hinzufügen möchten (wir empfehlen Ihnen, alle zu markieren). Sie werden dann alle E-Mails von diesen Adressen erhalten, egal welchen Inhalts.

   Um einen Kontakt zur Freundesliste hinzuzufügen klicken Sie auf **Alle auswählen**.
3. **Bayesianische Daten löschen**

   Beachten Sie
   Wenn Sie den Assistenten das erste Mal ausführen, gehen Sie einfach zum nächsten Schritt.

   Sie finden heraus, dass Ihr Antispam-Filter an Effektivität verloren hat. Dies kann daher kommen, dass das Training nicht genau durchgeführt worden ist (z. B. haben Sie versehentlich eine Anzahl legitimer Mails als Spam markiert oder umgekehrt). Falls Ihr Filter sehr ungenau arbeitet, müssen Sie Ihre Filterkriterien in Ihrer Datenbank löschen und neu anlegen. Dabei hilft Ihnen der Assistent.

   Wählen Sie **Antispam Datenbank leeren**, wenn Sie die bayesianische Datenbank neu starten wollen.

   Sie können die Bayes Datenbank in eine Datei speichern um Sie für andere Acronis Internet Security-Produkte oder nach einer Acronis Internet Security Neuinstallation verwenden zu können.Um die Trainingsdatenbank des bayesischen Filters zu speichern klicken Sie den Button **Bayes speichern** und wählen Sie den gewünschten Speicherort.Die Datei wird `.dat` als Erweiterung haben.

Um eine gsicherte Bayesianische Datenbank zu laden, wählen Sie **Loade Bayes** und öffnen die entsprechende Datei.

4. **Trainieren des Bayesianischen Filters mit legitimen (Nicht-Spam) Emails**

   Bitte wählen Sie einen Ordner, der legitime E-Mails enthält. Diese Nachrichten werden genutzt, um den Antispam Filter zu trainieren.

   Es gibt zwei weitere Optionen unter der Ordnerliste:
   - **Unterordner mit einbeziehen** - Um Unterordner in Ihre Auswahl zu übernehmen.
   - **Automatisch zur Freundesliste hinzufügen** - Um den Sender zu der Liste der Freunde hinzuzufügen.

5. **Trainieren des Bayesianischen Filter mit existierenden Spam-Emails**

   Bitte wählen Sie einen Ordner, der Spam-E-Mails enthält. Diese Nachrichten werden genutzt, um den Antispam-Filter zu trainieren.

   Wichtig

   Bitte vergewissern Sie sich, dass der von Ihnen gewählte Ordner keine legitimen E-Mails enthält, ansonsten wird die Antispam-Leistung beträchtlich reduziert.

   Es gibt zwei weitere Optionen unter der Ordnerliste:
   - **Unterordner mit einbeziehen** - Um Unterordner in Ihre Auswahl zu übernehmen.
   - **Automatisch zur Spamerliste hinzufügen** - Um den Sender zu der Liste der Spamer hinzuzufügen.E-Mail Nachrichten von diesem Sender werden immer als SPAM markiert und dementsprechend verarbeitet.

6. **Übersicht**

   In diesem Fenster können Sie alle Einstellungen einsehen, die mit dem Konfigurationsassistenten durchgeführt worden sind. Sie können noch Änderungen vornehmen, indem Sie zum vorherigen Fenster zurückkehren (**Zurück**).

   Wenn Sie keine Änderungen vornehmen wollen, klicken Sie auf **Fertigstellen**.

## 13.3. Verwendung der Antispam-Symbolleiste im Fenster "Ihr Mail Client"

Im oberen Teil Ihres Mail Client Fensters können Sie die Antispamleiste sehen.Die Antispamleiste hilft Ihnen beim Verwalten des Antispamschutzes direkt vom E-Mail Client aus.Sie können Acronis Internet Security ganz einfach korrigieren, falls eine reguläre Mail als Spam markiert wurde.

Wichtig

Acronis Internet Security integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste.Um die komplette Liste der

unterstützen E-Mail Clients, lesen Sie bitte: *„Unterstützte E-Mail-Clients und Protokolle“ (S. 72)*.

Unten stehend finden Sie eine Beschreibung aller Buttons der Acronis Internet Security-Symbolleiste:

- **Ist Spam** - Klicken Sie auf diesen Button und das bayesianische Modul erkennt die ausgewählten Mails als Spam. Sie werden als Spam markiert und in den **Spam**-Ordner verschoben.

  Zukünftige Mails mit diesem Muster werden alle als Spam markiert.

- **Kein Spam** - teilt dem Bayes-Filter mit, dass die ausgewählte Email kein Spam ist und Acronis Internet Security sie nicht hätte markieren sollen.Die E-Mail wird aus dem **Spam** Ordner ins **Inbox** Ordner verschoben.

  Zukünftige E-Mails mit diesem Muster werden nicht mehr als Spam markiert.

  > **Wichtig**
  > Der Button **Kein Spam** wird aktiv, wenn Sie eine Nachricht als Spam markiert haben von Acronis Internet Security (normalerweise werden diese Nachrichten in den **Spam**-Verzeichnis verschoben).

- **Spammer hinzufügen** - fügt den Absender der ausgewählten E-Mail zur Liste der Spammer hinzu.Klicken Sie zur Bestätigung **OK**.Die E-Mail-Nachrichten, die von den Adressen aus der Spammerliste empfangen werden, werden automatisch markiert als `[spam]`.

- **Freund hinzufügen** - fügt den Sender der ausgewählten E-Mail der Liste der Freunde hinzu.Klicken Sie zur Bestätigung **OK**.Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.

- **Spammer** - Öffnen Sie **Spammerliste**. Sie enthält alle E-Mail-Adressen, von denen Sie keine Nachricht erhalten wollen, gleichwelchen Inhalts.Für weitere Informationen lesen Sie bitte *„Konfigurieren der Spammerliste“ (S. 80)*.

- **Freunde** - Öffnen Sie **Freundenliste**. Sie enthält alle E-Mail-Adressen, von denen Sie immer Nachrichten erhalten wollen, gleichwelchen Inhalts.Für weitere Informationen lesen Sie bitte *„Freundesliste konfigurieren“ (S. 78)*.

- **Einstellungen** - Öffnet das Fenster **Einstellungen**, indem Sie weitere Optionen für das **Antispam**-Modul angeben können.

- **Assistent** - öffnet den Antispam Optimierungs-Assistenten.Mithilfe dieses Assistenten können Sie den Bayes-Filter füttern, um die Effizienz Ihres Antispam-Schutzes zu erhöhen.Sie können auch Adressen auch aus Ihrem Adreesbuch zum Freunde-/Spammer Liste hinzufügen.

- **Acronis Internet Security Antispam** - öffnet ein Fenster, in dem Sie die Antispam-Schutzeinstufung und die Antispam-Filter konfigurieren können.

### 13.3.1. Anzeige von Feststellungsfehler

Wenn Sie einen unterstützten Mail Client verwenden, können Sie einfach den Antispam Filter korrigieren (indem Sie angeben welche E-Mail Nachrichten nicht als [spam]). Dadurch wird die Effektivität des Antispam Filters erheblich verbessert.Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin verschoben werden.
3. Wählen Sie die Nachricht, die von Acronis Internet Security fälschlicherweise als [spam] markiert wurde, aus.
4. Klicken Sie auf **Freund hinzufügen** in der Acronis Internet Security Antispam Toolbar.Klicken Sie zur Bestätigung **OK**.Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.
5. Klicken Sie in der Acronis Internet Security Antispam-Symbolleiste (normalerweiseim oberen Teil des Mail Client-Fensters) auf **Kein Spam**. Dies teilt dem Bayes-Filter, dass die ausgewählte Nachricht kein Spam ist. Die Nachricht wird dann in den Posteingang verschoben.Die nächsten E-Mails, die dem gleichen Muster entsprechen, werden nicht als [spam] markiert.

### 13.3.2. Anzeige unentdeckter Spam-Nachrichten

Wenn Sie einen unterstützten Mail Client verwenden, können Sie einfach angeben, welche E-Mail Nachrichten als Spam hätten markiert werden sollen. Dies wird die Effizienz des Antispam Filters erhöhen.Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Begeben Sie sich zum Inbox Ordner.
3. Wählen Sie die unentdeckte Spam-Nachricht.
4. Klicken Sie in der Acronis Internet Security Antispam-Symbolleiste (normalerweise im oberen Teil des Mail Client-Fensters) auf **Ist Spam**. Dies sagt dem Bayes-Filter dass es sich bei den ausgewählten Nachrichten um eine Spam-Nachricht handelt. Sie wird dann sofort als [spam] markiert und in den Junk Mail-Verzeichnis verschoben.Die nächsten E-Mail-Nachrichten, die die gleiche Muster haben, werden folgendermaßen markiert [spam].

### 13.3.3. Erneutes Trainieren des Bayes Filters

Arbeitet Ihr Antispam-Filter sehr ungenau arbeiten, sollten Sie eventuell die Bayes Datenbank aufräumen und den Bayes Filter neu definieren.

Bevor Sie den Bayesian Filter tranieren, erstellen Sie einen Ordner der einen der legitimen Nachrichten enthält und sonst nur SPAM Nachrichten.Der Bayesian Filter

wird trainiert, indem er sie analysiert und lernt die Charakteristiken, die Spam und legitime Nachrichten definieren, zu unterscheiden. Um die Effektivität des Trainings zu gewährleisten, müssen midestens 50 Nachrichten jeder Kategorie vorhanden sein.

Um die Bayesian Datenbank zurückzusetzen und um es neu zu trainieren, follgen Sie diese Schritte:

1. Öffnen Sie den Mail Client.
2. Klicken Sie in der Acronis Internet Security Antispam-Leiste auf den Button **Assistent**, um den Antispam-Konfigurierungsassistent zu starten.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie **Überspringen** und klicken Sie auf **Weiter**.
5. Wählen Sie **Antispamfilter löschen** un klicken Sie auf **Weiter**.
6. Wählen Sie den Ordner mit legitime Nachrichten und klicken Sie auf **Weiter**.
7. Wählen Sie den Ordner mit SPAM Nachrichten und klicken Sie auf **Weiter**.
8. Klichen Sie auf **Fertigstellen** um mit dem Trainingsprozess zu starten.
9. Nach Abschluss des Trainings, klicken Sie **Schließen**.

### 13.3.4. Speichern und Laden der Bayes Datenbank

Sie können die Bayes Datenbank in eine Datei speichern um Sie für andere Acronis Internet Security-Produkte oder nach einer Acronis Internet Security Neuinstallation verwenden zu können.

Klicken Sie in der Acronis Internet Security Antispam-Symbolleiste auf den Button **Einstellungen**.

Um die Trainingsdatenbank des bayesischen Filters zu speichern klicken Sie den Button **Bayes speichern** und wählen Sie den gewünschten Speicherort.Die Datei wird `.dat` als Erweiterung haben.

Um eine gsicherte Bayesianische Datenbank zu laden, wählen Sie **Loade Bayes** und öffnen die entsprechende Datei.

### 13.3.5. Konfiguration der allgemeinen Einstellungen

Um die allgemeinen Antispam-Einstellungen für Ihren Mail Client zu konfigurieren, klicken Sie auf den Button **Einstellungen** in der Acronis Internet Security Antispam-Symbolleiste.

Die folgenden Optionen sind verfügbar:

- **Nachrichten nach "Gelöschte Objekte" verschieben** verschiebt als Spam erkannte E-Mails in einen Unterordner des **Papierkorbs** (gilt nur für Outlook Express bzw. Windows Mail).

- **Markieren Sie Spam-E-Mail Nachrichten als 'gelesen'** - Markiert die Spam-Nachrichten automatisch als gelesen, so dass sie nicht stören wenn Sie ankommen.

Klicken Sie auf **Alarma**, um Zugriff auf die Sektion haben, in der Sie die Erscheinung des Bestätigungsfensters für **Spammer hinzufügen** und **Freunde hinzufügen** deaktivieren können.

In dem **Alarma** Fenster können Sie den Alarm **Bitte wählen Sie eine E-Mail-Nachricht** aktivieren/deaktivieren.Dieses Alarm erscheint wenn Sie eine Gruppe anstatt einer E-Mail-Nachricht auswählen.

## 13.4. Anpassen der Sicherheitsstufe

Einige der Antispam-Filter können Spam-Emails direkt erkennen, andere fügen der Email eine Spam-Markierung hinzu, die auf den festgestellten Spam-Eigenschaften basiert.

Die Antispam-TresorSicherheitsstufe dient der Einschätzung einer Email als Spam, basierend auf deren Gesamt-Spam-Einstufung (die Sie erhalten, nachdem die Mail durch alle Antispam-Filter gelaufen ist).

Sie sollten die Antispam-TresorSicherheitsstufe nicht verändern, es sei denn, der Antispam-Tresor funktioniert nicht wie erwartet.Bevor Sie aber unabhängig die Tresoreinstellung ändern, empfehlen wir Ihnen, dass Sie sich zuerst den Punkt *„Antispamfilter funkioniert nicht richtig“ (S. 171)* durchlesen, um das Problem zu beheben.

Um die Antispam-Sicherheitsstufe anzupassen:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antispam > Status**.
3. Schieben Sie den Regler in die gewünschte TresorSicherheitsstufen-Position.Sie können das Level für den gewünschten Schutz einstellen. (**Moderat zu Aggressiv**)Klicken Sie **Level anpassen**.

Nutzen Sie die Beschreibung auf der rechten Seite, um die TresorSicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.Die Beschreibung informiert Sie auch über zusätzlichen Aktionen, die Sie durchführen sollten, um mögliche Probleme zu vermeiden oder um die Effizienz des Antispams zu erhöhen.

## 13.5. Freundesliste konfigurieren

**Liste der Freunde** – die Liste aller E-Mail-Adressen, von denen Sie immer Mails erhalten wollen, egal welchen Inhalts diese sind. Nachrichten Ihrer Freunde werden nicht als Spam deklariert, auch wenn der Inhalt dem von Spam ähnlich sein sollte.

### Beachten Sie

Jede Mail von einer Adresse Ihrer **Freundesliste** wird automatisch in Ihren Posteingang verschoben.

Konfigurierung und Verwaltung der Freundeliste:

- Wenn Sie Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird nutzen, klicken Sie auf den Button **Freunde** in der Acronis Internet Security Antispam-Symbolleiste, die in Ihren Mail Client integriert ist.
- Alternativ folgen Sie diesen drei Schritten:
  1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
  2. Gehen Sie zu **Antispam > Status**.
  3. Klicken Sie auf **Freunde verwalten**.

Um eine Email-Adresse hinzuzufügen, wählen Sie die Option **Email-Adresse**, geben Sie die Adresse ein und klicken Sie auf den Button neben dem Bearbeiten-Feld.Syntax: name@domain.com.

Um alle Email-Adressen einer bestimmten Domain hinzuzufügen, wählen Sie die Option **Domain-Name**, geben Sie den Domain-Namen ein und klicken Sie weiter zum Bearbeiten-Feld.Syntax:

- @domain.com, *domain.com und domain.com - alle eingehenden Mails von domain.com werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- *domain* - alle eingehenden Mails von domain werden ohne Überprüfung Ihres Inhaltes in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- *com - alle Mails mit der Endung com werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;

Wir empfehlen, keine kompletten Domains hinzuzufügen, in einigen Situationen kann dies jedoch sinnvoll sein.Sie können beispielsweise die Email-Domain der Firma, für die Sie arbeiten, oder die von vertrauenswürdigen Partnern hinzufügen.

Um einen Eintrag aus der Liste zu entfernen markieren Sie diesen und klicken Sie dann auf **Entfernen**.Um alle Einträge zu löschen, klicken Sie auf **Liste löschen** und danach auf **Ja** um dies zu bestätigen.

Sie können die Liste der Freunde speichern, so das diese auf einen anderen Rechner oder nach einer neuinstallation benutzt werden kann.Um die Freundesliste zu speichern klicken Sie auf **Speichern** und speichern sie diese an den gewünschten Ort.Die Datei wird `.bwl` als Erweiterung haben.

Um eine zuvor gespeicherte Freundesliste zu laden, klicken Sie **Laden** und öffnen die entsprechende `.bwl` Datei.Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Liste beim Laden leeren**.

Klicken Sie auf **Übernehmen** und **OK**, um zu speichern und um die **Freundesliste** zu schließen.

## 13.6. Konfigurieren der Spammerliste

**Liste der Spammer** - Liste die alle E-Mail-Adressen enthält, von denen Sie keine Nachrichten erhalten wollen, gleich welchen Inhalts.Jede Mail von einer Adresse Ihrer **Spammerliste** wird automatisch in Ihren Papierkorb verschoben.

Konfigurierung und Verwaltung der Spammer-Liste:

- Wenn Sie Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird nutzen, klicken Sie auf den Reiter **Spammer** in der Acronis Internet Security Antispam-Symbolleiste, die in Ihren Mail Client integriert ist.
- Alternativ folgen Sie diesen drei Schritten:
  1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
  2. Gehen Sie zu **Antispam > Status**.
  3. Klicken Sie auf **Spammer verwalten**.

Um eine Email-Adresse hinzuzufügen, wählen Sie die Option **Email-Adresse**, geben Sie die Adresse ein und klicken Sie auf den Button neben dem Bearbeiten-Feld.Syntax: name@domain.com.

Um alle Email-Adressen einer bestimmten Domain hinzuzufügen, wählen Sie die Option **Domain-Name**, geben Sie den Domain-Namen ein und klicken Sie weiter zum Bearbeiten-Feld.Syntax:

- @domain.com, *domain.com und domain.com - alle eingehenden Mails von domain.com werden als Spam markiert;
- *domain* - alle eingehenden Mails von domain (egal welcher Endung) werden als Spam markiert;
- *com - alle Mails mit dieser Endung com werden als Spam markiert.

Wir empfehlen, keine kompletten Domains hinzuzufügen, in einigen Situationen kann dies jedoch sinnvoll sein.

### Warnung

Fügen Sie keine legitime Webbasierte E-Mail Anbieter (wie: Yahoo, Gmail, Hotmail oder andere) zu der Spammerliste hinzu. Andernfalls werden die E-Mail-Nachrichten, die von jedem möglichem Benutzer solch eines Anbieters gesendet werden, als Spam eingestufft.z.B: wenn Sie `yahoo.com` zu Spammerliste hinzufügen, werden alle E-Mails die von `yahoo.com` Adressen kommen, als `[spam]` markiert.

Um einen Eintrag aus der Liste zu entfernen markieren Sie diesen und klicken Sie dann auf **Entfernen**.Um alle Einträge zu löschen, klicken Sie auf **Liste löschen** und danach auf **Ja** um dies zu bestätigen.

Sie können die Spammer Liste in eine Datei sichern, damit Sie sie nach einer Neuinstallation oder auf einem anderen Computer nutzen können.Um die Spammerliste zu speichern klicken Sie auf **Speichern** und speichern sie diese an den gewünschten Ort.Die Datei wird `.bwl` als Erweiterung haben.

Um eine zuvor gespeicherte Spammerliste zu laden, klicken Sie **Laden** und öffnen die entsprechende `.bwl` Datei.Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Liste beim Laden leeren**.

Klicken Sie auf **Übernehmen** und **OK**, um zu speichern und um die **Spammerliste** zu schließen.

## 13.7. Konfiguration der Antispam-Filter und -Einstellungen.

Wie in *„Antispam Einblicke“ (S. 69)* beschrieben, nutzt Acronis Internet Security eine Kombination aus unterschiedlichen Antispam-Filtern, um Spams zu identifizieren.Die Antispam-Filter sind für einen effizienten Tresor vorkonfiguriert.

Sie können jeden dieser Filter deaktivieren oder dessen Einstellungen verändern, dies wird jedoch nicht empfohlen.Dies sind einige Änderungen, die Sie eventuell vornehmen möchten:

- Abhängig davon, ob Sie legitime Emails mit asiatischen oder kyrillischen Zeichen erhalten, aktivieren oder deaktivieren Sie die Einstellung, die solche Emails automatisch abblockt.

  **Beachten Sie**

  Die entsprechende Einstellung ist in den lokalisierten Programmversion deaktiviert, die solche Zeichensätze verwendetn(wie z. B. in der russischen oder chinesischen Programmversion).

- Wenn Sie nicht möchten, dass der Empfänger Ihrer gesendeten Email automatisch der Freundeliste hinzugefügt wird, können Sie die entsprechende Einstellung deaktivieren.In diesem Fall fügen Sie Ihre Kontakte der Freundeliste wie in *„Freundesliste konfigurieren“ (S. 78)* beschrieben hinzu.

- Fortgeschrittene Anwender können versuchen, die Größe des Bayes-Wörterbuches anzupassen, um so bessere Antispam-Ergebnisse zu erzielen.Eine geringere Anzahl an Worten resultiert in einer schnelleren, aber weniger präzisen Antispam-Verarbeitung.Eine höhere Anzahl an Wörtern erhöht die Genauigkeit des Antispams, dadurch wird aber auch die Zugriffszeit auf Ihre Emails länger.

  **Beachten Sie**

  Es können mehrere Anpassungen des Bayes-Wörterbuches notwendig sein, um das gewünschte Ergebnis zu erzielen.Wenn das Ergebnis nicht wie erwartet ist, setzten Sie die Voreinstellung auf die empfohlene Größe von 200.000 Wörtern zurück.

Um die Antispam-Einstellungen und Filter zu konfigurieren:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antispam > Einstellungen**.
3. Konfigurieren Sie die Einstellungen nach Ihren Wünschen. Um herauszufinden was eine Option macht, halten Sie den Mauszeiger darüber und lesen die angezeigte Beschreibung im unteren Teil des Fensters.
4. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Wenn Sie die Standardeinstellungen anwenden möchten, klicken Sie auf **Standard**.

# 14. Kindersicherung

Die Acronis Internet Security Kindersicherung ermöglicht es Ihnen den Zugriff auf dasInternet und auf bestimmte Programme für jeden Benutzer mit einem Benutzerkontoauf dem System zu kontrollieren.

Sie können die Kindersicherung so konfigurieren, dass Folgendes blockiert wird:

- Unangemessene Webseiten.
- Den Internetzugang zu bestimmten Zeiten (beispielsweise während der Schule).
- Web-Seiten, Mails und Sofortnachrichten mit bestimmten Schlüsselwörtern.
- Anwendungen wie Spiele, Chat, Filesharing-Programme oder Andere.
- Sofortnachrichten, die von nicht erlaubten IM-Kontakten gesendet werden.

**Wichtig**

Nur Benutzer mit administrativen Rechten (Systemadministratoren) können auf die Kindersicherung zugreifen und sie konfigurieren.Um sicherzustellen, dass nur Sie die Einstellungen der Kindersicherung für alle Benutzer ändern können, sichern Sie sie mit einem Passwort.Sie werden dazu aufgefordert, das Passwort zu konfigurieren, wenn Sie die Kindersicherung für einen bestimmten Benutzer aktivieren.

Sobald Sie die Kindersicherung konfiguriert haben, können Sie einfach herausfinden, was Ihre Kinder auf dem Computer machen.

## 14.1. Kindersicherung konfigurieren

Bevor Sie mit der Konfiguration der Kindersicherung beginnen, erstellen Sie bitte für jedes Kind ein separates Benutzerkonto. Dadurch wissen Sie genau, was jedes Ihrer Kinder auf dem Computer macht. Sie sollten beschränkte (Standard) Benutzerkonten erstellen, so dass Ihre Kinder die Einstellungen der Kindersicherung nicht ändern können.Für weitere Informationen lesen Sie bitte *„Wie erstelle ich ein Windows Benutzerkonto?“* (S. 160).

Haben Ihre Kinder Zugriff auf ein Administrator-Benutzerkonto auf ihrem Computer, müssen Sie ein Passwort festlegen, um die Einstellungen der Kindersicherung zu schützen.Für weitere Informationen lesen Sie bitte *„Tresor der Kindersicherungs-Einstellungen“* (S. 85).

Konfiguration der Kindersicherung:

1. Stellen Sie sicher, dass Sie auf dem Computer eingeloggt sind, auf dem sich das Administrator-Benutzerkonto befindet.Nur Benutzer mit administrativen Rechten (Systemadministratoren) können auf die Kindersicherung zugreifen und sie konfigurieren.
2. Öffnen Sie Acronis Internet Security.

3. Abhängig von der gewählten Ansicht greifen Sie auf die Kindersicherung wie folgt zu:

   Standard-Ansicht
   Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Kindersicherung**.

   Experten-Ansicht
   Klicken Sie im linken Menü auf **Kindersicherung**.

Beachten Sie

In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Für weitere Informationen lesen Sie bitte *„Meine Werkzeuge“* (S. 17).

Sie können Informationen bezüglich des Status der Kindersicherung für jedes WindowsBenutzerkonto einsehen.Die Alterskategorie erscheint unterhalb jedes Benutzernamens, wenn die Kindersicherung aktiviert ist.Wenn die Kindersicherung deaktiviert, ist der Status **nicht konfiguriert**.

Konfiguration der Kindersicherung für ein bestimmtes Benutzerkonto:

1. Verwenden Sie den Regler, um die Kindersicherung für dieses Benutzerkontozu aktivieren.
2. Sie werden aufgefordert, das Passwort für die Kindersicherung festzulegen.Stellen Sie ein Passwort ein, um Ihre Einstellungen für die Kindersicherung zu schützen.Für weitere Informationen lesen Sie bitte *„Tresor der Kindersicherungs-Einstellungen“* (S. 85).
3. Stellen Sie die Alterkategorie so ein Ihrem Kind den Zugriff auf Webseiten nur seinem Alter gemäß zu gestatten.Durch die Angabe des Kindesalters werden automatisch für diese Altersstufe als geeignet eingeschätzte Einstellungen geladen. Diese Einstellungen basieren auf der Standard-Entwicklung von Kindern.
4. Wenn Sie die Einstellungen für die Kindersicherungen im Detail konfigurieren möchten, klicken Sie auf **Einstellungen**.Klicken Sie auf einen Reiter, um die entsprechenden Kindersicherungs-Funktionen zu konfigurieren.

   - **Web-Kontrolle** - um die Web-Navigation gemäß der von Ihnen festgelegten Regeln in dem Bereich Web zu filtern.
   - **Programm-Kontrolle** - blockiert den Zugang zu Programmen, die Sie in dem Abschnitt Programme festgelegt haben.
   - **Stichwort-Filter** - um den Web-, Mail- und Instant Messaging-Zugriff nach den Regeln zu filtern, die Sie im Abschnitt Stichwörter festgelegt haben.
   - **Messaging** - um den Chat mit IM-Kontakten, entsprechend der von Ihnen im Abschnitt Messaging festgelegten Regeln zu erlauben oder zu sperren.

Konfigurieren Sie die Überwachungsoptionen nach Ihren Bedürfnissen:

- **Sende mir einen Aktivitätsbericht per E-Mail.** Eine Email-Benachrichtigung wird versendet, sobald die Acronis Internet Security-Kindersicherung eine Aktivität dieses Nutzers blockiert hat.Sie müssen zuerst die Benachrichtigungseinstellungen konfigurieren.
- **Ein Internet Datenverkehrs Log speichern.** Protokolliert die besuchten Webseiten für Benutzer, für die die Kindersicherung aktiviert ist.

Für weitere Informationen lesen Sie bitte *„Kinderaktivität überwachen“ (S. 91)*.

### 14.1.1. Tresor der Kindersicherungs-Einstellungen

Wenn Sie nicht der einzige Benutzer des Computers mit administrativen Rechten sind, empfehlen wir Ihnen, Ihre vorgenommenen Einstellungen der Kindersicherung mit einem Passwort zu schützen.Wenn Sie ein Passwort festlegen, können andere Benutzer mit administrativen Rechten die Einstellungen der Kindersicherung nicht verändern.

Acronis Internet Security wird Sie nach der Festlegung eines Passwortes fragen, sobald Sie dieKindersicherung aktivieren.Um den Passwortschutz einzustellen, befolgen Sie die folgenden Schritte:

1. Geben Sie das Passwort in das Feld **Passwort** ein.
2. Geben Sie das Passwort erneut in das Feld **Passwort wiederholen** ein, um es zu bestätigen.
3. Klicken Sie auf **OK**, um das Passwort zu speichern und das Fenster zu schließen.

Von nun an werden Sie stets aufgefordert, Ihr Passwort einzugeben, wenn Sie die Einstellungen der Kindersicherung ändern wollen.Andere Systemadministratoren (falls vorhanden) müssen dieses Passwort ebenfalls angeben um Einstellungen der Kindersicherung zu ändern.

**Beachten Sie**
Dieses Passwort schützt nicht die anderen Einstellungen von Acronis Internet Security.

Wenn Sie kein Passwort definieren wollen und nicht möchten, dass dieses Fenster erneut eingeblendet wird, aktivieren Sie die Option **Nicht nach Passwort fragen,wenn die Kindersicherung aktiviert wird**.

**Wichtig**
Wenn Sie das Passwort vergessen haben, müssen Sie das Programm neu installieren oder sich an unseren Kundendienst wenden.

Entfernen des PasswortTresores:

1. Öffnen Sie Acronis Internet Security und klicken Sie in der rechten oberen Bildschirmecke auf **Optionen**.
2. Gehen Sie zu **Allgemeine Einstellungen**.
3. Über den Schalter können Sie die Option **Passworteinstellungen** deaktivieren.
4. Geben Sie das Passwort ein.
5. Klicken Sie auf **OK**.

### 14.1.2. Web Kontrolle

Die **Web-Seiten-Kontrolle** ermöglicht Ihnen, Web-Seiten mit fragwürdigem Inhalt zu sperren. Eine Liste geblockter Webseiten und Teilbereichen ist Ihnen bereits zur Verfügung gestellt und im Verlauf des normalen Update-Prozesses konstant erneuert.

**Beachten Sie**
Wenn Sie die Kindersicherung aktivieren und das Alter Ihres Kindes festlegen, wird die Internetkontrolle automatisch aktiviert und konfiguriert, um den Zugriff auf für das Alter Ihres Kindes unangemessene Webseiten zu blockieren.

Konfiguration der Internetkontrolle für ein bestimmtes Benutzerkonto:

1. Öffnen Sie das Einstellungen-Fenster der Acronis Internet Security-Kindersicherung für das entsprechende Benutzerkonto.
2. Klicken Sie auf den Reiter **Internet** .
3. Nutzen Sie den Schalter um die Internetkontrolle zu aktivieren.
4. Sie können nun überprüfen, welche Web-Kategorien für die aktuell ausgewählteAltersgruppe automatisch gesperrt/beschränkt werden.Wenn Sie mit den Standardeinstellungen nicht zufrieden sein sollten, können Sie diese nach Ihren Wünschen konfigurieren.

   Um die Aktion, die für bestimmte Kategorien von Webinhalten definiert wurde, zu ändern, klicken Sie auf den aktuellen Status und wählen Sie im Menü die gewünschte Aktion.
5. Wenn Sie eigene Regeln erstellen möchten, um bestimmte Webseiten zu blockieren oder zuzulassen.Wenn die Kindersicherung automatisch den Zugriff auf eine Webseite blockiert, können Sie eine Regel definieren, die den Zugriff auf diese Webseite explizit erlaubt.
6. Sie können Limits definieren, wie lange Ihr Kind im Internet surfen darf.Für weitere Informationen lesen Sie bitte „Zeitliche Beschränkung des Internetzugangs“ (S. 87).

### Web-Kontroll Regel erstellen

Um den Zugriff auf eine Webseite zu blockieren oder zu erlauben, folgen Sie diesen Schritten:

1. Klicken Sie auf **Webseite zulassen** oder **Webseite blockieren**.
2. Geben Sie die Webseiten Adresse in das **Webseite** Feld ein.
3. Wählen Sie die gewünschte Aktion für diese Regel aus - **Erlauben** oder **Blocken**.
4. Klicken Sie auf **Beenden** um die Regel hinzuzufügen.

### Web-Kontroll Regeln verwalten

Die bereits konfigurierten Webseitenkontrollregeln sind in der Tabelle am unteren Rand des Fensters aufgelistet. Die Adresse und der aktulle Status jeder Webkontroll-Regel sind aufgelistet.

Um eine Regel zu löschen, markieren Sie diese und klicken auf **Entfernen**.

Um eine Regel zu bearbeiten, markieren Sie diese und klicken auf **Bearbeiten** oder doppelklicken Sie auf die entsprechende Regel.Nehmen Sie die notwendigen Änderungen im Konfigurationsfenster vor.

### Zeitliche Beschränkung des Internetzugangs

Im Bereich "Internetzugriff festlegen" können Sie definieren, wie viel Zeit Ihr Kind im Internet surft.

Um den Zugriff auf das Internet komplett zu sperren, wählen Sie **Internetzugriff sperren**.

Um Beschränkung des Internetzugangs auf bestimmte Tageszeiten festzulegen:

1. Wählen Sie **Zeitlimit Internetzugang**.
2. Klicken Sie auf **Terminplan ändern**.
3. Wählen Sie im Raster die Zeitintervalle, in denen der Internetzugriff blockiert sein soll.Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren.
4. Klicken Sie auf **Speichern**.

**Beachten Sie**
Acronis Internet Security führt unabhängig davon, ob der Internetzugriff gesperrt ist, stündliche Updates durch.

## 14.1.3. Programmkontrolle (Anwendungskontrolle)

Die **Programm-Kontrolle** unterstützt Sie bei der Sperrung jeglicher Programmanwendungen. Spiele, Medien- und Messaging Software als auch andere

Kategorien von Programmen oder gefährlicher Software können auf diesem Wege blockiert werden. Programme, die über diesen Weg gesperrt sind, können weder verändert, kopiert noch verschoben werden.Sie können Anwendungen permanent blocken oder nur für bestimmte Zeitintervalle, wie solche in denen Ihre Kinder Hausaufgaben zu erledigen haben.

Konfiguration der Programmkontrolle für ein bestimmtes Benutzerkonto:

1. Öffnen Sie das Einstellungen-Fenster der Acronis Internet Security-Kindersicherung für das entsprechende Benutzerkonto.
2. Klicken Sie auf den Reiter **Anwendungen**.
3. Aktivieren Sie die Programmkontrolle.
4. Erstellen Sie für die Anwendungen, die Sie sperren oder beschränken möchten, Regeln.

## Anwendungskontrollregeln erstellen

Um den Zugriff auf eine Anwendung zu beschränken oder zu blockieren, befolgen Sie diese Schritte:

1. Klicken Sie auf **Anwendung blockieren** oder **Anwendung beschränken**.
2. Klicken Sie **Durchsuchen** um die Anwendung, für die Sie den Zugriff blockieren/einschränken wollen, herauszusuchen.Installierte Anwendungen befinden sich in Normalfall im Verzeichnis `C:\Programmdateien`.
3. Wählen Sie die Aktion der Regel:
   - **Dauerhaft blockieren** um den Zugriff auf die Anwendung vollständig zu blockieren.
   - **Blockieren basierend auf dieser Planung** um den Zugriff für bestimmte Zeitintervalle einzuschränken.

   Wenn Sie sich entscheiden den Zugriff einzuschränken statt die Anwendung komplett zu blockieren, so müssen Sie im Planungsgitter die Tage und das Zeitintervall auswählen währenddessen der Zugriff blockiert ist.
4. Klicken Sie auf **Speichern**, um die Regel hinzuzufügen.

## Anwendungs-Kontrolle Regeln verwalten.

Die bereits erstellten Anwenungskontrollregeln werden in der Tabelle am unteren Ende des Fensters aufgelistet. Es wird für jede Regel der Name der Anwendung, der Pfad und der aktuelle Status aufgelistet.

Um eine Regel zu löschen, markieren Sie diese und klicken auf **Entfernen**.

Um eine Regel zu bearbeiten, markieren Sie diese und klicken auf **Bearbeiten** oder doppelklicken Sie auf die entsprechende Regel.Nehmen Sie die notwendigen Änderungen im Konfigurationsfenster vor.

### 14.1.4. Schlüsselwortkontrolle

Mit der Schlüsselwortfilterung können Sie den Zugang zu E-Mail Nachrichten, Webseiten und Sofortnachrichten, die bestimmte Wörter enthalten, blockieren.Mit der Schlüsselwortfilterung können Sie verhindern, dass Ihre Kinder unangemessene Wörter oder Sätze sehen, wenn sie online sind.Zusätzlich können Sie sicher stellen dass sie keine persönlichen Daten (z.B. Adresse oder Telefonnummer) an Leute geben, die sie im Internet getroffen haben.

**Beachten Sie**
Die Schlüsselwortfilterung für Instant Messaging ist nur für Yahoo Messenger und Windows Live (MSN) Messenger verfügbar.

Konfiguration der Schlüsselwortkontrolle für ein bestimmtes Benutzerkonto:

1. Öffnen Sie das Einstellungen-Fenster der Acronis Internet Security-Kindersicherung für das entsprechende Benutzerkonto.
2. Klicken Sie auf den Reiter **Schlüsselwörter**.
3. Aktivieren Sie die Schlüsselwortfilterung.
4. Definiere Schlüsselwörter-Kontroll Regeln, um die Anzeige von unangebrachten Wörtern oder das Senden von wichtigen Informationen zu verhindern.

#### Erstellen von Regeln für die Schlüsselwortfilterung

Um ein Wort oder eine Phrase zu blockieren folgen Sie diesen Schritten:

1. Klicken Sie auf **Schlüsselwort blockieren**.
2. Schlüsselwort Informationen eingeben.

   Hier können Sie die Parameter auswählen:

   - **Schlüsselwort Kategorie** - tippen Sie den Namen der Regel in dieses Feld.
   - **Schlüsselwort** - geben Sie das Wort oder den Satzteil, den Sie blockieren möchten, in das Feld ein.Wenn Sie möchten dass nur ganze Wörter erkannt werden, wählen Sie **ganze Wörter** Kontrollkästchen.
3. Wählen Sie den Filtertyp.
   - **Blockiere Anzeige** - Wählen Sie diese Option für Regeln, die geschaffen wurden um die Anzeige unangemessener Wörter zu verhindern.
   - **Senden blockieren** - wählen Sie diese Option für Regeln, die geschaffen wurden um zu verhindern, dass wichtigen Informationen versendet werden.

4. Wählen Sie den Datenverkehrstyp, den Acronis Internet Security nach den definierten Wortenscannen soll.

| Optionen | Beschreibung |
|---|---|
| **Web** | Internet Seiten, die Schlüsselwörter enthalten, werden geblockt. |
| **E-Mail** | E-Mail Nachrichten, die das Schlüsselwort enthalten werden blockiert. |
| **Instant Messaging** | Sofortnachrichten, die das Schlüsselwort enthalten werden blockiert. |

5. Klicken Sie auf **Beenden** um die Regel hinzuzufügen.

Ab jetzt wird jeder Versuch, spezifizierte Daten (über Email, Instant Messaging odereine Webseite) zu senden, fehlschlagen. Es wird ein Warnhinweis eingeblendet, dass Acronis Internet Security nicht zugelassen hat, dass identitätsspezifische Inhalte versendet wurden.

### Regeln für die Schlüsselwortfilterung verwalten

Die konfigurierten Schlüsselwortfilterregeln werden in der Tabelle aufgelistet. Dort finden Sie detaillierte Informationen zu jeder Regel.

Um eine Regel zu löschen, markieren Sie diese und klicken auf **Entfernen**.

Um eine Regel zu bearbeiten, markieren Sie diese und klicken auf **Bearbeiten** oder doppelklicken Sie auf die entsprechende Regel.Nehmen Sie die notwendigen Änderungen im Konfigurationsfenster vor.

## 14.1.5. Instant Messaging (IM) Kontrolle

Die Instant Messaging (IM) Kontrolle gibt Ihnen die Möglichkeit IM-Kontakte festzulegen, mit denen Ihre Kinder chatten dürfen.

**Beachten Sie**

Die IM-Kontrolle ist nur für Yahoo Messenger und Windows Live (MSN) Messenger verfügbar.

Konfiguration der IM-Kontrolle für ein bestimmtes Benutzerkonto:

1. Öffnen Sie das Einstellungen-Fenster der Acronis Internet Security-Kindersicherung für das entsprechende Benutzerkonto.
2. Klicken Sie auf den Reiter **Messaging**.
3. Aktivieren Sie die Option Instant Messaging-Kontrolle.

4. Wählen Sie die bevorzugte Filtermethode und erstellen Sie die entsprechenden Regeln nach Ihren Wünschen.

   - **IM mit allen Kontakten zulassen, außer denen, die sich auf der Liste befinden.**

     In diesem Fall müssen Sie die IM-IDs angeben, die blockiert werden sollen (Menschen, mit denen Ihr Kind nicht kommunizieren sollte).

   - **IM mit alle Kontakten blockieren, außer denen, die sich auf der Liste befinden**

     In diesem Fall müssen Sie die IM-IDs, mit denen Ihr Kind über Instant Messagingkommunizieren darf, ausdrücklich festlegen.Sie können beispielsweise Instant Messaging mit Familienmitgliedern, Schulfreunden oder Nachbarn erlauben.

     Diese zweite Option wird empfohlen, wenn Ihr Kind unter 14 Jahren alt ist.

### Erstellen von Instant Messaging (IM)Kontroll-Regenl

Um IM-Konversationen mit einem Kontakt zu erlauben oder zu blockieren, folgen Sie diesen Schritten:

1. Klicken Sie auf **IM-ID blockieren** oder **IM-ID zulassen**.
2. Geben Sie die E-Mail Adresse oder den Nutzernamen, der von dem IM Kontakt genutzt wird, in das Feld **E-Mail oder IM ID** ein.
3. Wählen Sie das Chatprogramm das der Kontakt verwendet.
4. Wählen Sie die gewünschte Aktion für diese Regel aus - **Erlauben** oder **Blocken**.
5. Klicken Sie auf **Beenden** um die Regel hinzuzufügen.

### Erstellen von Instant Messaging (IM)Kontroll-Regeln

Die konfigurierten IM-Kontrollregeln werden in der Tabelle unten im Bildschirmfensteraufgelistet.

Um eine Regel zu löschen, markieren Sie diese und klicken auf **Entfernen**.

Um eine Regel zu bearbeiten, markieren Sie diese und klicken auf **Bearbeiten** oder doppelklicken Sie auf die entsprechende Regel.Nehmen Sie die notwendigen Änderungen im Konfigurationsfenster vor.

## 14.2. Kinderaktivität überwachen

Acronis Internet Security hilft Ihnen dabei festzustellen, was Ihre Kinder am Computer tun, auch wenn Sie nicht zu Hause sind.

Als Voreinstellung werden bei aktivierter Kindersicherung die Aktivitäten Ihrer Kinder aufgezeichnet. So wissen Sie jederzeit, welche Webseiten Ihre Kinder besucht,

welche Anwendungen sie verwendet haben und welche Aktivitäten von der Kindersicherung blockiert wurden etc.

Sie können Acronis Internet Security auch so konfigurieren, dass Sie eine Email-Benachrichtigungerhalten, wenn die Kindersicherung eine Aktivität blockiert.

### 14.2.1. Überprüfen der Kindersicherungsprotokolle

Eine Aufzeichnung darüber, was Ihre Kinder kürzlich auf dem Computer gemacht haben, finden Sie im Kindersicherungsprotokoll.Folgen Sie diesen Schritten:

1. Öffnen Sie Acronis Internet Security.
2. Klicken Sie unten rechts im Fenster auf den Link **Protokolle ansehen**.
3. Klicken Sie im linken Menü auf **Kindersicherung**.

Beachten Sie

Diese Protokolle können Sie auch aus dem Fenster der Kindersicherung heraus öffnen, indem Sie auf **Protokolle ansehen** klicken.

Wenn Ihre Kinder und Sie nicht denselben Computer benutzen, können Sie das Acronis Internet Security-Heimnetzwerk so konfigurieren, dass Sie per Fernabfrage auf die Kindersicherungsprotokolle zugreifen können (von Ihrem Computer aus).Für weitere Informationen lesen Sie bitte *„Heimnetzwerk“ (S. 142)*.

Das Kindersicherungsprotokoll bietet detaillierte Informationen über die Aktivitäten Ihrer Kinder auf dem Computer und im Internet.Die Information befinden sich in mehreren Reitern:

**Allgemein**

Bietet allgemeine Informationen über die kürzlichen Aktivitäten Ihrer Kinder, wie beispielsweise die am häufigsten aufgerufenen Webseiten und die am häufigsten verwendeten Anwendungen.

Sie können Informationen nach Benutzer und Zeitspanne filtern.

**Anwendungsprotokoll**

Hilft Ihnen herauszufinden, welche Anwendungen Ihre Kinder kürzlich aufgerufenhaben.

Doppelklicken Sie auf die Ereignisse in der Liste, um weitere Details zu erhalten.Um einen Protokolleintrag zu löschen, rechtsklicken Sie auf ihn und wählen **Löschen**.

**Internetbericht**

Hilft Ihnen herauszufinden, welche Webseiten Ihre Kinder kürzlich aufgerufen haben.

Sie können Informationen nach Benutzer und Zeitspanne filtern.

**Andere Ereignisse**

Hier erhalten Sie detaillierte Informationen über die Kindersicherungsaktivitäten (wie beispielsweise die Kindersicherung aktiviert/deaktiviert wird, welche Ereignisse gesperrt wurden).

Doppelklicken Sie auf die Ereignisse in der Liste, um weitere Details zu erhalten.Um einen Protokolleintrag zu löschen, rechtsklicken Sie auf ihn und wählen **Löschen**.

## 14.2.2. E-Mail-Benachrichtigungen konfigurieren

Um Email-Benachrichtigungen zu erhalten, wenn die Kindersicherung eine Aktivitätsperrt:

1. Öffnen Sie Acronis Internet Security.
2. Abhängig von der gewählten Ansicht greifen Sie auf die Kindersicherung wie folgt zu:

   Standard-Ansicht

   Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Kindersicherung**.

   Experten-Ansicht

   Klicken Sie im linken Menü auf **Kindersicherung**.

   Beachten Sie

   In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Für weitere Informationen lesen Sie bitte *„Meine Werkzeuge“ (S. 17)*.

3. Wählen Sie in den Einstellungen die Option **Aktivitätsbericht per Email senden**.
4. Sie werden aufgefordert die E-Mail-Kontoeinstellungen zu konfigurieren. Klicken Sie **Ja** um das Konfigurationsfenster zu öffnen.

   Beachten Sie

   Sie können das Konfigurationsfenster später öffnen indem Sie **Benachrichtigungseinstellungen** klicken.

5. Geben Sie die Email-Adresse, an die Benachrichtigungen gesendet werden sollen, ein.
6. Konfigurieren Sie die Email-Einstellungen des Servers, der für die Email-Benachrichtigungen genutzt wird.

Für die Konfiguration der Email-Einstellungen stehen drei Optionen zur Verfügung:

**Aktuelle Client-Einstellungen verwenden**

Diese Option ist voreingestellt, wenn Acronis Internet Security die Mail Server-Einstellungen von Ihrem Mail Client importieren kann.

Klicken Sie zur Bestätigung der Eingaben auf **Einstellungen testen**. Tretenwährend der Bestätigung Probleme auf, werden Sie darüber informiert, was Sietun müssen, um diese zu beheben.

**Aus einem der bekannten Server auswählen**

Wählen Sie diese Option, wenn Sie einen Email-Account bei einem der in der Liste genannten web-basierten Dienste haben.

Klicken Sie zur Bestätigung der Eingaben auf **Einstellungen testen**. Tretenwährend der Bestätigung Probleme auf, werden Sie darüber informiert, was Sietun müssen, um diese zu beheben.

**Ich möchte die Server-Einstellungen selbst konfigurieren.**

Wenn Sie die Mail Server-Einstellungen kennen, wählen Sie diese Option und konfigurieren Sie die Einstellungen wie folgt:

- **Ausgehnder SMTP Server** - geben Sie die Adresse des Mail Servers, der für das Verschicken der E-Mails zuständig ist, ein.
- Falls der Server einen anderen als den Standardport 25 nutzt, geben Sie diesen bitte im entsprechenden Feld an.
- Falls der Server Authentifikation verlangt, wählen Sie **Mein SMTP Server erfordert Authentifikation** aus und geben den Benutzernamen und das Passwort in die dazugehörigen Felder ein.

Klicken Sie zur Bestätigung der Eingaben auf **Einstellungen testen**. Tretenwährend der Bestätigung Probleme auf, werden Sie darüber informiert, was Sietun müssen, um diese zu beheben.

Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

# 15. Privatsphärekontrolle

Acronis Internet Security überwacht dutzende von möglichen Angriffspunkten (sog. "HotSpots") in Ihrem System, die durch Spyware befallen werden könnten. Es überprüft zudem jede Veränderung des Systems und der vorhandenen Software. Bekannte Spyware-Programme werden in Echtzeit blockiert. Die AntiSpyware ist effektiv in der Bekämpfung von Trojanischen Pferden anderen von Hackern installierten Tools, die versuchen Ihre Privatshpäre kompromittieren und Ihr persönlichen Daten wie z.B. Kreditkarennummern, von Ihrem Computer zum Hacker zu senden.

Die Privatsphäre-Funktion beinhaltet folgende Komponenten.

- Identitätskontrolle - stellt sicher, dass persönliche Informationen nicht ohne Ihre Zustimmung von Ihrem PC aus gesendet werden. Die Emails und Instant Messages Ihres PCs werden ebenso gescannt wie Daten, die über Internetseiten gesendet werden. Zudem werden alle Informationen geblockt, die über die von Ihnen definierten Regeln der Identitätskontrolle geschützt sind.
- Registry-Kontrolle - fragt um Erlaubnis immer wenn ein Programm versucht die Registry zu ändern um beim Windows Neustart ausgeführt zu werden.
- Cookie-Kontrolle- fragt nach Ihrer Einwilligung, sobald eine neue Webseite einen Cookie auf Ihrem Rechner installieren will.
- Skript-Kontrolle- fragt nach Ihrer Einwilligung, sobald eine Webseite versucht, ein Skript oder andere aktive Inhalte zu aktivieren.

In der Voreinstellung ist nur die Funktion "Identitätskontrolle" aktiviert.Sie müssen passende Identitätskontrollregeln konfigurieren, um das nicht autorisierte Senden von der vertraulichen Information zu verhindern.Für weitere Informationen lesen Sie bitte *„Konfiguration der Identitätskontrolle“* (S. 98).

Die weiteren Komponenten der Privatsphärekontrolle sind nicht aktiv. Falls Siediese aktivieren, werden Sie im Warnhinweisfenster gefragt, ob bestimmte Aktionenzugelassen oder geblockt werden sollen, wenn Sie auf neuen Internetseiten surfenoder eine neue Software installieren. Dies ist der Grund, wieso diese Einstellung im Normalfall von fortgeschrittenen Anwendern verwendet wird.

## 15.1. Sicherheitsstufe einstellen

Die TresorSicherheitsstufe hilft Ihnen, die Komponenten der Privatsphäre-Funktion einfach zu aktivieren/deaktivieren.

Um die TresorSicherheitsstufe zu konfigurieren:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Privatsphäre > Status**.

3. Stellen Sie sicher, dass die Privatsphärefunktion aktiviert ist.
4. Es stehen zwei Optionen zur Verfügung:
   - Schieben Sie den Regler in die gewünschte TresorSicherheitsstufen-Position.Mit dem Klick auf **Standard** laden Sie die Grundeinstellungen.

     Nutzen Sie die Beschreibung auf der rechten Seite, um die TresorSicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.
   - Sie können die Sicherheitsstufe für den gewünschten Schutz einstellen. Klicken Sie hierfür auf**Stufe anpassen**.Wählen Sie in dem Fenster das sich öffnet die gewünschten Sicherheitsstufen und klicken Sie auf **OK**.

## 15.2. Antispyware/Identitätskontrolle

Die Identitätskontrolle schützt Sie gegen den Diebstahl wichtiger Daten, wenn Sie online sind.

Betrachten wir ein einfaches Beispiel: Sie haben eine Identitätskontrollregel zum Tresor Ihrer Kreditkartennummer definiert.Wenn es eine Spyware-Software auf irgendeine Weise geschafft hat, sich auf Ihrem Computer zu installieren, können dennoch keine Daten wie Ihre Kreditkartennummer via Email, Instant Messaging oder Webseiten gesendet werden. Zudem können auch Ihre Kinder die Kreditkartendaten nicht für Online-Käufe verwenden oder sie über das Internet preisgeben.

Weitere Informationen zu folgenden Themen sind verfügbar:

- *„Über die Identitätskontrolle“* (S. 96).
- *„Konfiguration der Identitätskontrolle“* (S. 98).
- *„Regeln bearbeiten“* (S. 100).

### 15.2.1. Über die Identitätskontrolle

Vertrauliche Daten zu sichern ist für alle Anwender äußerst wichtig. Datenklau hat mit der Entwicklung der Internet Kommunikation standgehalten und wendet immer wieder neue Methoden an um Anwender zu täuschen und private Informationen zu erhalten.

Ob es sich um Ihre E-Mail Adresse handelt oder um Ihre Kreditkartennummer, wenn sie in die falschen Hände geraten können diese Informationen großen Schaden anrichten: Sie werden möglicherweise in Spam Mails ertrinken oder sich über ein geleertes Konto wundern.

Die Identitätskontrolle schützt Sie gegen den Diebstahl wichtiger Daten, wenn Sie online sind.Basierend auf Regeln, die von Ihnen erstellt wurden, prüft die Identitätskontrolle den Web-, Mail und IM-Datenverkehr auf spezielle Zeichenfolgen

(zum Beispiel Ihre Kreditkartennummer). Wenn eine Übereinstimmung mit einer Webseite, E-Mail Adresse oder IM-Nachricht gefunden wird, werden diese sofort geblockt.

Sie können Regeln erstellen, um jegliche Information zu schützen, die Sie als persönlich oder vertraulich betrachten, von Ihrer Telefonnummer oder E-Mail-Adresse bis hin zu Ihren Bankkontoangaben.Es wird eine Multiuser Unterstützung zur Verfügung gestellt, wodurch Benutzer die sich in verschiedene Windows-Benutzerkonten einloggen Ihre eigenen Regeln zur Identitätskontrolle konfigurieren können.Falls Ihr Windows-Benutzerkonto ein Administratorkonto ist, können die von Ihnen erstellten Regeln festgelegt werden, auch zu gelten wenn andere Benutzer mit deren Konten am Windows eingeloggt sind.

Warum sollten Sie die Identitätskontrolle verwenden?

- Die Identitätskontrolle kann Keylogger-Spyware effektiv blockieren.Diese schädlichen Anwendungen speichern Ihre eingegebenen Tastenfolgen und senden sie über das Internet zu Hackern.Der Hacker kann über diese gestohlenen Daten sensible Informationen erfahren, so wie Kontonummern und Passwörter und kann Sie zu seinem eigenen Profit verwenden.

  Auch wenn eine solche Anwendung es schafft die Antivirus-Entdeckung zu umgehen, kann es die gestohlenen Daten nicht über E-Mail, das Internet oder Chatprogramme senden, wenn Sie entsprechende Regeln für die Identitätskontrolle eingestellt haben.

- Die Identitätskontrolle kann Sie vor Phishing schützen (Versuche, persönliche Daten zu stehlen).Die meisten Phishing-Versuche verwenden eine betrügerische E-Mail, um Sie dazu zu bringen persönliche Daten an eine gefälschte Webseite zu senden.

  So können Sie beispielsweise eine E-Mail erhalten, die behauptet von Ihrer Bank zu kommen und Sie dazu auffordert, Ihre Bankangaben dringend zu aktualisieren.In der E-Mail befindet sich ein Link zu einer Webseite, auf der Sie Ihre persönlichen Daten angeben sollen.Auch wenn dies alles echt erscheint, sind sowohl die E-Mail als auch die genannte Webseite Fälschungen.Wenn Sie auf den Link in der Mail klicken und Ihre persönlichen Daten an die Webseite senden, werden Sie diese Informationen an Hacker weiterleiten, die diesen Phishing-Versuch erstellt haben.

  Wenn entsprechende Regeln für die Identitätskontrolle eingestellt sind, können Sie die persönlichen Daten (so wie Ihre Kreditkartennummer) nicht an eine Webseite senden, außer wenn Sie die entsprechende Seite explizit als Ausnahme festgelegt haben.

- Durch die Verwendung von Identitätskontrollregeln können Sie verhindern, dass Ihre Kinder persönliche Daten (wie z. B. Ihre Adresse oder Telefonnummer) über das Internet weitergeben. Zudem können Sie auch eine Regel zum Tresor Ihrer Kreditkartendaten definieren, so dass Ihre Kinder mit dieser Karte ohne Ihre Zustimmung nichts kaufen können.

## 15.2.2. Konfiguration der Identitätskontrolle

Wenn Sie die Identitätskontrolle verwenden möchten, befolgen Sie folgende Schritte:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Privatsphäre > Identität**.
3. Stellen Sie sicher, dass die Identitätskontrolle aktiviert ist.

   **Beachten Sie**
   Wenn die Option nicht konfiguriert werden kann, gehen Sie in den Reiter **Status** und aktivieren Sie die Funktion "Privatsphäre".

4. Erstellen Sie Regeln um wichtige Daten zu schützen.Für weitere Informationen lesen Sie bitte *„Erstellung von Regeln für die Identitätskontrolle“* (S. 98).
5. Wenn nötig, Erstellen Sie spezielle Ausnahmen zu den Regeln, die Sie erstellt haben.Wenn Sie beispielsweise eine Regel zum Tresor Ihrer Kreditkarte definiert haben, dann setzen Sie die Webseiten, auf denen Sie normalerweise Ihre Kreditkarte einsetzen, auf die Ausschlussliste.Für weitere Informationen lesen Sie bitte *„Definition von Ausnahmen“* (S. 99).

### Erstellung von Regeln für die Identitätskontrolle

Um eine Regel für die Identitätskontrolle zu erstellen, klicken Sie auf die Schaltfläche **Hinzufügen** und befolgen Sie die Schritte des Konfigurationsassistenten.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Begrüßungsfenster**
2. **Typ und Richtung auswählen**

   Hier können Sie die Parameter auswählen:

   - **Name der Regel** - Geben Sie einen Namen für die Regel in dieses Editierfeld ein.
   - **Art der Regel** - wählen Sie die Regel aus (Adresse, Name, Kreditkartennummer, PIN, TAN etc).
   - Geben Sie in das Feld **Daten der Regel** die Daten ein, die geschützt werden sollen.Wenn Sie zum Beispiel Ihre Kreditkartennummer schützen wollen, geben Sie sie zum Teil oder ganz ein.

     **Wichtig**
     Wenn Sie weniger als drei Zeichen angeben werden Sie aufgefordert die Daten zu überprüfen. Wir empfehlen die Eingabe von mindestens drei Zeichen um ein versehentliches blockieren von Nachrichten oder Webseiten zu verhindern.

Alle Daten, die Sie eingeben sind verschlüsselt. Um wirklich sicher zu gehen, geben Sie nicht alle Daten ein, die Sie schützen möchten.

3. **Art der Traffic und Benutzer auswählen**

   a. Bitte wählen Sie den Datenverkehrstyp, den Acronis Internet Security scannen soll.

   - **HTTP-Daten überprüfen** - prüft den HTTP (web) Datenverkehr und blockiert ausgehende Daten, die den Regeln entsprechen.
   - **SMTP-Daten überprüfen** - prüft alle ausgehenden E-Mail-Nachrichten, die den Regeln entsprechen.
   - **Instant Messaging überprüfen** - prüft den Instant Messaging Datenverkehr und blockiert ausgehende Nachrichten, die den Regeln entsprechen.

   Sie können wählen ob die Regeln nur zutreffen, wenn die Daten der Regeln wörtlich übereinstimmen oder ob die komplette Zeichenfolge übereinstimmen muss.

   b. Geben Sie den Benutzer an, für den die Regel angewendet werden soll.

   - **Nur für mich(Aktueller Nutzer)** - Die Regel wird nur für Ihren Benutzerkonto angewendet.
   - **Begrenzte Benutzerkonten** - Die Regel wird bei Ihren un alle anderen begrenzten Windows Benutzerkonten angewandt.
   - **Alle Benutzer** - Die Regel wird an alle Windows-Benutzerkonten angewandt.

4. **Beschreibung der Regel**

   Geben Sie eine kurze Beschreibung der Regel im Eingabefeld ein.Da die blockierten Daten (Zeichenfolgen) nicht als ein vollständiger Text angezeigt werden wenn auf die Regel zugegriffen wird, sollte Ihnen die Beschreibung dabei helfen sie einfach zu identifizieren.

   Klicken Sie auf **Fertigstellen**.Die Regel wird in der Tabelle erscheinen.

Ab jetzt wird jeder Versuch, spezifizierte Daten (über Email, Instant Messaging odereine Webseite) zu senden, fehlschlagen. Es wird ein Warnhinweis eingeblendet, dass Acronis Internet Security nicht zugelassen hat, dass identitätsspezifische Inhalte versendet wurden.

## Definition von Ausnahmen

In manchen Fällen wird es nötig sein Ausnahmen für bestimmte Identitätsregeln zu erstellen.Zum Beispiel haben Sie eine Regeln angelegt, welche verhindert das Ihre Kreditkartennummer per HTTP übertragen wird. Nun möchten Sie sich aber z.B. Schuhe auf einer bestimmten Webseite per Kreditkarte kaufen. In diesem Fall müssten Sie eine Ausnahme definieren um dies möglich zu machen.

Um eine solche Ausnahme zu erstellen klicken Sie auf die **Ausnahmen**-Schaltfläche.

Um eine Ausnahme zu erstellen befolgen Sie die folgenden Schritte:

1. Klicken Sie auf die Schaltfläche **Hinzufügen** um einen neuen Eintrag in die Tabelle hinzuzufügen.
2. Doppelklicken Sie auf **Entsprechende Ausschluss eingeben** und geben Sie die gewünschte URL, E-Mail Adresse oder IM-Kontakt ein, um sie Auszuschliessen.
3. Doppelklicken Sie dann auf **Typ wählen** und wählen Sie den gewünschten Eintrag aus dem Menü aus.
   - Wenn Sie eine Webseite eingegeben haben dann wählen Sie **HTTP**.
   - Wenn Sie eine E-Mail Adresse eingegeben haben dann wählen Sie **E-Mail (SMTP)**.
   - Wenn Sie einen IM-Kontakt eingegeben haben dann wählen Sie **IM**.

Um eine Ausnahme aus der Liste zu entfernen, wählen Sie diese aus und klicken auf die **Entfernen**-Schaltfläche.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

### 15.2.3. Regeln bearbeiten

Verwaltung der Identitätskontrollregeln:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Privatsphäre > Identität**.

Sie können eine Liste der Regeln in der Aufstellung ansehen.

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.

Um eine Regel zu bearbeiten wählen Sie die Regel aus und klicken **Bearbeiten**oder machen Sie einen Doppelklick. Ein neues Fenster erscheint.Hier können Sie Namen, Beschreibungen und Parameter der Regel ändern. (Typ, Daten und Datenverkehr). Klicken Sie **OK** um die Änderungen zu speichern.

## 15.3. Registry-Überprüfung

Ein sehr wichtiger Teil von Windows ist die **Registry**. Dort werden von Windows alle Einstellungen, installierten Programme, Nutzerinformationen und so weiter verwaltet.

Die **Registry** bestimmt u. a., welche Programme automatisch beim Start von Windows geladen werden. Viren versuchen häufig hier anzusetzen, damit auch sie automatisch mit geladen werden, wenn der Nutzer seinen Computer startet.

**Registry Kontrolle** beobachtet die Windows-Registry – dies ist auch sehr hilfreich beim Aufspüren von Trojanern. Sie werden alarmiert, wann immer ein Programm versucht, einen Eintrag in die Registry zu unternehmen, um beim nächsten Windows-Start geladen zu werden.Für weitere Informationen lesen Sie bitte *„Registry-Alarme.“ (S. 24)*.

Für die Konfigurierung der Registry Control:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Privatsphäre > Registry**.
3. Klicken Sie das entsprechende Kästchen an, um die Registry Control zu aktivieren.

Beachten Sie

Wenn die Option nicht konfiguriert werden kann, gehen Sie in den Reiter **Status** und aktivieren Sie die Funktion "Privatsphäre".

### Regeln bearbeiten

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.

## 15.4. Cookie-Kontrolle

Cookies werden von den meisten Webseiten im Internet verwendet. Es sind kleine Dateien, die auf Ihrem Computer gespeichert werden. Webseiten verschicken diese Cookies, um das Surfen zu beschleunigen, aber auch um Informationen über Sie zu erhalten.

Generell erleichtern Cookies das tägliche Internet-Leben. Zum Beispiel ermöglichen sie einer Webseite, Ihren Namen und sonstige Angaben zu speichern, so dass Sie diese nicht bei jedem Besuch eingeben müssen.

Cookies können jedoch auch missbräuchlich verwendet werden und Ihre Privatsphäre gefährden, indem Ihre Surfdaten an Dritte weitergegeben werden.

Hier hilft die Cookie-Kontrolle.Wenn Sie aktiviert ist, wird die Cookie-Kontrolle bei jedem Versuch einer Webseite, einen Cookie anzubringen, Ihr diesbezügliches Einverständnis erfragen.Für weitere Informationen lesen Sie bitte *„Cookie-Alarme“ (S. 25)*.

Um die Cookie-Steuerung zu konfigurieren:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Privatsphäre > Cookie**.
3. Markieren Sie das entsprechende Kästchen, um die Cookie Control zu aktivieren.

**Beachten Sie**
Wenn die Option nicht konfiguriert werden kann, gehen Sie in den Reiter **Status** und aktivieren Sie die Funktion "Privatsphäre".

4. Sie können für die Webseiten, die Sie regelmäßig besuchen, Regeln konfigurieren, dies ist aber nicht unbedingt notwendig.Basierend auf Ihrer Antwort werden durch das Warnhinweisfenster automatisch Regeln erstellt.

**Beachten Sie**
Aufgrund der großen Anzahl von Cookies, die heute im Internet verwendet werden, kann die **Cookie-Kontrolle** zu Beginn sehr oft nachfragen. Sobald Sie die von Ihnen regelmäßig besuchten Seiten in die Regelliste aufgenommen haben, wird Ihr Surfen im Internet aber wieder wie zuvor sein.

## Regeln manuell erstellen

Um eine Regel manuell zu erstellen, klicken Sie auf die Schaltfläche **Hinzufügen** und führen Sie die gewünschten Änderungen im Konfigurationsfenster durch.Hier können Sie die Parameter auswählen:

- **Domäne angeben** - schreiben Sie die Domäne, auf welche die Regel angewendet werden soll, in das darunter stehende Feld.
- **Aktion** - wählen Sie die Aktion der Regel.

| Aktion | Beschreibung |
|---|---|
| **Erlauben** | Das Cookie dieser Domäne wird ausgeführt. |
| **Blockieren** | Das Cookie dieser Domäne wird nicht ausgeführt. |

- **Richtung** - Wählen Sie die Richtung des Datenverkehrs aus.

| Typ | Beschreibung |
|---|---|
| **Ausgang** | Die Regel bezieht sich nur auf Cookies, welche von der verbundenen Seite versendet werden. |
| **Eingang** | Die Regel bezieht sich nur auf Cookies welche an die verbundene Seite versendet werden. |
| **Beide** | Die Regeln finden in beide Richtungen Anwendung. |

**Beachten Sie**
Sie können Cookies akzeptieren, diese aber nicht zurücknehmen, indem Sie die Aktion **Verweigern** und die Richtung **Ausgehend** angeben.

Klicken Sie auf **Fertigstellen**.

## Regeln bearbeiten

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.Zum bearbeiten von Regelparametern, wählen Sie die Regel aus und klicken auf die **Bearbeiten** oder machen Sie einen Doppelklick. Ein neues Fenster erscheint wo Sie die gewünschte konfigurierung durchführen können.

# 15.5. Skript-Kontrolle

Skripte und andere Programmierungen, wie z. B. ActiveX und Java applets, die für interaktive Webseiten verwendet werden, können verheerende Schäden verursachen. ActiveX-Elemente können zum Beispiel Zugriff auf Ihre Daten erlangen und sie auslesen, Daten von Ihrem Computer löschen, Passwörter auslesen und Nachrichten versenden, wenn Sie online sind. Sie sollten daher solche aktiven Elemente nur von Ihnen bekannten und zuverlässigen Seiten akzeptieren.

Wenn Sie die Funktion "Skript-Kontrolle" aktivieren, wird immer eine Anfrage an Sie gerichtet, wenn eine neue Webseite versucht, ein Skript oder einen anderen aktiven Inhalte zu verankern.Für weitere Informationen lesen Sie bitte *„Skript-Alarme“* (S. 25).

Um die Skript-Kontrolle zu konfigurieren:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Privatsphäre > Skript**.
3. Klicken Sie das entsprechende Kästchen an, um die Skript-Kontrolle zu aktivieren.

   **Beachten Sie**
   Wenn die Option nicht konfiguriert werden kann, gehen Sie in den Reiter **Status** und aktivieren Sie die Funktion "Privatsphäre".

4. Sie können für die Webseiten, die Sie regelmäßig besuchen, Regeln konfigurieren, dies ist aber nicht unbedingt notwendig.Basierend auf Ihrer Antwort werden durch das Warnhinweisfenster automatisch Regeln erstellt.

## Regeln manuell erstellen

Um eine Regel manuell zu erstellen, klicken Sie auf die Schaltfläche **Hinzufügen** und führen Sie die gewünschten Änderungen im Konfigurationsfenster durch.Hier können Sie die Parameter auswählen:

- **Domäne angeben** - schreiben Sie die Domäne, auf welche die Regel angewendet werden soll, in das darunter stehende Feld.
- **Aktion** - wählen Sie die Aktion der Regel.

| Aktion | Beschreibung |
|---|---|
| **Erlauben** | Die Scripts auf dieser Domäne werden ausgeführt. |
| **Blockieren** | Die Scripts auf dieser Domäne werden nicht ausgeführt. |

Klicken Sie auf **Fertigstellen**.

## Regeln bearbeiten

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.Zum bearbeiten von Regelparametern, wählen Sie die Regel aus und klicken auf die **Bearbeiten** oder machen Sie einen Doppelklick. Ein neues Fenster erscheint wo Sie die gewünschte konfigurierung durchführen können.

# 16. Firewall

Die Firewall schützt Ihren Computer vor unberechtigten eigehenden und ausgehenden Zugriffen. Sie überwacht Ihre Verbindung und lässt Sie Regeln definieren, welche Verbindung erlaubt ist und welche geblockt werden soll.

**Beachten Sie**
Die Firewall ist ein unersetzliches Instrument bei einer DSL- oder Breitbandverbindung.

Im Stealth-Modus wird ihr Computer im Netzwerk so gut wie unsichtbar vor Angriffen jeglicher Art. Das Firewall-Modul ist in der Lage Portscans zu erkennen und diese gezielt ins Leere laufen zu lassen - so als ob der Computer gar nicht existierte.

## 16.1. Tresoreinstellungen

Um den Firewall-Tresor zu aktivieren/deaktivieren und zu konfigurieren, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neu eingeblendeten Fenster den Reiter **Einstellungen**.

Experten-Ansicht
: Gehen Sie zu **Firewall > Einstellungen**.

**Wichtig**
Um den Schutz vor Angriffen aus dem Internet zu gewährleisten, halten Sie Ihre **Firewall** Funktion jederzeit aktiviert.

Zu Beginn des Bereichs sehen Sie verschiedene Statistiken zu den festgestellten Aktivitäten.

Im unteren Bereich finden Sie eine Acronis Internet Security-Statistik bezüglich des ein- und ausgehenden Datenverkehrs. Diese Grafik zeigt Ihnen das Volumen des Internet-Datentransfers der letzten zwei Minuten an.

**Beachten Sie**
Diese Graphik wird nur in der Experten-Ansicht dargestellt.

### 16.1.1. Standardaktion einstellen

Standardmäßig erlaubt Acronis Internet Security automatisch allen Programmen der White List eine Verbindung zum Netzwerk und dem Internet herzustellen.Für alle anderen Programme fordert Acronis Internet Security Sie über ein

Benachrichtigungsfenster dazu auf, die durchzuführende Aktion festzulegen.Die von Ihnen festgelgte Aktion wird dann immer durchgeführt, wenn das entsprechende Programm versucht auf das Netzwerk/Internet zuzugreifen.

**Beachten Sie**

Um die Acronis Internet Security White-List zu sehen, klicken Sie auf den entsprechenden Button im **Einstellungen** Register der Expertenansich oder im **Programme** Register in der Standard-Ansicht.

Ziehen Sie den Zeiger an der Skala entlang um die Standardaktion einzustellen, die durchgeführt werden soll, wenn das Programm versucht auf das Netzwerk/Internet zuzugreifen.

- Alles erlauben
- Bekannte Programme
- Bericht
- Alle verweigern

Wenn Sie eine Aktion auswählen, wird ein kurzer Erklärungstext eingeblendet.

## 16.1.2. Weitere Einstellungen der Firewall konfigurieren

In der Experten-Ansicht können Sie die erweiterten Firewall-Einstellungen durch Klicken auf **Erweiterte Einstellungen** konfigurieren.

Die folgenden Optionen sind verfügbar:

- **Unterstützung für Internet Connection Sharing aktivieren** - Erlaubt die Unterstützung von Internet Connection Sharing (ICS).

**Beachten Sie**

Diese Option erlaubt nicht automatisch ICS auf Ihrem System sondern erlaubt diese Art von Verbindung nur, wenn Sie es von Ihrem Betriebssystem aus freigeben.

- **Finde Anwendungen die sich seit dem Erstellen der Firewall-Regel verändert haben** - prüft jede Anwendung die versucht eine Verbindung zum Internet herzustellen, um zu erkennen ob sich bei dieser seit dem Hinzufügen der Regel, die den Zugriff überwacht, etwas verändert hat. Falls sich etwas verändert hat, wird eine Warnung Sie auffordern den Zugriff zu erlauben oder zu blockieren.

**Beachten Sie**

Anwendungen können durch Malware verändert werden.Wir empfehlen Ihnen die Option aktiviert zu lassen und nur Anwendungen Zugriff zu gewähren bei welchen Sie erwarten das diese Zugriff zum Internet benötigen.

Signierte Anwendungen sind in normalerweise vertrauenswürdig und haben einen höheren Sicherheitsgrad.Signierte Anwendungen haben einen höheren Sicherheitsfaktor. Sie können diesen Anwendungen den Zugriff erlauben auch wenn diese verändert wurden. Aktivieren Sie hierzu die Option **Änderungen bei signierten Prozessen ignorieren**.

- **WLAN Benachrichtigungen aktivieren** - wenn Sie mit einem drahtlosen Netzwerk verbunden sind, werden Informationsfenster bezüglich bestimmter Netzwerkereignisse angezeigt (z.B. wenn ein neuer Computer dem Netzwerk beitritt).
- **Portscans blockieren** - entdeckt und blockiert Versuche offene Ports zu finden.

  Portscans werden von Hackern verwendet, um herauszufinden, welche Ports auf Ihrem Computer geöffnet sind.Wenn Sie dann einen unsicheren Port finden, können Sie in Ihren Computer eindringen.
- **Genaue automatische Regeln** -erstellt genaue Regeln bezüglich der Verwendung des Benachrichtigungsfensters der Firewall.Wenn diese Option aktiviert ist, wird Acronis Internet Security Sie dazu auffordern für jede Anwendung, die versucht auf das Netzwerk oder das Internet zuzugreifen, eine Aktion durchzuführen und Regeln zu erstellen.

## 16.2. Zugriffsregel für Anwendungen

Um die Firewall-Regeln zu verwalten, die den Zugriff von Anwendungen auf Netzwerkressourcen und das Internet kontrollieren, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht

Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neu eingeblendeten Fenster den Reiter **Programme**.

Experten-Ansicht

Gehen Sie zu **Firewall > Programme**.

In der Standard-Ansicht haben Sie Zugriff auf die Basis-Konfigurationseinstellungen. Für zusätzliche benutzerdefinierte Optionen wechseln Sie in die Experten-Ansicht.

### 16.2.1. Aktuelle Regeln ansehen

Sie können die Programme (Prozesse), für die Firewall-Regel erstellt wurde, in der Tabelle sehen.

In der Experten-Ansicht erhalten Sie detaillierte Informationen zu jeder Regel, so wie in den Spalten der Tabelle dargestellt.Um die Regeln zu sehen, die für eine bestimmte Anwendung erstellt wurden, klicken Sie auf das + Kästchen neben der entsprechenden Anwendung.Deaktivieren Sie das Kontrollkästchen **Systemregeln**

**verbergen** frei, wenn Sie auch die Regeln bezüglich des Systems oder der Acronis Internet Security-Prozessen sehen möchten.

- **Prozess/Netzwerkarten** - der Prozess und die Netzwerkadapter-Typen für die die Regel angewendet wird.Regeln werden automatisch erstellt um den Netzwerk- oder Internetzugriff jedes Adapters zu filtern.Sie können manuell Regeln erstellen oder bestehende Regeln bearbeiten um den Zugriff einer Anwendung auf das Netzwerk/Internet über einen speziellen Adapter zu filtern (zum Beispiel ein drahtloser Netzwerkadapter).
- **Befehlszeile** - der Befehl in der Windows Befehlszeile der verwendet wird um den Prozess zu starten (**cmd**).
- **Protokoll** - das IP-Protokoll für das die Regel angewendet wird.Sie werden eines der Folgenden sehen:

| Protokoll | Beschreibung |
|---|---|
| **Alle** | Beinhaltet alle IP-Protokolle. |
| **TCP** | Transmission Control Protocol (TCP) ist eine Vereinbarung (Protokoll) darüber, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen. Alle am Datenaustausch beteiligten Computer kennen diese Vereinbarungen und befolgen sie. Es ist damit ein zuverlässiges, verbindungsorientiertes Transportprotokoll in Computernetzwerken. Es ist Teil der TCP/IP-Protokollfamilie. Entwickelt wurde TCP von Robert E. Kahn und Vinton G. Cerf. Ihre Forschungsarbeit, die sie im Jahre 1973 begannen, dauerte mehrere Jahre. Die erste Standardisierung von TCP erfolgte deshalb erst im Jahre 1981 als RFC 793. TCP stellt einen virtuellen Kanal zwischen zwei Endpunkten einer Netzwerkverbindung (Sockets) her. Auf diesem Kanal können in beide Richtungen Daten übertragen werden. TCP setzt in den meisten Fällen auf das IP-Protokoll auf. Es ist in Schicht 4 des OSI-Referenzmodells angesiedelt. |
| **UDP** | User Datagram Protocol (UDP) ist ein minimales, verbindungsloses Netzprotokoll. Es gehört zur Transportschicht der TCP/IP-Protokollfamilie und ist im Gegensatz zu TCP nicht auf Zuverlässigkeit ausgelegt. UDP erfüllt im Wesentlichen den Zweck, die durch die IP-Schicht hergestellte Endsystemverbindung um eine Anwendungsschnittstelle (Ports) zu erweitern. Die Qualität der darunter liegenden Dienste, insbesondere die Zuverlässigkeit der Übertragung, erhöht UDP hingegen nicht. |
| **Eine Nummer** | Stellt ein besonderes IP-Protokoll dar (anders als TCP und UDP).Die komplette Liste zugewiesener Nummern von IP-Protokollen finden Sie unter www.iana.org/assignments/protocol-numbers. |

- **Netzwerkereignisse** - die Netzwerkereignisse für die die Regel angewendet wird.Folgende Ereignisse können auftreten:

| Ereignis | Beschreibung |
|---|---|
| **Verbinden** | Vorausgehender Austausch von Standardnachrichten, die von Verbindungsprotokollen (wie TCP) verwendet werden, um eine Verbindung herzustellen.Mit Verbindungsprotokollen entsteht ein Datenverkehr zwischen zwei Computern nur nachdem eine Verbindung hergestellt wurde. |
| **Datenverkehr** | Datenfluss zwischen zwei Computern. |
| **Abhören** | Status in dem eine Anwendung das Netzwerk überwacht, das eine Verbindung herstellen oder Informationen über eine Peer-Anwendung erhalten möchte. |

- **Lokale Ports** - die Ports auf Ihrem Computer, für die die Regel angewendet wird.
- **Remote-Ports** - die Ports auf den Remote-Computern, für die die Regel angewendet wird.
- **Lokal** - ob die Regel nur für Computer im lokalen Netzwerk angewendet wird.
- **Aktion** - ob der Anwendung unter den festgelegten Umständen der Zugriff auf das Netzwerk/Internet erlaubt oder verweigert wird.

## 16.2.2. Regeln automatisch hinzufügen

Bei aktivierter **Firewall** überwacht Acronis Internet Security alle Anwendungen und erstellt automatisch eine Regel, wenn eine Anwendung versucht, eine Internetverbindung herzustellen.Abhängig von der Anwendung und den Acronis Internet Security Firewall-Einstellungen geschieht dies mit oder ohne Ihren Eingriff.

Wenn Sie die Basis- oder Standard-Ansicht verwenden, wird der Verbindungsaufbau von einer unbekannten Anwendung aus automatisch blockiert.

Wenn Sie die Experten-Ansicht verwenden, werden Sie über Warnhinweisfenster zu Aktionen aufgefordert, wenn eine unbekannte Anwendung versucht, sich mit dem Internet zu verbinden.

Sie können folgendes sehen: Die Anwendung, die versucht, auf das Internet, den Pfad zur Anwendungsdatei, dem Bestimmungsort, das Protokoll verwendet und Port , auf dem die Anwendung versucht in Verbindung zu stehen.

Wählen Sie **Erlauben** um allen Datenverkehr für diese Anwendung über das eingestellt Protokoll zu erlauben (eingehend und ausgehend). Wenn Sie **Verweigern**wählen, wird der Zugriff entsprechend blockiert.

**Wichtig**
Erlauben Sie nur eingehende Verbindungen von IP-Adressen oder Internet-Domänen, denen Sie wirklich vertrauen.

Bassierend auf Ihrer Wahl wird eine Regel erstellt. Das nächste Mal wenn die Anwendung versucht eine Verbindung herzustellen wird die Regeln direkt angewand.

### 16.2.3. Regeln manuell hinzufügen

Das manuelle Erstellen von Regeln unterscheidet sich in den verschiedenen Ansichtsmodi.

Standard-Ansicht

1. Klicken Sie in **Neues Programm hinzufügen** auf **Blättern**.
2. Finden Sie das Programm, für das die Regel erstellt werden soll und klicken Sie auf **Öffnen**.
3. Klicken Sie auf **Regel hinzufügen**.

   Beachten Sie, dass die Regel nun in der Tabelle angezeigt wird.
4. Wählen Sie in der Spalte **Aktion**: Zugriff erlauben oder verweigern.

   Die Aktion wird auf alle Regelparameter angewendet.

Experten-Ansicht

1. Klicken Sie auf den Button **Regel hinzufügen**.Das Konfigurationsfenster wird erscheinen.
2. Knofigurieren Sie die wichtigsten und erweiterten Parameter wie benötigt.
3. Klicken Sie auf **OK** um die neue Regel hinzuzufügen.

Regeln können nur modifiziert werden, wenn die Firewall in der Experten-Ansicht konfiguriert wird.Um eine bestehende Regel zu bearbeiten, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf den Button **Regel bearbeiten** oder doppelklicken Sie auf die Regel.Das Konfigurationsfenster wird erscheinen.
2. Knofigurieren Sie die wichtigsten und erweiterten Parameter wie benötigt.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

#### Allgemeine Parameter konfigurieren

Der Tab **Allgemein** des Konfigurationsfensters bietet Ihnen die Möglichkeit die allgemeinen Regelparameter zu verwalten.

Folgende Parameter können konfiguriert werden:

- **Programmpfad.** Klicken Sie auf **Durchsuchen** und wählen Sie das Programm für das die Regel angewendet wird.Wenn Sie möchten, dass die Regel für alle Programme angewendet wird, wählen Sie **Alle**.
- **Befehlszeile.** Wenn Sie möchten, dass die Regel nur angewendet wird, wenn die ausgewählte Anwendung mit einem bestimmten Befehl in der Befehlszeile von Windows geöffnet wird, lassen Sie das Kontrollkästchen **Alle** frei und geben Sie den entsprechenden Befehl in das Editierfeld ein.
- **Protokoll.** Wählen Sie aus dem Menu das IP-Protokoll für das die Regel angewendet wird.
  - ▶ Wenn Sie möchten, dass die Regel für alle Protokolle angewendet wird, wählen Sie **Alle**.
  - ▶ Wenn Sie möchten, dass die Regel für TCP-Protokolle angewendet wird, wählen Sie **TCP**.
  - ▶ Wenn Sie möchten, dass die Regel für UDP-Protokolle angewendet wird, wählen Sie **UDP**.
  - ▶ Wenn Sie möchten, dass die Regel für ein bestimmtes Protokoll angewendet wird, wählen Sie **Andere**.Ein Editierfeld wird erscheinen.Geben Sie die dem Protokoll, das gefiltert werden soll, zugewiesene Nummer in das Editierfeld ein.

**Beachten Sie**

Die Nummern von IP-Protokollen werden von der Internet Assigned Numbers Authority (IANA) zugewiesen.Die komplette Liste zugewiesener Nummern von IP-Protokollen finden Sie unter www.iana.org/assignments/protocol-numbers.

- **Ereignisanzeige.** Wählen Sie je nach ausgewähltem Protokoll die Netzwerkereignisse, für die die Regel angewendet werden soll.Folgende Ereignisse können auftreten:

| Ereignis | Beschreibung |
|---|---|
| **Verbinden** | Vorausgehender Austausch von Standardnachrichten, die von Verbindungsprotokollen (wie TCP) verwendet werden, um eine Verbindung herzustellen.Mit Verbindungsprotokollen entsteht ein Datenverkehr zwischen zwei Computern nur nachdem eine Verbindung hergestellt wurde. |
| **Datenverkehr** | Datenfluss zwischen zwei Computern. |
| **Abhören** | Status in dem eine Anwendung das Netzwerk überwacht, das eine Verbindung herstellen oder Informationen über eine Peer-Anwendung erhalten möchte. |

- **Adapter Typ:** Wählen Sie den Adaptertyp aus, für die diese Regel angewendet werden soll:
- **Aktion.** Folgende Aktionen sind wählbar:

| Aktion | Beschreibung |
|---|---|
| **Erlauben** | Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen erlaubt. |
| **Blockieren** | Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen verweigert. |

## Erweiterte Parameter konfigurieren

Der Tab **Erweitert** des Konfigurationsfensters gibt Ihnen die Möglichkeit erweiterte Regelparameter zu konfigurieren.

Folgende erweiterte Parameter können konfiguriert werden:

- **Richtung.** Wählen Sie aus dem Menu die Richtung des Datenverkehrs, für den die Regel angewendet wird.

| Richtung | Beschreibung |
|---|---|
| **Ausgehend** | Die Regeln beziehen sich nur auf ausgehenden Datenverkehr. |
| **Eingehend** | Die Regeln beziehen sich nur auch eingehenden Datenverkehr. |
| **Beide** | Die Regeln finden in beide Richtungen Anwendung. |

- **IP-Version.** Wählen Sie aus dem Menu die IP-Version (IPv4, IPv6 oder andere), für die die Regel angewendet werden soll.
- **Lokale Adresse.** Bestimmen Sie die lokale IP-Adresse und den Port, für die die Regel angewendet werden soll, wie folgt:
  - ▶ Wenn Sie mehr als einen Netzwerkadapter haben, können Sie das Kontrollkästchen **Alle** freilassen und eine bestimmte IP-Addresse eingeben.
  - ▶ Falls Sie TCP oder UDP als Protokoll ausgewählt haben, können Sie spezielle Ports in der Bandbreite von 0 und 65535 auswählen. Wenn Sie die definierten Regeln für alle Ports auswählen möchten, wählen Sie bitte **Alle**.
- **Entfernte Adresse.** Bestimmen Sie die Remote-IP-Adresse und den Port, für die die Regel angewendet werden soll, wie folgt:

- ▶ Um den Datenverkehr zwischen Ihrem Computer und einem bestimmten Computer zu filtern, lassen Sie das Kontrollkästchen **Alle** frei und geben Sie dessen IP-Adresse an.
- ▶ Falls Sie TCP oder UDP als Protokoll ausgewählt haben, können Sie spezielle Ports in der Bandbreite von 0 und 65535 auswählen. Wenn Sie die definierten Regeln für alle Ports auswählen möchten, wählen Sie bitte **Alle**.

- **Diese Regel nur für direkt verbundene Computer anwenden.** Wählen Sie diese Option, wenn Sie möchten dass diese Regel nur für den lokalen Datenverkehr angewendet werden soll.
- **Den Ablauf überprüfen um das ursprüngliche Ereignis festzustellen.** Sie können diesen Parameter nur verändern, wenn Sie **Genaue automatische Regeln** ausgewählt haben (öffnen Sie den Tab Einstellungen und klicken Sie auf **Erweiterte Einstellungen**).Genaue Regeln bedeuten, dass Acronis Internet Security Sie jedes Mal auffordert eine Aktion durchzuführen, wenn eine Anwendung versucht, eine Verbindung mit dem Netzwerk/Internet herzustellen, wenn der vorangegangene Prozess ein anderer war.

## 16.2.4. Erweiterte Regelverwaltung

Wenn Sie die Regeln, die die Anwendungen regeln, einsehen oder bearbeiten möchten, klicken Sie auf den Button **Erweitert**, der verfügbar wird, wenn Sie in der Experten-Ansicht die Firewall konfigurieren.

Sie können eine Liste der Firewall-Regeln, nach dem Datum der Erstellung geordnet, sehen.Die Spalten der Tabelle geben nützliche Informationenzu jeder Regel.

### Beachten Sie

Wenn ein Verbindungsversuch ausgeführt wurde (sowohl eingehend als auch ausgehend), wendet Acronis Internet Security die Aktion der ersten Regel an, die auf die entsprechende Verbindung zutrifft.Deshalb ist die Reihenfolge der Regeln sehr wichtig.

Um eine Regel zu löschen, markieren Sie diese und klicken dann auf den Button **Regel löschen**.

Um eine bereits existierende Regel zu bearbeiten, klicken Sie auf diese und danach auf **Regel bearbeiten** oder doppelklicken Sie darauf.

Sie können die Priorität einer Regel erhöhen oder heruntersetzen. Klicken Sie **In der Liste hochsetzen** um die ausgewählte Regel um ein Level nach oben zu setzen. Oder klicken Sie **In Liste heruntersetzen** um die Priorität der ausgewählten Regel herunterzusetzen.Um einer Regel die höchste Priorität zu geben klicken Sie auf die **Als erste**-Schaltfläche. Um einer Regel die niedrigste Priotität zu zuweisen klicken Sie auf die **Als letzte**-Schaltfläche.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.

### 16.2.5. Löschen und Zurücksetzen von Regeln

Nur bei einer Konfiguration in der Experten-Ansicht können die Firewall-Einstellungen gelöscht oder zurückgesetzt werden.

Um eine Regel zu löschen, markieren Sie diese und klicken dann auf den Button **Regel löschen**.Sie können eine oder auch mehrere Regeln auswählen und löschen.

Möchten Sie alle für eine bestimmte Anwendung erstellen Regeln löschen, wählen Sie die Anwendung aus der Liste und klicken auf den Button **Regel löschen**.

Falls Sie für die gewählte Vertrauensstufe den Standardregelsatz laden wollen, klicken Sie **Regeln Zurücksetzen**.

## 16.3. Netzwerk-Einstellungen

Um die Netzwerkverbindung-Einstellungen zu konfigurieren, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie auf den Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**. Wählen Sie im neu eingeblendeten Fenster den Reiter **Netzwerk**.

Experten-Ansicht
: Gehen Sie zu **Firewall > Netzwerk**.

Die Spalte **Netzwerkkonfiguration** bietet eine Reihe von Detailinformationen über das verbundene Netzwerk und ermöglicht eine Konfiguration folgender Einstellungen:

- **Adapter** - Der Netzwerkadapter, den Ihr Computer verwendet, um eine Verbindung mit dem Netzwerk oder dem Internet herzustellen.
- **Netzwerktypen** - der Netzwerktyp, mit dem der Adapter verbunden ist.Abhängig von der Netzwerkadapter-Konfiguration wird Acronis Internet Security automatisch einen Netzwerktyp wählen oder Sie um weitere Angaben bitten.

  Durch Klicken auf den Pfeil ▾ in der Spalte **Netzwerktyp** können Sie den Typ ändern oder aus der Liste einen verfügbaren Typ wählen.

| Netzwerktyp | Beschreibung |
|---|---|
| **Vertrauenswürdig** | Deaktiviert die Firewall für den entsprechenden Adapter. |
| **Zuhause/Büro** | Erlaubt den Datenverkehr zwischen Ihrem Computer und den Computern im lokalen Netzwerk. |
| **Öffentlichkeit** | Sämtlicher Datenverkehr wird gefiltert. |
| **Nicht vertrauenswürdig** | Der Netzwerk- und Internet-Datenverkehr über den entsprechenden Adapter wird vollständig blockiert. |

- **VPN** - ob es sich bei der Verbindung um eine VPN handelt.

  Der durch die VPN-Verbindung gehende Datenverkehr wird anders gefiltert als der Datenverkehr über Netzwerkverbindungen.Handelt es sich bei der Verbindung um eine VPN, klicken Sie auf den Pfeil ▾ der Spalte **VPN** und wählen Sie **Ja**.

In der Experten-Ansicht werden zwei zusätzliche Spalten angezeigt:

- **Stealth Modus** - Ob Sie von anderen Computern entdeckt werden können.

  Um den Stealth-Modus zu konfigurieren, klicken Sie auf den Pfeil ▾ in der Spalte **Stealth-Modus** und wählen Sie die gewünschte Option.

| Stealth-Option | Beschreibung |
|---|---|
| **Aktiviert** | Stealth-Modus ist aktiviert.Ihr Computer ist weder im lokalen Netzwerk noch im Internet sichtbar. |
| **Deaktiviert** | Stealth-Modus ist deaktiviert.Jeder Benutzer im lokalen Netzwerk oder im Internet kann Ihren Computer entdecken. |
| **Entfernt** | Ihr Computer kann nicht im Internet entdeckt werden.Benutzer im lokalen Netzwerk können Ihren Computer entdecken |

- **Allgemein** - ob die allgemeinen Regeln für diese Verbindung angewendet werden sollen.

  Wenn sich die IP-Adresse eines Netzwerkadapters geändert hat, verändert Acronis Internet Security die Vertrauensstufe entsprechend.Wenn Sie denselben Typ beibehalten möchten, klicken Sie auf den Pfeil ▾ in der Spalte **Generisch** und dann auf **Ja**.

### 16.3.1. Netzwerk-Zonen

Sie können erlaubte oder blockierte Computer für einen bestimmten Adpater hinzufügen.

Ein vertrauenswürdiger Bereich ist ein Computer, dem Sie vollständig vertrauen.Zwischen Ihrem Computer und den Computern, denen Sie vertrauen, ist jeglicher Datenaustausch erlaubt.Um Ressourcen mit speziellen Computern in ungesicherten WLAN-Netzwerken zu teilen, fügen Sie sie als erlaubte Computer hinzu.

Ein blockierter Bereich ist ein Computer, mit dem Ihr Computer in keiner Weise kommunizieren soll.

In der Tabelle **Netzwerkzonen** werden die aktuellen Netzwerkzonen pro Adapter angezeigt.

Um eine Zone hinzufügen, wählen Sie den Adapter und klicken dann auf **Zone hinzufügen**. Ein neues Fenster wird sich öffnen.

Gehen Sie wie folgt vor:

1. Wählen Sie die IP-Adresse des Computers der hinzugefügt werden soll.
2. Wählen Sie eine Aktion:
   - **Erlauben** - jeglicher Datenverkehr zwischen Ihrem Computer und dem ausgewählten Computer wird erlaubt.
   - **Verweigern** - jeglicher Datenverkehr zwischen Ihrem Computer und dem ausgewählten Computer wird blockiert.
3. Klicken Sie auf **OK**.

## 16.4. Geräte

Um die an das Netzwerk angeschlossenen Geräte zu verwalten, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neu eingeblendeten Fenster den Reiter **Geräte**.

Experten-Ansicht
: Gehe zu **Firewall > Geräte**.

Die Drucker, Faxgeräte und Scanner Ihres Netzwerks und die für diese Geräte voreingestellten Aktionen werden in der Tabelle aufgelistet.Um den Status eines Gerätes zu ändern, doppelklicken Sie auf die Tabelle und wählen Sie eine der eingeblendeten Aktionen: Kommunikation mit dem Gerät zulassen oder blockieren.

Über die verfügbaren Buttons können Sie die Geräteliste verwalten:

- **Add** - ein Gerät hinzufügen, das nicht in der Liste aufgeführt ist.
- **Entfernen** - ein ausgewähltes Gerät aus der Liste entfernen.
- **Geräte aktualisieren** - Durchführen eines neuen Scans, um die Geräteliste des Netzwerks zu aktualisieren.

## 16.5. Aktivitätsanzeige

Um die aktuellen Netzwerk-/Internetaktivitäten (über TCP und UDP), sortiert nach Anwendungen, zu überwachen und um das Acronis Internet Security Firewall-Protokoll zu öffnen, folgen Sie folgenden Schritten:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.

2. Gehen Sie zu **Firewall > Aktivität**.

Hier können Sie den Datenvekehr sortiert nach Anwendung einsehen. Für jede Anwendung können Sie die Verbindungen und offenen Ports sehen. Ausserdem Statistiken zum ausgehenden &eingehenden Datenverkehr.

Wenn Sie ebenfalls inaktive Prozesse sehen wollen, lassen Sie das Kontrollkästchen **Inaktive Prozesse verbergen** frei.

Die Bedeutung der Symbole ist wie folgt:

- Zeigt eine ausgehende Verbindung an.
- Zeigt eine eingehende Verbindung an.
- Zeigt einen offenen Port auf Ihrem Computer an.

Das Fenster zeigt die aktuellen Netzwerk/Internetaktivitäten in Echtzeit. Wenn einzelne Verbindungen oder Ports geschlossen werden können Sie sehen wie diese ausgrauen, und evtl. verschwinden.Das selbe kann auch mit Anwendungen im Fenster geschehen welche geschlossen werden.

Eine umfangreiche Ereignisliste zur Verwendung des Firewall-Moduls (Firewall aktivieren/deaktivieren, Datenverkehr blockieren, Einstellungen verändern) oder durch die von diesem Modul entdeckten Aktivitäten (Port-Scan, Verbindungsversuche oder Datenverkehr entsprechend den Regeln blockieren), finden Sie im Acronis Internet Security Firewall-Protokoll. Klicken Sie auf **Protokoll anzeigen**.Die Datei befindet sich im Verzeichnis Gemeinsame Dateien des aktuellen Windows-Benutzers unter dem folgenden Pfad: `...Acronis Internet Security\Acronis Internet Security Firewall\bdfirewall.txt`.

Wenn Sie möchten, dass das Protokoll noch mehr Informationen enthält, wählen Sie **Protokollumfang erweitern**.

## 16.6. Fehlersuche Firewall

Falls Sie ein Problem feststellen, dass möglicherweise mit der Acronis Internet Security-Firewall zusammenhängt, steht ein Fehlersuche-Assistent zur Verfügung, der Ihnen bei der Lösung des Problems hilft.

Um den Assistenten zu starten, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neuen Fenster den Reiter **Einstellungen** und klicken Sie auf **Fehlersuche**.

Experten-Ansicht
: Gehen Sie auf **Firewall > Einstellungen** und klicken Sie auf **Fehlersuche**.

Der Assistent kann Ihnen dabei helfen, die folgenden, normalerweise mit der Firewall-Konfiguration zusammenhängenden, Verbindungsprobleme schnell zu lösen:

- Ich versuche etwas auszudrucken, dies ist aber nicht möglich.
- Ich versuche auf einen Computer meines Netzwerks zuzugreifen, dies funktioniert aber nicht.
- Ich versuche ins Internet zu gehen, dies funktioniert aber nicht.

Falls keine der Beschreibungen auf Ihr Problem zutrifft, wählen Sie **Andere Firewall-Probleme**, um das **Support-Tool** zu öffnen.

Weitere Informationen zu diesem Assistenten finden Sie im Kapitel Fehlersuche in dieser Anleitung.

# 17. Schwachstellen

Ein wichtiger Schritt für den Schutz Ihres Computers gegen Hacker und schädliche Anwendungen besteht darin, das Betriebssystem und die Programme, die Sie oft verwenden, stets auf dem neusten Stand eu halten.Und um einen ungewünschten Zugriff auf Ihren Computer zu vermeiden sind sichere Passwörter (Passwörter die nicht einfach umgangen werden können) für jedes Windows-Benutzerkonto notwendig.

Acronis Internet Security scannt Ihr System regelmäßig auf Schwachstellen und benachrichtigt Sie über die bestehenden Probleme.

## 17.1. Auf Schwachstellen scannen

Sie können Schwachstellen überprüfen und diese beseitigen, indem Sie den Assistenten für den **Schwachstellen-Scan** zu Hilfe ziehen.Um den Assistenten zu starten, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Schwachstellen-Scan**.

Experten-Ansicht
: Gehen Sie zu **Schwachstellen> Status** und klicken Sie auf **Jetzt überprüfen**.

Folgen Sie der sechsstufigen Anleitung, um die Schwachstellen Ihres Systems zu entfernen.Innerhalb des Assistenten können Sie über den Button **Weiter** navigieren. Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Schützen Sie Ihren Rechner**

   Wählen Sie die zu scannenden Schwachstellen.

2. **Problemüberprüfung**

   Bitte warten Sie, bis Acronis Internet Security den Scan auf Schwachstellen beendet hat.

3. **Windows Updates**

   Sie können die Liste der wichtigen und weniger wichtigen Windows-Updates sehen, die zur Zeit nicht auf Ihrem Computer installiert sind.Wählen Sie die Updates, die Sie installieren möchten.

4. **Anwendungs-Updates**

   Wenn eine Anwendung nicht auf dem neusten Stand ist, klicken Sie auf den zur Verfügung stehenden Link um die aktuellste Version herunterzuladen.

5. **Unsichere Passwörter**

Sie können die Liste der auf Ihrem Computer konfigurierten Windows-Benutzerkonten sehen und die Sicherheit, die das jeweilige Passwort bietet.Klicken Sie auf **Beheben**, um unsichere Passwörter zu ändern.

6. **Übersicht**

   Hier können Sie das Ergebnis der Operation sehen.

## 17.2. Status

Um den aktuellen Schwachstellenstatus zu sehen und den automatischen Schwachstellen-Scan zu aktivieren/deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Schwachstellen> Status**.

Jede Tabelle zeigt die gelöste Objekte aus der letzten Schwachstellen Prüfung und deren aktuellen Status an.Hier können Sie sehen, welche Aktion Sie durchführen sollen, um jede Schwachstelle zu beheben, falls welche vorhanden.Wenn die Aktion**Keine** ist, dann wird diese Angelegenheit keine Schwachstelle darstellen.

Wichtig

Um automatisch über System- oder Anwendungsschwachstellen benachrichtigt zu werden, lassen Sie die Option **Automatischer-Scan** aktiviert.

Abhängig vom Problem, um eine spezifische Schwachstelle zu beheben, gehen Sie folgendermaßen vor:

- Wenn Windows Updates verfügbar sind, klicken Sie auf **Installieren** in die **Action** Leiste um diese zu installieren.
- Wenn eine Anwendung veraltet ist, klicken Sie auf **Mehr Infos**, um sich die Versionsinformationen anzusehen und um einen Link auf die Herstellerseite der jeweiligen Software zu finden, von der aus Sie die aktuellste Software-Version installieren können.
- Falls ein Windowskonto über ein schwaches Passwort verfügt, klicken Sie auf **Ansicht& Beheben** und fordern Sie den Benutzer beim nächsten Windows-Login auf, das Passwort zu ändern oder ändern Sie es selbst.Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (so wie #, $ or @).
- Wenn in Windows die Media Autorun-Funktion aktiviert ist, klicken Sie auf **Fest**, um diese zu deaktivieren.

## 17.3. Einstellungen

Um die Einstellungen für die automatische Schwachstellenüberprüfung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Schwachstellen> Einstellungen**.
3. Markieren Sie die Kontrollkästchen der entsprechenden Systemschwachstellen die regelmäßig überprüft werden sollen.
   - **Wichtige Windows Updates**
   - **Reguläre Windows Updates**
   - **Anwendungs-Updates**
   - **Unsichere Passwörter**
   - **Media Autorun**

### Beachten Sie

Wenn Sie das Kontrollkästchen für eine bestimmte Schwachstelle freilassen, wird Acronis Internet Security Sie nicht über die entsprechenden Probleme und Risiken informieren.

# 18. Instant-Messaging-Verschlüsselung

Die Inhalte Ihrer InstantMessaging-Konversationen sollten zwischen Ihnen und Ihrem Chat-Partner bleiben.Durch die Verschlüsselung Ihrer Konversationen können Sie sicherstellen, dass niemand die Inhalte dieser Konversationen auf dem Weg von und zu Ihnen lesen kann.

Acronis Internet Security verschlüsselt standardmäßig alle Ihre Unterhaltungen über IM-Chats, vorausgesetzt dass:

- Ihr Chat-Partner hat ein Acronis Internet Security Produkt installiert das Chat-Verschlüsselung und Chat-Entschlüsselung unterstützt und das für die zum Chatten genutzte Instant Messaging-Anwendung aktiviert ist.
- Sie und Ihr Chatpartner verwenden entweder Yahoo Messenger oder Windows Live (MSN) Messenger.

**Wichtig**
Acronis Internet Security wird die Konversationen nicht verschlüssel, wenn ein Chat-Partner eine webbasierte Chat-Anwendung (wie Meebo) oder eine andere Anwendung, die Yahoo Messenger oder Windows Live (MSN) Messenger unterstützt, verwendet.

Um die Instant Messaging-Verschlüsselung zu konfigurieren:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Verschlüsselung > IM-Verschlüsselung**.

**Beachten Sie**
Sie können die IM-Verschlüsselung für jeden Chat-Partner einfach über die Acronis Internet Security-Symbolleiste im Chat-Fenster konfigurieren.

Standardmäßig ist die Chat-Verschlüsselung sowohl für den Yahoo Messenger als auch für den Windows Live Messenger (MSN) aktiviert.Sie können die IM-Verschlüsselung für eine bestimmte Chat-Anwendung oder komplett deaktivieren.

Zwei Tabellen werden angezeigt:

- **Verschlüsselungsausnahmen** - listet die Benutzer-IDs und das entsprechende InstantMessaging-Programm auf, für das die Verschlüsselung deaktiviert ist.Um einen Kontakt aus der Liste zu entfernen, wählen Sie ihn aus und klicken Sie auf die Schaltfläche **Entfernen**.
- **Alle Aktuelle Verbindungen** - listet die aktuellen Instant Messaging Verbindungen auf (Benutzer ID und entsprechendes IM-Programm) und zeigt an, ob diese verschlüsselt sind oder nicht.Eine Verbindung kann aus folgenden Gründen nicht verschlüsselt sein:

- ▶ Sie haben die Verschlüsselung für den entsprechenden Kontakt deaktiviert.
- ▶ Ihr Kontakt ht kein Acronis Internet Security-Version installiert, die eine Chat-Verschlüsselung unterstützt.

## 18.1. Verschlüsselung für bestimmte Benutzer deaktivieren

Um die Verschlüsselung für einen bestimmten Benutzer zu deaktivieren, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf den Button **Hinzufügen**, um das Konfigurationsfenster zu öffnen.
2. Geben Sie die Benutzer-ID Ihres Kontaktes in das Editierfeld ein.
3. Wählen Sie die Chat-Anwendung des Kontaktes.
4. Klicken Sie auf **OK**.

## 18.2. Acronis Internet Security-Symbolleiste im Chat-Fenster

Sie können die IM-Verschlüsselung einfach über die Acronis Internet Security Symbolleiste aus dem Chat-Fenster heraus konfigurieren.

Die Symbolleiste sollte sich in der unteren rechten Ecke des Chat-Fensters befinden. Sehen Sie nach dem Acronis Internet Security Logo um sie zu finden.

**Beachten Sie**
Die Symbolleiste zeigt durch eine kleine Taste direkt neben dem Acronis Internet Security-Logo an, dass eine Konversation verschlüsselt wurde.

Durch Klicken auf die Acronis Internet Security-Symbolleiste, erhalten Sie die folgenden Optionen:

- **Dauerhaft die Verschlüsselung für Kontakt deaktivieren.**
- **Einladen Kontakt Verschlüsselung zu verwenden.** Um Ihre Konversation zu verschlüsseln, muss auch das Gegenüber Acronis Internet Security installiert haben und ein kompatibles IM Programm verwenden.
- **Kontakt zur Blacklist der Kindersicherung hinzufügen.** Wenn Sie den Kontakt zur Blacklist der Kindersicherung hinzufügen und diese aktiviert ist, so werden Sie keine weitere Nachricht von diesem Kontakt sehen.Um Kontakte aus der Blacklist zu entfernen klicken Sie in der Toolbar auf **Kontakt aus der Blacklist der Kindersicherung entfernen**.

# 19. Dateiverschlüsselung

Die Acronis Internet Security-Dateiverschlüsselung ermöglicht das Erstellen von verschlüsselten, passwortgeschützten logischen Laufwerken (oder einen Tresor) auf Ihrem Computer, in denen Sie sicher Ihre vertraulichen und sensiblen Dokumente speichern können. Auf die Daten, die im Tresor gespeichert sind, können nur die Personen zugreifen, die das Passwort kennen.Die Daten, die im Schutz gespeichert sind, können nur von der Person gesehen werden, die das Passwort kennt.

Mit dem Passwort können Sie einen Tresor öffnen, Daten speichern und den Tresor abschließen, wobei dieser sicher bleibt.Wenn ein Tresor geöffnet ist, können Sie neue Dateien hinzufügen, auf aktuelle Dateien zugreifen oder diese verändern.

Physikalisch ist der Tresor eine auf der lokalen Festplatte gespeicherte Datei mit der Endung bvd.Auch wenn die Dateien, die den Tresor darstellen von anderen Betriebssystemen (beispielsweise Linux) gelesen werden können, können die darin gespeicherten Informationen nicht gelesen werden, weil sie verschlüsselt sind.

Dateiverschlüsselung ist in der Voreinstellung aktiviert.Um diese Funktion zu deaktivieren, gehen Sie folgendermaßen vor:

1. Rechtsklicken Sie in der Systemleiste auf das Acronis Internet Security-Symbol und wählen Sie **Präferenzen**.
2. Im eingeblendeten Fenster "Präferenzen" klicken Sie auf das entsprechende Feld für **Dateiverschlüsselung**.

Wenn Sie Dateiverschlüsselung deaktivieren, wird jeder Tresor abgeschlossen und Sie haben keinen Zugriff mehr auf die sich darin befindenden Dateien.

Datentresore können aus dem Acronis Internet Security-Fenster heraus verwaltet werden oder über die Windows-Kontextmenüs und logischen Laufwerke, die mit dem Tresor verknüpft sind.

## 19.1. Verwaltung der Datentresore über die Acronis Internet Security-Benutzeroberfläche

Die Art und Weise, wie Sie auf Ihre Datentresore zugreifen und diese verwalten, unterscheidet sich je nach der Ansicht, die Sie gewählt haben. Die folgenden Abschnitte zeigen, wie Sie Datentresore verwalten können.

### 19.1.1. Datentresor erstellen

Um einen neuen Tresor zu erstellen, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie auf **Dateispeicherung** und klicken Sie im Bereich Dateiverschlüsselung auf **Datentresor erstellen**.

Experten-Ansicht

Gehen Sie in der Experten-Ansicht auf **Verschlüsselung> Dateiverschlüsselung** und wählen Sie eine der folgenden Alternativen:

- Klicke **Wähle Aktion** über der Datei-Tresor Tabelle und wähle **Neuer Datei-Tresor** aus dem Menü.
- Klicken Sie mit der rechten Maustaste auf die Tresor-Tabelle und wählen Sie **Erstellen**.

Ein neues Fenster wird sich öffnen.

1. Geben Sie den Speicherort und den Namen des Datentresors an.
   - Klicken Sie auf **Durchsuchen**, um den gewünschten Speicherort auszuwählen und den Datentresor unter dem gewünschten Namen zu speichern.
   - Tippen Sie Namen und Pfad des Datentresors auf der Festplatte in die entsprechenden Felder ein.
2. Wählen Sie einen Laufwerkbuchsbuchstaben aus dem Menü.Wenn Sie einen Datentresor öffnen, wird ein virtuelles Laufwerk mit dem gewählten Laufwerkbuchstaben unter Arbeitsplatz erscheinen.
3. Wenn Sie die Standardgröße (50 MB) des Datentresors ändern möchten, geben Sie den gewünschten Wert in das Feld **Tresor-Größe** ein.
4. Geben Sie das neue Passwort des Tresors in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein.Jeder, der den Datentresor öffnen und auf die Dateien zugreifen möchte muss zuerst das Passwort angeben.
5. Klicken Sie auf **Erstellen**, wenn Sie den Datentresor unter dem gewählten Speicherort erstellen möchten.Um den Datentresor als virtuelles Laufwerk unter Arbeitsplatz zu erstellen und anzuzeigen, klicken Sie auf **Erstellen&Öffnen**.

Acronis Internet Security wird Sie unmittelbar über das Ergebnis der Operation informieren.Ist ein Fehler aufgetreten, verwenden Sie die Fehlermeldung, um die Ursache des Fehlers zu finden.Klicken Sie auf **OK**, um dieses Fenster zu schließen.

Beachten Sie

Es ist praktischer, alle Datentresors am gleichen Speicherort zu speichern. So sind Sie einfacher zu finden.

### 19.1.2. Datentresor öffnen

Um auf die Dateien in einem Datentresor zugreifen und mit ihnen arbeiten zu können, muss der Datentresor geöffnet werden.Wenn Sie einen Datentresor öffnen, erscheint ein virtuelles Laufwerk unter Arbeitsplatz.Dieses Laufwerk verfügt über den Laufwerksbuchstaben, der dem Datentresor zugewiesen wurde.

Um einen Datentresor zu öffnen, gehen Sie folgendermaßen vor:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie auf **Verschlüsselung> Dateiverschlüsselung** und wählen Sie eine der folgenden Alternativen:
   - Wählen Sie den Dateitresor aus der Tabelle, klicken Sie auf **Wähle Aktion** oberhalb der Dateitresor-Tabelle und wählen Sie **Öffne Dateitresor** aus dem Menü.
   - Klicken Sie mit der rechten Maustaste auf den Datentresor in der Tabelle und wählen Sie **Öffnen**.

     Beachten Sie
     Wenn ein kürzlich erstellter Tresor nicht in der Tabelle erscheint, klicken Sie auf **Wähle Aktion**, wählen Sie **Einen existierenden Tresor hinzufügen** und blättern Sie zu dessen Speicherort.

   Ein neues Fenster wird sich öffnen.
3. Datentresor Name und Pfad werden angezeigtWählen Sie einen Laufwerkbuchsbuchstaben aus dem Menü.
4. Geben Sie das Datentresor-Passwort in das Feld **Passwort** ein.
5. Klicken Sie auf **Öffnen**.

Acronis Internet Security wird Sie unmittelbar über das Ergebnis der Operation informieren.Ist ein Fehler aufgetreten, verwenden Sie die Fehlermeldung, um die Ursache des Fehlers zu finden.

### 19.1.3. Datentresor abschließen

Wenn Sie mit Ihrer Arbeit im Datentresor fertig sind, müssen Sie diesen abschließen, um Ihre Daten zu schützen.Durch das Verschließen des Datentresors, wird das entsprechende virtuelle Laufwerk auf dem Arbeitsplatz ausgeblendet. Infolgedessen ist der Zugriff auf die sich im Datentresor befindlichen Daten vollständig blockiert.

Um einen Tresor zu sperren, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht

Gehen Sie zu **Dateispeicherung** und führen Sie Folgendes aus:

- Klicken Sie auf den Datentresor im Bereich **Dateiverschlüsselung** und wählen Sie im eingeblendeten Menü **Sperren**
- Klicken Sie im Quick Task-Bereich auf **Datentresor sperren**.

  Ein Assistent wird eingeblendet und hilft Ihnen, den Tresor zu sperren.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Datentresor auswählen**

   Hier können Sie den Datentresor, der abgeschlossen werden soll auswählen.

2. **Bestätigung**

   Hier können Sie die gewählten Prozesse noch einmal betrachten.

3. **Fertigstellen**

   Hier können Sie das Ergebnis der Operation sehen.

Experten-Ansicht

Gehen Sie auf **Verschlüsselung> Dateiverschlüsselung** und wählen Sie eine der folgenden Alternativen:

- Wählen Sie den Tresor aus der Tabelle, klicken Sie auf **Aktion wählen** über der Datei-Tresor Tabelle und wählen Sie **Lock Datei-Tresor abschließen** aus dem Menü.
- Klicken Sie mit der rechten Maustaste auf den Datentresor und wählen Sie **Abschließen**.

Acronis Internet Security wird Sie unmittelbar über das Ergebnis der Operation informieren.Ist ein Fehler aufgetreten, verwenden Sie die Fehlermeldung, um die Ursache des Fehlers zu finden.Klicken Sie auf **OK**, um dieses Fenster zu schließen.

### 19.1.4. Passwort für Datentresor ändern

Der Datentresor muss verschlossen sein, bevor das Passwort geändert werden kann.Zum Ändern des Datentresors passworts, gehen Sie folgendermaßenvor:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie auf **Verschlüsselung> Dateiverschlüsselung** und wählen Sie eine der folgenden Alternativen:

   - Wählen Sie den Tresor aus der Tabelle, klicken Sie auf **Aktion wählen** über der Datei-Tresor Tabelle und wählen Sie **Passwort ändern** aus dem Menü.
   - Klicken Sie mit der rechten Maustaste auf den Datentresor in der Tabelle und wählen Sie **Passwort ändern**.

   Ein neues Fenster wird sich öffnen.
3. Geben Sie das aktuelle Passwort des Datentresors in das Feld **Altes Passwort** ein.
4. Geben Sie das neue Passwort des Datentresors in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein.

**Beachten Sie**

Ihr Passwort muss mindestens 8 Zeichen lang sein.Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (so wie #, $ or @).

5. Klicken Sie auf **OK**, um das Passwort zu ändern.

Acronis Internet Security wird Sie unmittelbar über das Ergebnis der Operation informieren.Ist ein Fehler aufgetreten, verwenden Sie die Fehlermeldung, um die Ursache des Fehlers zu finden.Klicken Sie auf **OK**, um dieses Fenster zu schließen.

### 19.1.5. Dateien dem Datentresor hinzufügen

Um dem Tresor Dateien hinzuzufügen, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht

Gehen Sie auf **Dateispeicherung** und klicken Sie im Quick Task-Bereich auf **Datei dem Tresor hinzufügen**.

Ein Assistent wird eingeblendet und hilft Ihnen, die Dateien einem Tresor hinzuzufügen.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Dateien & Verzeichnisse auswählen**

   Klicken Sie auf **Ziel hinzufügen**, um die Dateien/Verzeichnisse auszuwählen, die im Tresor gespeichert werden sollen.

2. **Datentresor auswählen**

   Sie können einen existierenden Tresor auswählen, nach einem kürzlichverwendeten Tresor suchen oder einen neuen erstellen, in dem Sie dann die Dateien speichern.

3. **Datentresor erstellen**

   Wenn Sie die Anlage eines neuen Tresors gewählt haben, können Sie hier die notwendigen Informationen eingeben. Weitere Informationen finden Sie*„Datentresor erstellen“* (S. 124)

4. **Passwort eingeben**

   Falls Sie einen gesperrten Tresor ausgewählt haben, müssen Sie für dieses das Passwort eingeben.

5. **Bestätigung**

   Hier können Sie die gewählten Prozesse noch einmal betrachten.

6. **Inhalt Datentresor**

   Hier können Sie den Inhalt des Datentresor betrachten.

Experten-Ansicht

1. Gehen Sie auf **Verschlüsselung > Datei-Verschlüsselung**.
2. Wählen Sie aus der Tabelle den Datentresor aus, in dem Sie die Dateien speichern möchten.Falls der Datentresor verschlossen ist, müssen Sie ihn zunächst öffnen (Rechtklick auf den Datentresor und wählen Sie **Öffne Datentresor**).
3. Die Datentresor-Tabelle erscheint.Rechts-klicken Sie innerhalb und wählen Sie **Dateien / Ordner hinzufügen**.
4. Wählen Sie, welche Dateien / Verzeichnisse dem Datentresor hinzugefügt werden sollen.
5. Klicken Sie auf **OK**, um die ausgewählten Objekte in den Datentresor zu kopieren.

### 19.1.6. Dateien entfernen

Um eine Datei aus einem Tresor zu entfernen, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht

Gehen Sie auf **Dateispeicherung** und klicken Sie im Quick Task-Bereich auf **Tresor-Dateien entfernen**.

Ein Assistent wird eingeblendet und hilft Ihnen, die Dateien aus einem Tresor zu entfernen.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Datentresor auswählen**

   Hier können Sie den Datentresor auswählen, aus dem die Dateien entfernt werden sollen.

2. **Passwort eingeben**

   Falls Sie einen gesperrten Tresor ausgewählt haben, müssen Sie für dieses das Passwort eingeben.

3. **Inhalt Datentresor**

   Wählen Sie die Dateien/Verzeichnisse, die aus dem Tresor entfernt werden sollen, aus.

4. **Bestätigung**

   Hier können Sie die gewählten Prozesse noch einmal betrachten.

5. **Fertigstellen**

   Hier können Sie das Ergebnis der Operation sehen.

Experten-Ansicht

1. Gehen Sie auf **Verschlüsselung > Datei-Verschlüsselung**.
2. Wählen Sie aus der Tabelle den Datentresor, der die Dateien enthält, die Sie entfernen möchten.Falls der Datentresor verschlossen ist, müssen Sie ihn zunächst öffnen (Rechtklick auf den Datentresor und wählen Sie **Öffne Datentresor**).
3. Rechtsklicken Sie in der Tabelle die den Tresorinhalt anzeigt auf die zu entfernende Datei und wählen Sie **Löschen**.

### 19.1.7. Tresor-Inhalte ansehen

Um sich die Inhalte eines Datentresors anzusehen, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht

Gehen Sie zu **Dateispeicherung** und führen Sie Folgendes aus:

- Klicken Sie im Quick Task-Bereich auf **Datentresor ansehen**.
- Klicken Sie im Dateitresor-Bereich auf **Dateiverschlüsselung** und wählen Sie im eingeblendeten Menü **Ansicht.**

Ein Assistent wird eingeblendet und hilft Ihnen, die Dateien in einem Tresor anzusehen.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Datentresor auswählen**

   Hier können Sie den Datentresor, dessen Inhalte Sie sehen möchten, auswählen.

2. **Passwort eingeben**

   Falls Sie einen gesperrten Tresor ausgewählt haben, müssen Sie für dieses das Passwort eingeben.

3. **Bestätigung**

   Hier können Sie die gewählten Prozesse noch einmal betrachten.

4. **Inhalt Datentresor**

   Hier können Sie das Ergebnis der Operation sehen.

Experten-Ansicht

1. Gehen Sie auf **Verschlüsselung > Datei-Verschlüsselung**.
2. Wählen Sie aus der Tresor-Tabelle den Tresor, dessen Inhalte Sie einsehen möchten.Falls der Datentresor verschlossen ist, müssen Sie ihn zunächst öffnen (Rechtklick auf den Datentresor und wählen Sie **Öffne Datentresor**).

   Die untere Tabelle zeigt den Inhalt des ausgewählten Tresors an.

### 19.1.8. Datentresor löschen

Um einen Datentresor zu löschen, öffnen Sie Acronis Internet Security und fahren Sie, abhängig von der gewählten Anwendersicht, wie folgt fort:

Standard-Ansicht

1. Gehen Sie zu **Dateispeicherung**.
2. Klicken Sie im Bereich **Dateiverschlüsselung** auf den Datentresor.
3. Wenn der Tresor geöffnet ist, wählen Sie im eingeblendeten Menü die Option **Sperren** und klicken dann erneut auf den Tresor.Wenn der Tresor gesperrt ist, gehen Sie zum nächsten Schritt.
4. Wählen Sie im eingeblendeten Menü **Löschen**.

Experten-Ansicht

1. Gehen Sie auf **Verschlüsselung > Datei-Verschlüsselung**.
2. Wählen Sie den Dateitresor aus der Tabelle, klicken Sie auf **Wähle Aktion** oberhalb der Dateitresor-Tabelle und wählen Sie **Lösche Dateitresor** aus dem Menü.
3. Bestätigen Sie die Aktion indem Sie in dem erscheinenden Fenster auf **Yes** klicken.

Wichtig
Wenn Sie einen Datentresor löschen, werden alle Inhalte ebenfalls gelöscht.

## 19.2. Verwaltung von Datentresors in Windows

Acronis Internet Security integriert sich in Windows, wodurch die Verwaltung Ihrer Datentresors vereinfacht wird.

Das Kontextmenü erscheint wann immer Sie eine Datei oder ein Verzeichnis auf Ihrem Computer oder Desktop rechtsklicken.Gehen Sie in diesem Menü mit der Maus einfach auf den Acronis Internet Security Datentresor und Sie erhalten Zugriff auf alle verfügbaren Tresor-Aktionen.

Zusätzlich wird jedes Mal, wenn Sie einen Tresor öffnen, eine neue logische Partition (ein neues Laufwerk) angezeigt.Öffnen Sie einfach den Arbeitsplatz und Sie sehen ein neues Laufwerk, das den Datentresor darstellt. Sie können Dateiprozesse (kopieren, löschen, ändern, usw) auf diesem Laufwerk durchführen. Die Dateien sind geschützt, solange sie sich in diesem Laufwerk befinden (denn für das Mounten ist ein Passwort notwendig).Wenn Sie fertig sind, schließen Sie Ihren Datentresor ab (unmount), um dessen Inhalt zu schützen.

Sie können die Acronis Internet Security Datentresors auf Ihrem Rechner erkennen, leicht durch das Acronis Internet Security-Symbol und die .bvd-Erweiterung erkennen.

### 19.2.1. Datentresor erstellen

Beachten Sie bitte, dass ein Datentresor eigentlich nur eine Datei mit der Endung .bvd ist.Nur wenn Sie den Datentresor öffnem erscheint im Arbeitsplatz ein virtuelles Laufwerk, in dem Sie leicht Dateien speichern können.Wenn Sie einen Datentresor erstellen, müssen Sie festlegen wo und unter welchem Namen er zu speichern ist. Zudem muss ein Passwort zum Schutz des Inhalts bestimmt werden.Ausschließlich Benutzer, die das Passwort kennen, können den Datentresor öffnen und auf die darin abgelegten Dokumente und Daten zugreifen.

Um einen Datentresor zu erstellen, folgen Sie diesen Schritten:

1. Klicken Sie mit der rechten Maustaste auf Ihren Desktop oder auf ein Verzeichnis Ihres Computers, wählen Sie **Acronis Internet Security Datentresor** und wählen Sie dann **Datentresor erstellen**.Ein neues Fenster wird sich öffnen.
2. Geben Sie den Speicherort und den Namen des Datentresors an.
   - Klicken Sie auf **Durchsuchen**, um den gewünschten Speicherort auszuwählen und den Datentresor unter dem gewünschten Namen zu speichern.
   - Tippen Sie Namen und Pfad des Datentresors auf der Festplatte in die entsprechenden Felder ein.
3. Wählen Sie einen Laufwerkbuchsbuchstaben aus dem Menü.Wenn Sie einen Datentresor öffnen, wird ein virtuelles Laufwerk mit dem gewählten Laufwerkbuchstaben unter Arbeitsplatz erscheinen.
4. Geben Sie das gewünschte Passwort für den Tresor in das**Passwort**und**Bestätigung**Felder.Jeder, der den Datentresor öffnen und auf die Dateien zugreifen möchte muss zuerst das Passwort angeben.
5. Wählen Sie **Laufwerk formatieren**, um das virtuelle Laufwerk des virtuellen Laufwerks zu formatieren.Sie müssen das Laufwerk formatieren, bevor Sie Daten in den Datentresor speichern können.
6. Wenn Sie die Standardgröße (50 MB) des Datentresors ändern möchten, geben Sie den gewünschten Wert in das Feld **Tresor-Größe** ein.
7. Klicken Sie auf **Erstellen**, wenn Sie den Datentresor unter dem gewählten Speicherort erstellen möchten.Um den Datentresor als virtuelles Laufwerk unter Arbeitsplatz zu erstellen und anzuzeigen, klicken Sie auf **Erstellen&Öffnen**.

Acronis Internet Security wird Sie unmittelbar über das Ergebnis der Operation informieren.Ist ein Fehler aufgetreten, verwenden Sie die Fehlermeldung, um die Ursache des Fehlers zu finden.Klicken Sie auf **OK**, um dieses Fenster zu schließen.

**Beachten Sie**
Es ist praktischer, alle Datentresors am gleichen Speicherort zu speichern. So sind Sie einfacher zu finden.

## 19.2.2. Datentresor öffnen

Um auf die Dateien in einem Datentresor zugreifen und mit ihnen arbeiten zu können, muss der Datentresor geöffnet werden.Wenn Sie einen Datentresor öffnen, erscheint ein virtuelles Laufwerk unter Arbeitsplatz.Dieses Laufwerk verfügt über den Laufwerksbuchstaben, der dem Datentresor zugewiesen wurde.

Um einen Datentresor zu öffnen, gehen Sie folgendermaßen vor:

1. Suchen Sie auf Ihrem Computer nach der `.bvd`-Datei, die Sie öffnen möchten.
2. Rechtsklicken Sie auf die Datei, gehen Sie auf **Acronis Internet Security Datentresor** und wählen Sie **Öffnen**.Schneller geht es, wenn Sie auf die Datei doppeltklicken oder sie durch Rechtsklick und **Öffnen** auswählen.Ein neues Fenster wird sich öffnen.
3. Wählen Sie einen Laufwerkbuchsbuchstaben aus dem Menü.
4. Geben Sie das Datentresor-Passwort in das Feld **Passwort** ein.
5. Klicken Sie auf **Öffnen**.

Acronis Internet Security wird Sie unmittelbar über das Ergebnis der Operation informieren.Ist ein Fehler aufgetreten, verwenden Sie die Fehlermeldung, um die Ursache des Fehlers zu finden.Klicken Sie auf **OK**, um dieses Fenster zu schließen.

## 19.2.3. Datentresor abschließen

Wenn Sie mit Ihrer Arbeit im Datentresor fertig sind, müssen Sie diesen abschließen, um Ihre Daten zu schützen.Durch das Verschließen des Datentresors, wird das entsprechende virtuelle Laufwerk auf dem Arbeitsplatz ausgeblendet. Infolgedessen ist der Zugriff auf die sich im Datentresor befindlichen Daten vollständig blockiert.

Um einen Datentresor zu schließen, befolgen Sie die Schritte:

1. Öffnen Sie den Arbeitsplatz, (klicken Sie auf das start Windows Startmenü dann auf **Arbeitsplatz**).
2. Finden Sie das dem Datentresor entsprechende virtuelle Laufwerk.Suchen Sie nach dem Laufwerksbuchstaben, den Sie dem Datentresor beim Öffnen zugewiesen haben.
3. Rechtklicken Sie auf das dazugehörige Laufwerk, gehen Sie dann auf **Acronis Internet Security Datentresor** und klicken Sie auf **Schließssen**.

Sie können auch auf die `.bvd`-Datei rechtsklicken, auf **Acronis Internet Security Datentresor** gehen und auf **Schließen** klicken.

Acronis Internet Security wird Sie unmittelbar über das Ergebnis der Operation informieren.Ist ein Fehler aufgetreten, verwenden Sie die Fehlermeldung, um die Ursache des Fehlers zu finden.Klicken Sie auf **OK**, um dieses Fenster zu schließen.

### Beachten Sie

Sind mehrere Vaults geöffnet, sollten Sie die Experten-Ansicht von Acronis Internet Security verwenden.Wenn Sie auf **Verschlüsselung**, Reiter Datentresor gehen, sehen Sie eine Tabelle, die Ihnen Auskunft über die existierenden Datentresors gibt. Sie sehen, ob der Datentresor geöffnet ist und ggf. dessen Laufwerksbuchstaben.

## 19.2.4. Dem Datentresor hinzufügen

Bevor Sie dem Datentresor Dateien oder Verzeichnisse hinzufügen können, müssen Sie den Datentresor öffnen.Ist der Datentresor geöffnet, können Sie einfach mithilfe des Kontextmenüs Dateien oder Verzeichnisse hinzufügen.Rechtsklicken Sie auf die Datei oder Verzeichnis, das Sie in den Datentresor kopieren möchten, gehen Sie auf **Acronis Internet Security Datentresor** und klicken Sie auf **Dem Datentresor hinzufügen**.

- Wenn nur ein Datentresor geöffnet ist, wird die Datei oder Verzeichnis direkt in diesen kopiert.
- Sind mehrere Datentresors geöffnet, werden Sie aufgefordert auszuwählen in welchen Datentresor das Objekt kopiert werden soll. Wählen Sie aus dem Menü passend zum gewünschten Datentresor den Laufwerksbuchstaben und klicken Sie auf **OK**, um das Objekt zu kopieren.

Sie können auch das entsprechende virtuelle Laufwerk auswählen.Folgen Sie diesen Schritten:

1. Öffnen Sie den Arbeitsplatz, (klicken Sie auf das start Windows Startmenü dann auf **Arbeitsplatz**).
2. Geben Sie das virtuelle Laufwerk des entsprechenden Datentresors ein.Suchen Sie nach dem Laufwerksbuchstaben, den Sie dem Datentresor beim Öffnen zugewiesen haben.
3. Kopieren/Einfügen oder Drag&Drop Sie die Dateien und Verzeichnisse direkt in dieses virtuelle Laufwerk.

## 19.2.5. Aus dem Datentresor entfernen

Um Datein oder Verzeichnisse aus dem Datentresor zu entfernen, muss der Datentresor geöffnet sein.Um Dateien oder Verzeichnisse aus dem Datentresor zu entfernen, gehen Sie folgendermaßen vor:

1. Öffnen Sie den Arbeitsplatz, (klicken Sie auf das start Windows Startmenü dann auf **Arbeitsplatz**).

2. Geben Sie das virtuelle Laufwerk des entsprechenden Datentresors ein.Suchen Sie nach dem Laufwerksbuchstaben, den Sie dem Datentresor beim Öffnen zugewiesen haben.
3. Entfernen Sie Dateien oder Verzeichnisse wie Sie es normalerweise auch in Windows tun (z.B. Rechtsklicken Sie auf die Datei, die Sie löschen möchten und wählen sie **Löschen**)aus.

### 19.2.6. Passwort für Datentresor ändern

Das Passwort schützt den Inhalt des Datentresors vor unberechtigten Zugriffen.Ausschließlich Benutzer, die das Passwort kennen, können den Datentresor öffnen und auf die darin abgelegten Dokumente und Daten zugreifen.

Der Datentresor muss verschlossen sein, bevor das Passwort geändert werden kann.Zum Ändern des Datentresors passworts, gehen Sie folgendermaßenvor:

1. Suchen Sie auf Ihrem Computer nach der `.bvd`-Datei, in der sich die entsprechende Datei befindet.
2. Rechtsklicken Sie auf die Datei, gehen Sie auf **Acronis Internet Security Datentresor** und wählen Sie **Tresor-Passwort ändern**.Ein neues Fenster wird sich öffnen.
3. Geben Sie das aktuelle Passwort des Datentresors in das Feld **Altes Passwort** ein.
4. Geben Sie das neue Passwort des Datentresors in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein.

   #### Beachten Sie

   Ihr Passwort muss mindestens 8 Zeichen lang sein.Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (so wie #, $ or @).

5. Klicken Sie auf **OK**, um das Passwort zu ändern.

Acronis Internet Security wird Sie unmittelbar über das Ergebnis der Operation informieren.Ist ein Fehler aufgetreten, verwenden Sie die Fehlermeldung, um die Ursache des Fehlers zu finden.Klicken Sie auf **OK**, um dieses Fenster zu schließen.

# 20. Spiele-/Laptop-Modus

Das Modul Spiele-/Laptop-Modus bietet ihnen die Möglichkeit spezielle Betriebsmodi von Acronis Internet Security zu konfigurieren.

- Der Spiele-Modus verändert vorübergehend die Produkteinstellungen, um die Systembelastung während des Spielens möglichst gering ist.
- Der Laptop-Modus stoppt voreingestellte Aufgaben wenn der Laptop über einen Akku betrieben wird, um dessen Laufzeit zu verlängern.
- Stumm-Modus modifiziert vorübergehend die Produkteinstellungen, so dass das Ansehen eines Films oder das Halten einer Präsentation nicht unterbrochen wird.

## 20.1. Spiele-Modus

Der Spiele-Modus ändert die Schutzeinstellungen zeitweise, dass ihr Einfluss auf die Leistungsfähigkeit des Systems so gering wie möglich ist.Wenn Sie den Spiele-Modus aktivieren, werden folgende Einstellungen angewendet:

- Alle Acronis Internet Security-Alarme und Pop-ups werden deaktiviert.
- Der Acronis Internet Security Echtzeitschutz wird auf **Tolerant** gestellt.
- Die Acronis Internet Security Firewall ist auf**Alle zulassen** eingestellt.Das bedeutet, dass alle neuen Verbindungen (eingehend und ausgehend) automatisch erlaubt werden, unabhängig vom verwendeten Port oder Protokoll.
- Updates werden nicht standardmäßig durchgeführt.

> **Beachten Sie**
> Um diese Einstellung zu ändern, gehen Sie zu Update > Einstellungen und deaktivieren Sie das Kontrollkästchen **Kein Update im Spiele-Modus**.

Acronis Internet Security wechselt standardmäßig in den Spiele-Modus, wenn Sie ein Spiel starten, das sich auf der Liste der bekannten Spiele von Acronis Internet Security befindet, oder wenn eine Anwendung im Vollbildmodus ausgeführt wird.Sie können den Spiele-Modus manuell über das Tastaturkürzel `Strg+Alt+Shift+G` aktivieren.Es wird dringend empfohlen dass Sie den Spiele-Modus verlassen, wenn Sie mit dem Spielen fertig sind (Sie können dafür das selbe Tastenkürzel verwenden `Ctrl+Alt+Shift+G`).

> **Beachten Sie**
> Wenn der Spiele-Modus aktiviert ist, sehen Sie den Buchstaben G über dem Acronis Internet Security Symbol.

Konfiguration des Spiele-Modus:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Spiele-/Laptop-Modus> Spiele-Modus**.

Im oberen Bereich des Abschnitts können Sie den Status des Spiele-Modus sehen.Um den aktuellen Status zu ändern, können Sie auf **Spiele-Modus ist aktiviert** oder **Spiele-Modus ist deaktiviert** klicken.

### 20.1.1. Konfiguration des Automatischen Spiele-Modus

Im automatischen Spiele-Modus kann Acronis Internet Security selbständig den Spiele-Modus starten, wenn ein Spiel gefunden wird.Folgende Optionen können konfiguriert werden:

- **Die Acronis Internet Security-Standardspieleliste verwenden** - damit Acronis Internet Security automatisch in den Spiele-Modus wechselt, wenn Sie ein in der Liste aufgeführtes Spiel starten.Um diese Liste zu sehen, klicken Sie auf **Spiele verwalten** und dann **Erlaubte Spiele ansehen**.
- **Vollbildmodus** - Sie können wählen, ob automatisch in den Spiele- oder Stumm-Modus gewechselt werden soll, sobald eine Anwendung im Vollbildmodus angezeigt wird.
- **Frage mich ob ich Anwendungen in Full-Screen zur Whitelist hinzufügen möchte?** - um aufgefordert zu werden, ob ein neues Spiel zur Whitelist hinzugefügt werden soll, wenn Sie das Vollbild verlassen.Wenn Sie ein neues Spiel zur Spieleliste hinzufügen, wird Acronis Internet Security den Spiele-Modus automatisch starten, wenn Sie diese Anwendung das nächste Mal starten.

**Beachten Sie**
Wenn Sie nicht möchten, dass Acronis Internet Security den Spiele-Modus automatisch startet, lassen Sie das Kontrollkästchen **Automatischer Spiele-Modus ist aktiviert** frei.

### 20.1.2. Spieleliste verwalten

Acronis Internet Security startet den Spiele-Modus automatisch, wenn eine Anwendung gestartet wird, die sich auf der Spieleliste befindet.Um die Spieleliste zu sehen und zu verwalten, klicken Sie auf**Spiele verwalten**.Ein neues Fenster wird sich öffnen.

Neue Anwendungen werden automatisch zur Liste hinzugefügt, wenn:

- Sie ein Spiel starten, das Acronis Internet Security bekannt ist.Um diese Liste zu sehen, klicken Sie auf **Erlaubte Spiele betrachten**.
- Nachdem Sie das Vollbild beendet haben, können Sie das Spiel über das Aufforderungsfenster zur Spieleliste hinzufügen.

Wenn Sie den automatischen Spiele-Modus für eine bestimmte Anwendung auf der Liste deaktivieren möchten, lassen Sie das entsprechende Kontrollkästchen frei.Sie sollten den automatischen Spiele-Modus für reguläre Anwendungen, die den gesamten Bildschirm verwenden, wie Web-Browser und Mediaplayer, deaktiviert lassen.

Um die Spiele-Liste zu verwalten, können Sie die Schaltflächen verwenden, die sich im oberen Bereich der Tabelle befineden:

- Klicken Sie auf **Hinzufügen** um eine neue Anwendung zu der Spieleliste hinzufügen.
- **Entfernen** - dient zum Entfernen einer Anwendung von der Spieleliste.
- Klicken Sie auf **OK** um den Eintrag aus der Spieleliste zu editieren.

### 20.1.3. Spiele hinzufügen oder bearbeiten

Wenn Sie der Spieleliste einen Eintrag hinzufügen oder bearbeiten möchten, wird folgendes Fenster eingeblendet:

Klicken Sie auf **Durchsuchen** um die Anwendung auszuwählen oder geben Sie den vollständigen Pfad der Anwendung in das Editierfeld ein.

Wenn Sie nicht möchten, dass automatisch in den Spiele-Modus wechselt, wenn eine bestimmte Anwendung gestartet wird, wählen Sie **Deaktivieren**.

Klicken Sie auf **OK** um den Eintrag zu der Spieleliste hinzuzufügen.

### 20.1.4. Konfiguration der Einstellungen des Spiele-Modus

Um das Verhalten voreingestellter Aufgaben zu konfigurieren, verwenden Sie diese Optionen:

- **Dieses Modul aktivieren, um geplante Antivirus-Scan-Aufgaben zubearbeiten** - um zu verhindern, dass geplante Scan-Aufgaben starten, während der Spiele-Modus aktiviert ist.Folgende Optionen sind wählbar:

| Optionen | Beschreibung |
|---|---|
| **Aufgabe überspringen** | Die voreingestellte Aufgabe wird überhaupt nicht ausgeführt. |
| **Aufgabe verschieben** | Die geplante Aufgabe sofort ausgeführen, wenn der Spiele-Modus beendet wird. |

Um die Acronis Internet Security Firewall automatisch zu deaktivieren, wenn der Spiele-Modus ausgeführt wird, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **Weitere Einstellungen**.Ein neues Fenster wird sich öffnen.

2. Wählen Sie die **Stelle Firewall auf Alle erlauben** Check-Box.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

### 20.1.5. Änderung der Tastenkombination des Spiele-Modus

Sie können den Spiele-Modus manuell aktivieren, indem Sie die VoreinstellungCtrl+Alt+Shift+GHotkey.Wenn Sie die Tastenkombination ändern möchten, befolgen Sie folgende Schritte:

1. Klicken Sie auf **Weitere Einstellungen**.Ein neues Fenster wird sich öffnen.
2. Unter der Option **Aktiviere Spiele-Modus Hotkeys** können Sie die gewünschte Tastenkombination festlegen:
   - Wählen Sie die Tastenkombination die Sie verwenden möchten indem Sie folgende Tasten markieren : Steuerung (Strg), Shift (Shift) oder Alt-Taste (Alt).
   - Geben Sie im Editierfeld die Taste ein, die Sie benutzen möchten.

   Wenn Sie beispielsweise die Tastenkombination Strg+Alt+D benutzen möchten, markieren Sie Strg und Alt und geben Sie D ein.

   **Beachten Sie**
   Um den Hotkey zu deaktivieren, löschen Sie die **Aktiviere Spiele-Modus Hotkeys** Box.

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

## 20.2. Laptop-Modus

Der Laptop-Modus wurde für Nutzer von Laptops und Notebooks konzipiert. Er soll den Energieverbrauch von Acronis Internet Security so gering wie möglich halten um den Einfluss auf die Akkulaufzeit zu minimieren.

Während der Laptop-Modus ausgeführt wird, werden voreingestellte Aufgaben standardmäßig nicht durchgeführt.

Acronis Internet Security erkennt, wenn Ihr Laptop im Akkubetrieb läuft und startet den Laptop-Modus automatisch.Ebenso beendet Acronis Internet Security automatisch den Laptop-Modus, wenn erkannt wird dass der Laptop nicht mehr über einen Akku betrieben wird.

Konfiguration des Laptop-Modus:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Spiele-/Laptop-Modus> Laptop-Modus**.

Sie können sehen ob der Laptop-Modus aktiviert ist oder nicht.Ist der Laptop-Modus aktiviert, wird Acronis Internet Security die konfigurierten Einstellungen anwenden, während der Laptop über einen Akku betrieben wird.

### 20.2.1. Einstellungen des Laptop-Modus konfigurieren

Um das Verhalten voreingestellter Aufgaben zu konfigurieren, verwenden Sie diese Optionen:

- **Dieses Modul aktivieren, um geplante Antivirus-Prüfaufgaben zu bearbeiten** - um zu verhindern dass geplante Prüfaufgaben starten, während der Laptopmodus aktiviert ist.Folgende Optionen sind wählbar:

| Optionen | Beschreibung |
|---|---|
| **Aufgabe überspringen** | Die voreingestellte Aufgabe wird überhaupt nicht ausgeführt. |
| **Aufgabe verschieben** | Die Aufgabe wird sofort durchgeführt, sobald der Laptop-Modus beendet wird. |

## 20.3. Stumm-Modus

Der Stumm-Modus ändert die Tresoreinstellungen vorübergehend, so dass ihr Einfluss auf die Leistungsfähigkeit des Systems so gering wie möglich ist.Wenn der Stumm-Modus aktiviert ist, werden folgende Einstellungen angewendet:

- Alle Acronis Internet Security-Alarme und Pop-ups werden deaktiviert.
- Die Acronis Internet Security Firewall ist auf**Alle zulassen** eingestellt.Das bedeutet, dass alle neuen Verbindungen (eingehend und ausgehend) automatisch erlaubt werden, unabhängig vom verwendeten Port oder Protokoll.
- Voreingestellte Prüfaufgaben sind standardmäßig deaktiviert.

Als Voreinstellung wechselt Acronis Internet Security automatisch in den Stumm-Modus, sobald Sie einen Film ansehen, eine Präsentation halten oder eine Anwendung im Vollbildmodus nutzen.Wir empfehlen dringend, den Stumm-Modus zu verlassen, wenn Sie den Film zu Ende gesehen oder die Präsentation beendet haben.

**Beachten Sie**
Wenn Sie sich im Stumm-Modus befinden, verändert sich das kleine Acronis Internet Security-Symbol neben der Computeruhr ein wenig.

Konfiguration des Stumm-Modus:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.

2. Gehen Sie zu **Spiele-/Laptop-Modus> Stumm-Modus**.

Im oberen Bereich des Abschnitts können Sie den Status des Stumm-Modus sehen.Um den aktuellen Status zu ändern, können Sie auf **Stumm-Modus ist aktiviert** oder **Stumm-Modus ist deaktiviert** klicken.

### 20.3.1. Konfiguration Vollbildschirmaktion

Folgende Optionen können konfiguriert werden:

- **Vollbildmodus** - Sie können wählen, ob automatisch in den Spiele- oder Stumm-Modus gewechselt werden soll, sobald eine Anwendung im Vollbildmodus angezeigt wird.
- **Frage mich ob ich Anwendungen in Full-Screen zur Whitelist hinzufügen möchte?** - um aufgefordert zu werden, ob eine neue Anwendung zur Whitelist hinzugefügt werden soll, wenn Sie das Vollbild verlassen.Wenn Sie eine neue Anwendung zur Spieleliste hinzufügen, wird Acronis Internet Security den Spiele-Modus automatisch starten, wenn Sie diese Anwendung das nächste Mal starten.

**Beachten Sie**
Wenn Sie nicht möchten, dass Acronis Internet Security automatisch in den Stumm-Modus wechselt, deaktivieren Sie die Option **Vollbildschirm-Aktion**.

### 20.3.2. Konfiguration der Einstellungen des Stumm-Modus

Um das Verhalten voreingestellter Aufgaben zu konfigurieren, verwenden Sie diese Optionen:

- **Dieses Modul aktivieren, um geplante Antiviren-Scans zu bearbeiten** - um zu verhindern, dass geplante Scans starten, während der Stumm-Modus aktiviert ist.Folgende Optionen sind wählbar:

| Optionen | Beschreibung |
|---|---|
| **Aufgabe überspringen** | Die voreingestellte Aufgabe wird überhaupt nicht ausgeführt. |
| **Aufgabe verschieben** | Die Aufgabe wird sofort durchgeführt, sobald der Stumm-Modus verlassen wird. |

# 21. Heimnetzwerk

Mit dem Netzwerk-Modul können Sie die auf den Computern Ihres Haushalts installierten Acronis Internet Security-Produkte von einem Computer aus verwalten.Um auf das Modul "Heimnetzwerk" zuzugreifen, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
Gehen Sie auf den Reiter **Netzwerk**.

Experten-Ansicht
Gehe zu **Heimnetzwerk**.

Beachten Sie
Im Bereich Meine Werkzeuge können Sie eine Verknüpfung hinzufügen.

Um die Acronis Internet Security Produkte, die auf den Computern in Ihrem Haushalt installiert sind verwalten zu können, befolgen Sie diese Schritte:

1. Aktivieren Sie das Acronis Internet Security-Heimnetzwerk auf Ihrem Computer.Legen Sie Ihren Computer als Server fest.
2. Fügen Sie jeden Computer, den Sie verwalten möchten dem Home-Netzwerk hinzu (Passwort einstellen).Defenieren Sie jeden Computer als Normal.
3. Fügen Sie die Computer die Sie verwalten möchten ebenfalls auf Ihrem Computer hinzu.

## 21.1. Aktivierung des Acronis Internet Security-Netzwerks

Zur Aktivierung des Acronis Internet Security-Heimnetzwerks gehen Sie folgendermaßen vor:

1. Klicken Sie **Netzwerk aktivieren**.Sie werden dazu aufgefordert, das Passwort für die Home-Verwaltung zu konfigurieren.
2. Geben Sie das selbe Passwort in jedes der Editierfelder ein.
3. Legen Sie die Rolle des Computers im Acronis Internet Security-Heimnetzwerk fest:
   - **Server-Computer** - aktivieren Sie diese Option auf dem Computer, von dem aus alle anderen verwaltet werden sollen.
   - **Normaler Computer** - aktivieren Sie diese Option auf den Computern, die vom Server-Computer aus verwaltet werden.
4. Klicken Sie auf **OK**.

Sie sehen den Namen des Computers in der Netzwerkübersicht.

Der Button **Netzwerk deaktivieren** wird eingeblendet.

## 21.2. Computer dem Acronis Internet Security-Netzwerk hinzufügen

Jeder Computer, der die folgenden Kriterien erfüllt, wird automatisch dem Netzwerk hinzugefügt:

- das Acronis Internet Security-Heimnetzwerk ist auf diesem Computer aktiviert.
- der Computer wurde als normaler Computer definiert.
- das Passwort für die Aktivierung des Netzwerks ist dasselbe wie für den Server-Computer.

**Beachten Sie**
In der Experten-Ansicht können Sie jederzeit das Heimnetzwerk auf Computer scannen, die den Kriterien entsprechen, indem Sie auf den Button **Auto-Suche** klicken.

Um vom Master Computer aus einen Computer dem Acronis Internet Security-Heimnetzwerk hinzuzufügen, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **PC hinzufügen**.
2. Geben Sie das Passwort für die Home-Verwaltung ein und klicken Sie auf **OK**.Ein neues Fenster wird sich öffnen.

   Sie können eine Liste der Computer im Netzwerk sehen.Die Bedeutung des Symbols ist wie folgt:

    Zeigt einen Online-Computer an, auf dem keine Acronis Internet Security-Produkte installiert sind.

    Zeigt einen Online-Computer an, auf dem Acronis Internet Security installiert ist.

    Zeigt einen Offline-Computer an, auf dem Acronis Internet Security installiert ist.
3. Sie können hierzu eine der folgenden Methoden wählen:
   - Wählen Sie aus der Liste den Namen des Computers der hinzugefügt werden soll:
   - Geben Sie die IP-Adresse oder den Namen des Computers, der hinzugefügt werden soll in das dafür vorgesehene Feld ein.
4. Klicken Sie auf **Hinzufügen**.Sie werden dazu aufgefordert, das Passwort der Home-Verwaltung für den entsprechenden Computer einzugeben.
5. Geben Sie das Passwort für die Home-Verwaltung ein, das auf dem entsprechenden Computer konfiguriert wurde.

6. Klicken Sie auf **OK**.Wenn Sie das korrekt Passwort angegeben haben, wird der ausgewählte Computername in der Netzwerkübersicht erscheinen.

## 21.3. Verwaltung des Acronis Internet Security-Netzwerks

Wenn Sie das Acronis Internet Security Heimnetzwerk erstellt haben, können Sie alle Acronis Internet Security Produkte von einem Computer aus verwalten.

Wenn Sie den Mauszeiger auf einen Computer der Netzwerkübersicht bewegen, können Sie einige Informationen über diesen sehen (Name, IP-Adresse, Anzahl der Systemsicherheitsprobleme die, Acronis Internet Security-Registrierungsstatus).

Wenn Sie mit der rechten Mautaste auf einen Computernamen im Netzwerk klicken, können Sie alle administrativen Aufgaben sehen, die Sie auf dem Remote-Computer ausführen können.

- **Passwort für Einstellungen festlegen**

  Erlaubt Ihnen einen Passwort zu erstellen um den Zugang zu den Acronis Internet Security Einstellungen auf diesem PC einzuschränken.

- **Prüfaufgabe ausführen**

  Lässt sie eine On-Demand Prüfung auf dem Remote-PC durchführen. Sie können jede der folgenden Prüfungen tätigen: Meine Dokumente- System-, oder tiefgehende System-Prüfung.

- **Alle Probleme auf diesem PC beheben**

  Lässt Sie alle Risiken die die Sicherheit Ihres Systems gefährden beheben, indem Sie dem Alle Risiken beheben Assistenten folgen.

- **Historie/Ereignisse anzeigen**

  Erlaubt den Zugriff auf das Modul **Verlauf & Ereignisse** des auf diesem PC installierten Acronis Internet Security-Produkts.

- **Jetzt aktualisieren**

  Startet das Update für das auf diesem Computer installierte Acronis Internet Security-Produkt.

- **Kindersicherungsprofil festlegen**

  Erlaubt die Festlegung des Alterskategoriefilters, der für diesen PC verwendet werden soll.

- **Als Update Server für dieses Netzwerk festlegen**

  Erlaubt Ihnen, diesen Rechner als Update-Server, für alle Rechner des Netzwerks auf denen wo Acronis Internet Security installiert ist, festzulegen.Unter Verwendung dieser Option, wird der Internetverkehr verringert, weil nur ein Rechner aus dem Netzwerk sich an das Internet anschließt um die Updates herunterzuladen.

- **PC aus dem Heimnetzwerk entfernen**

  Erlaubt Ihnen einen Pc aus dem Netzwerk entfernen.

Wenn Acronis Internet Security in der Standard-Ansicht läuft, können Sie mehrere Aufgaben auf allen Netzwerk-Computern gleichzeitig ausführen, indem Sie auf die entsprechenden Buttons klicken.

- **Alle prüfen** - bietet Ihnen die Möglichkeit alle verwalteten Computer gleichzeitig zu prüfen.
- **Alle aktualisieren** - bietet Ihnen die Möglichkeit alle verwalteten Computer gleichzeitig zu aktualisieren.

Bevor Sie eine Aufgabe auf einem bestimmten Computer ausführen können, werden Sie dazu aufgefordert das Passwort der lokalen Home-Verwaltung anzugeben.Geben Sie das Passwort für die Home-Verwaltung ein und klicken Sie auf **OK**.

### Beachten Sie

Wenn Sie mehrere Aufgaben durchführen möchten, dann wählen Sie **In dieser Sitzung nicht nochmals fragen**.Wenn Sie diese Option wählen, werden Sie während der laufenden Sitzung nicht nochmals nach einem Passwort gefragt.

# 22. Aktualisierung

Jeden Tag werden neue Viren entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie das Programm Acronis Internet Security stets mit den neuesten Virensignaturen betreiben.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet die Acronis Internet Security-Software eigenständig. Sie überprüft beim Start des Computers, ob neue Virensignaturen verfügbar sind und sucht nach Bedarf anschließend jede **Stunde** nach Updates.

Wenn ein Update entdeckt wird, können Sie um eine Bestätigung für das Update gebeten werden oder das Update wird automatisch durchgeführt, je nach den Einstellungen für das automatische Update.

Der Updatevorgang wird "on the fly" durchgeführt, das bedeutet die entsprechenden Dateien stufenweise geupdated werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System wird nicht gefährdet.

Wichtig

Um den Schutz vor Spyware aus dem Internet zu gewährleisten, halten Sie Ihre **Automatisches Update** Funktion jederzeit aktiviert.

Folgende Update-Möglichkeiten stehen zur Verfügung:

- **Updates für die AntiViren-Schutz** - Täglich gibt es neue Bedrohungen für Ihren PC. Daher müssen die Virendefinitionen stets auf den neusten Stand gebracht werden. Diesen Vorgang nennt man **Virendefinitions-Update**.
- **Updates für die Antispam Prüfung** - Um den Spamschutz zu verbessern, werden neue Regeln zur Heuristik und zum URL-Filter hinzugefügt. Diesen Vorgang nennt man **Antispam-Update**.
- **Updates für die AntiSpyware Prüfung** - Neue Spyware Signaturen werden kontinuierlich zur Acronis Internet Security Datenbank hinzugefügt. Diesen Vorgang nennt man **AntiSpyware-Update**.
- **Produkt-Update** - Wenn eine neue Version von Acronis Internet Security erscheint, mit neuen Funktionen und Erkennungstechniken, die eine Verbesserung der Such- und Erkennungsleistung mit sich bringt. Diesen Vorgang nennt man **Produkt-Update**.

## 22.1. Durchführung eines Updates

Das automatische Update kann auch jederzeit über den Klick **Prüfen** erfolgen. Diese Funktion wird auch als **benutzergesteuertes Update** bezeichnet.

Für ein Acronis Internet Security-Update gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

**Basis-Ansicht**

Klicken Sie im Bereich "Meinen PC schützen" auf das Symbol **Jetzt aktualisieren**.

**Standard-Ansicht**

Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Jetzt aktualisieren**.

**Experten-Ansicht**

Gehen Sie zu **Update > Update**.

Das **Update**-Modul verbindet Ihren Computer automatisch mit dem Acronis Internet Security Update Server und informiert Sie bei einem verfügbaren Update. Wenn ein neues Update verfügbar ist, wird je nach vorgenommener Einstellung entweder abgefragt, ob das Update erfolgen soll oder das Update erfolgt automatisch.

Wichtig

Möglicherweise kann ein Neustart nach dem vollständig durchgeführten Update notwendig werden. Wir empfehlen Ihnen, den Neustart möglichst bald durchzuführen.

Beachten Sie

Falls Sie über eine Internetverbindung per Einwahl verfügen, ist es sinnvoll, regelmäßig ein manuelles Acronis Internet Security-Update durchzuführen.Für weitere Informationen lesen Sie bitte *„Wie Sie ein Acronis Internet Security-Update mit einer langsamen Internetverbindung durchführen.“* (S. 170).

## 22.2. Konfiguration der Update-Einstellungen

Updates können vom lokalen Netz, über das Internet, direkt oder durch einen Proxy-Server durchgeführt werden.Standardmäßig scannt Acronis Internet Security jede Stunde auf neue Updates und installiert diese ohne Ihr Zutun.

Konfiguration der Update-Einstellungen:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Update > Einstellungen**.
3. Konfigurieren Sie die Einstellungen nach Ihren Wünschen. Um herauszufinden was eine Option macht, halten Sie den Mauszeiger darüber und lesen die angezeigte Beschreibung im unteren Teil des Fensters.
4. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Wenn Sie die Standardeinstellungen anwenden möchten, klicken Sie auf **Standard**.

### 22.2.1. Update-Adresse

Um eine Update-Adresse festzulegen verwenden Sie die Optionen der **Update-Adresse** Kategorie.

**Beachten Sie**
Ändern Sie diese Einstellungn nur wenn Sie mit einem Acronis Internet Security lokalen Update-Server verbunden sind oder wenn das Update über einen Proxy erfolgt.

Um einen der Update-Orte zu verändern, geben Sie die Adresse des lokalen Updateservers in das entsprechende Feld ein.

**Beachten Sie**
Wir empfehlen den Primären Updateserver auf den lokalen Server zu ändern und den sekundären Server unverändert zu belassen sodass im Falle eines lokalen Serverausfalls dennoch Updates durchgeführt werden können.

Wenn Ihr Computer über einen Proxyserver mit dem Internet verbunden ist, wählen Sie **Proxy benutzen**und konfigurieren Sie die Proxyserver-Einstellungen .Weitere Informationen finden Sie unter „Verbindungseinstellungen“ (S. 37)

### 22.2.2. Automatisches Update konfigurieren

Um die Optionen des Acronis Internet Security Automatischen Updates zu konfigurieren verwenden Sie die Optionen der Kategorie **Einstellungen für das Automatische Update**.

Sie können die Anzahl der Stunden zwischen zwei aufeinander folgenden Updateprüfungen im Feld **Zeitinterval** festlegen. Standardmässig ist dieses auf eine Stunde eingestellt.

Um festzulegen wie das automatische Update durchgeführt werden soll können Sie zwischen den folgenden Optionen wählen:

- **Update im Hintergrund** - Acronis Internet Security führt Updates komplett selbständig durch.
- **Nachfragen bevor Update heruntergeladen werden** - Immer wenn ein Update verfügbar ist werden Sie gefragt ob dieser heruntergeladen werden soll.
- **Nachfragen bevor Updates installiert werden** - Acronis Internet Security frägt den Benutzer bevor ein Update installiert wird.

### 22.2.3. Manuelle Update Einstellungen

Um festzulegen wie ein manuelles Update durchgeführt wird wählen Sie ein der folgenden Optionen in der Kategorie **Einstellungen für das manuelle Update**:

- **Stilles Update** - Acronis Internet Security führt Updates, ohne Benutzereingriff, komplett selbständig im Hintergrund durch.

- **Nachfragen bevor Update heruntergeladen werden** - Immer wenn ein Update verfügbar ist werden Sie gefragt ob dieser heruntergeladen werden soll.

### 22.2.4. Weitere Einstellungen konfigurieren

Um sicherzustellen, dass Sie bei der Arbeit nicht vom Acronis Internet Security Update-Vorgang gestört werden, stehen in der Kategorie **Erweiterte Einstellungen** folgende Optionen zur Verfügung:

- **Auf Neustart warten, anstatt nachzufragen** - Ist für ein Update ein Neustart notwendig von Acronis Internet Security, arbeitet das System bis zum nächsten Neustart mit den alten Dateien weiter. Der Benutzer wird nicht um einen Neustart gebeten und somit nicht bei seiner Arbeit gestört.
- **Update-Sharing (P2P) aktivieren** - wenn Sie den Einfluss des Netzwerk-Datenverkehrs auf Ihre Systemleistung während der Durchführung von Updates minimieren möchten, verwenden Sie die Option "Update-Sharing".Acronis Internet Security benutzt Ports 8880 - 8889 für die Update-Sharing.
- **Acronis Internet Security-Dateien von diesem PC uploaden** - Acronis Internet Security ermöglicht das Teilen der neuesten Antiviren-Signaturen auf Ihrem PC mit anderen Acronis Internet Security-Benutzern.
- **Nicht aktualisieren, wenn ein Scan durchgeführt wird** - Acronis Internet Security wird kein Update durchführen, solange ein Scan läuft. Auf diese Weise beeinflusst der Acronis Internet Security Update-Vorgang nicht den Scan-Ablauf.

**Beachten Sie**
Sollte Acronis Internet Security während eines Scans aktualisiert werden, wird der Scan abgebrochen.

- **Nicht aktualisieren, wenn der Spiele-Modus aktiv ist** - wenn der Spiele-Modus aktiviert ist, wird Acronis Internet Security kein Update durchführen.Durch diese Option können Sie den Einfluss der Anwendung, auf die Geschindigkeit während des Spielens minimieren.

# Wie man

# 23. Wie kann ich Dateien und Verzeichnisse scannen?

Scannen mit Acronis Internet Security ist einfach und flexibel.Es gibt mehrere Arten, wie das Scannen von Dateien und Verzeichnissen auf Viren und andere Malware durch Acronis Internet Security gehandhabt werden kann:

- Unter Verwendung des Windows Kontext Menus
- Unter Verwendung von Prüfaufgaben
- Aktivitätsanzeige

Sobald Sie die Prüfung eingeleitet haben wird der Antivirus Prüfassistent erscheinen und Sie durch den Handlungsprozess leiten.Weitere Informationen zu diesem Assistenten finden Sie unter *„Antivirus Prüfassistent“ (S. 49)*.

## 23.1. Unter Verwendung des Windows Kontext Menus

Dies ist der einfachste und empfohlene Weg eine Datei oder Ordner auf Ihrem Computer zu prüfen.Rechtsklicken Sie das zu prüfende Objekt und wählen Sie **Mit Acronis Internet Security prüfen** aus dem Menü aus.Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.

Typische Situationen in welchen Sie diese Prüfmethode verwenden würden schliessen das Folgende ein:

- Sie verdächtigen eine bestimmte Datei oder Ordner infiziert zu sein.
- Wann immer Sie vom Internet Dateien herunterladen von denen Sie glauben infiziert zu sein.
- Prüfen Sie einen freigegebnen Ordner bevor Sie von ihm Dateien auf Ihren Rechner kopieren.

## 23.2. Unter Verwendung von Prüfaufgaben

Wenn Sie Ihren Computer oder bestimmte Ordner regelmässig prüfen lassen möchten, so sollten Sie in Betracht ziehen hierfür eine Prüfaufgabe zu verwenden.Scan-Aufgaben weisen Acronis Internet Security an, wo zu scannen ist und welche Option und Aktionen zu tätigen sind. Außerdem können Sie diese Aufgaben planen und sie regelmäßig oder zu einer bestimmten Zeit laufen lassen.

Um Ihren Computer unter Verwendung von Scan-Aufgaben scannen zu lassen, öffnen Sie die Acronis Internet Security Benutzeroberfläche und starten dort die gewünschte Scan-Aufgabe.Abhängig von der Benutzeransicht, ist verschiedenen Schritten zur Durchführung einer Prüfaufgabe zu folgen.

## Starten von Scan-Aufgaben in der Basisansicht

In der Basis-Ansicht können Sie eine Reihe von vorkonfigurierten Scan-Aufgaben ausführen.Klicken Sie auf den Button **Sicherheit** und wählen Sie eine der verfügbaren Scan-Aufgaben.Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.

## Ausführen einer Scan-Aufgabe in der Standard-Ansicht

In der Standard-Ansicht können Sie eine Reihe von vorkonfigurierten Scan-Aufgaben ausführen. Zudem können benutzerdefinierte Scan-Aufgaben konfiguriert und ausgeführt werden, um bestimmte Bereiche Ihres PCs zu scannen.Folgen Sie diesen Schritten, um in der Standard-Ansicht eine Scan-Aufgabe auszuführen:

1. Klicken Sie das **Security** Tab.
2. Klicken Sie im Quick Task-Bereich links auf **Vollsystem-Scan** und wählen Sie die gewünschte Scan-Aufgabe.Um eine benutzerdefinierte Prüfung zu konfigurieren und zu starten, klicken Sie **benutzerdefinierte Prüfung**.
3. Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.Falls Sie einen benutzerdefinierte Scan durchführen, müssen Sie zuerst den entsprechende Assistenten komplettieren.

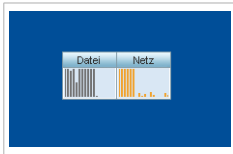
## Ausführen der Scan-Aufgaben in der Experten-Ansicht

In der Experten-Ansicht können Sie alle vorkonfigurierten Scan-Aufgaben durchführen und deren Scan-Optionen ändern. Außerdem können Sie dort selbst Scan-Aufgaben erstellen, wenn Sie bestimmte Bereiche Ihres Computers scannen möchten.Folgen Sie diesen Schritten, um in der Experten-Ansicht eine Scan-Aufgabe auszuführen:

1. Klicken Sie auf **Antivirus** in dem Menü auf der linken Seite.
2. Klicken Sie auf den Tab **Virenscan** Hier finden Sie eine Reihe von Standartprüfaufgaben und Sie können hier Ihre eigenen Prüfaufgaben erstellen.
3. Doppelklicken Sie auf die Scan-Aufgabe, die Sie ausführen möchten.
4. Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.

# 23.3. Aktivitätsanzeige

Die **Scan Aktions-Anzeige** ist eine graphische Visualisierung der Prüfaktivität auf Ihrem System.Dieses kleine Fenster steht in der Voreinstellung nur in der Experten-Ansicht zur Verfügung.



Scanaktivitsänzeige

Sie können die Aktivitätsanzeige verwenden um kurzerhand Dateien und Ordner zu prüfen. Ziehen Sie & die gewünschte Datei oder Ordner um sie zu prüfen in die

Aktivitätsanzeige.Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.

**Beachten Sie**
Für weitere Informationen lesen Sie bitte *„Scanaktivitsänzeige“ (S. 3)*.

# 24. Wie erstelle ich eine benutzerdefinierte Scan-Aufgabe?

Um eine neue Scan-Aufgabe zu definieren, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht

Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Benutzerdefinierter Scan**.

Ein Assistent wird eingeblendet, um Ihnen beim Erstellen der gewünschten Scan-Aufgabe zu helfen.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Willkommen**
2. **Ziel wählen**

   Klicken Sie auf **Ziel hinzufügen**, um die zu scannenden Dateien oder Verzeichnisse auszuwählen.

   Klicken Sie auf **Weitere Einstellungen**.Im Reiter **Übersicht** können Sie die Scan-Optionen durch Verschieben des Reglers anpassen.Wenn Sie die Scan-Optionen konfigurieren möchten, klicken Sie auf **Benutzerdefiniert**.Gehen Sie auf den Reiter **Planer**, um zu wählen, wann die Aufgabe ausgeführt werden soll.
3. **Fertigstellen**

   Hier können Sie einen Aufgabennamen eingeben und optional den Scan dem Quick Task-Bereich hinzufügen.

   Klicken Sie auf **Scan starten**, um die Aufgabe zu erstellen und den Scan-Assistenten zu öffnen.

Experten-Ansicht

1. Gehen Sie zu **Antivirus > Virusen-Scan**.
2. Klicken Sie auf **Neue Aufgabe**, ein neues Fenster wird geöffnet.

### Beachten Sie

Sie können auch per Mausdoppelklick auf eine vordefinierte Scan-Aufgabe wie **Vollsystem-Scan** klicken und dann **Aufgabe kopieren** wählen.Dies ist sinnvoll, wenn neue Aufgaben erstellt werden, weil die Einstellungen für die Aufgabe, die Sie dupliziert haben, geändert werden können.

3. Geben Sie im Reiter **Übersicht** den Aufgabennamen ein und passen Sie die Scan-Optionen an, indem Sie den Cursor des Schiebers entsprechend verschieben.

   Wenn Sie die Scan-Optionen konfigurieren möchten, klicken Sie auf **Benutzerdefiniert**.

4. Gehen Sie auf den Reiter **Pfade**, um das Scan-Ziel auszuwählen. Klicken Sie auf **Eintrag(e) hinzufügen**, um die zu scannenden Dateien oder Verzeichnisse auszuwählen.

5. Gehen Sie auf den Reiter **Planer**, um zu wählen, wann die Aufgabe ausgeführt werden soll.

6. Klicken Sie auf **OK**, um die Aufgabe zu speichern.Die neue Aufgabe erscheint unter den benutzerdefinierten Aufgaben und kann jederzeit aus diesem Fenster heraus bearbeitet, entfernt oder gestartet werden.

# 25. Wie plane ich einen Scan?

Ihren Computer regelmässig prüfen zu lassen ist die beste Art ihn frei von Maleware zu halten.Acronis Internet Security bietet Ihnen die Möglichkeit, Scan-Aufgaben einzuplanen, so dass Sie Ihren Computer automatisch scannen lassen können.

Um Acronis Internet Security eine geplante Scan-Aufgabe durchführen zu lassen folgen Sie den Schritten:

1. Öffnen Sie Acronis Internet Security.
2. Gehen Sie, abhängig von der gewählten Ansicht, wie folgt vor:

   Standard-Ansicht
   Gehe zum **Sicherheit** Register, klicke auf **Kompletter Systemscan** im Quick Task - Bereich und wähle **Plane meine Scans**.

   Experten-Ansicht
   Klicken Sie auf **Antivirus** in dem Menü auf der linken Seite.
3. Klicken Sie auf den Tab **Virenscan** Hier finden Sie eine Reihe von Standartprüfaufgaben und Sie können hier Ihre eigenen Prüfaufgaben erstellen.

   - Systemaufgaben sind verfügbar und können unter jedem Windows Benutzerkonto gestartet werden.
   - Benutzeraufgaben sind ausschliesslich für den Benutzer verfügbar der sie erstellt hat und können auch nur von diesem gestartet werden.

   Dies sind die Standartprüfaufgeben welche Sie einplanen können:

   **Vollsystem-Scan**
   Prüft alle Dateien mit Ausnahme von Archiven.In der standard Konfiguration, wird nach allen Arten von Malware geprüft, ausser rootkits.

   **Quick Scan**
   Beim Quick Scan wird das sog In-the-cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren.Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.

   **Prüfvorgang für Autologon**
   Prüft die Objekte, die ausgeführt werden, wenn ein Benutzer sich bei Windows anmeldet.Um diese Aufgabe zu nutzen, muss sie eingeplant werden beim Systemstart zu laufen.Standardmäßig ist die Prüfung im Hintergrund deaktiviert.

   **Tiefe Systemprüfung**
   Prüft das komplette SystemIn der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.

**Meine Dokumente**

Verwenden Sie diese um die folgenden für den jeweiligen Benutzer wichtigen Ordner zu prüfen: `Eigene Dateien`, `Desktop` und `Autostart`. Dies stellt sicher das Ihre Eigenen Dateien, Ihr Desktop und die beim Starten von Windows geladenen Programme schädlingsfrei sind.

Falls keine der Prüfaufgaben Ihren Bedürfnissen entspricht können Sie eine neue Prüfaufgabe erstellen, welche Sie dann wiederum so einplanen können wie Sie wünschen.

4. Wählen Sie eine Scan-Aufgabe und wählen Sie **Planen**.Ein neues Fenster wird sich öffnen.
5. Planen Sie die Aufgabe ein wie erforderlich:
   - Um die Aufgabe einmalig durchzuführen, wählen Sie **Einmalig** und bestimmen Sie das Startdatum und die Zeit.
   - Um die Prüfaufgabe nach dem Systemstart, wählen Sie **Beim Systemstart**.Geben Sie an wie lange nach dem Systemstart die Aufgabe gestartet sein wird.(Minuten)
   - Um die Aufgabe auf regulärer Basis laufen zu lassen, wählen Sie **Periodisch** und bestimmen Sie die Häufigkeit, das Startdatum und die Zeit.

   Beachten Sie

   Als Beispiel, um Ihren Computer jeden Samstag um 2:00Uhr prüfen zu lassen, müssen Sie wie folgt einplanen:

   a. Wählen Sie **Periodisch**.

   b. Im **Täglich** Feld, geben Sie 1 ein und wählen dann**Wochen** im Menu.Auf diese Art wird die Aufgabe einmal wöchentlich laufen.

   c. Legen Sie als Startdatum den kommenden Samstag fest.

   d. Legen Sie als Startzeit `2:00:00 Uhr`fest.

6. Klicken Sie **OK** um die Planung zu speichern.Die Prüfaufgabe wird automatisch, gemäß der definierten Planung, ablaufen.Falls der Computer im Moment der geplanten Aufgabe abgeschaltet ist, so wird die Aufgabe beim nächsten Computerstart starten.

# 26. Wie benutze ich einen Datentresor?

Der Acronis Internet Security Datentresors bieten die Möglichkeit, verschlüsselte, passwortgeschützte logische Laufwerke (oder Datentresors) auf Ihrem Computer zu erstellen, in denen Sie sicher Ihre wichtigen und vertraulichen Daten speichern können.Physikalisch ist der Tresor eine auf der lokalen Festplatte gespeicherte Datei mit der Endung .bvd.

Wenn Sie einen Datentresor erstellen, sind zwei Aspekte wichtig: die Größe und das Passwort.Die voreingestellte Größe von 50 MB sollte für Ihre privaten Dokumente wie z. B. Exel-Dateien und andere ausreichen. Für Videos und andere große Dateien jedoch benötigen Sie mehr Speicherplatz.

Um Ihre vertraulichen Dateien und Verzeichnisse sicher in einem Acronis Internet Security Datentresor zu speichern, gehen Sie folgendermaßen vor:

- **Erstellen Sie einen Datentresor und vergeben Sie ein sicheres Passwort dafür.**

  Um einen Vault zu erstellen, rechtsklicken Sie auf einen leeren Bereich auf dem Desktop oder auf ein Verzeichnis Ihres Computers, wechseln Sie in den Acronis Internet Security Datentresor und wählen Sie **Vault erstellen**.

  Ein neues Fenster wird geöffnet. Gehen Sie wie folgt vor:

  1. Klicken Sie auf **Durchsuchen**, um den gewünschten Speicherort auszuwählen und den Datentresor unter dem gewünschten Namen zu speichern.
  2. Wählen Sie einen Laufwerkbuchsbuchstaben aus dem Menü. Wenn Sie einen Datentresor öffnen, wird ein virtuelles Laufwerk mit dem gewählten Laufwerkbuchsbuchstaben unter **Arbeitsplatz** eingeblendet.
  3. Tippen Sie das Datentresor-Passwort im Feld **Passwort** ein und bestätigen Sie dieses im dem Feld **Bestätigen**.
  4. Wenn Sie die Standardgröße (50 MB) des Datentresors ändern möchten, geben Sie den gewünschten Wert in das Feld **Tresor-Größe** ein.
  5. Klicken Sie auf "Erstellen", wenn Sie den Datentresor unter der gewählten Speicherort definieren möchten. Um den Datentresor unter **Mein Computer** als virtuelles Laufwerk zu erstellen und anzuzeigen, klicken Sie auf **Erstellen und öffnen**.

  Beachten Sie

  Wenn Sie den Datentresor öffnen, wird unter **Mein Computer** ein virtuelles Laufwerk angezeigt. Dieses Laufwerk ist mit dem Laufwerksbuchstaben versehen, den Sie dem Datentresor zugewiesen haben.

- **Dateien oder Verzeichnisse, die Sie sichern möchten, demVault hinzufügen.**

Um eine Datei in einem Vault zu speichern, müssen Sie den entsprechenden Vault zuerst öffnen.

1. Blättern Sie zum entsprechenden .bvd-Vault File.
2. Rechtsklicken Sie auf die Vault-Datei, wechseln Sie in den Acronis Internet Security-Vault File und wählen Sie **Öffnen**.
3. Wählen Sie im eingeblendeten Fenster den Laufwerksbuchstaben, in dem der Vault gespeichert werden soll, geben Sie das Passwort ein und klicken Sie auf **Öffnen**.

Sie können nun in dem Laufwerk, in dem der entsprechende Datentresor gespeichert ist, wie gewohnt Windows Explorer Operationen durchführen.Um einem offenen Datentresor eine Datei hinzuzufügen, rechtsklicken Sie auf die Datei, zeigen Sie auf den Acronis Internet Security Datentresor und wählen Sie **Dem Datentresor hinzufügen**.

- **Der Vault sollte jederzeit geschlossen sein.**

  Öffnen Sie einen Vault nur, wenn Sie auf eine der Dateien zugreifen oder dessen Inhalt verwalten möchten.Um einen Vault zu sperren, klicken Sie mit der rechten Maustaste im Verzeichnis **Mein Computer** auf den entsprechenden Vault, gehen Sie auf **Acronis Internet Security Datentresor** und wählen Sie **Schließen**.

- **Stellen Sie sicher, dass Sie den Vault File .bvd nicht löschen.**

  Durch das Löschen der Datei werden auch die Vault-Inhalte gelöscht.

Weitere Informationen zur Handhabung von Datentresor finden Sie unter *„Dateiverschlüsselung“* (S. 124).

# 27. Wie erstelle ich ein Windows Benutzerkonto?

Ein Windows-Benutzerkonto ist ein eindeutiges Profil, zu dem alle Einstellungen, Zugriffsrechte und persönlichen Dateien des entsprechenden Benutzers gehören.

Windows-Benutzerkonten lassen den Heim PC-Administrator den Zugriff für jeden Benutzer kontrollieren.

Das Anlegen von Benutzerkonten ist dann sinnvoll, wenn sowohl Erwachsene als auch Kinder den PC benutzen - ein Elternteil kann für jedes Kind ein separates Benutzerkonto anlegen.

Wählen Sie Ihr Betriebssystem, um so herauszufinden, wie Sie Windows Benutzerkonten erstellen können.

- Windows XP:
  1. Loggen Sie sich in Ihren Computer als Administrator ein.
  2. Klicken Sie auf "Start", klicken Sie auf "Systemsteuerung" und dann auf "Benutzerkonten".
  3. Klicken Sie auf "Neues Benutzerkonto erstellen".
  4. Geben Sie den Namen des Benutzers ein. Sie können den vollständigen Namen der Person, den Vornamen oder einen Spitznamen verwenden. Klicken Sie dann auf "Weiter".
  5. Für diesen Benutzerkontentyp wählen Sie "Begrenzt" und dann "Benutzerkonto anlegen". Begrenzte Benutzerkonten sind vor allem für Kinder geeignet, da keine systemübergreifenden Änderungen vorgenommen oder bestimmte Anwendungen nicht installiert werden können.
  6. Ihr neues Benutzerkonto wird erstellt und dieses wird im Bildschirm "Benutzerkonten verwalten" aufgelistet.
- Windows Vista oder Windows 7:
  1. Loggen Sie sich in Ihren Computer als Administrator ein.
  2. Klicken Sie auf "Start", klicken Sie auf "Systemsteuerung" und dann auf "Benutzerkonten".
  3. Klicken Sie auf "Neues Benutzerkonto erstellen".
  4. Geben Sie den Namen des Benutzers ein. Sie können den vollständigen Namen der Person, den Vornamen oder einen Spitznamen verwenden. Klicken Sie dann auf "Weiter".
  5. Für diesen Benutzerkontentyp klicken Sie auf "Standard" und dann auf "Benutzerkonto anlegen". Beschränkte Benutzerkonten sind vor allem für Kinder geeignet, da keine systemübergreifenden Änderungen vorgenommen oder bestimmte Anwendungen nicht installiert werden können.

6. Ihr neues Benutzerkonto wird erstellt und dieses wird im Bildschirm "Benutzerkonten verwalten" aufgelistet.

### Beachten Sie

Nun, da Sie neue Benutzerkonten hinzugefügt haben, können Sie für diese Passwörter vergeben.

# 28. Wie kann ich Acronis Internet Security über einen Proxy-Server aktualisieren?

Normalerweise findet und importiert Acronis Internet Security automatisch die Proxy-Einstellungen Ihres Systems.Wenn Ihre Internetverbindung über einen Proxy Server hergestellt wird, müssen Sie eventuell die Proxy-Einstellungen finden und Acronis Internet Security dementsprechend konfigurieren.Um herauszufinden, wie Sie dafür vorgehen sollen, lesen Sie bitte *„Wo finde ich "Meine Proxy-Einstellungen"?“ (S. 190)*.

Nachdem Sie die Proxy-Einstellungen gefunden haben, gehen Sie folgendermaßen vor:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Allgemein> Einstellungen**.
3. Klicken Sie in den **Verbindungseinstellungen** auf **Proxy-Einstellungen**.
4. Geben Sie im entsprechenden Feld die Proxy-Einstellungen ein.
5. Klicken Sie auf **OK**.

### Beachten Sie

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

# Fehlediagnose und Problemlösung

# 29. Problemlösung

In diesem Kapitel werden einige Probleme, die Ihnen bei der Verwendung von Acronis Internet Security begegnen können, erläutert. Zudem finden Sie hier Lösungsvorschläge für diese Probleme.Die meisten dieser Probleme können über eine passende Konfiguration der Produkteinstellungen gelöst werden.

Wenn Sie Ihr Problem hier nicht finden oder wenn die vorgeschlagene Lösung nicht zum Erfolg führt, können Sie den technischen Kundendienst von Acronis wie in Kapitel „*Support*“ (S. 187) beschrieben, kontaktieren.

## 29.1. Der Scan startet nicht

Dieses Problem kann folgende Ursachen haben:

- **Eine vorherige Installation von Acronis Internet Security wurde nicht vollständig entfernt oder es handelt sich um eine fehlerhafte Acronis Internet Security-Installation**.

  Sollte dies der Fall sein, ist die einfachste Lösung, Acronis Internet Security komplett vom System zu entfernen und wieder neu zu installieren.

- **Acronis Internet Security ist nicht die einzige auf Ihrem System installierte Sicherheitssoftware**.

  Befolgen Sie dafür die folgenden Schritte:

  1. Entfernen Sie die anderen Sicherheitslösungen entfernen.
  2. Löschen Sie Acronis Internet Security vollständig vom System.
  3. Installieren Sie Acronis Internet Security neu.

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter „*Support*“ (S. 187) beschrieben kontaktieren.

## 29.2. Ich kann eine Anwendung nicht länger benutzen

Dieses Problem tritt auf, wenn Sie versuchen, ein Programm zu verwenden, das vor der Installation von Acronis Internet Security einwandfrei funktioniert hatte.

Es könnten folgende Situationen eintreten:

- Sie könnten einen Benachrichtigung von Acronis Internet Security erhalten, dass das Programm versucht, Veränderungen am System durchzuführen.
- Es ist möglich, dass Sie von dem Programm, das Sie starten möchten, eine Fehlermeldung erhalten.

Diese Situation tritt ein, wenn das Active Virus Control-Modul versehentlich eine Anwendung als Malware einstuft.

Active Virus Control ist ein Acronis Internet Security-Modul, das ständig die laufenden Programme Ihres Systems überwacht und einen Bericht über jene sendet, die sich potentiell gefährlich verhalten.Da diese Funktion auf dem heuristischen System basiert, kann es Fälle geben, in denen einwandfreie Anwendungen im Bericht der Active Virus Control aufgelistet werden.

Wenn diese Situation eintritt, können Sie die entsprechende Anwendung von der Überwachung durch Active Virus Control ausschließen.

Wenn Sie das Programm der Ausschlussliste hinzufügen möchten, gehen Sie folgendermaßen vor:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Weitere Einstellungen**.
4. Gehen Sie im neuen Fenster auf den Reiter **Ausschlüsse**, klicken Sie auf den Button **Hinzufügen** und suchen Sie die .exe-Datei des Programms (normalerweise unter `C:\Programmdateien`).
5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
6. Schließen Sie das Acronis Internet Security-Fenster und überprüfen Sie, ob das Problem weiterhin auftritt.

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 29.3. Ich kann keine Verbindung zum Internet herstellen.

Nach einer Installation von Acronis Internet Security werden Sie unter Umständen bemerken, dass ein Programm keine Verbindung mehr zum Internet herstellen oder auf Netzwerkdienste zugreifen kann.

Der Fehlersuche-Assistent hilft Ihnen, die Verbindungsprobleme zu identifizieren und zu lösen.Um den Assistenten zu starten, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neuen Fenster den Reiter **Einstellungen** und klicken Sie auf **Fehlersuche**.

Experten-Ansicht
: Gehen Sie auf **Firewall > Einstellungen** und klicken Sie auf **Fehlersuche**.

Folgen Sie der dreiteiligen Anleitung, um die Fehlersuche zu starten.Über den Button **Weiter** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Willkommen**

   Wählen Sie **Ich versuche ins Internet zu gehen, dies funktioniert aber nicht**.

2. **Problem identifizieren**

   Klicken Sie auf **Anwendung wählen** und **Blättern**, um die .exe-Datei der Anwendung zu finden (normalerweise finden Sie diese unter `C:\Programmdateien`, z.B. Firefox.exe).Klicken Sie auf **Hinzufügen**.

3. **Empfohlene Problemlösung**

   Wählen Sie **Ja, Zugriff zulassen**.Klicken Sie auf **Beenden** und überprüfen Sie, ob das Problem weiterhin auftritt.

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 29.4. Ich kann den Drucker nicht benutzen

Abhängig vom angeschlossenen Netzwerk könnte die Acronis Internet Security-Firewall die Verbindung zwischen Ihrem Computer und einen Netzwerkdrucker blockieren.

In diesem Fall ist die beste Lösung, Acronis Internet Security so zu konfigurieren, dass eine Verbindung von und zum entsprechenden Drucker automatisch zugelassen wird.

Der Fehlersuche-Assistent hilft Ihnen, die Verbindungsprobleme zu identifizieren und zu lösen.Um den Assistenten zu starten, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neuen Fenster den Reiter **Einstellungen** und klicken Sie auf **Fehlersuche**.

Experten-Ansicht
: Gehen Sie auf **Firewall > Einstellungen** und klicken Sie auf **Fehlersuche**.

Folgen Sie der dreiteiligen Anleitung, um die Fehlersuche zu starten.Über den Button **Weiter** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Willkommen**

   Wählen Sie **Ich versuche etwas auszudrucken, dies ist aber nicht möglich**.

2. **Problem identifizieren**

   Klicken Sie auf **Drucker wählen**.Wählen Sie den Drucker aus der Liste aus (entweder Druckername oder IP-Adresse).Wenn Sie das Gerät in der Liste nicht

finden können, geben Sie die IP-Adresse manuell im Bearbeiten-Feld ein.Klicken Sie auf **Hinzufügen**.

3. **Empfohlene Problemlösung**

   Wählen Sie **Ja, Zugriff zulassen**.Klicken Sie auf **Beenden** und überprüfen Sie, ob das Problem weiterhin auftritt.

Falls der Fehlersuche-Assistent anzeigt, dass das Problem nicht von der Acronis Internet Security-Firewall auf Ihrem Computer verursacht wird, überprüfen Sie andere potentielle Ursachen, wie beispielsweise:

- Die Firewall auf dem anderen Computer könnte die Nutzung des gemeinsamen Druckers oder der Datei blockieren.
  - ▶ Wenn die Windows Firewall benutzt wird, kann diese so konfiguriert werden um Datei und Druckerfreigabe, wie gefolgt, zu erlauben: öffnen Sie die Windows Firewall Einstellungsfenster, unter **Ausnahme** wählen Sie die option **Datei- und Druckerfreigabe**.
  - ▶ Wenn eine andere Firewall verwendet wird, beziehen Sie sich bitte auf dessen Unterlagen oder Hilfsdateien.
- Allgemeine Bedingungen, die die Benutzung oder Verbindung an den freigegebenen Drucker verhindern können:
  - ▶ Möglicherweise müssen Sie sich mit einen Windows Adminstratorkonto anmelden um auf die Druckerfreigabe zugreifen zu können.
  - ▶ Rechte werden für den freigegebenen Drucker gesetzt so dass dieser nur spezifische Computer und Benutzer erlaubt.Falls Sie Ihren Drucker freigegeben haben, überprüfen Sie die Rechte, die für den Drucker gesätzt sind, um zu sehen, ob der Benutzer auf dem anderen Computer, der Zugang zum Drucker erlaubt wird.Wenn Sie versuchen eine Verbindung zum freigegebenen Drucker aufzubauen, sollten Sie mit Benutzer auf dem anderen Computer überprüfen, ob Sie die benötigte Rechte haben.
  - ▶ Der Drucker der mit Ihren Computer oder einem anderen verbunden ist, ist nicht freigegeben.
  - ▶ Der freigegebene Drucker wurde an dem Computer nicht hinzugefügt.

    **Beachten Sie**
    Um mehr darüber zu erfahren, wie Sie die Druckerfreigabe verwalten können um Drucker im Netz freizugeben oder die Rechte anzupassen, öffnen sie im Windows-Startmenü **Hilfe und Support**).

- Der Zugriff auf einen Netzwerk-Drucker könnte auf bestimmte Computer oder Nutzer beschränkt sein. Fragen Sie Ihren Netzwerk-Administrator, ob Sie die notwendigen Rechte besitzen, um auf diesen Drucker zuzugreifen.

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 29.5. Ich kann keine Dateien mit anderen Computern teilen

Abhängig vom angeschlossenen Netzwerk könnte die Acronis Internet Security-Firewall die Verbindung zwischen Ihrem Computer und einem anderen Netzwerkcomputer blockieren.Als Ergebnis können Sie nicht mehr länger Dateien mit anderen Computern teilen.In diesem Fall ist die beste Lösung, Acronis Internet Security so zu konfigurieren, dass eine Verbindung von und zum entsprechenden System automatisch zugelassen wird.

Der Fehlersuche-Assistent hilft Ihnen, die Verbindungsprobleme zu identifizieren und zu lösen.Um den Assistenten zu starten, öffnen Sie Acronis Internet Security und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neuen Fenster den Reiter **Einstellungen** und klicken Sie auf **Fehlersuche**.

Experten-Ansicht
: Gehen Sie auf **Firewall > Einstellungen** und klicken Sie auf **Fehlersuche**.

Folgen Sie der dreiteiligen Anleitung, um die Fehlersuche zu starten.Über den Button **Weiter** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Willkommen**

   Wählen Sie **Ich versuche auf einen Computer meines Netzwerks zuzugreifen, dies funktioniert aber nicht**.

2. **Problem identifizieren**

   Klicken Sie auf **Computer wählen**.Wählen Sie den Computer aus der Liste aus (entweder Computername oder IP-Adresse).Wenn Sie den Computer nicht in der Liste finden können, geben Sie die IP-Adresse manuell im Bearbeiten-Feld ein.Klicken Sie auf **Hinzufügen**.

3. **Empfohlene Problemlösung**

   Wählen Sie **Ja, Zugriff zulassen**.Klicken Sie auf **Beenden** und überprüfen Sie, ob das Problem weiterhin auftritt.

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 29.6. Meine Internetverbindung ist langsam

Diese Situation könnte nach der Installation von Acronis Internet Security eintreten.Das Problem könnte aufgrund von Konfigurationsfehlern der Acronis Internet Security-Firewall auftreten.

Zur Behebung dieses Problems gehen Sie folgendermaßen vor:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Firewall > Einstellungen**.
3. Deaktivieren Sie das Häkchen der Option **Firewall ist aktiviert**, um diese vorübergehend auszuschalten.
4. Überprüfen Sie, ob Sie nun eine Internetverbindung herstellen können, wenn die Acronis Internet Security-Firewall deaktiviert ist.

   - Wenn Sie weiterhin keine Internetverbindung herstellen können, wird das Problem wahrscheinlich nicht von Acronis Internet Security verursacht. Sie sollten Ihren Internet Service Provider kontaktieren, um abzuklären, dass es keine Verbindungsprobleme gibt.

     Wenn Ihr Internetserviceprovider Ihnen bestätigt, dass es von seiner Seite aus keine Verbindungsprobleme gibt, das Problem aber weiterhin bestehen bleibt, kontaktieren Sie uns wie unter *„Support“ (S. 187)* beschrieben.

   - Falls Sie nach der Deaktivierung der Acronis Internet Security-Firewall eine Internetverbindung herstellen können, gehen Sie folgendermaßen vor:

     a. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.

     b. Gehen Sie zu **Firewall > Einstellungen** und setzen Sie ein Häkchen, um die Firewall zu aktivieren.

     c. Klicken Sie auf **Erweiterte Einstellungen**, wählen Sie **Internetverbindungs-Sharing aktivieren** und deaktivieren Sie **Port Scans blockieren**.

     d. Gehen Sie im Hauptfenster auf den Reiter **Netzwerk** .

     e. Blättern Sie im Drop-Down-Menü der Spalte **Netzwerktyp** nach unten und wählen Sie **Zuhause/ Büro**.

     f. Gehen Sie in die Spalte **Allgemein** und wählen Sie dort **Ja** vor. Setzen Sie den **Stealth-Modus** auf **Remote**.

     g. Überprüfen Sie, ob Sie eine Verbindung zum Internet herstellen können.

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 29.7. Wie Sie ein Acronis Internet Security-Update mit einer langsamen Internetverbindung durchführen.

Falls Sie über eine langsame Internetverbindung (wie z. B. ein Modem) verfügen, können während des Updates Fehler auftreten.

Um Ihr System hinsichtlich Acronis Internet Security Malware-Signaturen auf dem neuesten Stand zu halten, gehen Sie folgendermaßen vor:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Update > Einstellungen**.
3. Unter **Manuelle Update-Einstellungen** wählen Sie **Vor dem Download von Updates nachfragen**.
4. Klicken Sie auf **Anwenden** und gehen Sie zum Reiter **Update**.
5. Klicken Sie auf **Jetzt updaten**, es wird ein neues Fenster eingeblendet.
6. Wählen Sie nur **Signatur-Updates** und klicken Sie dann auf **OK**.
7. Acronis Internet Security wird nur die Malware-Signatur-Updates downloaden und installieren.

## 29.8. Acronis Internet Security-Dienste antworten nicht.

Dieser Artikel hilft Ihnen bei der Lösung des Problems *Acronis Internet Security Dienste antworten nicht*.Diese Fehlermeldung kann folgendermassen auftauchen:

- Das Acronis Internet Security-Symbol in System Tray ist ausgegraut und ein Pop-up informiert Sie, dass die Acronis Internet Security-Dienste nicht antworten.
- Das Acronis Internet Security-Fenster zeigt an, dass die Acronis Internet Security-Dienste nicht antworten.

Der Fehler kann durch einen der folgenden Bedingungen verursacht werden:

- ein wichtiges Update wird installiert.
- Temporäre Kommunikationsstörungen zwischen den Acronis Internet Security-Diensten.
- Einige der Acronis Internet Security-Dienste wurden angehalten.
- Andere Sicherheitslösungen laufen gleichzeitig mit Acronis Internet Security auf Ihrem Rechner.
- Viren auf Ihrem System beeinflussen den Normalbetrieb von Acronis Internet Security.

Um diese Störung zu überprüfen, versuchen Sie diese Lösungen:

1. Warten Sie einen Moment und sehen Sie ob sich was ändert.Die Störung könnte temporär sein.
2. Starten Sie den Rechner neu und warten Sie einige Momente, bis Acronis Internet Security geladen ist. Öffnen Sie Acronis Internet Security und überprüffen Sie ob das Problem weiterhin besteht.Das neustarten des Rechners behebt normalerweise das Problem.
3. Überprüfen Sie, ob Sie ein anderes Sicherheitsprogramm installiert haben, da diese den Normalbetrieb von Acronis Internet Security stören könnte. Sollte dies der Fall sein, empfehlen wir Ihnen alle anderen Sicherheitsprogramme zu entfernen und Acronis Internet Security wieder neu zu installieren.
4. Besteht das Problem auch weiterhin, kann es sich um ein ernsteres Problem handeln (z.B. könnte der Rechner mit einem Virus infiziert sein, wodurch Acronis Internet Security behindert wird).Kontaktieren Sie unseren Kundendienst wie unter „*Support*“ (S. 187) beschrieben.

## 29.9. Antispamfilter funkioniert nicht richtig

Dieser Artikel hilft Ihnen, folgende Probleme mit dem Acronis Internet Security Antispam-Filter lösen:

- Eine Anzahl von seriösen E-Mails werden markiert als `[spam]`.
- Viele Spams werden entsprechend nicht durch den Antispam Filter markiert.
- Der Antispam-Filter entdeckt keine Spamnachrichten.

### 29.9.1. Seriöse Nachrichten werden markiert als [spam]

Seriöse Nachrichten werden als `[spam]` markiert, einfach deshalb weil sie für den Acronis Internet Security Antispam-Filter wie solche aussehen.Im Normalfall können Sie dieses Problem lösen indem Sie den Antispam Filter angemessen konfigurieren.

Acronis Internet Security fügt die Empfänger Ihrer Mails automatisch der Freundeliste hinzu.Die erhaltenen E-Mail der in der Freundesliste geführten Kontakte werden als seriös angesehen. Sie werden nicht vom Antispam Filter geprüft und deshalb auch nicht als `[spam]` markiert.

Die automatische Konfiguration der Freundesliste verhindert nicht die entdeckte Störungen, die in dieser Situationen auftreten können:

- Sie empfangen viele angeforderte Werb-E-Mails resultierend aus der Anmeldung auf verschiedene Webseiten.In diesem Fall ist die Lösung, die E-Mail Adressen, von denen Sie solche E-Mails bekommen, auf die Freunde Liste zu setzen.
- Ein erheblicher Teil Ihrer legitimen Email ist von Leuten, die bisher nie E-Mails von Ihnen erhalten haben. bspw. Kunden, potentielle Geschäftspartner und andere.Andere Lösungen sind in diesem Fall erforderlich.

Wenn Sie einen Email Client benutzen, in den sich Acronis Internet Security integriert, versuchen Sie folgendes:

1. Zeige Erkennungsfehler. Dadurch wird der Bayesian Filter trainiert, (Teil des Antispam Filters) und es hilft zukünftig, Erkennungsfehler zu verhindern.Der Bayesian Filter analysiert die Nachrichten und lernt ihr Muster.Die nächsten E-Mail-Nachrichten, die die gleiche Muster haben, werden nicht als [spam] markiert.
2. Antispam Sicherheitsstufe reduzieren. Indem die Sicherheitsstufe reduziert wird, benötigt der Antispam Filter mehr Spamanzeigen, um eine E-Mail-Nachricht als Spam einzustufen.Probieren Sie diese Lösung nur, wenn legitime Nachrichten (inklusive kommerzielle Nachrichten) fälschlicherweise als Spam erkannt werden.
3. Trainieren Sie die lernfähige Engine (Bayesian filter) erneut. Probieren Sie diese Lösung nur, wenn vorangegangene Lösung keinen Erfolg gebracht haben.

**Beachten Sie**

Acronis Internet Security integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste.Um die komplette Liste der unterstützen E-Mail Clients, lesen Sie bitte: *„Unterstützte E-Mail-Clients und Protokolle“ (S. 72)*.

Wenn Sie einen anderen Mail Client benutzen, können Sie keine Erkennungsfehler angeben und den Bayesian Filter trainieren. Um das Problem zu lösen, versuchen Sie den Antispam Schutz herabzusetzen.

## Kontakte zur Freundesliste hinzufügen

Wenn Sie einen unterstützten E-Mail Client verwenden, können Sie den Absernder ganz leicht zu der Freundesliste hinzufügen.Folgen Sie diesen Schritten:

1. Wählen Sie in Ihrem Mail Client eine Mail eines Senders, den Sie der Freundesliste hinzufügen möchten.
2. Klicken Sie in der Acronis Internet Security Antispam-Systemleiste auf den Button **Freund hinzufügen**, um den Adressaten Ihrer Freundeliste hinzuzufügen.
3. Es kann sein das Sie die Adressen, die zur Freundesliste hinzugefügt wurden, bestätigen müssen.Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie **OK**.

Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.

Falls Sie einen anderen Mail Client verwenden, können Sie von der Acronis Internet Security-Oberfläche aus Kontakte der Freundeliste hinzufügen.Folgen Sie diesen Schritten:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.

2. Klicken Sie auf **Antispam** im Menü auf der linken Seite.
3. Klicken Sie auf das **Status** Tab.
4. Klicken Sie auf **Freunde verwalten**.Ein Konfigurationsfenster wird sich öffnen.
5. Geben Sie die E-Mail Adresse ein, von der Sie E-Mail Nachrichten erhalten wollen und klicken, um die Adresse zur Freunde Liste hiunzu zu fügen.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

## Erfassungsfehler anzeigen

Wenn Sie einen unterstützten Mail Client verwenden, können Sie einfach den Antispam Filter korrigieren (indem Sie angeben welche E-Mail Nachrichten nicht als [spam]). Dadurch wird die Effektivität des Antispam Filters erheblich verbessert.Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin verschoben werden.
3. Wählen Sie die Nachricht, die von Acronis Internet Security fälschlicherweise als [spam] markiert wurde, aus.
4. Klicken Sie auf **Freund hinzufügen** in der Acronis Internet Security Antispam Toolbar.Klicken Sie zur Bestätigung **OK**.Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.
5. Klicken Sie in der Acronis Internet Security Antispam-Symbolleiste (normalerweiseim oberen Teil des Mail Client-Fensters) auf **Kein Spam**. Dies teilt dem Bayes-Filter, dass die ausgewählte Nachricht kein Spam ist. Die Nachricht wird dann in den Posteingang verschoben.Die nächsten E-Mails, die dem gleichen Muster entsprechen, werden nicht als [spam] markiert.

## Antispam Sicherheitsstufe herabsetzen.

Um die Antispam Sichereitsstufe herabzusetzen, folgen Sie diese Schritte:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Klicken Sie auf **Antispam** im Menü auf der linken Seite.
3. Klicken Sie auf das **Status** Tab.
4. Verschieben Sie den Schieber auf der Skala nach unten.

Es wird empfohlen den Schutz um nur eine Stufe herabzusetzen und nach einer ausreichenden Zeit die Resultate zu sichten.Wenn weiterhin legitime E-Mail Nachrichten als [spam] markiert werden, können sie den Schutz-Grad weiter

herabstufen. Stellen Sie fest, dass viele Nachrichten nicht als Spam erkannt werden, sollten Sie den Schutz-Grad nicht herabsetzen.

### Trainieren Sie den Bayesian Filter

Bevor Sie den Bayesian Filter tranieren, erstellen Sie einen Ordner der einen der legitimen Nachrichten enthält und sonst nur SPAM Nachrichten.Der Bayesian Filter wird trainiert, indem er sie analysiert und lernt die Charakteristiken, die Spam und legitime Nachrichten definieren, zu unterscheiden. Um die Effektivität des Trainings zu gewährleisten, müssen midestens 50 Nachrichten jeder Kategorie vorhanden sein.

Um die Bayesian Datenbank zurückzusetzen und um es neu zu trainieren, follgen Sie diese Schritte:

1. Öffnen Sie den Mail Client.
2. Klicken Sie in der Acronis Internet Security Antispam-Leiste auf den Button **Assistent**, um den Antispam-Konfigurierungsassistent zu starten.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie **Überspringen** und klicken Sie auf **Weiter**.
5. Wählen Sie **Antispamfilter löschen** un klicken Sie auf **Weiter**.
6. Wählen Sie den Ordner mit legitime Nachrichten und klicken Sie auf **Weiter**.
7. Wählen Sie den Ordner mit SPAM Nachrichten und klicken Sie auf **Weiter**.
8. Klichen Sie auf **Fertigstellen** um mit dem Trainingsprozess zu starten.
9. Nach Abschluss des Trainings, klicken Sie **Schließen**.

### Nach Hilfe fragen

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 29.9.2. Viele Spam Nachrichten werden nicht entdeckt.

Wenn Sie viele Nachrichten erhalten, die nicht als `[spam]` markiert sind, konfigurieren Sie den Acronis Internet Security Antispam-Filter, um seine Effektivität zu erhöhen.

Wenn Sie einen Email Client benutzen, in den sich Acronis Internet Security integriert, versuchen Sie folgende Schritte (einzeln):

1. Indizieren Sie unentdeckte Spam Nachrichten. Dadurch wird der Bayesianische Filter trainiert (Teil des Antispam Filters) und die Antispam Erkennungsrate erhöht.Der Bayesian Filter analysiert die Nachrichten und lernt ihr Muster.Die nächsten E-Mail-Nachrichten, die die gleiche Muster haben, werden folgendermaßen markiert `[spam]`.

2. Spammer zur Spammerliste hinzufügen. Die E-Mail-Nachrichten, die von den Adressen aus der Spammerliste empfangen werden, werden automatisch markiert als [spam].
3. Antispam Sicherheitsstufe erhöhen. Indem die Sicherheitsstufe erhöht wird, benötigt der Antispam Filter weniger Spamanzeigen, um eine E-Mail-Nachricht als Spam einzustufen.
4. Trainieren Sie die lernfähige Engine (Bayesian filter) erneut. Nutzen Sie diese Lösung, wenn die Erkennungsrate des Antispam Filters sehr schlecht ist und das Anzeigen nicht markierter Nachrichten nicht funktioniert.

**Beachten Sie**

Acronis Internet Security integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste.Um die komplette Liste der unterstützen E-Mail Clients, lesen Sie bitte: *„Unterstützte E-Mail-Clients und Protokolle“ (S. 72)*.

Wenn Sie einen anderen Mail Client benutzen, können Sie keine Erkennungsfehler angeben und den Bayesian Filter trainieren. Um das Problem zu lösen, versuchen Sie den Antispam Schutz heraufzusetzen und setzen Sie Spammer auf die Spammer Liste.

## Zeigt unentdeckte Spam-Nachrichten

Wenn Sie einen unterstützten Mail Client verwenden, können Sie einfach angeben, welche E-Mail Nachrichten als Spam hätten markiert werden sollen. Dies wird die Effizienz des Antispam Filters erhöhen.Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Begeben Sie sich zum Inbox Ordner.
3. Wählen Sie die unentdeckte Spam-Nachricht.
4. Klicken Sie in der Acronis Internet Security Antispam-Symbolleiste (normalerweise im oberen Teil des Mail Client-Fensters) auf **Ist Spam**. Dies sagt dem Bayes-Filter dass es sich bei den ausgewählten Nachrichten um eine Spam-Nachricht handelt. Sie wird dann sofort als [spam] markiert und in den Junk Mail-Verzeichnis verschoben.Die nächsten E-Mail-Nachrichten, die die gleiche Muster haben, werden folgendermaßen markiert [spam].

## Spammer zu Liste der Spammer hinzufügen

Wenn Sie einen unterstützten E-Mail Client verwenden, können Sie den Absernder der Spamnachricht ganz leicht zu der Spammerliste hinzufügen.Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.

2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin verschoben werden.
3. Markieren Sie die Nachricht die von Acronis Internet Security als [spam] markiert wurde.
4. Klicken Sie in der Acronis Internet Security Antispam-Leiste auf **Spammer hinzufügen**.
5. Es kann sein das Sie die Adresse bestätigen müssen, die in der Spammerliste hinzugefügt wurde.Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie **OK**.

Benutzen Sie einen anderen Mail Client, können Sie manuell von der Acronis Internet Security Benutzeoberfläche aus Spammer der Spammer Liste hinzufügen. Dies macht nur Sinn, wenn Sie bereits mehrere Spam-Nachrichten vom gleichen Absender erhalten haben.Folgen Sie diesen Schritten:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Klicken Sie auf **Antispam** im Menü auf der linken Seite.
3. Klicken Sie auf das **Status** Tab.
4. Klicken Sie auf **Spammer verwalten**.Ein Konfigurationsfenster wird sich öffnen.
5. Geben Sie die E-Mail Adresse des Spammer ein und klicken, um die Adresse zur Spammer Liste hinzu zu fügen.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

## Erhöhen Sie die Antispam Schutzstufe

Um die Antispam Schutzstufe zu erhöhen, folgen Sie diese Schritte:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Klicken Sie auf **Antispam** im Menü auf der linken Seite.
3. Klicken Sie auf das **Status** Tab.
4. Verschieben Sie den Schieber höher auf der Skala.

## Trainieren Sie den Bayesian Filter

Bevor Sie den Bayesian Filter tranieren, erstellen Sie einen Ordner der einen der legitimen Nachrichten enthält und sonst nur SPAM Nachrichten.Der Bayesian Filter wird trainiert, indem er sie analysiert und lernt die Charakteristiken, die Spam und legitime Nachrichten definieren, zu unterscheiden. Um die Effektivität des Trainings zu gewährleisten, müssen midestens 50 Nachrichten in jedem Ordner sein.

Um die Bayesian Datenbank zurückzusetzen und um es neu zu trainieren, follgen Sie diese Schritte:

1. Öffnen Sie den Mail Client.
2. Klicken Sie in der Acronis Internet Security Antispam-Leiste auf den Button **Assistent**, um den Antispam-Konfigurierungsassistent zu starten.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie **Überspringen** und klicken Sie auf **Weiter**.
5. Wählen Sie **Antispamfilter löschen** un klicken Sie auf **Weiter**.
6. Wählen Sie den Ordner mit legitime Nachrichten und klicken Sie auf **Weiter**.
7. Wählen Sie den Ordner mit SPAM Nachrichten und klicken Sie auf **Weiter**.
8. Klichen Sie auf **Fertigstellen** um mit dem Trainingsprozess zu starten.
9. Nach Abschluss des Trainings, klicken Sie **Schließen**.

### Nach Hilfe fragen

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 29.9.3. Antispam-Filter entdeckt keine Spamnachrichten.

Wenn keine Nachrichten als [spam] markiert werden, könnte es möglicherweise am Acronis Internet Security Antispam Fileter liegen.Vor der Fehlersuche dieses Problems, sollten Sie sicherstellen , dass es nicht durch einen der folgenden Bedingungen verursacht wird:

- Der Acronis Internet Security Antispam-Schutz ist nur für Email Clients verfügbar, die Emails über das POP3-Protokoll zu empfangen.Das bedeutet folgendes:
  - Die Email-Nachrichten, die über web-basierte Email-Dienstleistungen empfangen werden (wie Yahoo, Gmail, Hotmail oder andere) gehen nichtdurch den Acronis Internet Security Spam-Filter.
  - Wenn Ihr Email Client konfiguriert ist, Emails unter Verwendung anderer Protokolle als POP3 zu empfangen (z.B., IMAP4), scannt der Acronis Internet Security Antispam-Filter diese Emails nicht auf Spam-Mails.

  **Beachten Sie**

  POP3 ist eines der am meisten benutzten Protokolle für das Downloaden der E-Mail-Nachrichten vom Mail-Server.Falls Sie das Protokoll nicht kennen, das von Ihrem E-Mail Client benutzt wird, um E-Mail Nachrichten herunterzuladen, fragen Sie die Person, die Ihren E-Mail Client konfiguriert hat.

- Acronis Internet Security 2011 scannt keine POP3-Übertragungen von Lotus Notes.

Sie sollten ausserdem die folgenden möglichen Ursachen nachprüfen:

1. Vergewissern Sie sich dass Antispam aktiviert ist.
   a. Öffnen Sie Acronis Internet Security.
   b. Klicken Sie in der oberen rechten Bildschirmecke auf **Optionen** und wählen Sie **Einstellungen**.
   c. Überprüfen Sie in der Kategorie Sicherheitseinstellungen den Antispamstatus.

   Falls Antispam deaktiviert ist, so liegt hier der Grund ihres Problems.Aktiviere Antispam und überwache den Antispam-Betrieb um zu erkennen ob das Problem behoben wurde.

2. Auch wenn es sehr unwahrscheinlich ist, sollten Sie überprüfen, ob Acronis Internet Security von Ihnen (oder einer anderen Person) so konfiguriert wurde, dass SPAM-Nachrichten nicht als `[spam]` markiert werden.
   a. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
   b. Klicken Sie auf **Update** im Baummenu und dann auf den Tab **Einstellungen** um diesen Bereich zu öffnen.
   c. Stellen Sie sicher das die Option **Spam-Nachrichten im Betreff markieren** ausgewählt ist.

Eine mögliche Lösung wäre auch, das Produkt zu reparieren oder erneut zu installieren. Falls Sie lieber den Acronis-Kundendienst kontaktieren möchten, folgen Sie der Beschreibung wie im Abschnitt „*Support*“ (S. 187) beschrieben.

# 30. Malware von Ihrem System entfernen

Malware kann Ihr System auf vielfältige Art und Weise beeinflussen. Wie Acronis Internet Security auf diese Malware reagiert, hängt von der Art des Malware-Angriffs ab.Da Viren Ihr Verhalten ständig ändern, ist es schwierig ein Muster für Verhalten und Aktionen festzulegen.

Es gibt Situationen, in denen Acronis Internet Security eine Malware-Infizierung Ihres Systems nicht automatisch entfernen kann.In solch einem Fall ist Ihre Intervention nötig.

Wenn Sie Ihr Problem hier nicht finden oder wenn die vorgeschlagene Lösung nicht zum Erfolg führt, können Sie den technischen Kundendienst von Acronis wie in Kapitel „*Support*“ (S. 187) beschrieben, kontaktieren.

## 30.1. Was ist zu tun, wenn Acronis Internet Security auf Ihrem Computer einen Virus findet?

Sie erfahren wahrscheinlich auf folgende Weisen, ob sich auf Ihrem Computer Viren befinden:

- Sie haben einen Scan durchgeführt und Acronis Internet Security hat infizierte Einträge gefunden.
- Ein Virenwarnhinweis informiert Sie, dass Acronis Internet Security eine oder mehrere Viren auf Ihrem Computer geblockt hat.

In solchen Situationen führen Sie bitte ein Acronis Internet Security-Update durch, um sicherzustellen, dass Sie über die neuesten Malware-Signaturen verfügen und führen Sie einen Vollsystem-Scan durch, um Ihr System zu analysieren.

Sobald der Tiefen-Scan abgeschlossen ist, wählen Sie die gewünschte Aktion für die infizierten Einträge (Desinfizieren, Löschen, In Quarantäne verschieben).

Falls die ausgewählte Aktion nicht durchgeführt werden konnte und im Scan-Protokoll ersichtlich ist, dass Ihr PC mit einer Bedrohung infiziert ist, die nicht gelöscht werden kann, müssen Sie die Datei(en) manuell entfernen.

**Die erste Methode kann im Normalmodus durchgeführt werden**:

1. Deaktivieren Sie denAcronis Internet Security Echtzeit-Antivirenschutz.Um herauszufinden, wie Sie dafür vorgehen sollen, lesen Sie bitte „*Wie aktiviere/deaktiviere ich den Echtzeitschutz?*“ (S. 190).
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen.Um herauszufinden, wie Sie dafür vorgehen sollen, lesen Sie bitte „*Wie kann ich verborgene Objekte in Windows anzeigen lassen?*“ (S. 191).
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.

4. Aktivieren Sie den Acronis Internet Security Echtzeit-Antivirenschutz wieder.

**Sollte die erste Methode, die Infizierung zu entfernen, fehlgeschlagen sein, gehen Sie folgendermaßen vor:**

1. Starten Sie Ihren Computer im abgesicherten Modus neu.Um herauszufinden, wie Sie dafür vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“ (S. 189)*.
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen.
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Starten Sie Ihren Computer im Normalmodus neu.

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 30.2. Wenn Ihr System nicht startet

Wenn Ihr System nicht startet, kann die Acronis Antimalware Scan CD helfen.

Acronis Antimalware Scan CD ist eine bootfähige CD, mit der Sie alle vorhandenen Laufwerke prüfen und desinfizieren können, bevor Ihr Betriebssystem startet.Diese Funktion kann Ihnen auch helfen, Daten von einem gefährdeten Windows PC auf einen Wechseldatenträger speichern.

Wichtig

Wenn Sie ein ISO-Image der Acronis Antimalware Scan CD wünschen, kontaktieren Sie uns wie unter *„Support“ (S. 187)* beschrieben.Danach können Sie die ISO-Datei mit einem beliebigen Brennprogramm auf eine CD oder DVD brennen.

### Systemprüfung mit der Acronis Antimalware Scan CD

Sie können Ihr System mit der Acronis Antimalware Scan CD prüfen, indem Sie folgende Schritte ausführen:

1. Konfigurieren Sie das BIOS Ihres Computers so, dass er von CD bootet.
2. Legen Sie die CD in das Laufwerk und booten Sie Ihren Computer neu.
3. Warten Sie, bis der Acronis Antimalware Scan CD-Bildschirm angezeigt wird.Wählen Sie die Option, die Acronis Antimalware Scan CD zu starten, und drücken Sie dann die **Eingabetaste**.
4. Warten Sie, bis der Neustart abgeschlossen ist. Dies kann eine Weile dauern.
5. Sobald der Neustartvorgang abgeschlossen ist, werden die Acronis Internet Security-Signaturen automatisch aktualisiert und ein Scan aller festgestellten Festplattenpartitionen wird gestartet.

## Datenspeicherung mit der Acronis Antimalware Scan CD

Angenommen, Sie können aus ungeklärten Gründen Ihren Windows-PC nicht starten. Sie müssen aber dringend auf wichtige Daten auf ihrem Computer zugreifen. Für solche Situationen ist die Acronis Antimalware Scan CD ideal.

Um Ihre Daten von Ihrem Computer auf einen Wechseldatenträger, wie z.B. einen USB-Stick zu sichern, gehen Sie folgendermaßen vor:

1. Konfigurieren Sie das BIOS Ihres Computers so, dass er von CD bootet.
2. Legen Sie die CD in das Laufwerk und booten Sie Ihren Computer neu.
3. Warten Sie, bis der Acronis Antimalware Scan CD-Bildschirm angezeigt wird.Wählen Sie die Option, die Acronis Antimalware Scan CD zu starten, und drücken Sie dann die **Eingabetaste**.
4. Warten Sie, bis der Neustart abgeschlossen ist. Dies kann eine Weile dauern.
5. Sobald der Neustartvorgang abgeschlossen ist, werden die Acronis Internet Security-Signaturen automatisch aktualisiert und ein Scan aller festgestellten Festplattenpartitionen wird gestartet.Bitte warten Sie, bis die Prüfung abgeschlossen ist.
6. Ihre Festplattenpartitionen werden auf dem Desktop angezeigt. Sollen die Inhalte einer Festplatte ähnlich wie in Windows Explorer dargestellt werden, doppelklicken Sie darauf.

   **Beachten Sie**
   Wenn Sie die Acronis Antimalware Scan CD verwenden, werden Ihnen Partitionsnamen begegnen, wie sie bei Linux üblich sind. Laufwerke, die unter Windows nicht mit einem Namen versehen wurden, werden als `[LocalDisk-0]` angezeigt, was vermutlich der Windows-Partition `(C:)` entspricht, als `[LocalDisk-1]`, was der Partition `(D:)` entspricht, etc.

7. Stecken Sie den Wechseldatenträger in einen USB-Anschluss Ihres Computers. In wenigen Augenblicken wird ein Fenster eingeblendet, in dem die Inhalte des Geräts angezeigt werden.
8. Das Kopieren von Dateien und Verzeichnissen erfolgt wie im normalen Windows-Umfeld.

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 30.3. Wie entferne ich einen Virus aus einem Archiv?

Bei einem Archiv handelt es sich um eine Datei oder eine Dateisammlung, die mit einem speziellen Format komprimiert wurde, um so den benötigten Festplattenplatz zu reduzieren.

Einige dieser Formate sind offene Formate und bieten Acronis Internet Security die Möglichkeit, diese zu scannen und die entsprechenden Aktionen durchzuführen, um sie zu entfernen.

Andere Archivformate sind teilweise oder komplett geschlossen und Acronis Internet Security kann nur das Vorhandensein von Viren innerhalb dieser Archive feststellen, nicht jedoch andere Aktionen ausführen.

Wenn Acronis Internet Security Sie darüber informiert, dass ein Virus innerhalb eines Archivs gefunden wurde und keine Aktion verfügbar ist, bedeutet dies, dass der Virus aufgrund möglicher Restriktionen der Zugriffseinstellungen des Archivs nicht entfernt werden kann.

So können Sie einen in einem Archiv gespeicherten Virus entfernen.

1. Identifizieren Sie das Archiv, in dem der Virus verborgen ist, indem Sie einen Vollsystem-Scan durchführen.
2. Deaktivieren Sie denAcronis Internet Security Echtzeit-Antivirenschutz.
3. Gehen Sie zum Speicherort des Archivs und dekomprimieren Sie es mit einem Archivierungsprogramm wie beispielsweise WinZip.
4. Identifizieren Sie die infizierte Datei und löschen Sie sie.
5. Löschen Sie das Originalarchiv, um sicherzugehen, dass die Infizierung vollständig entfernt ist.
6. Komprimieren Sie die Dateien erneut in einem neuen Verzeichnis und verwenden Sie dafür ein Komprimierprogramm wie WinZip.
7. Aktivieren Sie den Acronis Internet Security-Echtzeit-Virenschutz und führen Sie einen Vollsystem-Scan durch, um so sicherzustellen, dass Ihr System nicht anderweitig infiziert ist.

**Beachten Sie**

Es ist wichtig zu beachten, dass ein in einem Archiv gespeicherter Virus für Ihr System keine unmittelbare Bedrohung darstellt, da der Virus dekomprimiert und ausgeführt werden muss, um Ihr System zu infizieren.

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 30.4. Wie entferne ich einen Virus aus einem Email-Archiv?

Acronis Internet Security kann auch Viren von auf Festplatten gespeicherten Email-Datenbanken und Email-Archiven aufspüren.

Manchmal ist es notwendig, die infizierte Nachricht über die im Scan-Bericht zur Verfügung gestellten Informationen zu identifizieren und sie dann manuell zu löschen.

So können Sie in einem Email-Archiv gespeicherte Viren entfernen:

1. Scannen Sie die Email-Datenbank mit Acronis Internet Security.
2. Deaktivieren Sie denAcronis Internet Security Echtzeit-Antivirenschutz.
3. Öffnen Sie den Scan-Bericht und nutzen Sie die Identifikationsinformation (Betreff, Von, An) der infizierten Nachricht, um den dazugehörigen Email-Client zu finden.
4. Löschen Sie die infizierte Nachricht.Die meisten Email-Clients verschieben gelöschte Nachrichten in ein Wiederherstellungs-Verzeichnis, von dem aus sie wiederhergestellt werden können.Sie sollten sicherstellen, dass die Nachricht auch aus diesem Recovery-Verzeichnis gelöscht ist.
5. Komprimieren Sie das Verzeichnis, in dem die infizierte Nachricht gespeichert wird.
   - In Outlook Express:klicken Sie im Dateimenü auf "Verzeichnis", dann auf "Alle Verzeichnisse komprimieren".
   - In Microsoft Outlook:klicken Sie im Dateimenü auf "Dateidatenverwaltung".Wählen Sie das persönliche Verzeichnis (.pst), das Sie komprimieren möchten und klicken Sie auf "Einstellungen".Klicken Sie auf Kompakt.
6. Aktivieren Sie den Acronis Internet Security Echtzeit-Antivirenschutz wieder.

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 30.5. Was ist zu tun, wenn Acronis Internet Security eine saubere Datei als infiziert klassifiziert?

Es gibt Fälle, in denen Acronis Internet Security einwandfreie Dateien irrtümlicherweise als Bedrohung (ein falsches Positiv) einstuft.Um diesen Fehler zu korrigieren, fügen Sie die Datei der Acronis Internet Security Ausschlussliste hinzu:

1. Deaktivieren Sie denAcronis Internet Security Echtzeit-Antivirenschutz.Um herauszufinden, wie Sie dafür vorgehen sollen, lesen Sie bitte *„Wie aktiviere/deaktiviere ich den Echtzeitschutz?“ (S. 190)*.
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen.Um herauszufinden, wie Sie dafür vorgehen sollen, lesen Sie bitte *„Wie kann ich verborgene Objekte in Windows anzeigen lassen?“ (S. 191)*.
3. Stellen Sie die Datei aus der Quarantäne wieder her.
4. Geben Sie im Ausschlussbereich die Datei ein.
5. Aktivieren Sie den Acronis Internet Security Echtzeit-Antivirenschutz wieder.

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 30.6. Wie säubern Sie infizierte Dateien in den System Volume Information

Das Verzeichnis "System Volume Information" ist ein Bereich auf Ihrer Festplatte, der vom Betriebssystem erstellt und von Windows zum Speichern von kritischen Informationen genutzt wird, die in Zusammenhang mit der Systemkonfiguration stehen.

Die Acronis Internet Security-Engine kann infizierte Dateien, die im Verzeichnis "System Volume Information" gespeichert wurden, aufspüren. Da es sich hierbei aber um einen geschützten Bereich handelt, kann die infizierte Datei unter Umständen nicht entfernt werden.

Die in den Systemwiederherstellungs-Verzeichnissen gefundenen infizierten Dateien werden im Scan-Protokoll wie folgt angezeigt:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

Um infizierte Datei(en) sofort und vollständig aus der Datenspeicherung zu entfernen, deaktivieren und reaktivieren Sie die Funktion "Systemwiederherstellung".

Wenn die Option "Systemwiederherstellung" deaktiviert ist, werden alle Wiederherstellungspunkte entfernt.

Wenn die Systemwiederherstellung erneut aktiviert wird, werden neue Wiederherstellungspunkte entsprechend dem Zeitplan und den Ereignissen erstellt.

Um die Systemwiederherstellung zu deaktivieren, gehen Sie folgendermaßen vor:

- **In Windows XP:**
  1. Folgen Sie diesem Pfad: **Start → Alle Programme → Zubehör → System Tool → Systemwiederherstellung**
  2. Klicken Sie in der linken Bildschirmseite auf **Einstellungen Systemwiederherstellung**.
  3. Wählen Sie **Systemwiederherstellung ausschalten** für alle Laufwerke und klicken dann auf **Anwenden**.
  4. Wenn Sie einen Warnhinweis erhalten, dass alle existierenden Wiederherstellungspunkte gelöscht werden, klicken Sie zum Fortfahren auf **Ja**.
  5. Um die Systemwiederherstellung einzuschalten, deaktivieren Sie das Kästchen der Option **Systemwiederherstellung ausschalten** für alle Laufwerke und klicken dann auf **Anwenden**.
- **In Windows Vista:**
  1. Folgen Sie diesem Pfad: **Start → Systemsteuerung → System und Wartung → System**
  2. Klicken Sie im linken Feld auf **Systemschutz**.

Wenn Sie zur Eingabe eines Administrator-Passwortes oder einer Bestätigung aufgefordert werden, geben Sie das Passwort oder die gewünschte Bestätigung ein.

3. Um die Funktion "Systemwiederherstellung" auszuschalten, deaktivieren Sie die entsprechenden Kästchen für jedes Laufwerk und klicken Sie auf **Ok**.
4. Um die Systemwiederherstellung zu aktivieren, klicken Sie für jedes Laufwerk die entsprechenden Kästchen an und klicken Sie auf **Ok**.

- **In Windows 7:**
  1. Klicken Sie auf **Start**, rechtsklicken Sie auf **Computer** und danach auf **Eigenschaften**.
  2. Klicken Sie im linken Feld auf den Link **Systemschutz**.
  3. Wählen Sie im Optionenfenster die Option **Systemschutz**, markieren Sie jeden Laufwerksbuchstaben und klicken dann auf **Konfigurieren**.
  4. Wählen Sie **Systemschutz ausschalten** und klicken Sie auf **Anwenden**.
  5. Klicken Sie auf **Löschen**, dann auf **Fortfahren**, wenn Sie dazu aufgefordert werden, und dann auf **Ok**.

Wenn Ihnen diese Informationen nicht weitergeholfen haben, können Sie unseren Kundendienst wie unter *„Support“ (S. 187)* beschrieben kontaktieren.

## 30.7. Welches sind die passwortgeschützten Dateien im Scan-Protokoll?

Dies ist nur eine Benachrichtigung, dass die von Acronis Internet Security gefundenen Dateien entweder passwortgeschützt oder anderweitig verschlüsselt sind.

Am häufigsten sind passwortgeschützte Objekte:

- Dateien, die zu einer anderen Sicherheitslösung gehören.
- Dateien, die zum Betriebssystem gehören.

Um die Inhalte tatsächlich zu scannen, müssen diese Dateien entweder extrahiert oder anderweitig entschlüsselt werden.

Sollten diese Inhalte extrahiert werden, wird der Echtzeit-Scanner von Acronis Internet Security diese automatisch scannen, um so den Schutz Ihres Computers zu gewährleisten.Wenn Sie diese Dateien mit Acronis Internet Security scannen möchten, müssen Sie den Produkthersteller kontaktieren, um nähere Details zu diesen Dateien zu erhalten.

Unsere Empfehlung ist, diese Dateien zu ignorieren, da Sie für Ihr System keine Bedrohung darstellen.

## 30.8. Was sind die übersprungenen Einträge im Scan-Protokoll?

Alle Dateien, die im Scan-Protokoll als "Übersprungen" ausgewiesen werden, sind sauber.

Für eine bessere Leistung scannt Acronis Internet Security keine Dateien, die seit dem letzten Scan nicht verändert wurden.

## 30.9. Was sind die überkomprimierten Dateien im Scan-Protokoll?

Die überkomprimierten Einträge sind Elemente, die durch die Scanning-Engine nicht extrahiert werden konnten oder Elemente, für die eine Entschlüsselung zu viel Zeit in Anspruch genommen hätte und die dadurch das System instabil machen würden.

Überkomprimiert bedeutet, dass Acronis Internet Security das Scannen von Archiven übersprungen hat, da das Entpacken dieser zu viele Systemressourcen in Anspruch genommen hätte. Der Inhalt wird, wenn nötig, in Echtzeit gescannt.

## 30.10. Warum hat Acronis Internet Security eine infizierte Datei automatisch gelöscht?

Wird eine infizierte Datei gefunden, versucht Acronis Internet Security automatisch, diese zu desinfizieren.Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung in Schach zu halten.

Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

Dies geschieht normalerweise bei Installationsdateien, die von nicht vertrauenswürdigen Webseiten downgeloadet werden.Wenn Sie auf ein solches Problem stoßen, downloaden Sie die Installationsdatei von der Hersteller-Webseite oder einer anderen vertrauenswürdigen Webseite.

# 31. Support

Sollten Sie Hilfe oder weiterführende Informationen zu Acronis Internet Security 2011 benötigen, kontaktieren Sie uns über die unten angegebenen Wege.

**Acronis Germany Gmbh**
Balanstr. 59
81541 München
Deutschland

Kaufen: http://www.acronis.de/homecomputing/products/backup-security

Web: http://www.acronis.de/homecomputing/products/backup-security

Um den Support zu kontaktieren benutzen Sie das Webformular unter http://www.acronis.de/support > Kontakt > Starten Sie hier.

Erreichbarkeit:

- Montag - Freitag:
  - 08:00 – 18:00 Support in Deutsch
  - 18:00 – 08:00 Support in Englisch
- Am Wochenende Support in Englisch

Medien:

- E-Mail (Webmail): in Deutsch 24x7
- Chat: abhängig von der Verfügbarkeit der Sprache
- Telefon: abhängig von der Verfügbarkeit der Sprache

# 32. Nützliche Information

In diesem Kapitel finden Sie einige wichtige Vorgehensweisen, über die Sie Bescheid wissen sollten, bevor Sie wegen eines technischen Problems die Fehlersuche starten.

Für die Fehlersuche und -behebung eines technischen Problems in Acronis Internet Security sind etwas tiefergehende Kenntnisse von Windows erforderlich. Deshalb beziehen sich die nächsten Schritte vor allem auf das Windows Betriebssystem.

## 32.1. Wie entferne ich andere Sicherheitsprogramme?

Der Hauptgrund für den Einsatz einer Sicherheitslösung ist der Schutz und die Sicherheit Ihrer Daten.Aber was geschieht, wenn mehr als ein Sicherheitsprogramm auf demselben System läuft?

Wenn Sie mehr als nur eine Sicherheitslösung auf Ihrem Computer verwenden, wird dadurch das System instabil.Der Acronis Internet Security 2011-Installer findet automatisch andere auf dem System existierende Sicherheitssoftware und bietet an, diese zu deinstallieren.

Falls Sie weitere bereits auf dem PC existierende Sicherheitssoftware nicht während der Installation entfernt haben, gehen Sie folgendermaßen vor:

- In **Windows XP**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme hinzufügen/entfernen**.
  2. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
  3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
  4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
- In **Windows Vista** und **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
  3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
  4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

Wenn es Ihnen nicht gelingt, weitere auf Ihrem Rechner installierte Sicherheitssoftware zu entfernen, besorgen Sie sich das Deinstalllations-Werkzeug von der Webseite des entsprechenden Herstellers oder kontaktieren Sie ihn direkt für eine Anleitung zum sauberen Deinstallieren der Software.

## 32.2. Wie führe ich einen Neustart im abgesicherten Modus durch?

Der abgesicherte Modus ist ein diagnostischer Operations-Modus, der hauptsächlich bei der Fehlersuche von normalen Windows-Operationen zum Einsatz kommt.Solche Probleme reichen von sich widersprechenden Treibern bis hin zu Viren, die Windows daran hindern, normal hochzufahren.Im abgesicherten Modus funktionieren nur einige wenige Anwendungen und Windows lädt nur die wichtigsten Treiber und ein Minimum an Betriebssystemkomponenten.Deshalb sind bei einer Verwendung von Windows im abgesicherten Modus die meisten Viren inaktiv und können einfach entfernt werden.

Start von Windows im abgesicherten Modus:

1. Starten Sie Ihren Computer neu.
2. Drücken Sie die **F8**-Taste mehrere Male, bevor Windows startet, um so Zugriff auf das Boot-Menü zu erhalten.
3. Wählen Sie im Boot-Menü die Option **abgesicherter Modus** und drücken Sie auf **Enter**.
4. Warten Sie, während Windows im abgesicherter Modus geladen wird.
5. Dieser Vorgang endet mit einer Bestätigungsbenachrichtigung.Klicken Sie zur Bestätigung auf **Ok**.
6. Um Windows normal zu starten, rebooten Sie einfach Ihr System.

## 32.3. Ist auf meinem System die 32- oder 64-bit-Version von Windows installiert?

Um herauszufinden, ob auf Ihrem Computer ein 32- oder 64-bit-Betriebssystem installiert ist, gehen Sie vor wie folgt:

- In **Windows XP**:
  1. Klicken Sie auf **Start**.
  2. Finden Sie **Mein Computer** im Menü **Start**.
  3. Rechtsklicken Sie auf **Mein Computer** und wählen Sie **Eigenschaften**.
  4. Wenn unter **System x64 Edition** aufgelistet ist, ist auf Ihrem System die 64-Bit-Version von Windows XP installiert.

Wenn die Option **64 Edition** nicht aufgelistet ist, ist auf Ihrem System die 32-bit-Version von Windows XP installiert.

- In **Windows Vista** und **Windows 7**:
  1. Klicken Sie auf **Start**.
  2. Finden Sie **Mein Computer** im Menü **Start**.
  3. Rechtsklicken Sie auf **Mein Computer** und wählen Sie **Eigenschaften**.
  4. In **System** können Sie die Systeminformationen einsehen.

## 32.4. Wo finde ich "Meine Proxy-Einstellungen"?

Um diese Einstellungen zu finden, gehen Sie folgendermaßen vor:

- In Internet Explorer 8:
  1. Öffnen Sie den Internet Explorer.
  2. Wählen Sie **Werkzeuge** > **Internet-Optionen**.
  3. Klicken Sie im Reiter **Verbindungen** auf **LAN-Einstellungen**.
  4. Suchen Sie unter **Für Ihr LAN einen Proxy-Server verwenden**, dort sollten Sie die **Adresse** und den **Port** des Proxys finden.
- In Mozilla Firefox 3.6:
  1. Öffnen Sie den Firefox.
  2. Wählen Sie **Werkzeuge** > **Optionen**.
  3. Gehen Sie im Reiter **Erweitert** auf **Netzwerk**.
  4. Klicken Sie auf **Einstellungen**.
- In Opera 10.51:
  1. Öffnen Sie Opera.
  2. Wählen Sie **Werkzeuge** > **Präferenzen**.
  3. Gehen Sie im Reiter **Erweitert** auf **Netzwerk**.
  4. Klicken Sie auf den Button **Proxy Server**, um das Dialogfenster mit den Proxy-Einstellungen zu öffnen.

## 32.5. Wie aktiviere/deaktiviere ich den Echtzeitschutz?

Acronis Internet Security bietet einen dauerhaften Echtzeitschutz gegen verschiedene Malware, indem alle Dateien auf die zugegriffen wird sowie Email-Nachrichten und die Kommunikationen per Instant Messaging Software (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) gescannt werden.

Normalerweise ist der Echtzeitschutz von Acronis Internet Security aktiviert, diesen sollten Sie auch nicht deaktivieren.

Wenn Sie ein Problem beheben oder einen Virus entfernen möchten, müssen Sie eventuell den Echtzeitschutz deaktivieren. Dies gilt für folgende Situationen:

- Ein Verlangsamungsproblem des Systems nach der Installation von Acronis Internet Security
- Ein Problem mit einem der Programme oder Anwendungen nach der Installation Acronis Internet Security
- Kurz nach der Installation von Acronis Internet Security könnten Fehlermeldungen eingeblendet werden.

Gehen Sie folgendermaßen vor, um den Echtzeitschutz vorübergehend zu aktivieren/deaktivieren:

1. Öffnen Sie Acronis Internet Security, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus** > **Schild**.
3. Deaktivieren Sie die Option **Echzeitschutz ist aktiviert**, um so den Antiviren-Schutz vorübergehend auszuschalten (oder platzieren Sie das Häkchen, falls Sie den Schutz einschalten möchten).
4. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll.

Beachten Sie

Die Schritte zur Deaktivierung des Echtzeitschutzes von Acronis Internet Security sollten nur als vorübergehende Lösung betrachtet und nur für einen kurzen Zeitraum angewendet werden.

## 32.6. Wie kann ich verborgene Objekte in Windows anzeigen lassen?

Diese Schritte sind sinnvoll in den Fällen, in denen Sie es mit einer Malware-Situation zu tun haben und Sie infizierte Dateien, die eventuell verborgen sind, finden und entfernen müssen.

Gehen Sie folgendermaßen vor, um versteckte Objekte in Windows anzuzeigen:

1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und wählen Sie **Verzeichnisoptionen**.
2. Gehen Sie auf den Reiter **Ansicht**.
3. Wählen Sie **Inhalte des Systemverzeichnisses anzeigen** (nur für Windows XP).

4. Wählen Sie **Verborgene Dateien und Verzeichnisse anzeigen**.
5. Deaktivieren Sie **Dateierweiterungen für bekannte Dateitypen verbergen**.
6. Deaktivieren Sie **Geschützte Betriebssystemdateien verbergen**.
7. Klicken Sie auf **Anwenden** und dann auf **Ok**.

# Glossar

**Adware**

Adware ist häufig mit einer Absenderanwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware Anwendungen müssen in der Regel installiert werden, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

**AktiveX**

AktiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann.Die AktiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden.Mit AktiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen.AktiveX Controls werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.

**Aktualisierung**

Neue Softwareversionen oder Hardwareprodukte, die eine ältere Version ersetzen.Die Update-Installationsroutine sucht nach älteren Versionen auf dem Rechner, da sonst kein Update installiert werden kann.

Acronis Internet Security verfügt über ein eigenes Update-Modul, das manuelle oderautomatische Scans nach Updates ermöglicht.

**Arbeitsspeicher**

Interne Speicherzonen im Rechner.Der Begriff Arbeitsspeicher bedeutet Datenträger in Form von sehr schnellen Chips.Das Wort Speicher ist der Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet.Jeder Rechner hat eine gewisse Menge Arbeitsspeicher.Dieser wird auch Hauptspeicher oder RAM genannt.

**Archive**

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

**Backdoor (Hintertür)**

Eine Sicherheitslücke eines Systems, die der Entwickler oder Verwalter absichtlich hinterlässt.Der Grund dafür muss nicht immer bösartig sein.Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

**Befehlszeile**

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

**Bootsektor**

Der erste Sektor einer Festplatte oder Diskette.Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

**Bootvirus**

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert.Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert.Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

**Cookie**

In der Internetindustrie werden Cookies als kleine Dateien beschrieben, die Daten über einzelne Computer enthalten und die von den Werbern analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden.Die Cookie-Technologie wurde deshalb weiter entwickelt, damit der Benutzer nur solche Werbung zugeschickt bekommt, die seinen Interessen dient.Für viele ist es aber wie ein zweischneidiges Messer.Einerseits ist es wirksam und sachbezogen, da man nur Anzeigen, an denen man interessiert ist, betrachten kann, anderseits heißt es dem Benutzer "auf die Spur zu kommen" und ihn auf Schritt und "Klick " zu verfolgen.Es ist verständlich, dass der Datenschutz ein umstrittenes Thema ist und viele sich von dem Begriff als SKU-Nummern (die Streifencodes auf den Packungen, die im Geschäft an der

Theke gescannt werden) betrachtet zu werden, angegriffen fühlen.Auch wenn dieser Gesichtspunkt extrem erscheint ist er manchmal korrekt.

**Dateierweiterung**

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS.Sie enthalten gewöhnlich ein bis zwei Buchstaben (alte Betriebssysteme können nicht mehr als drei Buchstaben unterstützen), Beispiele dafür sind "c" für C-Quellcode, "ps" für PostScript oder "txt" für beliebige Texte.Windows zeigt bei ihm bekannten Dateitypen keine Dateierweiterung in der graphischen Benutzeroberfläche an, stattdessen wird häufig ein Symbol verwendet.

**Download**

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät.Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner.Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

**Durchsuchen**

Kurzform für Web-Browser, eine Softwareanwendung, die zum Lokalisieren und Anzeigen von Webseiten verwendet wird.Die bekanntesten Browser sind Netscape Navigator und Microsoft Internet Explorer.Beide sind graphische Browser, das heißt sie können sowohl Grafiken als auch Texte anzeigen.Weiterhin können die meisten Browser Multimedia-Informationen wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

**E-Mail**

Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

**E-Mail Client**

Ein E-Mail Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

**Ereignisanzeige**

Ereignisse oder Erscheinungen, die in einem Programm vorkommen.Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

**Fehlalarm**

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist. Kann bei heuristischem Virenprüfen auftreten.

**Heuristik**

Eine Methode, um neue Viren zu identifizieren.Diese Prüfmethode beruht nicht auf spezifische Virussignaturen.Der Vorteil einer heuristischen Prüfung ist, dass man nicht von einer neuen Virusvariante getäuscht werden kann.Manchmal kann auch ein verdächtiger Code in einemnormalen Programm gemeldet werden, ein sogenannter Fehlalarm wird angezeigt.

**IP**

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

**Java Applet**

Ein Java Programm, das nur auf Webseiten läuft.Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) des Applets an.Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus.Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets auf dem Client laufen, können diese keine Daten auf der Clientmaschine lesen oder schreiben.Zusätzlich sind die Applets weiter begrenzt, so dass sie nur Daten aus der Domäne lesen und beschreiben können, die sie unterstützen.

**Komprimierte Programme**

Eine Datei in einem komprimierten Format.Viele Betriebssysteme und Anwendungen enthalten Befehle, die das Komprimieren einer Datei ermöglichen, so dass diese weniger Speicherplatz benötigt.Zum Beispiel: Angenommen Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält.Normalerweise nehmen diese 10 Bytes Speicherplatz ein.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein spezielles Zeichen „Leerzeichenreihe“ ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden.In diesem Fall sind nur noch zwei Bytes notwendig statt zehn.Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

**Laufwerk**

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

**Logdatei (Berichtsdatei)**

Eine Datei, die stattgefundene Aktivitäten aufzeichnet.Zum Beispiel speichert Acronis Internet Security eine Logdatei mit den gescannten Pfaden, Verzeichnissen und der Archivanzahl sowie den gescannten, infizierten oder verdächtigen Dateien.

**Makrovirus**

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird.Viele Anwendungen, wie Microsoft Word und Excel, unterstützen mächtige Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

**Nicht heuristisch**

Diese Prüfmethode beruht auf einer spezifischen Virussignatur.Der Vorteil einer nicht heuristischen Prüfung ist, dass diese nicht von einem Scheinvirus getäuscht werden kann, und dass dieser keinen falschen Alarm auslöst.

**Pfad**

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet.Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

**Phishing**

Dabei wird eine E-Mail mit einer betrügerischen Absicht an einen Nutzer gesendet.Der Inhalt dieser E-Mail gibt vor, von einem bekannten und seriös arbeitenden Unternehmen zu stammen.Zweck dieser E-Mail ist es dann, private und geheime Nutzerdaten zu erhalten, worauf der Absender beabsichtigt, die Identität des Nutzers anzunehmen.Die E-Mail führt den Benutzer dann auf eine Webseite, in der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TAN's oder PIN's preiszugeben.Dies soll aus Gründen der Aktualisierung geschehen.Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

**Polymorpher Virus**

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert.Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

**Rootkit**

Bei einem Rootkit handelt es sich um einen Satz von Softwarewerkzeugen die einem Administrator Low-End Zugriff zu einem System verschaffen. Rootkits traten zunächst nur auf UNIX-Systemen auf und haben im Laufe der Zeit auch Ihren Einzug auf Linux- und Windows-Systemen gehalten.

Die Hauptaufgabe eines Rootkits besteht darin, seine Existenz zu verstecken indem Prozesse und Dateien versteckt werden, Anmeldedaten und Berichtsdateien zu fälschen und jegliche Art von Daten abzufangen.

Rootkits zählen von Haus aus nicht zu schadensverursachender Software da Sie keine Schadroutinen besitzen. Jedoch verändern Sie die vom Betriebssystem zurückgegebenen Daten und verstecken auf diese Weise ihre Präsenz. Dennoch kann über ein solches Rootkit schädliche Software nachträglich eingeschleust werden und auch der wirtschaftliche Schaden ist nicht zu unterschätzen.

**Schnittstelle**

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann.Rechner haben verschiedenartige Schnittstellen.Intern gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen.Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen.Die Schnittstellennummer gibt die Art der Schnittstelle an.Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

**Script**

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

**Spam**

Junk-E-Mail oder Junk-Postings in Newsgroups.Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

**Spyware**

Software, die unentdeckt vom Nutzer Anwenderdaten über seine Internetverbindung sammelt und abruft. Dies geschieht in der Regel zu Werbezwecken. Typischerweise werden Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Sharewareprogrammen gebündelt, die aus dem Internet herunter geladen werden können. Es ist jedoch darauf hinzuweisen, dass die Mehrzahl der Shareware- und Freeware-Anwendungen frei von Spyware ist. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an jemand anderen. Spyware kann auch Informationen über E-Mail Adressen und sogar Kennwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren.Eine weit verbreitete Möglichkeit, ein Opfer von Spyware zu werden, ist der Download von bestimmten heute erhältlichen Peer-to-Peer-Dateiaustauschprogrammen (Direktverbindungen von Computern).

Abgesehen von den Fragen der Ethik und des Datenschutzes bestiehlt Spyware den Anwender, indem sie Speicherressourcen seines Rechners nutzt und den Internetzugriff verlangsamt, indem über seine Internetverbindung Informationen an den Spyware-Heimatserver gesendet werden.Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

**Startup Objekt (Autostart-Objekt)**

Jede Datei, die sich in diesem Ordner befindet, öffnet sich, wenn der Rechner gestartet wird.Zum Beispiel ein Startbildschirm, eine Sounddatei, die abgespielt wird, wenn der Rechner gestartet wird, ein Erinnerungskalender oder Anwendungsprogramme können Autostart-Objekte sein.Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

**Symbolleiste**

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Icons zur Information und zum leichteren Zugriff, zum Beispiel: Fax, Drucker, Modem, Lautstärke und mehr. Um auf die Details und Steuerungen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

**TCP/IP**

Transmission Control Protocol/Internet Protocol - Im Internet werden eine Vielzahl von verschiedener Hardware und Betriebssystemen miteinander verbunden.TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

**Trojaner**

Ein vernichtendes Programm, das sich als eine freundliche Anwendung tarnt und auftritt.Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können zerstörerisch sein.Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.Viele Trojaner öffnen den Rechner für den Zugriff von außen.

Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenkten.Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, kamen die in dem Bauch des hölzernen Pferdes versteckten

Soldaten heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsmännern in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

**Virus**

Ein Programm oder ein Codestück, das auf einen Rechner geladen wird, ohne dass der Benutzer Kenntnis davon hat und welches sich allein ausführt.Die Resultate von Viren können einfache Scherzmeldungen aber auch die Zerstörung von Hardware sein.Die meisten Viren können sich selber vervielfältigen.Alle Computerviren sind von Menschenhand geschrieben.Ein Virus, der sich immer wieder vervielfältigen kann ist sehr einfach zu schreiben.Sogar ein solch einfacher Virus ist fähig, sich durch Netzwerke zu verschicken und Sicherheitssysteme zu überbrücken.

**Virusdefinition**

Ein binäres Virusmuster, das von einem AntiVirus Programm verwendet wird, um einen Virus zu entdecken und zu entfernen.

**Wurm**

Ein Programm, das sich über ein Netzwerk verbreitet.Es kann sich nicht an andere Programme anhängen.