Internet**Security**

Optimaler Schutz & Sicherheit im Internet

BEDIENBUCH

BUFFALO

WISO InternetSecurity

Optimaler Schutz &
Sicherheit im Internet

Vertrieb:
Buhl Data Service GmbH
Am Siebertsweiher 3/5
57290 Neunkirchen

Redaktionsschluss 01.09.2017

Inhalt

Teil 1 Installation

A Installation PC

A 1.1 Vor der ersten Installation

Vielen Dank, dass Sie sich für unser Produkt entschieden haben.

Um das Produkt zu installieren, benötigen Sie Folgendes:

- Ihre Garantie-Nummer
- Eine Internetverbindung
- Internet Explorer oder anderen aktuellen Webbrowser

Wenn Sie ein Sicherheitsprodukt von einem anderen Anbieter verwenden, wird das Installationsprogramm versuchen, dieses automatisch zu entfernen. Sollte dies nicht automatisch geschehen, entfernen Sie es bitte manuell.

> Hinweis

Wenn auf dem Computer mehr als ein Konto vorhanden ist, melden Sie sich bei der Installation mit einem Konto an, welches über Administratorrechten verfügt.

A 1.2 Erstmalige Installation des Produkts

Gehen Sie zur Installation des Produkts wie folgt vor:

Haben Sie Ihr Produkt im Rahmen Ihres Aktualitäts-Garantie Vertrags erhalten, oder die Downloadversion erworben, überspringen Sie bitte Schritt 1 bis 3.

1. Wenn Sie die Software im Handel erworben haben, öffnen Sie im Internet Explorer oder einem beliebigen anderen Webbrowser folgende Seite:

   http://www.buhl.de/lizenzen_aktivieren.html

2. Verfügen Sie bereits über Anmeldedaten für **www.buhl.de**? Dann melden Sie sich mit Ihrer E-Mail Adresse oder Kundennummer und Ihrem Passwort an. Andernfalls erstellen Sie bitte ein Konto mit E-Mail Adresse und Passwort.

3. Tragen Sie nach erfolgreicher Anmeldung/ Registrierung Ihre Garantie-Nummer in die entsprechenden dafür vorgesehenen Felder ein.

- Wenn Sie die Software im Handel erworben haben, finden Sie Ihre Garantie-Nummer auf der Innenseite Ihrer CD-Hülle.
  Als Vertragskunde finden Sie Ihre Garantie-Nummer auf Ihrer Vertragsrechnung oder im Online-Kundenkonto.

4. Wechseln Sie über „Meine Produkte und Verträge“ zur Vertragsübersicht und wählen dort die „Details“ Ihres neuen Produktes.
5. Klicken Sie auf die Option „Erweitert“, um die lizenzspezifischen Installer herunterzuladen und starten das Setup mittels Doppelklick.
6. Befolgen Sie die Anweisungen auf dem Bildschirm.

Sie müssen Ihren Computer möglicherweise neu starten, bevor Ihr Abonnement validiert werden kann und die neuesten Updates aus dem Internet heruntergeladen werden können. Wenn Sie die Installation mithilfe der CD gestartet haben, entnehmen Sie diese, bevor Sie Ihren Computer neu starten.

A 2.1 Einstieg PC

Erste Schritte mit dem Produkt

In diesem Abschnitt wird beschrieben, wie Sie die allgemeinen Einstellungen ändern und Ihre Abonnements für das Produkt verwalten können.

Die Einstellungen umfassen:

- Updates. Hier können Sie sehen, welche Updates heruntergeladen wurden und die Verfügbarkeit neuer Updates manuell überprüfen.
- Verbindungseinstellungen. Hier können Sie die Internetverbindung Ihres Computers ändern.
- Installierte Anwendungen. Hier finden Sie die installierten Bestandteile der WISO Internet Security.

2.1.1 Wo finde ich meine Konto-ID oder Garantie-Nummer?

Wenn Sie unseren Kundensupport kontaktieren möchten, benötigen Sie unter Umständen Ihre Konto-ID. So können Sie sich Ihr Konto und Ihre Gerätekennungen ansehen:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste. Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie „Allgemeine Einstellungen öffnen".
3. Wählen Sie die Option Identifizierungscodes.

Auf dieser Seite finden Sie Ihr Konto und die Kennungen Ihrer aktuellen Geräte. Mit diesen Kennungen können Sie Ihre Abonnements verwalten.

Wenn Sie Ihr Produkt im Handel erworben haben, finden Sie Ihre Garantie-Nummer im Karton auf Ihrem Aktivierungszertifikat. Als Vertragskunde finden Sie Ihre Garantie-Nummer auf Ihrer Vertragsrechnung oder im Online-Kundenkonto unter www.buhl.de/vertraege.html.

2.1.2 Verwendung des Wartungscenters

Das Wartungcenter zeigt Ihnen wichtige Meldungen an.

Wenn im Wartungscenter noch Aktionen ausstehen, werden Sie regelmäßig daran erinnert.

2.1.2.1 Öffnen des Wartungscenters

Öffnen Sie das Wartungscenter, um alle wichtigen Meldungen anzuzeigen.

Öffnen des Wartungscenters:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste. Das Element **Offen - Wartungscenter** im Pop-up-Menü zeigt an, wie viele Aktionen bei Ihnen ausstehen.
2. Wählen Sie **Wartungscenter öffnen.**

Im Wartungscenter wird eine Liste aller durchzuführenden Aktionen angezeigt.

3. Klicken Sie auf die entsprechenden Elemente in der Liste, um weitere Informationen anzuzeigen.
4. Wenn Sie momentan keine der ausstehenden Aktionen durchführen möchten, klicken Sie auf **Verschieben,** um diese später durchzuführen.

> Hinweis

Wenn Sie mehrere ausstehende Aktionen in Ihrem Wartungscenter haben, klicken Sie auf **Alle verschieben**, um das Wartungscenter zu schließen und alle Aktionen später durchzuführen.

2.1.2.2 Installation einer Produktaktualisierung

Wenn eine kostenlose Aktualisierung für ein Produkt verfügbar ist, das Sie installiert haben, müssen Sie diese installieren, um die neue Version zu verwenden.

Aktualisierung des Produkts:

1. Wartungscenter öffnen.
   Im Wartungscenter wird das Element **Produkt-Upgrade** verfügbar angezeigt. Wenn mehrere Elemente im Wartungscenter angezeigt werden, klicken Sie auf das Element, um dieses zu öffnen.
2. Klicken Sie auf **Aktualisieren.**

> Hinweis

Sie haben die neuen Lizenzbedingungen zur Aktualisierung des Produkts nicht akzeptiert, falls diese sich geändert haben.

Möglicherweise müssen Sie Ihren Computer neu starten, sobald die Aktualisierung abgeschlossen ist.

2.1.3 Woher weiß ich, ob mein Vertrag gültig ist?

Angaben zu Art und Status Ihres Abonnements finden Sie auf der Seite Abonnements.

Wenn Ihr Abonnement bald abläuft oder bereits abgelaufen ist, ändert sich der allgemeine Schutzstatus des Programms.

So prüfen Sie die Gültigkeit Ihrer Anmeldung:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **„Allgemeine Einstellungen öffnen > Abonnementschlüssel“** anzeigen.

Falls Ihr Abonnement abgelaufen ist, müssen Sie es erneuern, um weiterhin Updates zu erhalten und das Produkt verwenden zu können.

2.1.3.2 Verlängerung Ihres Nutzungszeitraums

Sie können Ihren Nutzungszeitraum in unserem Online Store verlängern.

www.buhl.de

2.1.4 Verwendung von Automatische Updates

Automatische Updates schützen Ihren Computer vor den neuesten Bedrohungen.

Das Produkt lädt die neuesten Updates auf Ihren Computer herunter, wenn Sie mit dem Internet verbunden sind. Es erkennt den Netzwerkverkehr und stört auch bei einer langsamen Netzwerkverbindung nicht die Internetnutzung.

2.1.4.1 Den Update-Status überprüfen

Datum und Uhrzeit der letzten Aktualisierung anzeigen.

Normalerweise müssen Sie nicht selbst um Updates anfragen, das das Produkt die neuesten Updates automatisch erhält, sobald Sie mit dem Internet verbunden sind.

So prüfen Sie, ob Sie die neuesten Updates besitzen:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen** öffnen.
3. Wählen Sie **Updates.**
4. Klicken Sie auf **Jetzt prüfen.**

Das Produkt lädt die neuesten vorhandenen Updates herunter.

> Hinweis

Ihre Internetverbindung muss aktiv sein, wenn Sie überprüfen möchten, ob es neue Updates gibt.

2.1.4.2 Ändern der Einstellungen für die Internetverbindung

Normalerweise müssen die Standardeinstellungen nicht geändert werden, aber Sie können konfigurieren, wie der Computer mit dem Internet verbunden ist, damit Sie automatisch Updates erhalten.

Gehen Sie wie folgt vor, um die Einstellungen für die Internetverbindung zu ändern:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen** öffnen.
3. Wählen Sie **Verbindung**.
4. Wählen Sie **Internetverbindung** aus, wenn Ihr Computer mit dem Internet verbunden ist.
5. Wählen Sie in der Liste HTTP-Proxy, ob Ihr Computer einen Proxyserver nutzt, um eine Verbindung mit dem Internet herzustellen.

- Wählen Sie Kein HTTP-Proxy, wenn Ihr Computer direkt mit dem Internet verbunden ist.
- Wählen Sie HTTP-Proxy manuell konfigurieren aus, um die HTTP-Proxy-Einstellungen zu konfigurieren.
- Wählen Sie HTTP-Proxy meines Browsers verwenden, um die gleichen HTTP-Proxy-Einstellungen zu verwenden, die in Ihrem Browser konfiguriert sind.

2.1.4.3 Einstellungen für mobiles Breitband ändern

Wählen Sie, ob Sie bei der Verwendung von mobilem Breitband Sicherheitsupdates herunterladen möchten.

> Hinweis

Diese Funktion ist nur in Microsoft Windows 7 und neueren Windows-Versionen verfügbar.

Standardmäßig werden Sicherheitsupdates immer heruntergeladen, wenn Sie mit dem Netzwerk Ihres Privatanbieters verbunden sind. Die Updates werden jedoch unterbrochen, sobald Sie auf ein Netzwerk eines anderen Anbieters zugreifen. Dies liegt daran, dass die Verbindungspreise zwischen Anbietern, beispielsweise in verschiedenen Ländern, variieren können. Sie sollten diese

Einstellung nicht ändern, wenn Sie bei Ihrem Besuch Bandbreite und möglicherweise auch Kosten sparen möchten.

> Hinweis

Diese Einstellung gilt nur für mobile Breitbandverbindungen. Wenn der Computer mit einem Festnetz oder Drahtlosnetzwerk verbunden ist, wird das Produkt automatisch aktualisiert.

So ändern Sie die Einstellung:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.

Ein Pop-up-Menü wird angezeigt.

2. Wählen Sie Allgemeine Einstellungen öffnen.
3. Wählen Sie Verbindung.
4. Wählen Sie die bevorzugte Update-Option für Mobilverbindungen:

- **Nie**
  Es werden keine Updates heruntergeladen, wenn Sie mobiles Breitband verwenden.
- **Nur im Netz meines Betreibers**
  Updates werden im Netzwerk Ihres Privatanbieters immer heruntergeladen. Wenn Sie ein Netzwerk eines anderen Anbieters besuchen, werden die Updates unterbrochen. Wir empfehlen Ihnen, diese Option zu wählen, um Ihr Sicherheitsprodukt zu den erwarteten Kosten auf dem neuesten Stand zu halten.
- **Immer**
  Updates werden immer heruntergeladen, egal welches Netzwerk Sie verwenden. Wählen Sie diese Option, wenn Sie sicherstellen möchten, dass die Sicherheit Ihres Computers, unabhängig von den Kosten, stets aktuell ist.

> Hinweis

Wenn Sie jedes Mal erneut auswählen möchten, sobald Sie das Netzwerk Ihres Heimbetreibers verlassen, wählen Sie **Jedes Mal nachfragen, sobald ich das Netzwerk meines Heimbetreibers verlasse.**

Sicherheitsupdates unterbrochen

Die Sicherheitsupdates können unterbrochen werden, wenn Sie mobiles Breitband außerhalb des Netzwerks Ihres Privatanbieters nutzen.

In diesem Fall sehen Sie die Benachrichtigung **Angehalten** in der unteren rechten Ecke Ihres Bildschirms. Die Updates werden unterbrochen, da die Verbindungspreise je nach Anbieter und Land variieren können. Sie sollten in Betracht ziehen, diese Einstellung nicht zu ändern, wenn Sie Bandbreite und dadurch mögliche Kosten sparen möchten. Wenn Sie jedoch die Einstellungen trotzdem ändern möchten, klicken Sie auf den Link **Ändern.**

> Hinweis

Diese Funktion ist nur in Microsoft Windows 7 und neueren Windows-Versionen verfügbar.

2.1.5 Wie erkennt man, was das Produkt geleistet hat?

Auf der Seite **Produktzeitleiste** können Sie sehen, welche Aktionen das Produkt ausgeführt hat, um Ihren Computer zu schützen.

Das Produkt zeigt eine Benachrichtigung an, wenn es eine Aktion durchführt, beispielsweise um Dateien zu schützen, die auf Ihrem Computer gespeichert sind. Möglicherweise werden manche Benachrichtigungen auch an Ihren Service Provider gesendet, beispielsweise um Sie über neue verfügbare Services zu informieren.

So zeigen Sie die Produktzeitleiste an:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.
2. Klicken Sie auf **Produktzeitleiste öffnen.**

Die Benachrichtigungsliste der Produktzeitleiste wird geöffnet.

2.1.6 Spielmodus

Aktivieren Sie den Spielmodus, wenn Sie während des Spielens Systemressourcen freigeben wollen.

Computerspiele benötigen häufig viele Systemressourcen, um reibungslos zu funktionieren.

Andere Anwendungen, die im Hintergrund ausgeführt werden, können die Leistung von Spielen verschlechtern, da Sie Systemressourcen und das Netzwerk belegen.

Der Spielmodus verringert den Einfluss des Produkts auf Ihren Computer und reduziert seine Netzwerkverwendung. Dadurch werden mehr Systemressourcen für Computerspiele freigegeben, während die Grundfunktionen des Produktes unbeeinflusst bleiben. So werden z. B. automatische Updates, geplante Scans und andere Vorgänge ausgesetzt, die viele Systemressourcen und Netzwerkverkehr benötigen.

Wenn Sie eine Anwendung im Vollbildmodus verwenden, z. B. eine Präsentation, Slideshow oder ein Video ansehen oder ein Spiel im Vollbildmodus spielen, zeigen wir nur essentielle Benachrichtigungen an, die Ihre unmittelbare Aufmerksamkeit erfordern. Andere Benachrichtigungen werden erst angezeigt, wenn Sie den Vollbildmodus oder Spielmodus verlassen.

2.1.6.1 Spielmodus aktivieren

Aktivieren Sie den Spielmodus, um die Leistung von Spielen auf Ihrem Computer zu verbessern.

Spielmodus aktivieren:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.

Ein Pop-up-Menü wird angezeigt.

2. Wählen Sie **Spielmodus**.

Die Nutzung der Systemressourcen durch das Produkt ist nun optimiert und Spiele können auf Ihrem Computer reibungslos ausgeführt werden.

Vergessen Sie nicht den Spielmodus auszuschalten, wenn Sie das Spiel beenden. Der Spielmodus wird automatische deaktiviert, wenn Sie Ihren Computer neu starten oder den Energiesparmodus verlassen.

B Installation Mac

B 1.1 Vor der ersten Installation

Um das Produkt zu installieren, benötigen Sie Folgendes:

- Ihre Garantie-Nummer
- Eine Internetverbindung
- Safari oder anderen aktuellen Webbrowser

> Hinweis

Die Installation setzt Administratorrechte bei der Installation voraus. Das Passwort eines administrativen Kontos sollte zur Hand sein.

B 1.2 Erstmalige Installation des Produkts

Gehen Sie zur Installation des Produkts wie folgt vor:

1. Öffnen Sie im Safari oder einem beliebigen anderen Webbrowser folgende Seite:
   http://www.buhl.de/lizenzen_aktivieren.html
2. Verfügen Sie bereits über Anmeldedaten für **www.buhl.de**? Dann melden Sie sich mit Ihrer E-Mail Adresse oder Kundennummer und Ihrem Passwort an. Andernfalls erstellen Sie bitte ein Konto mit E-Mail Adresse und Passwort.
3. Tragen Sie nach erfolgreicher Anmeldung/Registrierung Ihre Garantie-Nummer in die entsprechenden Felder ein.
   Wenn Sie die Software im Handel erworben haben, finden Sie Ihre Garantie-Nummer im Karton auf Ihrem Aktivierungszertifikat. Als Vertragskunde finden Sie Ihre Garantie-Nummer auf der Innenseite Ihrer CD-Hülle.

4. Wechseln Sie über „Meine Produkte und Verträge“ zur Vertragsübersicht und wählen dort die „Details“ Ihres neuen Produktes.
5. Klicken Sie auf die Option „Erweitert“, um die lizenzspezifischen Installer herunterzuladen und starten das Setup mittels Doppelklick.
6. Befolgen Sie die Anweisungen auf dem Bildschirm.
7. Sie müssen Ihren Computer möglicherweise neu starten, bevor Ihr Abonnement validiert werden kann und die neuesten Updates aus dem Internet heruntergeladen werden können. Wenn Sie die Installation mithilfe der CD durchführen, entnehmen Sie die Installations-CD, bevor Sie Ihren Computer neu starten.

B 2.1 Einstieg Mac

Die **Status**-Seite zeigt den aktuellen Schutzstatus und andere wichtige Informationen zum Produkt an.

1. Klicken Sie auf das Produktsymbol in der Menüleiste.
2. Die **Status**-Seite wird beim Öffnen des Produkts geöffnet.

Auf der **Status**-Seite können Sie:

- Den aktuellen Schutzstatus überprüfen,
- sicherstellen, dass alle Funktionen auf dem neuesten Stand sind, sehen, wann das letzte Update durchgeführt wurde und
- überprüfen, wie lang Ihr Abonnement noch gültig ist.

2.1.1 Wie kann ich sicherstellen, dass mein Computer geschützt ist?

Die Status-Seite zeigt den aktuellen Schutzstatus und andere wichtige Informationen zum Produkt an.

Zum Öffnen der Status-Seite:

1. Klicken Sie auf das Produktsymbol in der Menüleiste.
2. Die Status-Seite wird beim Öffnen des Produkts geöffnet.

Auf der Status-Seite können Sie:

- Den aktuellen Schutzstatus überprüfen,
- sicherstellen, dass alle Funktionen auf dem neuesten Stand sind, sehen, wann das letzte Update durchgeführt wurde und
- überprüfen, wie lang Ihr Abonnement noch gültig ist.

2.1.2 Schutzstatus-Symbole

Die Symbole auf der Status-Seite zeigen den Gesamtstatus des Produkts und seine Funktionen an. Die folgenden S ymbole zeigen Ihnen den Status des Programms und seiner Sicherheits-funktionen an.

> Status-Symbol	> Statusbezeichnung	> Beschreibung
	ok	Ihr Computer ist geschützt. Die Funktionen sind aktiviert und arbeiten ordnungsgemäß.
	Informationen	Das Produkt informiert Sie über einen besonderen Status. Alle Funktionen arbeiten korrekt, aber das Produkt lädt z. B. gerade Updates herunter.
	Warnung	Ihr Computer ist nicht vollständig geschützt. Sie sollten das Produkt überprüfen, z. B. weil es seit langem keine Updates mehr erhalten hat.
	Fehler	Ihr Computer ist nicht geschützt. Das ist z. B. der Fall, wenn Ihr Abonnement abgelaufen ist oder eine kritische Funktion deaktiviert wurde.
	Aus	Eine nicht-kritische Funktion ist ausgeschaltet.

2.1.3 Deinstallation

Das Produkt kann nicht deinstalliert werden, indem man die Anwendung in den Papierkorb verschiebt. Sie müssen das Deinstallationsprogramm für das Produkt verwenden, um es von Ihrem Computer zu entfernen.

Sie benötigen Administratorrechte für den jeweiligen Computer, um das Produkt zu deinstallieren.

Befolgen Sie diese Anweisungen:

1. Öffnen Sie den Ordner, in dem Sie das Produkt installiert haben. In der Standardeinstellung befindet sich das Produkt im Ordner Anwendungen.
2. Doppelklicken Sie auf das Symbol **WISO Internet Security deinstallieren.** Das Deinstallationsprogramm wird geöffnet.
3. Klicken Sie auf **Deinstallieren.**

Sie müssen Ihr Administratorpasswort eingeben, um das Produkt zu deinstallieren.

4. Geben Sie Ihren Administrator-Benutzernamen und das Passwort ein und klicken Sie auf OK.

Das Produkt wird vom Computer entfernt.

B 3.1 Update Mac

Automatische Updates schützen Ihren Computer vor den neuesten Bedrohungen.

Das Produkt lädt die neuesten Updates auf Ihren Computer herunter, wenn Sie mit dem Internet verbunden sind. Es erkennt den Netzwerkverkehr und stört auch bei einer langsamen Netzwerkverbindung nicht die Internetnutzung.

3.1.1 Den Update-Status überprüfen

Datum und Uhrzeit der letzten Aktualisierung anzeigen.

Normalerweise müssen Sie nicht selbst um Updates anfragen, das Produkt erhält die neuesten Updates automatisch, sobald Sie mit dem Internet verbunden sind.

So prüfen Sie, ob Sie die neuesten Updates besitzen:

1. Klicken Sie auf das Produktsymbol in der Menüleiste.
2. Wählen Sie **Nach Updates suchen** aus dem Menü.

Das Produktmenü zeigt das Datum der zuletzt installierten Datenbank.

C Installation Android Smartphone/Tablet

C 1.1 Vor der ersten Installation

Um das Produkt zu installieren, benötigen Sie Folgendes:

- Ihren Lizenzschlüssel.
  Dieser wird in Ihrem Kundenkonto unter „**Meine Produkte und Verträge > Details > Erweitert**“ erzeugt.
- Eine Internetverbindung
- Einen aktuellen Webbrowser
- Smartphone/Tablet mit dem Betriebssystem Android
- ca. 15 MB freier interner Gerätespeicher

> Hinweis | Die Installation auf einer SD-Karte ist nicht möglich

Nach Abschluss der Installation müssen Sie das Produkt aktivieren. Erst mit der Aktivierung schützt das Produkt Ihr Gerät.

Wählen Sie eine der folgenden Möglichkeiten zur Installation des Produkts auf Ihrem Gerät:

C 1.2 Laden Sie die App WISO Internet Security aus dem Google Play Store herunter und verschieben Sie sie auf den internen Speicher oder auf die SD-Karte

Gehen Sie zur Installation des Produkts wie folgt vor:

Haben Sie Ihr Produkt im Rahmen Ihres Aktualitäts-Garantie Vertrags erhalten, oder die Downloadversion erworben, überspringen Sie bitte Schritt 1 - 3.

1. Wenn Sie die Software im Handel erworben haben, öffnen Sie im Internet Explorer oder einem beliebigen anderen Webbrowser folgende Seite: **http://www.buhl.de/lizenzen_aktivieren.html**
2. Verfügen Sie bereits über Anmeldedaten für www.buhl.de? Dann melden Sie sich mit Ihrer E-Mail Adresse oder Kundennummer und Ihrem Passwort an. Andernfalls erstellen Sie bitte ein Konto mit E-Mail Adresse und Passwort.

3. Wechseln Sie über „Meine Produkte und Verträge“ zur Vertragsübersicht und wählen dort die „Details“ Ihres neuen Produktes.
4. Erstellen Sie über „Hinzufügen“ eine neue Lizenz und legen Sie als Gerät „Android“ fest.
5. Benennen Sie Ihre Gerät, um es zukünftig identifizieren zu können.
6. Wählen Sie Gerät jetzt einrichten.
7. Notieren Sie den Aktivierungsschlüssel, der nach Abschluss des vorherigen Schrittes neben Ihrer Android-Lizenz erscheint.
8. Besuchen Sie den Google Play Store und laden sich die App WISO Internet Security herunter.
9. Starten Sie das Installationspaket auf Ihrem Gerät, um das Produkt zu installieren. Beachten Sie, dass Sie zum Starten des Installationspakets von der Speicherkarte aus einen Dateimanager eines Drittanbieters benötigen. Das Installationspaket installiert das Produkt auf Ihrem Gerät.
10. Starten Sie die App. Betätigen Sie die Menü-Schaltfläche und gehen Sie über „Mehr > Abonnement > Sie haben bereits einen Schlüssel?“ Ihren in Schritt 7 erzeugten Lizenzschlüssel.

C 2.1 Aktivierung Android

Erst mit der Aktivierung schützt das Produkt Ihr Gerät.

So aktivieren Sie das Produkt:

1. Starten Sie die Anwendung.
   Beim ersten Produktstart werden die Lizenzbedingungen angezeigt.
2. Lesen Sie die Lizenzbedingungen. Wenn Sie sie akzeptieren, aktiveren Sie das Kontrollkästchen und drücken Sie auf Weiter.
   Sobald Sie die Lizenzbedingungen akzeptiert haben, kann die Aktivierung beginnen.
3. Wählen Sie den Aktivierungstyp aus.
   Sie können das Produkt entweder im kostenlosen Testmodus oder mit Ihrem Abonnement-Code aktivieren.

- Wenn Sie das Produkt testen möchten, wählen Sie den Aktivierungstyp **Kostenlose Testversion.**
- Wenn Sie bereits einen Abonnementschlüssel haben, wählen Sie den Abonnementtyp **Abonnementschlüssel** und geben Sie Ihren Abonnementschlüssel ein. Ihr Abonnementschlüssel findet Sie in Ihrem Kundenkonto auf **www.buhl.de**, siehe Abschnitt Fehler! Verweisquelle konnte nicht gefunden werden.

4. Drücken Sie auf Aktivieren.

> Hinweis

Bei der Aktivierung muss das Produkt eine Verbindung zum Update-Dienst aufbauen.

Sobald Sie die Aktivierung abgeschlossen haben, öffnet sich der Konfigurationsassistent, mit dem Sie das Produkt einrichten können.

Auf Android 2.2 und jüngeren Versionen müssen Sie den Geräteadministrator aktivieren, damit Sie Anti-Theft verwenden können.

C 3.1 Update Android

Der automatische Update-Dienst des Produkts sucht regelmäßig nach neuen Updates und hält das Produkt auf dem neuesten Stand.

Nachdem Sie das Produkt aktiviert haben, ist die automatische Update-Funktion eingeschaltet. Für automatische Updates ist eine aktive Internetverbindung erforderlich. Wenn eine Internetverbindung verfügbar ist, sucht das Produkt regelmäßig nach Updates und lädt ggf. neue Updates
herunter.

> Hinweis

Solange Sie über ein aktives Abonnement verfügen, können Sie das Produkt uneingeschränkt aktualisieren. Damit Ihr Gerät ständig geschützt bleibt, sollten Sie die Dienstdauer rechtzeitig vor dem Ablaufdatum verlängern.

Teil 2 Bedienanleitung PC/Mac

1. Security Cloud

1.1 Worum handelt es sich bei der Security Cloud?

Die Security Cloud ist ein Online-Service, der bei aktuellen Internet-Gefahren schnell reagiert. Als Teilnehmer erlauben Sie der Security Cloud, Daten zu sammeln, die es uns ermöglichen, Ihren Schutz vor neuen und aufkommenden Bedrohungen zu erhöhen. Die Security Cloud sammelt Informationen zu bestimmten unbekannten, bösartigen oder verdächtigen Anwendungen und nicht klassifizierten Websites. Diese Informationen sind anonym und werden zur kombinierten Datenanalyse an die F-Secure Corporation gesendet. Wir verwenden die analysierten Informationen, um Sie besser vor den aktuellsten Bedrohungen und bösartigen Dateien zu schützen.

So funktioniert die Security Cloud

Die Security Cloud sammelt Informationen zu unbekannten Anwendungen und Websites sowie bösartigen Anwendungen und Website-Exploits.

Die Security Cloud verfolgt weder Ihre Webaktivitäten nach noch sammelt sie Informationen auf Websites, die bereits analysiert wurden. Desweiteren sammelt sie auch keine Informationen zu sauberen Anwendungen, die auf Ihrem Computer installiert sind.

Falls Sie diese Daten nicht bereitstellen möchten, werden die Informationen zu installierten Anwendungen oder besuchten Websites nicht von der Security Cloud gesammelt. Das Produkt muss jedoch die F-Secure-Server abfragen, um die Zuverlässigkeit von Anwendungen, Websites, Nachrichten und anderen Objekten zu gewährleisten. Die Abfrage geschieht mithilfe einer kryptographischen Prüfsumme. Das abgefragte Objekt wird dabei nicht an F-Secure gesendet.

Wir verfolgen keine Daten einzelner Benutzer nach; lediglich der Zugriffszähler der Datei oder der Website wird erhöht.

Es ist nicht möglich, jeglichen Netzverkehr zur Security Cloud zu unterbinden, da hierdurch der vom Produkt hergestellte Schutz grundlegend gewährt wird.

1.1.1 Überprüfen Sie den Status der Security Cloud.

Bei vielen Produktfunktionen hängt die richtige Funktionsweise von der Verbindung der Security-Cloud ab.

Falls Netzwerkprobleme bestehen oder Ihre Firewall den Netzwerkverkehr der Security Cloud blockiert, ist der Status getrennt. Wenn keine Produktfunktionen installiert sind, die eine Verbindung mit der Security Cloud erfordern, lautet der Status nicht in Verwendung.

So prüfen Sie den Status:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste. Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Wählen Sie **Verbindung**.

Unter **Security Cloud** wird Ihnen der aktuelle Status der Security Cloud angezeigt.

1.2 Vorteile der Security Cloud

Mit der Security Cloud haben Sie einen schnelleren und genaueren Schutz vor aktuellen Bedrohungen. Zudem werden Sie bei verdächtigen, aber nicht schädlichen Anwendungen nicht unnötig alarmiert.

Als Teilnehmer an der Security Cloud können Sie uns dabei helfen, neue und unentdeckte Malware zu finden und mögliche falsch positive Bewertungen zu entfernen.

Alle Teilnehmer an einer Security Cloud helfen sich gegenseitig. Wenn die Security Cloud eine verdächtige Anwendung findet, profitieren Sie von den Analyseergebnissen, wenn das gleiche Programm bereits von jemand anderem gefunden wurde. Die Security Cloud verbessert die Leistung insgesamt, da das installierte Sicherheitsprodukt keine Anwendungen scannen muss, die bereits von der Security Cloud analysiert und als sauber befunden wurden. Gleichermaßen werden Informationen zu schädlichen Websites und unange-

forderte Bulk-Nachrichten in der Security Cloud geteilt. Somit können wir Sie zuverlässiger vor Website-Exploits und Spam-Nachrichten schützen.

Je mehr Personen an der Security Cloud teilnehmen, desto besser werden die einzelnen Teilnehmer geschützt.

1.3 Welche Daten steuern Sie bei?

Als Teilnehmer gestatten Sie der Security Cloud, Informationen zu den Anwendungen zu sammeln, die Sie installiert haben, und zu den Websites, die Sie besuchen. Somit kann die Security Cloud Sie besser vor den neuesten bösartigen Anwendungen und verdächtigen Websites schützen.

Analyse der Dateibewertung

Die Security Cloud sammelt nur Informationen von unbekannten Anwendungen und Dateien, die entweder verdächtig sind oder als Malware gelten.

Es werden ausschließlich Informationen zu Anwendungsdateien (ausführbare Dateien) gesammelt, nicht zu anderen Dateitypen.

Abhängig vom Produkt können die gesammelten Informationen Folgendes beinhalten:

- den Dateipfad der Anwendung (ohne personenbezogene Informationen),
- die Dateigröße sowie das Datum, an dem sie erstellt oder geändert wurde,
- Dateiattribute und Berechtigungen,
- Signaturinformationen der Datei,
- die aktuelle Version der Datei und das Unternehmen, das sie erstellt hat,
- den Dateiursprung oder seine Download-URL (ohne personenbezogene Informationen),
- Ergebnisse von F-Secure DeepGuard und Antivirusanalyse gescannter Dateien und
- sonstige ähnliche Informationen.

Die Security Cloud erfasst keine Informationen zu Ihren persönlichen Dokumenten, wenn diese nicht als infiziert gemeldet wurden. Für alle Arten von bösartigen Dateien erfasst das Programm die Bezeichnung der Infektion sowie den Bereinigungsstatus der Datei.

Dateien zur Analyse übermitteln

Bei einigen Produkten können Sie außerdem verdächtige Anwendungen zur Analyse an die Security Cloud senden.

Sie können einzelne verdächtige Anwendungen manuell übermitteln, wenn das Produkt Sie dazu auffordert. Oder Sie können in den Produkteinstellungen das automatische hochladen verdächtiger Anwendungen aktivieren. Die Security Cloud lädt niemals Ihre persönlichen Dokumente hoch.

Die Website-Bewertung analysieren

Die Security Cloud verfolgt Ihre Internetaktivität nicht nach. Es sorgt dafür, dass von Ihnen besuchte Websites sicher sind, wenn Sie im Internet surfen. Sobald Sie eine Website besuchen, wird deren Sicherheit von der Security Cloud untersucht und Sie werden benachrichtigt, falls die Website als verdächtig oder schädlich eingestuft wird.

Damit wir unseren Service verbessern und eine Einstufungen immer korrekt vornehmen können, sammelt die Security Cloud gegebenenfalls Informationen über besuchte Websites. Die Informationen werden gesammelt, falls die von Ihnen besuchte Website bösartige oder verdächtige Inhalte aufweist oder einen bekannten Exploit, bzw. falls die Inhalte der Website noch nicht bewertet oder kategorisiert wurden. Die gesammelten Informationen umfassen die URL und die Metadaten, die mit dem Besuch und der Website verbunden sind. Die Security Cloud führt strenge Kontrollen durch, damit sichergestellt wird, dass keine persönlichen Daten gesendet werden. Die Anzahl der gesendeten URLs ist begrenzt. Alle eingereichten Daten werden nach personenbezogenen Informationen gefiltert, bevor sie gesendet werden, und alle Felder, die Informationen enthalten könnten, die mit Ihnen in Verbindung gebracht werden könnten, werden entfernt. Die Security Cloud bewertet und analysiert keine Webseiten in privaten Netzwerken und es sammelt keine Informationen zu privaten Netzwerkadressen oder Aliasen.

Die Systeminformationen analysieren

Die Security Cloud sammelt den Namen und die Version Ihres Betriebssystems, Informationen zur Internetverbindung und Verwendungsstatistiken zur Security Cloud (z. B. wie oft die Website-Bewertung abgefragt wurde oder wie lange es durchschnittlich dauert, bis die Abfrage ein

Ergebnis liefert). Auf diese Weise können wir unseren Service überwachen und verbessern.

1.4 So schützen wir Ihre Daten

Wir übertragen die Informationen sicher und entfernen automatisch alle persönlichen Informationen, die in den Daten enthalten sein könnten.

Die gesammelten Informationen werden einzeln verarbeitet. Sie werden mit Informationen anderer Teilnehmer an der Security Cloud kombiniert. Alle Daten werden statistisch und anonym analysiert. Das bedeutet, dass keine Daten mit Ihnen in Verbindung gebracht werden.

Jegliche Informationen, die Sie persönlich identifizieren könnten, sind nicht in den gesammelten Daten enthalten. Die Security Cloud sammelt keine privaten IP-Adressen oder privaten Informationen, wie E-Mail-Adressen, Benutzernamen und Passwörter. Wir bemühen uns sehr, alle persönlich identifizierbaren Daten zu entfernen. Trotz allem ist es möglich, dass in den gesammelten Informationen noch immer einige identifizierbaren Daten enthalten sind.

In diesen Fällen verwenden wir diese versehentlich gesammelten Daten nicht, um Sie zu identifizieren.

Wir legen großen Wert auf strenge Sicherheitsmaßnahmen sowie physische, administrative und technische Schutzmaßnahmen, um die gesammelten Informationen während deren Übertragung, Speicherung und Verarbeitung zu schützen. Die Informationen werden an gesicherten Orten und auf Servern gespeichert, die von uns kontrolliert werden und sich entweder in unseren Büros oder den Büros unserer Zulieferbetriebe befinden. Nur berechtigtes Personal darf auf diese gesammelten Informationen zugreifen.

F-Secure darf diese gesammelten Daten an seine Tochtergesellschaften, Zulieferbetriebe, Vertriebshändler und Partner weitergeben, jedoch grundsätzlich in einer nicht identifizierbaren, anonymen Art und Weise.

1.5 Werden Sie Teilnehmer an der Security Cloud.

Sie helfen uns bei der Verbesserung der Security Cloud, indem Sie uns Informationen zu schädlichen Programmen und Websites mitteilen.

Sie können während der Installation entscheiden, ob Sie an der Security Cloud teilnehmen möchten. Standardmäßig ist angegeben, dass Sie Daten in der Security Cloud bereitstellen möchten. Sie können diese Einstellung jedoch später im Produkt ändern.

Befolgen Sie diese Anweisungen, um die Einstellungen der Security Cloud zu ändern:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste. Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen** öffnen.
3. Wählen Sie **Sonstiges > Datenschutz.**
4. Aktivieren Sie das entsprechende Kontrollkästchen, um an der Security Cloud teilzunehmen.

1.6 Fragen zu Security Cloud

Kontaktdetails für Fragen zur Security Cloud Für alle weiteren Fragen zur Security Cloud wenden Sie sich an:

- F-Secure Corporation
- Tammasaarenkatu 7
- PL 24
- 00181 Helsinki Finnland

http://www.f-secure.com/de/web/home_global/support/contact

Die aktuelle Version dieser Bestimmung finden Sie jederzeit auf unserer Website.

2. Computer wird vor schädlichen Anwendungen geschützt

2.1 Computer wird vor schädlichen Anwendungen geschützt

Dieses Produkt schützt Ihren Computer vor Viren und anderen schädlichen Anwendungen.

Das Produkt schützt Ihren Computer vor Anwendungen, die möglicherweise Ihre persönlichen Daten stehlen, Ihre Dateien beschädigen oder Ihren Computer für illegale Zwecke benutzen.

Das Viren-Scanning durchsucht Ihren Computer automatisch nach schädlichen Dateien.

DeepGuard überwacht Anwendungen, um potenziell schädliche Änderungen an Ihrem System zu erkennen und zu verhindern. Zudem hält es Eindringlinge und schädliche Anwendungen davon ab, über das Internet Zugang zu Ihrem Computer zu erhalten.

Das Produkt sorgt dafür, dass Ihr Schutz immer auf dem neuesten Stand ist. Es lädt Datenbanken herunter, die Informationen über das automatische Finden und Entfernen von schädlichen Inhalten enthalten.

> Hinweis

Das Produkt lädt die aktuellsten Datenbanken herunter, nachdem die Installation abgeschlossen ist. Währenddessen kann das Viren-Scanning nicht alle Gefahren erkennen.

Andere Produktfunktionen, wie etwa DeepGuard, schützen Ihren Computer jedoch während dieser Zeit.

2.1.1 Schutzstatus-Symbole

Die Symbole auf der Status-Seite zeigen den Gesamtstatus des Produkts und seine Funktionen an.

Die folgenden Symbole zeigen Ihnen den Status des Programms und seiner Sicherheits- funktionen an.

> Status-Symbol	> Statusbezeichnung	> Beschreibung
	ok	Ihr Computer ist geschützt. Die Funktionen sind aktiviert und arbeiten ordnungsgemäß.
	Informationen	Das Produkt informiert Sie über einen besonderen Status. Alle Funktionen arbeiten korrekt, aber das Produkt lädt z. B. gerade Updates herunter.
	Warnung	Ihr Computer ist nicht vollständig geschützt. Sie sollten das Produkt überprüfen, z. B. weil es seit langem keine Updates mehr erhalten hat.
	Fehler	Ihr Computer ist nicht geschützt. Das ist z. B. der Fall, wenn Ihr Abonnement abgelaufen ist oder eine kritische Funktion deaktiviert wurde.
	Aus	Eine nicht-kritische Funktion ist ausgeschaltet.

2.1.2 Anzeigen der Produktstatistikdaten

Sie können sehen, was das Produkt seit dem letzten Installieren auf der Seite Statistiken geleistet hat. Zum Öffnen der Seite **Statistiken:**

Klicken Sie auf **Statistiken.**

Die Seite **Statistiken** zeigt folgende Informationen:

- Der **Virenschutz** zeigt an, wie viele Dateien das Produkt seit der Installation gescannt und gesäubert hat.
- Unter **Anwendunge**n sehen Sie, wie viele Programme DeepGuard seit der Installation zugelassen oder blockiert hat.

2.1.3 Handhabung der Produkt-Updates

Das Produkt sorgt für eine regelmäßige und automatische Aktualisierung des gebotenen Schutzes.

Einstellungen für mobiles Breitband ändern

Wählen Sie, ob Sie bei der Verwendung von mobilem Breitband Sicherheitsupdates herunterladen möchten.

> Hinweis

Diese Funktion ist nur in Microsoft Windows 7 und neueren Windows-Versionen verfügbar.

Standardmäßig werden Sicherheitsupdates immer heruntergeladen, wenn Sie mit dem Netzwerk Ihres Privatanbieters verbunden sind. Die Updates werden jedoch unterbrochen, sobald Sie auf ein Netzwerk eines anderen Anbieters zugreifen. Dies liegt daran, dass die Verbindungspreise zwischen Anbietern, beispielsweise in verschiedenen Ländern, variieren können. Sie sollten diese Einstellung nicht ändern, wenn Sie bei Ihrem Besuch Bandbreite und möglicherweise auch Kosten sparen möchten.

> Hinweis

Diese Einstellung gilt nur für mobile Breitbandverbindungen. Wenn der Computer mit einem Festnetz oder Drahtlosnetzwerk verbunden ist, wird das Produkt automatisch aktualisiert.

So ändern Sie die Einstellung:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste. Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen öffnen.**
3. Wählen Sie **Verbindung.**
4. Wählen Sie die bevorzugte Update-Option für Mobilverbindungen:

- **Nie**
  Es werden keine Updates heruntergeladen, wenn Sie mobiles Breitband verwenden.
- **Nur im Netz meines Betreibers**
  Updates werden im Netzwerk Ihres Privatanbieters immer heruntergeladen. Wenn Sie ein Netzwerk eines anderen Anbieters besuchen, werden die Updates unterbrochen. Wir empfehlen Ihnen, diese Option zu wählen, um Ihr Sicherheitsprodukt zu den erwarteten Kosten auf dem neuesten Stand zu halten.
- **Immer**
  Updates werden immer heruntergeladen, egal welches Netzwerk Sie verwenden. Wählen Sie diese Option, wenn Sie sicherstellen möchten, dass die Sicherheit Ihres Computers, unabhängig von den Kosten, stets aktuell ist.

> Hinweis

Wenn Sie jedes Mal erneut auswählen möchten, sobald Sie das Netzwerk Ihres Heimbetreibers verlassen, wählen Sie **Jedes Mal nachfragen, sobald ich das Netzwerk meines Heimbetreibers verlasse.**

Sicherheitsupdates unterbrochen

Die Sicherheitsupdates können unterbrochen werden, wenn Sie mobiles Breitband außerhalb des Netzwerks Ihres Privatanbieters nutzen.

In diesem Fall sehen Sie die Benachrichtigung **Angehalten** in der unteren rechten Ecke Ihres Bildschirms. Die Updates werden unterbrochen, da die Verbindungspreise je nach Anbieter und Land variieren können. Sie sollten in Betracht ziehen, diese Einstellung nicht zu ändern, wenn Sie Bandbreite und dadurch mögliche Kosten sparen möchten. Wenn Sie jedoch die Einstellungen trotzdem ändern möchten, klicken Sie auf den Link Ändern.

> Hinweis

Diese Funktion ist nur in Microsoft Windows 7 und neueren Windows-Versionen verfügbar.

2.1.4 Was sind Viren und Malware?

Als Malware werden Programme bezeichnet, die speziell entwickelt wurden, um Ihren Computer zu beschädigen oder ohne Ihr Wissen zu illegalen Zwecken zu verwenden oder aber um Informationen von Ihrem Computer zu stehlen.

Malware kann:

- die Kontrolle über Ihren Webbrowser übernehmen,
- Ihre Suche umleiten,
- unerwünschte Werbung einblenden,
- die von Ihnen besuchten Websites aufzeichnen,
- persönliche Informationen stehlen, wie Ihre Kontodaten,
- Ihren Computer zum Versenden von Spam benutzen und
- Ihren Computer benutzen, um andere Computer anzugreifen.

Malware kann außerdem dazu führen, dass Ihr Computer langsam und instabil wird. Der Verdacht, dass sich Malware auf Ihrem Computer befindet, liegt dann nahe, wenn er plötzlich sehr langsam wird und häufig abstürzt.

Viren

Ein Virus ist in der Regel ein Programm, das sich selbst an Dateien anhängt und sich ständig selbst repliziert; es kann die Inhalte anderer Dateien so verändern oder ersetzen, dass Ihr Computer dadurch beschädigt wird.

Ein Virus ist ein Programm, das normalerweise ohne Ihr Wissen auf Ihrem Computer installiert wird. Anschließend versucht der Virus, sich zu replizieren. Der Virus:

- verwendet einige der Systemressourcen Ihres Computers,
- kann Dateien auf Ihrem Computer verändern oder beschädigen,
- versucht wahrscheinlich, Ihren Computer zu benutzen, um andere Computer zu infizieren,
- kann zulassen, dass Ihr Computer für illegale Zwecke verwendet wird.

Spyware

Spyware sind Programme, die Ihre persönlichen Informationen sammeln. Spyware kann persönliche Daten sammeln, wie:

- Internet-Websites, die Sie besucht haben,
- E-Mail-Adressen auf Ihrem Computer,
- Passwörter oder
- Kreditkartennummern.

Spyware installiert sich fast immer selbst, ohne Ihre ausdrückliche Erlaubnis. Spyware wird unter Umständen zusammen mit einem nützlichen Programm installiert. Es ist aber auch möglich, dass Sie in einem irreführenden Popup-Fenster versehentlich auf eine Option klicken.

Rootkits

Rootkits sind Programme, die dafür sorgen, dass Malware schwer zu finden ist.

Rootkits verstecken Dateien und Prozesse. In der Regel, um schädliche Aktivitäten auf dem Computer zu verbergen. Wenn ein Rootkit Malware versteckt, ist es nicht einfach, die Malware auf Ihrem Computer zu finden.

Dieses Produkt besitzt einen Rootkit-Scanner, der gezielt nach Rootkits sucht, wodurch Malware sich nicht problemlos verstecken kann.

Riskware

Riskware wurde nicht speziell entwickelt, um Ihrem Computer zu schaden, sie kann Ihrem Computer aber schaden, wenn sie missbräulich verwendet wird.

Riskware ist genau genommen keine Malware. Riskware-Programme führen einige nützliche, aber potenziell gefährliche Funktionen durch.

Beispiele für Riskware-Programme:

- Programme für Instant Messaging, etwa IRC (Internet Relay Chat),
- Programme zur Übertragung von Dateien über das Internet von einem Computer auf einen anderen,
- oder Programme für die Internet-Telefonie, etwa VoIP (Voice over Internet Protocol).
- Fernzugriffs-Software, z. B. VNC,
- Scareware; versucht durch Verschrecken oder Betrug zum Kauf gefälschter Sicherheitssoftware zu bewegen

- Software, die für die Umgehung von CD-Prüfungen oder Kopierschutz programmiert ist

Wenn Sie das Porgramm explizit installiert und richtig eingerichtet haben, ist es wahrscheinlich ungefährlich.

Wenn die Riskware ohne Ihr Wissen installiert wurde, wurde sie wahrscheinlich in böser Absicht installiert und sollte entfernt werden.

2.2 Wie scanne ich meinen Computer?

Wenn Sie das Viren-Scanning aktivieren, wird Ihr Computer automatisch nach schädlichen Dateien durchsucht. Sie können Dateien auch manuell scannen und Scanvorgänge für einen bestimmten Zeitpunkt planen.

Das Viren-Scanning sollte stets aktiviert sein. Führen Sie für Ihre Dateien einen manuellen Scanvorgang durch, wenn Sie sichergehen möchten, dass auf Ihrem Computer keine schädlichen Dateien vorhanden sind, oder wenn Sie Dateien prüfen möchten, die Sie vom Echtzeit-Scan ausgeschlossen haben.

Durch die Planung von Scanvorgängen können schädliche Dateien zu einem ganz bestimmten Zeitpunkt über das Viren-Scanning von Ihrem Computer entfernt werden.

2.2.1 Automatisches Scannen von Dateien

Beim Echtzeit-Scanning wird der Computer geschützt, indem alle Dateien gescannt werden, wenn auf sie zugegriffen wird, und der Zugriff auf Dateien, die Malware enthalten, gesperrt wird.

Wenn Ihr Computer versucht auf eine Datei zuzugreifen, scannt der Echtzeit-Scan die Datei auf Malware bevor der Zugriff auf die Datei erlaubt wird.

Wenn der Echtzeit-Scan gefährliche Inhalte findet, wird die Datei in Quarantäne gesetzt, bevor Schaden entstehen kann.

Beeinträchtigt das Echtzeit-Scanning die Leistung meines Computers?

Normalerweise bemerken Sie den Scanvorgang nicht, da er nur kurz dauert und wenig Systemressourcen benötigt. Wie lange das Scannen in Echtzeit dauert und wie viele Systemressourcen benötigt werden, hängt beispielsweise vom Inhalt, dem Speicherort und dem Typ der Datei ab.

Dateien, bei denen das Scannen länger dauert:

- Dateien auf Wechseldatenträgern wie CDs, DVDs und tragbaren USB-Laufwerken.
- Komprimierte Dateien, wie .zip.

> Hinweis | Komprimierte Dateien werden nicht automatisch gescannt.

Das Scannen in Echtzeit kann Ihren Computer verlangsamen, wenn:

- Sie mit einem Computer arbeiten, der nicht den Systemanforderungen entspricht.
- Sie auf zahlreiche Dateien gleichzeitig zugreifen. Wenn Sie z. B. ein Verzeichnis öffnen, das eine große Anzahl Dateien enthält, die gescannt werden müssen.

Aktivieren oder Deaktivieren des Echtzeit-Scannings

Das Echtzeit-Scanning sollte stets aktiviert sein, damit Malware gestoppt wird, noch bevor sie Schaden auf Ihrem Computer anrichten kann.

So aktivieren bzw. deaktivieren Sie das Echtzeit-Scanning:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> Hinweis | Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. So wird der **Virenschutz** ein- oder ausgeschaltet.
3. Klicken Sie auf **OK.**

Automatische Handhabung schädlicher Dateien

Beim Echtzeit-Scanning können schädliche Dateien automatisch, d. h. ohne Ausgabe von Fragen an den Benutzer, verwaltet werden.

So bestimmen Sie die automatische Handhabung schädlicher Dateien beim Echtzeit-Scanning:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> Hinweis Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Virenschutz.**
3. Wählen Sie **Schädliche Dateien automatisch verwalten.**

Wenn schädliche Dateien nicht automatisch verwaltet werden sollen, werden Sie beim Echtzeit-Scanning aufgefordert, die durchzuführende Aktion auszuwählen, wenn eine schädliche Datei identifiziert wird.

Handhabung von Spyware

Der Virenschutz blockiert Spyware sofort beim Ausführungsversuch.

Bevor eine Spyware-Anwendung ausgeführt werden kann, wird sie vom Scanner blockiert. Sie können dann die weitere Vorgehensweise bestimmen.

Wählen Sie eine der folgenden Aktionen, wenn Spyware identifiziert wird:

> Durchzuführende Aktion	> Was mit der Spyware geschieht
Automatisch handhaben	Die Scanfunktion sucht die beste Aktion für die identifzierte Spyware aus.
Spyware in Quarantäne stellen	Die Spyware wird in eine Quarantänezone verschoben, in der Sie keinen Schaden auf Ihrem Computer anrichten kann
Spyware löschen	Alle Spyware-bezogenen Dateien werden vom Computer entfernt.
Spyware nur blockieren	Der Zugriff auf die Spyware wird blockiert, die Spyware verbleibt jedoch auf Ihrem Computer
Spyware vom Scan ausschließen	Die Ausführung von Spyware wird zugelassen und Spyware wird bei allen weiteren Scanvorgängen nicht mehr berücksichtigt.

Handhabung von Riskware

Der Virenschutz blockiert Riskware direkt beim Ausführungsversuch.

Bevor eine Riskware-Anwendung ausgeführt werden kann, wird sie blockiert. Sie können dann die weitere Vorgehensweise bestimmen.

Wählen Sie eine der folgenden Aktion, wenn Riskware identifiziert wurde:

> Durchzuführende Aktion	> Was mit der Riskware geschieht
Riskware nur blockieren	Der Zugriff auf die Riskware wird blockiert, die Riskware verbleibt jedoch auf Ihrem Computer
Riskware in Quarantäne stellen	Die Riskwarewird in eine Quarantänezone verschoben, in der Sie keinen Schaden auf Ihrem Computer anrichten kann
Riskware löschen	Alle Riskware-bezogenen Dateien werden vom Computer entfernt.
Riskware vom Scan ausschließen	Die Ausführung von Riskware wird zugelassen und Riskware wird bei allen weiteren Scanvorgängen nicht mehr berücksichtigt.

2.2.2 Manuelles Scannen von Dateien

Sie können Ihre Dateien manuell scannen, wenn Sie z. B. ein externes Gerät an Ihren Computer anschließen. Dadurch können Sie sicherstellen, dass keine Malware vorhanden ist.

Starten des manuellen Scanvorgangs

Sie können Ihren gesamten Computer scannen oder nach einem bestimmten Typ von Malware oder einen bestimmten Bereich scannen.

Wenn Sie einen bestimmten Typ von Malware befürchten, können Sie nur nach diesem Typ scannen. Wenn Sie im Bezug auf einen bestimmten Bereich Ihres Computers einen Verdacht haben, dann scannen Sie nur diesen Bereich. Diese Scans verlaufen viel schneller als ein vollständiger Scan des gesamten Computers.

So starten Sie das Scannen Ihres Computers manuell:

> Hinweis

Wenn Sie das System schnell Scan möchten, klicken Sie auf der Statusseite auf **Scannen**.

1. Klicken Sie auf der Toolsseite auf den Pfeil neben **Erweiterter Scan**. Die Scan-Optionen werden angezeigt.
2. Wählen Sie den Scan-Typ.
   Wählen Sie **Scanning-Einstellungen ändern,** um den Ablauf der manuellen Scanvorgänge auf Ihrem Computer für die Suche nach Viren und anderen schädlichen Anwendungen zu optimieren.
3. Bei Auswahl von **Elemente für Scan wählen** wird ein Fenster geöffnet, in dem Sie das zu prüfende Verzeichnis oder Objekt angeben kön- nen. **Der Scan-Assistent** wird geöffnet.

Scantypen

Sie können Ihren gesamten Computer scannen oder nach einem bestimmten Typ von Malware oder einen bestimmten Bereich scannen.

Dies sind die verschiedenen Scantypen:

> Scantyp	> Was wird gescannt?	> Wann dieser Typ verwendet werden sollte
Viren- und Spyware-Scanning	Teile Ihres Computers auf Viren, Spyware und Riskware	Diese Art des Scannens ist weitaus schneller als ein vollständiger Scan.Es werden nur die Teile Ihres Systems durchsucht, die installierte Programmdateien enthalten. Dieser Scantyp wird empfohlen, wenn Sie rasch überprüfen möchten, ob Ihr Computer sauber ist, da Sie mit dieser Funktion aktive Malware auf Ihrem Computer rasch entdecken können.
Vollständiger Scan des Computers	Ihr gesamter Computer (interne und externe Festplatten) auf Viren, Spyware und Riskware	Wenn Sie absolut sicher sein wollen, dass keine Malware oder Riskware auf Ihrem Computer ist.Diese Art des Scannens dauert am längsten.Sie kombiniert den schnellen Malware-Scan und den Festplattenscan. Außerdem sucht sie nach Elementen, die unter Umständen durch ein Rootkit verborgen sind.
Auwahl für Scan...	Ein spezieller Ordner oder ein spezielles Laufwerk für Viren, Spyware und Riskware	Wenn Sie den Verdacht haben, dass sich an einem bestimmten Speicherort Ihres Computers Malware befindet, weil sich dort Downloads von potenziell gefährlichen Quellen, wie Peer-to-Peer File Sharing-Netzwerken, befinden. Wie lange der Scan dauert, hängt von der Größte des zu scannenden Ziels ab.Der Scan wird beispielsweise schnell abgeschlossen, wenn Sie einen Ordner mit nur ein paar kleinen Dateien scannen.

Im Windows Explorer scannen

Sie können Datenträger, Ordner und Dateien im Windows Explorer in Bezug auf Viren, Spyware und Riskware scannen.

So scannen Sie einen Datenträger, einen Ordner oder eine Datei:

1. Platzieren Sie den Mauszeiger auf dem zu scannenden Datenträger, dem Ordner oder der Datei und klicken Sie mit der rechten Maustaste.
2. Wählen Sie im Kontextmenü **Ordner nach Viren scannen**. (Der Name der Option hängt davon ab, ob Sie einen Datenträger, einen Ordner oder eine Datei scannen.) Das Fenster **Scan-Assistent** wird geöffnet und der Scanvorgang beginnt.

Wenn ein Virus oder Spyware gefunden wird, führt Sie der **Scan-Assistent** durch die für die Bereinigung erforderlichen Schritte.

Auswählen von Dateien für den Scanvorgang

Sie können die Dateitypen auswählen, die auf Viren und Spyware manuell oder geplant gescannt werden sollen.

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> Hinweis | Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Manuelle Scans.**

3. Wählen Sie unter **Suchoptionen** aus den folgenden Einstellungen:

> Nur bekannte Dateitypen scannen

Um nur die Dateitypen zu scannen, die mit einer höheren Wahrscheinlichkeit infiziert sind, beispielsweise ausführbare Dateien. Das Auswählen dieser Option beschleunigt den Scanvorgang. Dateien mit den folgenden Erweite- rungen werden gescannt: ani, asp, ax, bat, bin, boo, chm, cmd, com, cpl, dll, doc, dot, drv, eml, exe, hlp, hta, htm, html, htt, inf, ini, job, js, jse, lnk, lsp, mdb, mht, mpp, mpt, msg, ocx, pdf, php, pif, pot, ppt, rtf, scr, shs, swf, sys, td0, vbe, vbs, vxd, wbk, wma, wmv, wmf, wsc, wsf, wsh, wri, xls, xlt, xml, zip, jar, arj, lzh, tar, tgz, gz, cab, rar, bz2, hqx.

> Komprimierte Dateien scannen

Zum Scannen von Archivdateien und -ordnern.

> Erweiterte Heuristik verwenden

Zur Verwendung aller verfügbaren heuristischen Methoden während des Scans, um neue oder unbekannte Malware besser aufzuspüren.

> Hinweis

Wenn Sie diese Option wählen, dauert der Scanvorgang länger und kann zu mehr Fehlarmen führen (harmlose Dateien, die als verdächtig gemeldet werden).

4.Klicken Sie auf **OK**.

> Hinweis

Die ausgeschlossenen Dateien in der Liste der ausgeschlossenen Elemente werden nicht gescannt, selbst wenn Sie sie hier für einen Scanvorgang auswählen.

Durchzuführende Aktionen bei der Identifizierung schädlicher Dateien

Sie können bestimmen, wie schädliche Dateien nach ihrer Identifzierung gehandhabt werden.

So wählen Sie die Aktion, die bei der Identifizierung von schädlichem Inhalt im Rahmen eines manuellen Scanvorgangs durchzuführen ist:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> Hinweis

Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Manuelle Scans.**

3. Wählen Sie unter **Wenn Viren oder Spyware gefunden wird** eine der folgenden Optionen:

> Option	Beschreibung
> Mich immer fragen (Standart)	Sie können für jedes beim manuellen Scanning identifizierte Element die jeweils durchzuführende Aktion wählen.
> Dateien säubern	Das Produkt versucht, die beim manuellen Scanning gefundenen infizierten Dateien automatisch zu säubern.

> Hinweis

Wenn eine infizierte Datei nicht gesäubert werden kann, wird sie in Quarantäne gestellt (es sei denn, sie wurde im Netzwerk oder auf einem Wechseldatenträger gefunden), damit sie keinen Schaden auf dem Computer anrichten kann.

> Option	Beschreibung
> Dateien unter Quarantäne stellen	Das Produkt verschiebt alle beim manuellen Scanning identifizierten schädlichen Dateien in eine Quarantänezone, in der sie keinen Schaden auf dem Computer anrichten können.
> Dateien löschen	Alle beim manuellen Scanning identifizierten schädlichen Dateien werden gelöscht.
> Nur Bericht	Die beim manuellen Scanning gefundenen schädlichen Dateien bleiben unberührt, ihre Identifizierung wird im Scanbericht aufgezeichnet.

> Hinweis

Bei der Wahl dieser Option kann Malware auf Ihrem Computer immer noch Schaden anrichten, wenn das Echtzeit-Scanning deaktiviert ist.

> Hinweis

Wenn beim manuellen Scanning schädliche Dateien identifiziert werden, werden diese automatisch gesäubert.

Planen von Scans

Programmieren Sie Ihren Computer für die Durchführung automatischer Scanvorgänge und das Entfernen von Viren und anderen schädlichen Anwendungen, wenn Sie nicht arbeiten. Sie können auch periodische Scanvorgänge planen, um sicherzustellen, dass Ihr Computer virusfrei ist.

So planen Sie einen Scan:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> **Hinweis** Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Geplante Scans.**
3. Aktivieren Sie **Geplantes Scanning.**
4. Geben Sie an, wann der Scanvorgang gestartet werden soll.

> Option	Beschreibung
> Täglich	Der Computer wird jeden Tag gescannt.
> Wöchentlich	Ihr Computer wird an den angegebenen Wochentagen gescannt. Wählen Sie die gewünschten Tage in der Liste aus.
> Monatlich	Ihr Computer wird an den angegebenen Monatstagen gescannt. So wählen Sie die gewünschten Tage aus: 1. Wählen Sie eine Option für **Tag** aus. 2. Wählen Sie in der Liste neben dem ausgewählten Tag den Tag des Monats aus.

5. Wählen Sie aus, wann Sie den Scan an den ausgewählten Tagen starten möchten.

> Option	Beschreibung
> Startzeit	Der Scanvorgang wird zur vorgegebenen Uhrzeit gescannt.
> Nachdem der Computer nicht benutzt wurde für	Der Scanvorgang wird gestartet, nachdem der Computer während des angegebenen Zeitraums nicht verwendet wurde.

Für das geplante Scanning werden die Einstellungen des manuellen Scannings verwendet. Allerdings werden bei jedem geplanten Scanvorgang die Archive gescannt und schädliche Dateien automatisch gesäubert.

> Hinweis

Geplante Scans werden ausgesetzt wenn der Spielmodus an ist. Wenn er ausgeschaltet wird, wird der ausgesetzte Scan automatisch fortgesetzt.

2.2.3 Scannen von E-Mails

Durch das Scannen Ihrer E-Mail schützen Sie sich vor dem Empfang schädlicher Dateien in den an Sie gesendeten E-Mails.

Die Viren- und Spyware-Scanfunktion muss aktiviert werden, damit E-Mails auf Viren überprüft werden. So aktivieren Sie den E-Mail-Scan:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> Hinweis

Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Virenschutz.**
3. Wählen Sie **Schädliche E-Mail-Anhänge entfernen.**
4. Klicken Sie auf **OK.**

Wann werden E-Mail-Nachrichten und Anhänge gescannt?

Der Virenschutz kann schädliche Inhalte aus von Ihnen empfangenen E-Mails entfernen.

Der Virenschutz entfernt schädliche E-Mails, die von E-Mail-Programmen wie Microsoft Outlook und Outlook Express, Microsoft Mail oder Mozilla Thunderbird empfangen werden. Er durchsucht verschlüsselte E-Mail-Nachrichten und Anhänge, sobald Ihr E-Mail-Programm diese vom Mail Server unter Verwendung des POP3-Protokolls empfängt.

Der Virenschutz kann jedoch keine E-Mail-Nachrichten in Webmail scannen. Dazu gehören auch E-Mail-Anwendungen, die in Ihrem Webbrowser ausgeführt werden, z. B. Hotmail, Yahoo! Mail oder Gmail. Sie sind aber dennoch vor Viren geschützt, auch wenn schädliche Anhänge nicht entfernt werden oder Sie Webmail verwenden.

Beim Öffnen von E-Mail-Anhängen entfernt die Echtzeit-Scanfunktion alle schädlichen Anhänge, bevor diese Schaden anrichten können.

> Hinweis

Das Echtzeit-Scanning schützt nur Ihren Computer, jedoch nicht Ihre Freunde. Dabei werden angehängte Dateien erst dann gescannt, wenn Sie den Anhang öffnen. Wenn Sie folglich Webmail verwenden und eine Nachricht weiterleiten, bevor sie den Anhang öffnen, leiten Sie ggf. infizierte E-Mail an Ihre Freunde weiter.

2.2.4 Anzeigen der Scanergebnisse

Im Virus- und Spyware-Verlauf werden alle vom Produkt identifizierten schädlichen Dateien angezeigt.

In manchen Fällen kann das Produkt die Aktion, die sie als Reaktion auf die Identifizierung eines schädlichen Elements ausgewählt haben, nicht durchführen. Wenn Sie z. B. Dateien säubern möchten und eine Datei nicht gesäubert werden kann, wird sie in Quarantäne gestellt. Sie können diese Informationen im Virus- und Spyware-Verlauf anzeigen.

So rufen Sie den Verlauf auf:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> Hinweis

Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Virenschutz.**
3. Klicken Sie auf **Entfernungsverlauf anzeigen.**

Der Virus- und Spyware-Verlauf enthält folgende Informationen:

- Datum und Uhrzeit der Identifizierung der schädlichen Datei
- Name der Malware und deren Speicherort auf Ihrem Computer
- Durchgeführte Aktion

2.3 Ausschließen von Dateien aus dem Scanvorgang

In manchen Fällen müssen bestimmte Dateien oder Anwendungen vom Scanvorgang ausgeschlossen werden. Ausgeschlossene Elemente werden nicht gescannt, bis sie aus der Liste der ausgeschlossenen Elemente wieder entfernt werden.

> Hinweis

Für das Echtzeit- und das manuelle Scanning sind separate Ausschlusslisten vorhanden. Wenn Sie beispielsweise eine Datei vom Echtzeit-Scan ausschließen, wird diese beim manuellen Scanning dennoch gescannt, bis Sie sie auch vom manuellen Scanning ausschließen.

2.3.1 Ausschließen bestimmter Dateitypen

Beim Ausschluss von Dateien nach Dateityp werden alle Dateien mit den angegebenen Erweiterungen nicht nach schädlichem Inhalt untersucht.

So fügen Sie auszuschließende Dateitypen hinzu bzw. entfernen Sie sie:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> Hinweis

Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Geben Sie an, ob der Dateityp vom Echtzeit- oder vom manuellen Scanning ausgeschlossen werden soll:

- Wählen Sie **Virenschutz**, um den Dateityp vom Echtzeit-Scanning auszuschließen.
- Wählen Sie **Manuelles Scanning**, um den Dateityp vom manuellen Scanning auszuschließen.

3. Klicken Sie auf Dateien vom **Scan ausschließen.**

4. So schließen Sie einen Dateityp aus:

a) Wählen Sie die Registerkarte **Dateitypen** aus.

b) Wählen Sie Dateien mit diesen **Erweiterungen ausschließen.**

c) Geben Sie eine Dateierweiterung, die den Typ der Dateien angibt, die Sie ausschließen möchten, in das Feld neben der Schaltfläche **Hinzufügen** ein.
Um Dateien ohne Erweiterung anzugeben, geben Sie ‚.' ein. Sie können den Platzhalter ‚?' für ein beliebiges Zeichen verwenden oder den Platzhalter ‚*' für eine beliebige Anzahl von Zeichen.
Um beispielsweise ausführbare Dateien auszuschließen, geben Sie in das Feld exe ein.

d) Klicken Sie auf **Hinzufügen.**

5. Wiederholen Sie den vorherigen Schritt für alle anderen Erweiterungen, die Sie aus dem Virenscan ausschließen möchten.

6. Klicken Sie auf **OK**, um das Dialogfeld **Vom Scanning ausschließen** zu schließen.

7. Klicken Sie auf **OK**, um die neuen Einstellungen zu übernehmen.

Die angegebenen Dateitypen werden von allen weiteren Scanvorgängen ausgeschlossen.

2.3.2 Ausschließen von Dateien nach Speicherort

Bei einem Ausschluss von Dateien nach Speicherort werden alle Dateien auf den angegebenen Laufwerken bzw. in den angegebenen Ordnern nicht beim Scanning nach schädlichem Inhalt berücksichtigt.

So fügen Sie vom Scanning auszuschließende Dateispeicherorte hinzu bzw. entfernen Sie sie:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> **Hinweis** Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Geben Sie an, ob der Speicherort vom Echtzeit- oder vom manuellen Scanning ausgeschlossen werden soll:

- Wählen Sie **Virenschutz,** um den Speicherort vom Echtzeit-Scanning auszuschließen.

- Wählen Sie **Manuelles Scanning**, um den Speicherort vom manuellen Scanning auszuschließen.

3. Klicken Sie auf **Dateien vom Scan ausschließen.**
4. So schließen Sie eine Datei, ein Laufwerk oder einen Ordner aus:

a) Klicken Sie auf die Registerkarte **Objekte.**

b) Wählen Sie die Option **Objekte ausschließen (Dateien, Ordner, ...)** aus.

c) Klicken Sie auf **Hinzufügen.**

d) Wählen Sie die Datei, das Laufwerk oder den Ordner aus, der beim Virenscan nicht berücksichtigt werden soll.

> Hinweis

Einige Laufwerke sind möglicherweise Wechseldatenträger, etwa CDS, DVDs oder Netzwerkdatenträger. Netzwerkdatenträger und leere Wechseldatenträger können nicht ausgeschlossen werden.

e) Klicken Sie auf **OK.**

5. Wiederholen Sie die vorherigen Schritte, um andere Dateien, Laufwerke oder Ordner vom Scanvorgang auszuschließen.
6. Klicken Sie auf **OK**, um das Dialogfeld **Vom Scanning ausschließen** zu schließen.
7. Klicken Sie auf **OK,** um die neuen Einstellungen zu übernehmen.

Die ausgewählten Dateien, Laufwerke oder Ordner werden von allen weiteren Scanvorgängen ausgeschlossen.

2.3.3 Anzeigen von ausgeschlossenen Anwendungen

Sie können die Anwendungen anzeigen, die Sie vom Scanning ausgeschlossen haben, und sie aus der Liste der ausgeschlossenen Elemente entfernen, wenn sie bei den nächsten Scanvorgängen wieder berücksichtigt werden sollen.

Wenn beim Echtzeit- oder beim manuellen Scanning eine Anwendung identifiziert wird, die sich wie Spyware oder Riskware verhält, von der Sie jedoch wissen, dass sie sicher ist, dann können Sie sie vom Scanning ausschließen. In diesem Fall erhalten Sie keine Warnmeldung bezüglich dieser Anwendung mehr.

> Hinweis

Wenn sich eine Anwendung wie ein Virus oder eine andere bösartige Software verhält, kann sie nicht ausgeschlossen werden.

Sie können Anwendungen nicht direkt ausschließen. Neue Anwendungen werden nur dann in der Ausschlussliste aufgeführt, wenn Sie sie während des Scanvorgangs ausschließen.

So zeigen Sie vom Scanvorgang ausgeschlossene Anwendungen an:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> Hinweis

Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Geben Sie an, ob Sie die vom Echtzeit- oder die vom manuellen Scanning ausgeschlossenen Anwendungen anzeigen möchten:

- Wählen Sie **Virenschutz**, um die vom Echtzeit-Scanning ausgeschlossenen Anwendungen anzuzeigen.
- Wählen Sie **Manuelles Scanning**, um die vom manuellen Scanning ausgeschlossenen Anwendungen anzuzeigen.

3. Klicken Sie auf **Dateien vom Scan ausschließen.**

4. Wählen Sie die Registerkarte **Anwendungen.**

> Hinweis

Ausgeschlossen werden können Spyware- und Riskware-Anwendungen, nicht aber Viren.

5. Wenn eine ausgeschlossene Anwendung erneut gescannt werden soll:

a) Wählen Sie die Anwendung, die erneut beim Scanning berücksichtigt werden soll.

b) Klicken Sie auf **Entfernen.**

6. Klicken Sie auf **OK**, um das Dialogfeld **Vom Scanning ausschließen** zu schließen.

7. Klicken Sie zum Beenden auf **OK.**

2.4 Wie verwende ich die Quarantäne?

Als Quarantäne wird ein sicheres Repository für möglicherweise schädliche Dateien bezeichnet. Dateien, die sich in Quarantäne befinden, können sich weder verbreiten noch Ihrem Computer schaden.

Das Produkt kann Malware, Spyware und Riskware unter Quarantäne stellen, damit sie keinen Schaden anrichten kann. Sie können Anwendungen oder Dateien später aus der Quarantäne wiederherstellen, wenn Sie sie benötigen.

Wenn Sie ein unter Quarantäne stehendes Element nicht benötigen, können Sie es löschen. Das Löschen eines Elements aus der Quarantäne entfernt es endgültig von Ihrem Computer.

- Malware, die sich in Quarantäne befindet, können Sie in der Regel löschen.
- Spyware, die sich in Quarantäne befindet, können Sie in den meisten Fällen löschen. Es ist möglich, dass die isolierte Spyware Teil eines seriösen Softwareprogramms ist und das Löschen dazu führt, dass das Programm nicht mehr richtig ausgeführt werden kann. Wenn Sie das Programm auf Ihrem Computer lassen möchten, können Sie die Spyware aus der Quarantäne wiederherstellen.
- Riskware, die sich in Quarantäne befindet, kann ein seriöses Softwareprogramm sein. Wenn Sie das Programm selbst installiert und eingerichtet haben, können Sie es aus der Quarantäne wiederherstellen. Wenn die Riskware ohne Ihr Wissen installiert wurde, wurde sie sehr wahrscheinlich mit böser Absicht installiert und kann gelöscht werden.

2.4.1 Anzeigen von unter Quarantäne gestellten Elementen

Sie können weitere Informationen zu Elementen unter Quarantäne anzeigen. So zeigen Sie detaillierte Informationen zu Elementen unter Quarantäne an:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> **Hinweis** Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Virenschutz.**
3. Klicken Sie auf **Quarantäne anzeigen**. Die Seite **Quarantäne** zeigt die Gesamtzahl der in der Quarantäne gespeicherten Elemente an.
4. Um detaillierte Informationen zu einem ausgewählten Element unter Quarantäne anzuzeigen, klicken Sie auf Details.
5. Wenn Sie weitere Informationen zu einem unter Quarantäne gestellten Element anzeigen möchten, klicken Sie neben dem Element auf das Symbol .

2.4.2 Wiederherstellen von Elementen aus der Quarantäne

Unter Quarantäne gestellte Elemente, die Sie benötigen, können Sie wiederherstellen.

Anwendungen oder Dateien, die Sie benötigen, können Sie aus der Quarantäne wiederherstellen.

Stellen Sie keine Elemente aus der Quarantäne wieder her, wenn Sie nicht sicher sind, dass sie keine Bedrohung sind. Wiederhergestellte Elemente werden an den Originalspeicherort auf dem Computer verschoben.

Wiederherstellen von Elementen aus der Quarantäne

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> **Hinweis** Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Virenschutz.**
3. Klicken Sie auf **Quarantäne anzeigen.**
4. Wählen Sie die unter Quarantäne stehenden Elemente aus, die wiederhergestellt werden sollen.
5. Klicken Sie auf **Wiederherstellen.**

3. Was ist DeepGuard?

3.1 Wählen Sie aus, was DeepGuard überwachen soll.

DeepGuard überwacht wichtige Systemeinstellungen und -dateien sowie jegliche Versuche, wichtige Anwendungen – einschließlich dieses Sicherheitsprodukts – zu deaktivieren.

Um zu wählen, was DeepGuard überwachen soll:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> **Hinweis** Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **DeepGuard.**
3. Stellen Sie sicher, dass **DeepGuard** aktiviert ist.
4. Wählen Sie die Einstellungen für DeepGuard:

> Bei verdächtiger Aktivität warnen	Stellen Sie sicher, dass diese Einstellung aktiv ist, damit verdächtiges Verhalten angezeigt wird. Wird die Einstellung deaktiviert, beendet DeepGuard die Überwachung von verdächtigem Verhalten und das Sicherheitsniveau wird gesenkt.
> Warnungen zu Anwendungs-Exploits anzeigen	Stellen Sie sicher, dass diese Einstellung aktiv ist, damit Sie bei potenziellen Exploit-Versuchen gewarnt werden. Wenn diese Warnung ausgeben Einstellung deaktiviert wird, können schädliche Websites und Dokumente auf Ihre Anwendungen zugreifen. Dadurch wird die Sicherheit beeinträchtigt. Wir empfehlen, dass Sie diese Einstellung nie deaktivieren.
> Internetverbindung nur mit Erlaubnis herstellen	Stellen Sie sicher, dass diese Einstellung aktiv ist, damit Sie benachrichtigt werden, wenn eine unbekannte Anwendung versucht, eine Verbindung zum Internet herzustellen.
> Wählen Sie Kompatibilitätsmodus verwenden (senkt die Sicherheit)	Um maximalen Schutz zu gewährleisten, nimmt DeepGuard an aktiven Programmen temporäre Änderungen vor. Bestimmte Programme überprüfen allerdings, ob sie nicht beschädigt oder geändert wurden und sind deshalb unter Umständen nicht mit dieser Funktion kompatibel. Online-Spiele mit Anti-Betrug-Tools z. B. prüfen, ob sie bei ihrer Ausführung nicht auf die eine oder andere Weise geändert wurden. In diesem Fall können Sie den Kompatibilitätsmodus aktivieren.

5. Klicken Sie auf **OK**.

3.1.1 Zulassen der von DeepGuard blockierten Anwendungen

Sie können bestimmen, welche Anwendungen von DeepGuard zugelassen und blockiert werden.

Es kann vorkommen, dass DeepGuard die Ausführung einer sicheren Anwendung verhindert, obwohl Sie mit dieser Anwendung arbeiten möchten und genau wissen, dass sie sicher ist. Das ist darauf zurückzuführen, dass die Anwendung versucht, Systemänderungen vorzunehmen, die sich als potenziell schädlich erweisen könnten. Oder Sie haben die Anwendung bei der Anzeige eines DeepGuard-Popupfensters versehentlich blockiert.

So genehmigen Sie die Ausführung einer von DeepGuard blockierten Anwendung:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> **Hinweis**
>
> Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **DeepGuard.**
3. Klicken Sie auf **Anwendungsberechtigungen ändern.** Die Liste **Überwachte Anwendungen** wird angezeigt.
4. Wählen Sie die Anwendung aus, die Sie zulassen möchten, und klicken Sie auf **Details.**

> **Hinweis**
>
> Sie können die Liste durch einen Klick auf die verschiedenen Spaltenüberschriften sortieren. Wenn Sie z. B. auf die Spalte Genehmigung klicken, wird die Liste nach genehmigten und zurückgewiesenen Programmen sortiert.

5. Wählen Sie **Zulassen.**
6. Klicken Sie auf **OK.**
7. Klicken Sie auf den Link **Schließen.**

DeepGuard lässt erneut Systemänderungen durch die Anwendung zu.

3.2 Handhabung von Warnmeldungen zu verdächtigem Verhalten

DeepGuard blockiert die überwachten Anwendungen, wenn sie verdächtig agieren oder versuchen eine Verbindung zum Internet herzustellen.

Sie können je nach Situation entscheiden, ob Sie der Anwendung erlauben fortzufahren oder nicht.

3.2.1 DeepGuard blockiert eine schädliche Anwendung.

Sie erhalten eine Benachrichtigung von DeepGuard, wenn eine schädliche Anwendung erkannt und blockiert wurde.

Wenn die Benachrichtigung geöffnet wird:

Klicken Sie auf **Details,** um mehr Informationen zur Anwendung anzuzeigen. Der Detailbereich enthält folgende Angaben:

- Speicherort der Anwendung
- die Bewertung der Anwendung in Security-Cloud,
- Verbreitung der Anwendung und
- Name der erkannten Malware.

Sie können eine verdächtige Anwendung zur Analyse einsenden.

3.2.2 DeepGuard blockiert eine verdächtige Anwendung.

Wenn die Einstellung **Bei verdächtigem Verhalten Warnung ausgeben i**n DeepGuard aktiviert ist, werden Sie benachrichtigt, wenn sich eine Anwendung verdächtig verhält. Wenn Sie der Anwendung vertrauen, können Sie das Fortfahren zulassen.

So geben Sie an, wie eine von DeepGuard blockierte Anwendung gehandhabt werden soll:

1. Klicken Sie auf **Details,** um mehr Informationen zur Anwendung anzuzeigen. Der Detailbereich enthält folgende Angaben:

- Speicherort der Anwendung
- die Bewertung der Anwendung in Security-Cloud,
- Verbreitung der Anwendung und
- Name der Malware.

2. Geben Sie an, ob Sie der von DeepGuard blockierten Anwendung vertrauen

- Wählen Sie **Ich vertraue der Anwendung. Ausführung fortsetzen**, wenn die Anwendung nicht blockiert werden soll.

In folgenden Fällen ist eine Anwendung mit großer Wahrscheinlichkeit sicher:

- DeepGuard hat die Anwendung nach einer von-Ihnen durchgeführten Aktion blockiert.
- Sie kennen die Anwendung.
- Sie haben die Anwendung von einer vertrauenswürdigen Quelle erhalten.
- Wählen Sie **Ich vertraue der Anwendung nicht. Ausführung blockieren**, wenn die Anwendung blockiert werden soll.

In folgenden Fällen ist eine Anwendung mit großer Wahrscheinlichkeit nicht sicher:

- Die Anwendung ist nicht sehr geläufig.
- Der Ruf der Anwendung ist nicht bekannt.
- Sie kennen die Anwendung nicht.

Sie können eine verdächtige Anwendung zur Analyse einsenden.

3.2.3 Eine unbekannte Anwendung versucht eine Verbindung zum Internet herzustellen.

Wenn die Einstellung **Internetverbindung nur mit Erlaubnis herstellen** in DeepGuard aktiviert wird, werden Sie benachrichtigt, wenn eine unbekannte Anwendung versucht, eine Verbindung zum Internet herzustellen. Wenn Sie der Anwendung vertrauen, können Sie das Fortfahren zulassen.

So geben Sie an, wie eine von DeepGuard blockierte Anwendung gehandhabt werden soll:

1. Klicken Sie auf **Details**, um mehr Informationen zur Anwendung anzuzeigen. Der Detailbereich enthält folgende Angaben:

- Speicherort der Anwendung
- die Bewertung der Anwendung in Security-Cloud,
- Verbreitung der Anwendung
- was die Anwendung zu tun versucht hat und
- wo die Anwendung eine Verbindung herzustellenversucht hat.

2. Geben Sie an, ob Sie der von DeepGuard blockierten Anwendung vertrauen:

- Wählen Sie **Ich vertraue der Anwendung. Ausführung fortsetzen,** wenn die Anwendung nicht blockiert werden soll.

In folgenden Fällen ist eine Anwendung mit großer Wahrscheinlichkeit sicher:

- DeepGuard hat die Anwendung nach einer von Ihnen durchgeführten Aktion blockiert.
- Sie kennen die Anwendung.
- Sie haben die Anwendung von einer vertrauenswürdigen Quelle erhalten.
- Wählen Sie **Ich vertraue der Anwendung nicht. Ausführung permanent blockieren,** wenn die Anwendung blockiert werden soll.

In folgenden Fällen ist eine Anwendung mit großer Wahrscheinlichkeit nicht sicher:

- Die Anwendung ist nicht sehr geläufig.
- Der Ruf der Anwendung ist nicht bekannt.
- Sie kennen die Anwendung nicht.

Wenn der Spielmodus an ist, erlaubt DeepGuard auch unbekannten Anwendungen den Zugriff auf das Internet. Es blockiert aber weiterhin gefährliche Anwendungen, die versuchen eine Verbindung zum Internet herzustellen, auch wenn der Spielmodus an ist.

Sie können eine verdächtige Anwendung zur Analyse einsenden.

3.2.4 DeepGuard hat einen möglichen Exploit entdeckt.

Wenn die Einstellung **Bei Auftreten von Anwendungs-Exploits Warnung** ausgeben in DeepGuard aktiviert ist, erhalten Sie einen Hinweis, dass DeepGuard verdächtiges Verhalten entdeckt hat, nachdem Sie eine schädliche Website oder ein Dokument geöffnet haben.

So geben Sie an, wie eine von DeepGuard blockierte Anwendung gehandhabt werden soll:

1. Klicken Sie auf **Details,** um mehr Informationen zur Anwendung anzuzeigen. Der Detailbereich enthält folgende Angaben:

- Name der Malware und
- die Quelle des Exploits (eine schädliche Website oder ein Dokument), falls bekannt.

2. Geben Sie an, ob Sie der von DeepGuard blockierten Anwendung vertrauen:

- Wählen Sie **Anwendung nicht schließen (kann Ihr Gerät gefährden)**, wenn die Anwendung nicht geschlossen werden soll. Möglicherweise wollen Sie die Anwendung zu diesem Zeitpunkt nicht schließen, wenn dadurch nicht gespeicherte Daten verloren gehen könnten.
- Wählen Sie **Anwendung schließen, um Exploit zu verhindern,** wenn Sie die Anwendung schließen und sicherstellen möchten, dass Ihr Gerät keinem Risiko ausgesetzt wird. Wir empfehlen, dass Sie die Anwendung schließen, um Ihr Gerät keinem Risiko auszusetzen.

Wenn die Quelle des Exploits identifziert wurde, können Sie eine Probe zur Analyse einsenden.

3.3 Eine verdächtige Anwendung zur Analyseeinsenden

Sie können dazu beitragen, den Schutz zu verbessern, wenn Sie verdächtige Anwendungen zur Analyse einsenden.

Wenn DeepGuard eine Anwendung blockiert, weil sie beispielsweise ein mögliches Sicherheitsrisiko für Ihren Computer darstellt oder versucht hat, eine möglicherweise schädliche Aktion auszuführen, können Sie uns ein Muster der Anwendung zur Sicherheitsforschung senden.

Sie können dies tun, wenn Sie wissen, dass die von DeepGuard blockierte Anwendung sicher ist oder wenn Sie den Verdacht haben, dass es sich um eine schädliche Anwendung handelt. Um eine Probe zur Analyse einzusenden:

1. Wenn DeepGuard eine Anwendung blockiert,- können Sie wählen, ob Sie die Anwendung blockieren oder dennoch ausführen möchten.
2. DeepGuard fragt, ob Sie die Anwendung zur Analyse einreichen möchten. Klicken Sie auf **Einreichen**, um das Muster einzureichen.

> Hinweis

DeepGuard fordert Sie nicht immer auf, ein Muster einzureichen. Beispielsweise dann nicht, wenn Sie bereits Informationen zu der blockierten Anwendung haben

4. Was ist eine Firewall?

4.1 Aktivieren oder Deaktivieren der Firewall

Die Firewall sollte stets aktiviert sein, um ungewollten Zugriff auf Ihren Computer zu verhindern. So aktivieren bzw. deaktivieren Sie die Firewall:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> **Hinweis** Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Aktivieren bzw. deaktivieren Sie **Firewall.**

> **Hinweis** Ihr Computer ist nicht vollständig geschützt, wenn Sie die Sicherheitsfunktionen deaktivieren.

3. Klicken Sie auf **OK.**

Sie sollten die Firewall nicht deaktivieren, da Sie dadurch Ihren Computer ungeschützt Netzwerkangriffen aussetzen. Wenn eine Anwendung nicht ausgeführt werden kann, da sie auf das Internet zugreifen muss, deaktivieren Sie keinesfalls die Firewall, sondern ändern Sie die Firewall-Einstellungen entsprechend.

4.2 Ändern der Firewall-Einstellungen

Wenn die Firewall aktiviert ist, begrenzt sie den Zugriff von Ihrem Computer sowie auf Ihren Computer. Für manche Anwendungen müssen Sie ggf. die Firewall durchlässig machen, damit sie ordnungsgemäß funktionieren.

Das Produkt greift für den Schutz Ihres Computers auf die Windows Firewall zurück. So ändern Sie die Einstellungen für die Windows Firewall:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> Hinweis

Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Firewall.**
3. Klicken Sie auf die **Einstellungen der Windows Firewall ändern.**

> Hinweis

Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

Detaillierte Informationen zur Windows Firewall finden Sie in der Dokumentation von Microsoft Windows.

4.3 Verhindern, dass Anwendungen schädliche Dateien herunterladen

Sie können verhindern, dass Anwendungen auf Ihrem Computer schädliche Dateien aus dem Internet herunterladen.

Manche Websites nutzen Sicherheitslücken des Comupters aus oder enthalten schädliche Dateien, die Ihren Computer beschädigen können. Mit dem erweiterten Netzwerkschutz verhindern Sie, dass Anwendungen schädliche Dateien herunterladen, noch bevor diese auf Ihrem Computer gespeichert werden.

So verhindern Sie, dass Anwendungen schädliche Dateien herunterladen:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> Hinweis

Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Firewall.**
3. Wählen Sie **Nicht zulassen, dass Anwendungen schädliche Dateien herunterladen.**

> Hinweis

Diese Einstellung gilt auch dann, wenn Sie die Firewall deaktivieren.

4.4 Verwendung von persönlichen Firewalls

Dieses Produkt ist auf die Verwendung mit Windows Firewall eingerichtet. Zur Verwendung mit anderen persönlichen Firewalls muss das Produkt individuell eingerichtet werden.

Das Produkt verwendet Windows Firewall für alle Firewall-Grundfunktionen, wie z. B. die Kontrolle des eingehenden Netzwerkverkehrs und die Trennung Ihres internen Netzwerks vom öffentlichen Internet. Zusätzlich überwacht DeepGuard installierte Anwendungen und verhindert, dass verdächtige Anwendungen ohne Ihre Zustimmung auf das Internet zugreifen.

Stellen Sie sicher, dass wenn Sie Windows Firewall durch eine andere persönliche Firewall ersetzen, diese allen ein- und ausgehenden Netzwerkverkehr für alle F-Secure-Prozesse zulässt, und dass Sie die F-Secure-Prozesse zulassen, wenn die persönliche Firewall dies anfragt.

> Tipp

Wenn Ihre persönliche Firewall über einen manuellen Filtermodus verfügt, verwenden Sie diesen, um alle F-Secure-Prozesse zuzulassen.

5. Blockieren von Spams

5.1 Aktivieren oder Deaktivieren der Spam-Filterung

Die Spam-Filterung sollte stets aktiviert sein, damit Spam- und Phishing-Nachrichten aus dem Posteingang entfernt werden.

So aktivieren bzw. deaktivieren Sie die Spam- Filterung:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> **Hinweis** Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Aktivieren oder deaktivieren Sie den **Spamfilter.**
3. Klicken Sie auf **OK.**

> **Tipp** Erstellen Sie eine Spamfilterregel in Ihrem E-Mail-Programm, um Massenwerbung und betrügerische E-Mails automatisch in einen Spam-Ordner zu verschieben.

5.2 Spam-Nachrichten kennzeichnen

Spam-Filter können das Betrefffeld von Spam-Nachrichten kennzeichnen. Hinzufügen des Textes [SPAM] zu Spam- und Phishing-Nachrichten:

1. Klicken Sie auf der Statusseite auf **Einstellungen.**

> **Hinweis** Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Spamfilter**.
3. Wählen Sie **Spam im E-Mail-Betreff mit [SPAM] markieren**.

4. Klicken Sie auf **OK.**

Wenn Sie Spam- oder Phishing-E-Mails erhalten, fügt die Spam-Filterung den Text [SPAM] in die Betreffzeile des E-Mails ein.

5.3 Einrichten meiner E-Mail-Programme zum Spam-Filtern

Sie können in Ihrem E-Mail-Programm Regeln zur Spam- und Phishing-Filterung erstellen, damit unerwünschte Nachrichten direkt in einen separaten Ordner verschoben werden.

Der Spam-Filter markiert alle entdeckten E-Mails im Betrefffeld mit dem Präfix [SPAM]. Falls Sie diese Nachrichten automatisch aus Ihrem Posteingang entfernen möchten, müssen Sie einen Spam-Ordner und entsprechende Filterregeln

in Ihrem E-Mail-Programm erstellen. Falls Sie mehrere E-Mail-Konten besitzen, müssen Sie für jedes Konto separat Filterregeln erstellen.

In diesem Abschnitt finden Sie Anleitungen zur Erstellung des Spam-Ordners und der Filterregeln für Windows Mail, Microsoft Outlook, Mozilla Thunderbird, Eudora und Opera. Mithilfe dieser Anleitungen können Sie auch ähnliche Filterregeln in anderen E-Mail-Programmen erstellen.

> Hinweis

Die Spam-Filterung unterstützt nur das POP3-Protokoll. Web- basierte E-Mail-Programme oder andere Protokolle werden nicht unterstützt.

5.3.1 Spam in Windows Mail blockieren

Um Spam- und Phishing-E-Mails zu filtern, müssen Sie einen Spam-Ordner und die Filterregel erstellen.

Wenn Sie Spam- und Phishing-Filterung für Windows Mail verwenden, stellen Sie sicher, **dass Spam im E-Mail-Betreff mit [SPAM] markieren** in den Einstellungen **Spamfilterung** aktiviert ist.

So erstellen Sie eine Spam-Filterregel:

1. Wählen Sie im Menü von **Windows Mail** die Option Ordner > **Nachrichtenregeln.**

> Hinweis

Wenn das Fenster **Neue E-Mail- Regel** nicht automatisch angezeigt wird, klicken Sie auf der Registerkarte **E-Mail-Regeln** auf **Neu.**

2. Erstellen Sie im Fenster **Neue E-Mail-Regel** eine Regel, um eine E-Mail-Nachricht in den Spam-Ordner zu verschieben:

a) Wählen Sie im Feld „Bedingungen“ **Betreff enthält Suchbegriffe.**

b) Wählen Sie im Aktionsfeld **In angegebenen Ordner verschieben.**

3. Klicken Sie im Feld für die Regelbeschreibung auf den **Link Enthält Suchbegriffe.**

a) Geben Sie im Fenster **Suchbegriffe eingeben** [SPAM] ein und klicken Sie auf Hinzufügen.

b) Klicken Sie auf **OK**, um das Fenster **Suchbegriffe eingeben** zu schließen.

4. Klicken Sie im Feld für die Regelbeschreibung auf den Link **Angegebener** Ordner.

a) Klicken Sie im Fenster **Verschieben** auf **Neuer Ordner.**

b) Geben Sie als neuen Ordnernamen Spam ein und klicken Sie auf **OK**.

c) Klicken Sie auf **OK**, um das Fenster **Verschieben** zu schließen.

5. Geben Sie in das Feld für den Regelnamen Spam ein.

6. Klicken Sie auf **Regel speichern**, um das Fenster **Neue E-Mail-Regel** zu schließen. Das Fenster **Regeln** wird geöffnet.

7. Klicken Sie auf „OK“, um das Fenster **Regeln** zu schließen.

Wenn Sie die neue Regel für E-Mail-Nachrichten verwenden möchten, die sich bereits in Ihrem Posteingang befinden, wählen Sie die Regel **Spam** und klicken Sie auf **Jetzt anwenden.**

Sie haben jetzt die Spam-Filterregel erstellt. Ab sofort werden Spam-E-Mails in den Spam-Ordner gefiltert.

5.3.2 Spam in Microsoft Outlook blockieren

Um Spam- und Phishing-E-Mails zu filtern, müssen Sie einen Spam-Ordner und die Filterregel erstellen.

Wenn Sie Spam- und Phishing-Filterung für Microsoft Outlook verwenden, stellen Sie sicher, dass **Spam im E-Mail-Betreff mit [SPAM] markieren** in den Einstellungen **Spamfilterung** aktiviert ist.

> Hinweis

Die hier angegebenen Schritte beziehen sich auf Microsoft Outlook 2007. Die Schritte für andere Versionen können leicht abweichen.

So erstellen Sie eine Spam-Filterregel:

1. Wählen Sie im Menü **Extras Regeln und , Benachrichtigungen.**
2. Klicken Sie auf der Registerkarte **E-Mail-Regeln** auf **Neue Regel.**
3. Wählen Sie in der Liste **Den Überblick behalten** die Vorlage **Nachrichten mit bestimmten Wörtern im Betreff in einen Ordner verschieben.**
4. Klicken Sie auf **Weiter.**
5. Klicken Sie im Bereich **2. Schritt: Regelbeschreibung bearbeiten** auf den Link **bestimmten Wörtern.**

a) Geben Sie im Feld **Im Betreff oder Text zu suchende Wörter** [SPAM] ein und klicken Sie auf **Hinzufügen.**

b) Klicken Sie auf **OK**, um das Fenster **Suchbegriffe eingeben** zu schließen.

6. Klicken Sie im Bereich **2. Schritt: Regelbeschreibung bearbeiten** auf den Ordnerlink **Zielordner.**

a) Klicken Sie im Fenster **Regeln und Benachrichtigungen** auf **Neu.**

b) Geben Sie als neuen Ordnernamen Spam ein und klicken Sie auf **OK.**

c) Klicken Sie auf **OK**, um das Fenster **Regeln und Benachrichtigungen** zu schließen.

7. Klicken Sie auf **Fertig stellen.**
8. Klicken Sie auf **OK.**

Wenn Sie die neue Regel für E-Mail-Nachrichten verwenden möchten, die sich bereits in Ihrem Posteingang befinden, klicken Sie auf **Regeln jetzt anwenden**, bevor Sie das Fenster schließen.

Sie haben jetzt die Spam-Filterregel erstellt. Ab sofort werden Spam-E-Mails in den Spam-Ordner gefiltert.

5.3.3 Blockieren von Spams in Mozilla Thunderbird und Eudora OSE

Um Spam- und Phishing-E-Mails zu filtern, müssen Sie einen Spam-Ordner und die Filterregel erstellen.

So erstellen Sie eine Spam-Filterregel:

1. Erstellen eines neuen Ordners für Spam- und Phishing-Nachrichten:

a) Rechtsklicken Sie auf den Namen Ihres E-Mail-Kontos und wählen Sie **Neuer Ordner.**

b) Geben Sie Spam als neuen Ordnernamen ein.

c) Klicken Sie auf **Ordner erstellen**.

2. Stellen Sie sicher, dass Ihr Kontoname ausgewählt ist und klicken Sie auf **Nachrichtenfilter verwalten** in der Liste **Erweiterte Funktionen.**

3. Klicken Sie auf **Neu**.

4. Geben Sie Spam als **Filtername** ein.

5. Erstellen Sie einen benutzerdefinierten Headereintrag:

a) In der Liste **Trifft auf alle folgenden** zu öffnen Sie das erste Drop-Down-Menü, das standardmäßig B**etreff** ausgewählt hat.

b) Wählen Sie in der ersten Dropdown-Liste Anpassen aus.

c) Geben Sie im Dialogfeld **Header anpassen** als neuen Nachrichten-Header X-Spam-Flag ein und klicken sie auf H**inzufügen.**

d) Klicken Sie auf **OK**, um das Dialogfeld **Header anpassen** zu schließen.

6. Erstellen einer Regel zum Filtern von Spam-Nachrichten:

a) In der Liste **Trifft auf alle folgenden zu** öffnen Sie das erste Drop-Down-Menü und wählen Sie das im vorhergehenden Schritt erstellte **X-Spam-Flag** aus.

b) Wählen Sie **enthält** aus dem zweiten Drop-Down-Menü aus.

c) Geben Sie Ja als Text ein, der auf die letzte Textbox in der Zeile zutreffen soll.

7. Erstellen Sie eine Aktivität, die Spam-Nachrichten in den Spam-Ordner verschiebt:

a) In der Liste **Diese Aktionen ausführen** wählen Sie **Nachricht verschieben nach.**

b) Wählen Sie den Spam-Ordner in der zweiten Dropdown-Liste aus.

8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

9. Schließen Sie das Dialogfenster **Nachrichtenfilter.**

Sie haben jetzt die Spam-Filterregel erstellt. Ab sofort werden Spam-E-Mails in den Spam-Ordner gefiltert.

5.3.4 Blockieren von Spams in Opera

Um Spam- und Phishing-E-Mails zu filtern, müs- sen Sie einen Spam-Ordner und die Filterregel erstellen.

> Hinweis

Die hier angegebenen Schritte gelten für Opera Version 12. Die erforderlichen Schritte für die anderen Versionen können leicht abweichen.

So erstellen Sie eine Spam-Filterregel:

1. Öffnen Sie **Opera Mail.**

2. Klicken Sie rechts auf Ihren standardmäßigen Spam-Ordner und wählen Sie **Eigenschaften.**

3. Klicken Sie auf **Regel hinzufügen.**

4. Erstellen Sie eine Regel für das Verschieben einer E-Mail-Nachricht in den Spam-Filter:

a) Wählen Sie aus der ersten Liste die Option **Beliebiger Header.**

b) Wählen Sie aus der zweiten Liste die Option **enthält.**

c) Geben Sie im Textfeld X-Spam-Flag: Yes als Text für die Übereinstimmung ein.

Achten Sie darauf, dass sich zwischen dem Dop- pelpunkt und Ja ein Leerzeichen befinden muss.

5. Klicken Sie auf **Schließen**, um Ihre neue Spam-Filterregel zu bestätigen.

Sie haben jetzt die Spam-Filterregel erstellt. Ab sofort werden Spam-E-Mails in den Spam-Ordner gefiltert.

6. Sichere Nutzung des Internets

6.1 Schützen von verschiedenen Benutzerkonten

Um den bestmöglichen Schutz gegen Online-Bedrohungen zu gewährleisten, sollten Sie separate Windows-Benutzerkonten für jeden Benutzer des Computers verwenden.

Mithilfe des Produkts können Sie verschiedene Einstellungen für die jeweiligen Benutzerkonten auf Ihrem Computer einrichten. Nur Benutzer mit Administratorrechten können die Produkteinstellungen für andere Benutzerkonten ändern.

Alle Benutzer, mit Ausnahme des Administrators, sollten nur über normale Zugriffsrechte verfügen, damit Sie nicht die von Ihnen festgelegten Einstellungen ändern können.

6.1.1 Erstellen von Windows-Benutzerkonten

Über dieses Produkt können Sie neue Windows-Benutzerkonten erstellen.

So erstellen Sie Windows-Benutzerkonten:

1. Klicken Sie auf der Browsing Protection und dort auf **Neu erstellen.**
   Hierüber werden die Benutzerkonteneinstellungen in Windows geöffnet.
2. Geben Sie die erforderlichen Informationen ein, um das Benutzerkonto zu erstellen oder zu bearbeiten.

Auf der Hauptseite des Produkts werden sowohl der Benutzername als auch die Art des Benutzerkontos angezeigt.

6.1.2 Anzeigen der Statistik

Auf der Seite **Einstellungen > Sonstige > Statistik** können Sie sehen, welche Webseiten angezeigt und blockiert wurden.

Das Produkt sammelt Informationen zu besuchten und blockierten Websites. Diese Informationen sind benutzerspezifisch und werden für jedes Windows-Benutzerkonto erstellt.

Die Informationen geben an, ob die blockierte Seite über von Ihnen bewusst blockierte Inhalte verfügt oder ob das Produkt die Seite als potentiell schädlich einstuft.

6.2 Surfen auf sicheren Websites

Das Produkt installiert eine Erweiterung auf allen Ihren Browsern, um den Browser-Schutz auf sicheren (HTTPS-)Websites vollständig zu unterstützen.

Ihr Browser sollte die Erweiterung automatisch erkennen und aktivieren. In manchen Fällen kann es jedoch sein, dass Sie die Erweiterung manuell aktivieren müssen.

Zur Aktivierung der Browser-Erweiterung, bearbeiten Sie Ihre Browser-Einstellungen:

- Wählen Sie in Firefox aus der Menüleiste **Extras > Add-ons** und klicken Sie dann neben der Erweiterung auf **Aktivieren.**
- Wählen Sie im Chrome-Menü **Einstellungen** aus, klicken Sie auf **Erweiterungen** und wählen Sie die Option **Aktivieren** neben der Erweiterung.
- Gehen Sie in Internet Explorer auf **Extras > Add-ons** verwalten, wählen Sie die Browser-Erweiterung aus und klicken Sie auf **Aktivieren.**

> Hinweis

Wenn Sie die Erweiterung manuell aktivieren müssen, sollten Sie die Aktivierung separat für die einzelnen Benutzerkonten auf Ihrem Computer vornehmen.

6.3 Was sind Sicherheitsbewertungen?

Sicherheitsbewertungen in den Suchergebnissen helfen bei der Vermeidung von Gefahren aus dem Internet.

Die Sicherheitsbewertungen basieren auf Informationen aus mehreren Quellen, wie Malware-Analysten und Partnern von F-Secure.

> Status-Symbol	> Statusbezeichnung	> Beschreibung
	ok	Ihr Computer ist geschützt. Die Funktionen sind aktiviert und arbeiten ordnungsgemäß.
	Informationen	Das Produkt informiert Sie über einen besonderen Status. Alle Funktionen arbeiten korrekt, aber das Produkt lädt z. B. gerade Updates herunter.
	Warnung	Ihr Computer ist nicht vollständig geschützt. Sie sollten das Produkt überprüfen, z. B. weil es seit langem keine Updates mehr erhalten hat.
	Fehler	Ihr Computer ist nicht geschützt. Das ist z. B. der Fall, wenn Ihr Abonnement abgelaufen ist oder eine kritische Funktion deaktiviert wurde.
	Aus	Eine nicht-kritische Funktion ist ausgeschaltet.

6.4 Was ist Surfschutz

Der Surfschutz erlaubt Ihnen, die Sicherheit von Webseiten, die Sie besuchen, zu beurteilen und bewahrt Sie so davor, unabsichtlich auf schädliche Webseiten zuzugreifen.

Der Browser-Schutz zeigt Sicherheitsbewertungen für die in den Suchmaschinenergebnissen aufgeführten Websites an. Er erkennt Websites mit Sicherheitsbedrohungen wie Malware (Viren, Würmer, Trojaner) und Phishing. So können Sie die aktuellsten Internetbedrohungen umgehen, die von herkömmlichen Virenschutzprogrammen noch nicht erkannt werden.

Die Sicherheitsbewertungen basieren auf Informationen aus mehreren Quellen, wie Malware-Analysten und Partnern von F-Secure.

6.4.1 Den Surfschutz ein- oder ausschalten

Wenn der Surfschutz eingeschaltet ist, wird Ihr Zugriff auf schädliche Webseiten blockiert.

So wird der Surfschutz ein- oder ausgeschaltet:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen.**
   Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie **Browser-Schutz.**
3. Klicken Sie oben rechts auf die Umschalttaste.
4. Wenn Ihr Browser geöffnet sie, starten Sie ihn neu, um die geänderten Einstellungen wirksam werden zu lassen.

Beurteilungen für Weblinks anzeigen

Wenn Sie im Browser-Schutz die Anzeige von Bewertungen aktivieren, zeigt er Sicherheitsbe wertungen für Websites in Suchmaschinenergeb nissen (Google, Yahoo und Bing) an. Bewertungen für Websites anzeigen:

1. Wählen Sie auf der Hauptseite das-Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen.**
   Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie **Browser-Schutz.**

3. Wählen Sie **Reputationswerte für Websites in Suchergebnissen anzeigen.**

4. Klicken Sie auf **OK**.

Wenn Sie das Web mit einer Suchmaschine durchsuchen, zeigt der Browser-Schutz Sicherheitsbewertungen für die gefundenen Websites an.

6.4.2 Was tun, wenn eine Webseite blockiert wird

Es erscheint eine Surfschutz-Blockierungsseite, wenn Sie versuchen, auf eine Webseite zuzugreifen, die als schädlich eingestuft wurde.

Wenn eine Blockierungsseite erscheint:

Wenn Sie die Webseite trotzdem aufrufen möchten, klicken Sie auf **Webseite zulassen.**

6.5 Sichere Verwendung von Online-Banken

Der Banking-Schutz schützt Sie vor schädlichen Aktivitäten beim Zugriff auf Ihre Online-Bank oder beim Durchführen von Online-Transaktionen.

Banking-Schutz erkennt automatisch sichere Verbindungen zu Online-Banking-Websites und blockiert alle Verbindungen, die nicht zur gewünschten Seite führen. Wenn Sie eine Online-Banking-Website öffnen, sind lediglich Verbindungen zu Online-Banking-Websites oder zu Websites, die als sicher für Online-Banking eingestuft werden, zulässig.

Banking-Schutz unterstützt derzeit die folgenden Browser:

- Internet Explorer 9 oder höher
- Firefox 13 oder höher
- Google Chrome

6.5.1 Aktivierung des Banking-Schutzes

Wenn der Banking-Schutz aktiviert ist, sind Ihre Online-Banking-Sitzungen und -Transaktionen geschützt. Aktivierung des Banking-Schutzes:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen.** Das Dialogfeld **Einstellungen** wird geöffnet.

2. Wählen Sie **Banking-Schutz.**

3. Klicken Sie oben rechts auf die Umschalttaste.
4. Wenn Ihre aktuellen Verbindungen offen bleiben sollen, wählen Sie **Meine aktiven Internetverbindungen nicht unterbrechen.**
   Wenn Sie die Website Ihrer Bank aufrufen oder Online-Zahlungen durchführen, wird der Banking-Schutz aktiviert und blockiert alle für Online-Banking nicht notwendige Verbindungen. Das bedeutet, dass auch alle Ihre aktuellen Internetverbindungen getrennt werden, es sei denn, Sie wählen diese Einstellung.

6.5.2 Verwendung des Banking-Schutzes

Wenn der Banking-Schutz aktiviert ist, erkennt er automatisch, wenn Sie eine Online-Banking-Website aufrufen.

Wenn Sie eine Online-Banking-Webseite in Ihrem Browser öffnen, wird die Benachrichtigung **Banking-Schutz** oben auf Ihrem Bildschirm angezeigt. Während die Banking-Schutz-Sitzung geöffnet ist, sind alle anderen Verbindungen blockiert.

> Tipp

Wenn Sie Ihre anderen aktiven Verbindungen während des Online-Banking nicht unterbrechen möchten, klicken Sie **Einstellungen ändern** auf der Benachrichtigung, um die Produkteinstellungen für Ihr Benutzerkonto zu ändern.

So beenden Sie die Banking-Schutz-Sitzung und stellen Ihre anderen Verbindungen wieder her:

Klicken Sie in der Benachrichtigung **Banking-Schutz auf Beenden.**

6.6 Sicheres Surfen

Sie können sich vor vielen dieser Internetbedrohungen schützen, indem Sie die Surfaktivitäten aller Ihrer Windows-Benutzerkonten auf Ihrem Computer überwachen.

Das Internet enthält viele interessante Webseiten, aber es lauern auch viele Risiken. Viele Webseiten enthalten Materialien, die Sie möglicherweise als unangemessen empfinden. Benutzer können auf unangemessene Materialien stoßen oder belästigende Nachrichten per E-Mail oder in einem

Chat erhalten. Sie können versehentlich Dateien herunterladen, die für den Computer schädliche Viren enthalten.

> Hinweis

Der eingeschränkte Zugriff auf Online-Inhalte schützt Ihre Benutzerkonten vor Chat- und E-Mail-Programmen, die in Ihrem Webbrowser ausgeführt werden.

Sie können die Webseiten einschränken, die angezeigt werden können. Darüber hinaus können Sie die Zeit beschränken, die online verbracht werden kann. Sie können auch verhindern, dass Links zu nicht jugendfreien Inhalten in Suchmaschinenergebnissen angezeigt werden. Diese Einschränkungen werden auf die Windows-Benutzerkonten angewandt, d. h. immer wenn sich jemand mit seinem Benutzerkonto anmeldet, gelten die eingerichteten Beschränkungen.

6.6.1 Beschränken des Zugriffs auf Webinhalte

Sie können die Filterart auswählen, die Sie für die verschiedenen Windows-Benutzerkonten verwenden möchten.

Der Webseitenfilter blockiert den Zugriff auf von Ihnen nicht zugelassene Webseiten oder auf Webseiten, die Inhalte enthalten, die Sie blockiert haben.

Zugriff auf Webseiten ermöglichen

Sie können den Zugriff auf die Webseiten eingrenzen, denen Sie vertrauen. Fügen Sie diese hierzu zur Liste der zulässigen Webseiten hinzu.

So gewähren Sie Zugriff auf bestimmte Webseiten:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen.** Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie **Inhaltssperre.**
3. Klicken Sie oben rechts auf die Umschalttaste.
4. Wählen Sie die Option **Nur ausgewählte Websites zulassen.**
5. Klicken Sie auf **Hinzufügen**, um Websites zur Liste **Zugelassene Websites** hinzuzufügen.

6. Wenn Sie alle Websites, die Sie zulassen möchten, hinzugefügt haben, klicken Sie auf **OK.**

Wenn sich jemand mit dem von Ihnen bearbeiteten Windows-Benutzerkonto auf Ihrem Computer anmeldet, kann er auf die Webseiten zugreifen, die Sie zur Liste der zulässigen Webseiten hinzugefügt haben.

Webseiten anhand ihres Inhalts sperren

Sie können den Zugang zu Websites mit ungeeigneten Inhalten blockieren. So wählen Sie die zu blockierenden Inhaltstypen aus:

1 .Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen.** Das Dialogfeld **Einstellungen** wird geöffnet.

2. Wählen Sie **Inhaltssperre.**

3. Klicken Sie oben rechts auf die Umschalttaste.

4. Wählen Sie **Webinhalte blockieren.**

5. Wählen Sie die Inhaltstypen aus, die Sie blockieren möchten.

6. Wenn Sie alle Inhaltstypen, die Sie blockieren möchten, ausgewählt haben, klicken Sie auf **OK.**

Wenn sich jemand mit dem von Ihnen bearbeiteten Windows-Benutzerkonto auf Ihrem Computer anmeldet, kann er nicht auf Webseiten zugreifen, die Inhaltstypen enthalten, die Sie blockiert haben.

Zugelassene und blockierte Websites bearbeiten

Sie können bestimmte Websites zulassen, die von der Webfilterung blockiert werden. Sie können auch einzelne Websites blockieren, die in keinem Webfilter-Inhaltstyp eingeschlossen sind.

> Hinweis

Abhängig von der verwendeten Produktversion kann es sein, dass Sie den Zugang zu Websites entweder erlauben oder blockieren können, nicht jedoch beides.

Möglicherweise stufen Sie eine Webseite als sicher ein, obwohl Sie andere Webseiten mit diesem Inhaltstyp blockieren möchten. Sie können ebenso eine bestimmte Webseite blockieren, obwohl andere Webseiten dieses Inhaltstyps zulässig sind.

Website zulassen oder blockieren:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen.**
   Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie **Inhaltssperre.**
3. Klicken Sie auf **Website-Ausnahmen anzeigen.**

Wird die Website, die Sie bearbeiten möchten, bereits als zugelassen oder blockiert aufgelistet und Sie möchten diese von einer zur anderen Liste verschieben, gehen Sie folgendermaßen vor:

a) Klicken Sie abhängig von der Website-Liste, die Sie bearbeiten möchten auf die Registerkarte **Zulassen** oder **Blockieren.**

b) Klicken Sie mit der rechten Maustaste auf die Website in der Liste und wählen Sie **Zulassen** oder **Blockieren.**

Ist die Website in keiner Liste enthalten, gehen Sie folgendermaßen vor:

a) Klicken Sie auf die Registerkarte **Zulassen,** wenn Sie eine Website zulassen möchten. Klicken Sie auf die Registerkarte **Blockieren**, wenn Sie eine Website sperren möchten.

b) Klicken Sie auf **Hinzufügen,** um die neue Website zur Liste hinzuzufügen.

c) Geben Sie die Adresse der Website ein, die Sie hinzufügen möchten, und klicken Sie auf OK.

d) Klicken Sie im Dialogfeld **Website-Ausnahmen** auf **Schließen.**

4. Klicken Sie auf **OK**, um zur Hauptseite zurückzukehren.

Um die Adresse einer zugelassenen oder blockierten Website zu ändern, klicken Sie mit der rechten Maustaste auf die Website in der Liste und wählen Sie die Option Bearbeiten.

Um eine zugelassene oder blockierte Website von der Liste zu entfernen, wählen Sie die entsprechende Website aus und klicken Sie auf Entfernen.

6.6.2 Suchergebnisfilter verwenden

Sie können den Suchergebnisfilter aktivieren, um explizite Inhalte aus den Suchergebnissen zu blockieren.

Der Suchergebnisfilter blendet nicht-jugendfreie Inhalte aus, indem sichergestellt wird, dass Google, Yahoo und Bing das SafeSearch-Level „streng" verwenden. Dadurch können unangemessene und explizite Inhalte zwar nicht völlig aus den Suchergebnissen blockiert werden, aber das meiste Material dieser Art wird vermieden.

So aktivieren Sie den Suchergebnisfilter:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen.**
   Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie **Online Safety > Suchergebnisfilter.**
3. Klicken Sie oben rechts auf die Umschalttaste.

Wenn der Suchergebnisfilter aktiviert ist, werden die Einstellungen von SafeSearch für Websites für alle überschrieben, die über dieses Windows-Benutzerkonto eingeloggt sind.

6.7 Online-Zeiten festlegen

Sie können die Zeit kontrollieren, die mit dem Surfen im Internet über Ihren Computer verbracht werden darf.

Sie können für jedes Windows-Benutzerkonto unterschiedliche Einschränkungen auf Ihrem Computer einrichten. Folgendes können Sie kontrollieren:

- Wenn jemand im Internet surfen darf, können Sie beispielsweise festlegen, dass das Surfen nur vor 8 Uhr abends möglich ist.
- Wie lange jemand im Internet surfen darf. Sie können beispielsweise festlegen, dass täglich nur eine Stunde im Internet gesurft werden darf.

> Hinweis

Wenn Sie die Zeitbeschränkungen aufheben, ist das Surfen im Internet ohne zeitliche Einschränkungen möglich.

6.7.1 Internetsuche nur zu bestimmten Zeiten zulassen

Sie können den Zugriff auf die Internetsuche für bestimmte Nutzer einschränken, indem Sie Nutzungszeiten für das jeweilige Windows-Benutzerkonto festlegen.

Einstellung der Internetnutzungszeiten:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen**. Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie **Surfzeitbeschränkungen.**
3. Klicken Sie oben rechts auf die Umschalttaste.
4. Wählen Sie aus der Tabelle Browser-Zeit die Zeiten aus, zu denen der Zugriff auf das Internet an den einzelnen Wochentagen erlaubt ist.
5. Wählen Sie aus, für wie viele Stunden an Wochentagen und am Wochenende der Zugriff auf das Internet erlaubt ist.
   Wenn Sie die Suchzeit im Internet nicht einschränken wollen, vergewissern Sie sich, dass die eingestellte Zeit für Wochentage und Wochenende auf **Max** eingestellt ist.
6. Klicken Sie auf **OK**.

Wenn sich jemand mit dem von Ihnen bearbeiteten Windows-Benutzerkonto auf Ihrem Computer anmeldet, kann er nur während zu den zulässigen Zeiten im Internet surfen.

6.7.2 Tägliche Internetzeiten einschränken

Sie können tägliche Zeitbeschränkungen verwenden, um den Internetzugriff einzugrenzen.

Sie können auf Ihrem Computer unterschiedliche zeitliche Beschränkungen für jedes Windows-Benutzerkonto einrichten.

So richten Sie zeitliche Beschränkungen ein:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen.**
   Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie **Surfzeitbeschränkungen.**
3. Klicken Sie oben rechts auf die Umschalttaste.
4. Wählen Sie aus der Tabelle Browser-Zeit die Zeiten aus, zu denen der Zugriff auf das Internet an den einzelnen Wochentagen erlaubt ist. Wenn Sie die Internetsuche nicht auf bestimmte Zeiten einschränken wollen, vergewissern Sie sich, dass alle Zellen in der Tabelle Suchzeiten ausgewählt sind.
5. Wählen Sie aus, für wie viele Stunden an Wochentagen und am Wochenende der Zugriff auf das Internet erlaubt ist, und klicken Sie dann auf **OK.**

Wenn sich jemand mit dem von Ihnen bearbeiteten Windows-Benutzerkonto auf Ihrem Computer anmeldet, kann er nur während zu den zulässigen Zeiten im Internet surfen.

7. Was ist Safe Search?

7.1 Was sind Sicherheitsbewertungen?

Sicherheitsbewertungen in den Suchergebnissen helfen bei der Vermeidung von Gefahren aus dem Internet.

Die Sicherheitsbewertungen basieren auf Informationen aus mehreren Quellen, wie Malware-Analysten und Partnern von F-Secure.

> Status-Symbol	> Statusbezeichnung	> Beschreibung
	ok	Ihr Computer ist geschützt. Die Funktionen sind aktiviert und arbeiten ordnungsgemäß.
	Informationen	Das Produkt informiert Sie über einen besonderen Status. Alle Funktionen arbeiten korrekt, aber das Produkt lädt z. B. gerade Updates herunter.
	Warnung	Ihr Computer ist nicht vollständig geschützt. Sie sollten das Produkt überprüfen, z. B. weil es seit langem keine Updates mehr erhalten hat.
	Fehler	Ihr Computer ist nicht geschützt. Das ist z. B. der Fall, wenn Ihr Abonnement abgelaufen ist oder eine kritische Funktion deaktiviert wurde.
	Aus	Eine nicht-kritische Funktion ist ausgeschaltet.

7.2 Safe Search in Ihrem Webbrowser einrichten

Sie können Safe Search während der Installation in Ihrem Webbrowser als Standard-Such-Tool festlegen. Safe Search unterstützt die folgenden Internetbrowser:

- Internet Explorer 8 für Windows XP SP3
- Internet Explorer, zwei zuletzt veröffentlichte Versionen für Windows Vista, Windows 7 und Windows 8
- Firefox, zwei zuletzt veröffentlichte Versionen
- Google Chrome, zwei zuletzt veröffentlichte Versionen.

7.2.1 Verwenden von Safe Search mit Internet Explorer

Sie können Safe Search als Ihre Standard-Homepage und Ihren Standard-Suchanbieter festlegen und die Suchleiste installieren, wenn Sie Internet Explorer benutzen.

Befolgen Sie diese Anweisungen, um Safe Search mit Internet Explorer zu verwenden:

1. Internet Explorer öffnen.
2. Klicken Sie auf **Ändern** wenn Internet Explorer eine Nachricht anzeigt, dass ein Programm Ihren Suchanbieter ändern möchte.

> **Hinweis**
>
> Diese Nachricht erscheint nicht, wenn Sie Safe Search während der Installation nicht als Standard-Suchanbieter gewählt haben

3. Wenn Internet Explorer eine Nachricht anzeigt, dass das Toolbar-Add-On jetzt verwendet werden kann, klicken Sie auf **Aktivieren**. Wenn stattdessen in einem Dialogfenster angezeigt wird **Mehrere Add-Ons können jetzt verwendet werden**, klicken Sie zunächst auf **Add-Ons auswählen.**

> **Hinweis**
>
> In Internet Explorer 8 ist die Toolbar automatisch bereit zur Verwendung.

> **Hinweis**
>
> Diese Nachricht erscheint nicht, wenn Sie die Suchleiste während der Installation nicht installiert haben.

7.2.2 Verwenden von Safe Search mit Firefox

Sie können Safe Search als Ihre Standard-Homepage festlegen und die Suchleiste installieren, wenn Sie Firefox benutzen.

> Hinweis

Wenn Ihre Firefox-Konfiguration die Änderung der Homepage und des Standard-Suchanbieters verhindert, kann auch Safe Search diese Einstellungen nicht ändern.

Folgen Sie diesen Anweisungen, um die Safe Search-Suchleiste mit Firefox zu verwenden, nachdem Sie das Produkt installiert haben.

1. Firefox öffnen.
2. Gehen Sie zum Reiter **Add-on installieren.**
3. Stellen Sie sicher, dass es sich beim zu installierenden Add-on um Safe Search handelt.
4. Markieren Sie das Kontrollkästchen **Diese Installation zulassen.**
5. Klicken Sie auf **Fortfahren.**
6. Klicken Sie auf **Firefox neu starten.**

7.2.3 Verwenden von Safe Search mit Chrome

Sie können Safe Search als Ihren Standard-Suchanbieter festlegen und die Suchleiste installieren, wenn Sie Chrome benutzen.

Wenn Sie Chrome als Standardbrowser verwenden, können mit der Produktinstallation auch die Suchleiste installiert und Ihr Suchanbieter automatisch geändert werden.

7.3 Safe Search entfernen

7.3.1 Safe Search aus Internet Explorer entfernen

Befolgen Sie diese Anweisungen, um Safe Search aus Internet Explorer zu entfernen:

1. Öffnen Sie die Windows Systemsteuerung.
2. Öffnen Sie **Netzwerk und Internet > Interneteoptionen**. Das Fenster **Interneteigenschaften** wird geöffnet.
3. Um Safe Search als Standard-Homepage zu deaktivieren, befolgen Sie diese Anweisungen:

a) In **Interneteigenschaften** öffne den Reiter **Allgemein.**

b) Unter **Homepage** klicken Sie auf **Standardeinstellung verwenden.**

4. In **Interneteigenschaften** öffnen Sie den Reiter **Programme.**

5. Klicken Sie auf **Add-ons verwalten.** Das Fenster **Add-ons verwalten** wird geöffnet.

6. Um Safe Search nicht mehr als Suchanbieter zu verwenden, befolgen Sie diese Anweisungen:

a) In **Add-ons verwalten** wählen Sie **Suchanbieter.**

b) Wählen Sie Safe Search.

c) Klicken Sie auf **Entfernen.**

7. Um die Safe Search-Symbolleiste zu entfernen, befolgen Sie diese Anweisungen:

a) In **Add-ons verwalten** wählen Sie **Symbolleisten und Erweiterungen.**

b) Wählen Sie Safe Search.

c) Klicken Sie auf **Deaktivieren.**

> Hinweis

Deinstallieren Sie Safe Search, um die Safe Search-Suchmaschine und die Symbolleiste vollständig zu entfernen.

7.3.2 Safe Search aus Firefox entfernen

Befolgen Sie diese Anweisungen, um Safe Search aus Firefox zu entfernen.

1. Um Safe Search als Standard-Homepage zu deaktivieren, befolgen Sie diese Anweisungen:

a) Gehen Sie zu **Extras > Einstellungen.**

b) Im Fenster **Optionen** öffnen Sie den Reiter **Allgemein.**

b) Klicken Sie **Auf Standard zurücksetzen** unter dem Feld **Homepage.**

2. Um Safe Search nicht mehr als Suchanbieter zu verwenden, befolgen Sie diese Anwendungen.

a) Klicken Sie auf das Symbol Suchanbeiter im Suchfeld, um das Menü Suchmaschine zu öffnen.

b) Klicken Sie auf **Suchmaschinen verwalten.**

c) Wählen Sie Safe Search aus der Liste und

klicken Sie auf **Entfernen.**

d) Klicken Sie auf **OK.**

3. Um die Safe Search-Symbolleiste zu entfernen, befolgen Sie diese Anweisungen:

a) Gehen Sie zu **Extras > Add-ons.**

b) Im Fenster A**dd-ons-Manager** öffnen Sie den Reiter **Erweiterungen.**

c) Klicken Sie auf **Deaktivieren** in der Zeile Safe Search-Erweiterung.

d) Starten Sie Ihren Browser neu, um die Symbolleiste zu entfernen.

> Hinweis

Deinstallieren Sie Safe Search, um die Safe Search-Suchmaschine und die Symbolleiste vollständig zu entfernen.

7.3.3 Safe Search aus Chrome entfernen

Befolgen Sie diese Anweisungen, um Safe Search aus Chrome zu entfernen.

1. Um Safe Search nicht mehr als Suchanbieter zu verwenden, befolgen Sie diese Anweisungen:

a) Öffnen Sie die **Einstellungen** im Chrome- Menü.

b) Finden Sie die Einstellungen zu **Suche.**

c) Klicken Sie auf **Suchmaschinen verwalten.**

d) Klicken Sie auf X am Ende der Safe Search-Zeile.

2. Um die Safe Search-Symbolleiste zu entfernen, befolgen Sie diese Anweisungen:

a) Rechtsklicken Sie auf das Symbol für die Safe Search-Symbolleiste.

b) Wählen Sie **Aus Chrome-Browser entfernen.**

> Hinweis

Deinstallieren Sie Safe Search, um die Safe Search-Suchmaschine und die Symbolleiste vollständig zu entfernen.

Teil 3 Bedienanleitung Smartphone/Tablet (Android)

1. Schutz vertraulicher Informationen

1.1 Aktivieren von Remote-Anti-Theft

Wenn Remote-Anti-Theft-Funktionen aktiviert sind, können Sie Ihr Gerät mithilfe von SMS-Textnachrichten sperren oder Informationen darauf löschen.

So konfigurieren Sie Remote-Anti-Theft:

1. Öffnen Sie in der Hauptansicht die Option Diebstahlsicherung.
2. Wählen Sie im Menü Diebstahlsicherung die Option Einstellungen aus.
3. Wenn Sie Ihr Gerät per Fernzugriff orten können möchten, wählen Sie Locator aktivieren. Zur Verwendung von Locator sollten Sie sicherstellen, dass die Positionierungsmethoden auf Ihrem Gerät aktiviert sind. Diese sind normalerweise standardmäßig aktiviert. Weitere Informationen finden Sie in der Dokumentation, die mit Ihrem Gerät mitgeliefert wurde.
4. Wählen Sie Remote-Diebstahlsicherung, um die Funktion zu aktivieren.

Die Remote-Anti-Theft-Funktion ist aktiviert.

1.1.1 Sperren des Geräts per Fernzugriff

Wenn Sie Ihr Gerät aus der Ferne sperren, kann es nicht ohne Ihre Erlaubnis verwendet werden. So sperren Sie Ihr verlorenes oder gestohlenes Gerät:

1. Senden Sie folgende SMS an Ihr Gerät, um es zu sperren: #LOCK#<Sicherheitscode> (Beispiel: #LOCK#12345678)
2. Sobald das Gerät gesperrt ist, schickt es eine Antwort-SMS an das Telefon, von dem aus die SMS mit dem Sperrwunsch geschickt wurde. Wenn Sie den Remote-Locator aktiviert haben, steht in der Antwort die Ortsangabe des Geräts.

Gesperrte Geräte können nur mit der Methode zur Bildschirmentsperrung entsperrt werden, die Sie ausgewählt haben.

1.1.2 Fern-Reinitialisieren Ihres Geräts

Wenn Sie Ihr Gerät reinitialisieren, löscht Anti-Theft die persönlichen Informationen, die auf dem Gerät gespeichert sind.

So reinitialisieren Sie Ihr verlorenes oder gestohlenes Gerät:

1. Senden Sie folgende SMS an Ihr Gerät, um es zu reinitialisieren: #WIPE#<Sicherheitscode> (Beispiel: #WIPE#12345678)
2. Wenn das Gerät gelöscht ist, sendet es eine Antwort an das Telefon, von dem aus Sie die SMS mit dem Löschungswunsch gesendet haben.

Wenn Sie das Gerät löschen, werden alle Informationen von der SD-Karte entfernt, das heißt alle SMS- und MMS-Nachrichten sowie Kontakt- und Kalenderinformationen. Auf Android 2.2 und jüngeren Versionen werden die Standardeinstellungen zurückgesetzt.

1.1.3 Orten Ihres Geräts

Sie können eine SMS an Ihr verlorenes Gerät senden, um es zu orten.

> Hinweis

Stellen Sie sicher, dass Sie GPS in Ihrem Gerät aktiviert haben, um die Ortungsinformationen zu erhalten.

Gehen Sie wie folgt vor, um Ihr Gerät zu orten:

Um das Gerät zu orten, senden Sie folgende SMS an Ihr Gerät: #LOCATE#<Sicherheitscode>

(Beispiel: #LOCATE#12345678)

Anti-Theft antwortet mit einer SMS, die Informationen zum aktuellen Ort des Geräts enthält.

> Tipp

Senden Sie nach der Einrichtung die Ortungsnachricht an Ihr Gerät, um sicherzustellen, dass es ordnungsgemäß funktioniert.

> Hinweis

Anti-Theft speichert keine Standortdaten. Die einzigen Informationen bezüglich des Standorts sind in der an Sie gesendeten SMS enthalten.

1.2 Nutzen des SMS-Alarms

Sie können von Anti-Theft eine SMS-Warnung erhalten, wenn jemand die SIM-Karte in Ihrem Gerät austauscht.

So aktivieren Sie den SMS-Alarm:

1. Öffnen Sie in der Hauptansicht die Option Diebstahlsicherung.
2. Wählen Sie im Menü Diebstahlsicherung die Option Einstellungen aus.
3. Wählen Sie Vertrauenswürdige Nummer. Das Dialogfenster Vertrauenswürdige Nummer öffnet sich.
4. Geben Sie die Telefonnummer an, an die die SMS gesendet werden soll, wenn jemand die SIM-Karte des Geräts austauscht.

Wenn der SMS-Alarm aktiviert ist, erhalten Sie eine SMS, sobald jemand die SIM-Karte Ihres Geräts austauscht.

1.3 Verwenden des Anti-Theft-Alarms

Sie können einen Alarmton einstellen, der losgeht, wenn Sie Ihr Gerät verlieren oder es gestohlen wird. Gehen Sie wie folgt vor, um einen Alarmton auf Ihrem Gerät abzuspielen:

1. Senden Sie zum Abspielen des Alarms folgende SMS-Nachricht an Ihr Gerät:
   #ALARM#<Sicherheitscode>#
   <Wiederholungsanzahl>

> Hinweis

Sie können mit dem Wiederholungszähler einstellen, wie oft der Alarmton ertönen soll. Dafür ist es jedoch nicht notwendig, den Alarm abzuspielen.

(Zum Beispiel: #ALARM#abcd1234)

2. Wenn das Gerät die Nachricht erhält, wird es gesperrt und das Alarmsignal ertönt. Es schickt eine Antwort an das Telefon, von dem aus Sie die Alarm-Nachricht versendet haben.

Schalten Sie den Alarm mit der Methode zur Bildschirmentsperrung ab, die Sie ausgewählt haben.

> Tipp

Senden Sie zum ferngesteuerten Abschalten des Alarms folgende SMS-Nachricht an Ihr Gerät:
#ALARM#<security code>#0

1.4 Location Sharing verwenden

Sie können eine Nachricht an Ihre Freunde und Familie senden und auf einer Karte anzeigen, wo Sie sich gerade befinden.

Dafür müssen Sie das GPS auf Ihrem Gerät aktiviert haben. So versenden Sie die die Location Sharing-Nachricht:

1. Öffnen Sie in der Hauptansicht die Option Diebstahlsicherung.
2. Wählen Sie im Menü Diebstahlsicherung Location sharing aus.
   Mithilfe des GPS ermittelt das Gerät Ihren Aufenthaltsort und öffnet die Messaging-Anwendung.
3. Fügen Sie in der Messaging-Anwendung die Empfänger der Standortinformationen hinzu und klicken Sie auf Senden.
   Die Nachricht enthält Informationen über Ihren Standort und einen Link zu Google Maps. Dort wird angezeigt, wo Sie sich gerade befinden.

2. Schutz beim Internetsurfen

2.1 Browser-Schutz verwenden

Sie müssen den F-Secure-Browser verwenden. Bei jedem anderen Browser ist der Browser-Schutz nicht aktiv.

Führen Sie die folgenden Schritte aus, um beim Surfen im Web den Browser-Schutz zu verwenden: So starten Sie den Webbrowser:

- Öffnen Sie den sicheren Browser im Produkt. Wählen Sie in der Hauptansicht **Browser-Schutz** aus und dann **Sicherer Browser.**
- Öffnen Sie den **F-Secure Browser** auf der Android-Startseite.

2.2 Sichere Nutzung des Internets

Mithilfe des Browser-Schutzes können Sie die Sicherheit von Websites einschätzen und unabsichtliche Besuche gefährlicher Websites vermeiden.

Sobald Sie eine Website besuchen, prüft das Produkt automatisch deren Sicherheit. Ist die Website als verdächtig oder gefährlich eingestuft, blockiert das Produkt den Zugriff auf diese Website. Die Sicherheitseinstufung einer Website basiert auf Informationen aus mehreren Quellen, wie Malware-Analysten und Partner von F-Secure.

2.2.1 Zurückkehren von einer oder zugreifen auf eine blockierte Website

Anleitungen für mögliche Aktionen, wenn der Browser-Schutz den Zugriff auf eine schädliche Website blockiert hat.

Wenn der Browser-Schutz aktiviert ist, sperrt das Produkt den Zugang zu gefährlichen Websites. Der Browser-Schutz zeigt eine Seite an, die zwei mögliche Aktionen bietet.

1. Wenn Sie zur vorherigen Seite zurückkehren möchten, wählen Sie auf der Blockseite **Zur Homepage wechseln.**
2. Wenn Sie die Website öffnen möchten, obwohl sie vom Browser-Schutz gesperrt wurde, rufen Sie den Link **Ich möchte diese Seite trotzdem öffnen** auf der gesperrten Seite auf.

3. Überprüfen auf Viren

3.1 Manuelles Scannen

Sie können Ihr Gerät zu jedem beliebigen Zeitpunkt auf Viren und anderen bösartigen Code überprüfen. Gehen Sie wie folgt vor, um alle Dateien auf Ihrem Gerät und der eingelegten Speicherkarte zu überprüfen:

1. Wählen Sie in der Hauptansicht **Virenschutz** aus.
2. Wählen Sie **Jetzt scannen.**
   Der Viren-Scan wird gestartet.
3. Nach erfolgtem Viren-Scan zeigt die Anwendung folgende Informationen an.

- **Infiziert**
  Anzahl der gefundenen Infektionen.
- **Nicht gescannt**
  Anzahl der Dateien, die während des Scans nicht geprüft wurden. Eine Datei, die von einem anderen Programm gesperrt oder beschädigt ist, kann nicht gescannt werden.
- **Gescannt**
  Anzahl der gescannten Dateien.

4. Drücken Sie auf **Zurück**, um den Scan zu beenden.

3.2 Planmäßiger Scanvorgang

Sie können eine Zeit festlegen, zu der Ihr Gerät automatisch in regelmäßigen Intervallen auf Viren und anderen schädlichen Code überprüft wird.

Sie können Ihr Gerät in regelmäßigen Intervallen überprüfen, z. B. täglich, wöchentlich oder monatlich. Befolgen Sie diese Anweisungen, um einen planmäßigen Scanvorgang festzulegen:

1. Wählen Sie in der Hauptansicht **Virenschutz** aus.
2. Wählen Sie die Option **Geplanter Scanvorgang** aus.
3. Wählen Sie **Planmäßiger Scanvorgang** aus, um diese Einstellung zu aktivieren.

4. Wählen Sie unter **Scanintervall** die Häufigkeit der durchgeführten Scans aus:

- **Täglich**
  Das Gerät wird täglich überprüft.
- **Wöchentlich**
  Das Gerät wird jede Woche an einem ausgewählten Tag überprüft.
- **Monatlich**
  Das Gerät wird am ersten Tag jedes Monats überprüft.

5. Legen Sie unter Scanzeitpunkt fest, wann der Scan starten soll. Der planmäßige Scanvorgang startet automatisch und wird im Hintergrund ausgeführt.

Eine Benachrichtigungsmeldung informiert Sie über Beginn und Ende jedes geplanten Scanvorgangs.

3.3 Verarbeitung infizierter Dateien

Wenn das Produkt einen Virus oder bösartigen Code in einer Datei findet, können Sie die infizierte Datei von Ihrem Gerät entfernen.

Gehen Sie wie folgt vor, um infizierte Dateien zu verarbeiten:

1. Wählen Sie in der Hauptansicht **Virenschutz** aus.
2. Wählen Sie **Infizierte Dateien.**
   Die **Ansicht Infizierte Dateien** wird geöffnet.
3. Scrollen Sie in der **Ansicht Infizierte Dateien** zur infizierten Datei, die verarbeitet werden soll.
4. Wählen Sie die infizierte Datei aus, um weitere Details über sie anzuzeigen. Die **Ansicht Details zu infizierten Dateien** zeigt den Pfad und den Dateinamen der infizierten Datei sowie den Namen der Infektion an.
5. Wählen Sie **Löschen** oder **Deinstallieren**, um die infizierte Datei oder Anwendung von Ihrem Gerät zu entfernen.

Beschreibungen und Informationen zu Viren, Trojanern, Würmern und anderen Formen unwillkommener Software finden Sie auf der F-Secure-Website:
http://www.f-secure.com/virus-info/.

3.4 Ändern der Virenschutzeinstellungen

Ändern Sie die Virenschutzeinstellungen, um auszuwählen, wann Sie den Virenscan durchführen möchten. Befolgen Sie die folgenden Anweisungen, um die Virenschutzeinstellungen zu ändern:

1. Wählen Sie in der Hauptansicht die Option **Einstellungen**. Die Einstellungs-Auswahlliste wird geöffnet.
2. Wählen Sie in der Einstellungs-Auswahlliste die Option **Virenschutz** aus.
3. Wählen Sie **Installations-Scan**, um alle Programme nach der Installation auf Ihren Computer automatisch zu überprüfen.
4. Wählen Sie **Speicherkarten-Scan,** um eine Speicherkarte automatisch jedes Mal zu überprüfen, wenn Sie sie in Ihr Gerät eingeben.
5. Wählen Sie einen der folgenden Modi für **Cloud-Schutz verwenden** aus:

- **Nur mein eigener Netzanbieter**
  Die Anwendung überprüft Ihr Gerät nur dann auf die aktuellsten Bedrohungen, wenn Sie das Netzwerk Ihres eigenen Anbieters benutzen.
- **Alle Netzanbieter**
  Die Anwendungen überprüft Ihr Gerät unabhängig von Ihrem verwendeten Netzwerk auf die aktuellsten Bedrohungen.
- **Nie**
  Die Anwendung verwendet den Cloud-Schutz nicht.

Durch den Cloud-Schutz wird Ihr Gerät schneller und präziser vor den aktuellsten Bedrohungen geschützt. Sie können den Cloud-Schutz deaktivieren, wenn Sie nicht das Netzwerk Ihres eigenen Operators verwenden. Sie können den Cloud-Schutz auch vollständig deaktivieren, um ungewollte Datenroaming-Gebühren zu vermeiden.

4. Sicheres Surfen für Kinder

4.1 Was sind Altersgruppen?

Über Altersgruppen können Sie Web-Inhalte festlegen, die für Teenager und Kinder geeignet sind.

Die Kindersicherung analysiert Webseiten und blockiert den Zugriff auf unerwünschte Webseiten, abhängig von deren Inhalt.

Die Kindersicherung verfügt über drei voreingestellte Profile mit unterschiedlichen Zugriffsbeschränkungen auf Webinhalte. Jugendliche können uneingeschränkter im Internet surfen, wohingegen für die

Online-Aktivitäten kleiner Kinder stärkere Beschränkungen gelten. Erwachsene dürfen ohne Einschränkung im Internet surfen.

Sie können das Alter des Benutzers während der Installation oder später in den Einstellungen der Kindersicherung festlegen.

4.1.1 Die Altersgruppe der Benutzer auswählen

Mithilfe der Altersgruppe können Sie auswählen, wer dieses Gerät verwendet. Die Kindersicherung schränkt die Webinhalte auf der Basis dieser Auswahl ein.

So ändern Sie die Altersgruppe des Benutzers:

1. Wählen Sie in der Hauptansicht die Option **Einstellungen.**
2. Wählen Sie **Kindersicherung.**
3. Aktivieren Sie die **Kindersicherung,** um den Zugriff auf unerwünschte Webseiten zu blockieren.
4. Wählen Sie unter **Altersgruppe** aus, wer dieses Gerät benutzt. Die Kindersicherung schränkt die Webinhalte auf der Basis dieser Auswahl ein. Durch eine Anpassung der Altersgruppe ändern Sie die Inhalte, die ein Benutzer im Internet aufrufen kann.

5. Sie prüfen und ändern erlaubte Kategorien über **Eingeschränkte Web-Inhalte.**

6. Wählen Sie zulässige Inhalte aus.

Wenn Sie die Altersgruppe geändert haben, werden durch die Kindersicherung nur die Websites angezeigt, die Sie eingestellt haben.

4.2 Inhaltstypen

Sie können den Zugriff auf verschiedene Arten von Inhalten blockieren.

- **Nicht jugendfreie Inhalte**
Eindeutig sexuell geprägte Inhalte oder Inhalte, die sexuelle Anspielungen enthalten. Darunter fallen beispielsweise Sexshop-Seiten oder Seiten, auf denen nackte Menschen zu sehen sind.

- **Chat**
Darunter fallen beispielsweise webbasierte Chatprogramme, Instant Messaging-Programme und Chatseiten.

- **Dating**
Darunter fallen beispielsweise Webseiten zur Heiratsvermittlung oder für Kontaktanzeigen.

- **Drogen**
Seiten, die Drogenkonsum fördern. Beispielsweise Seiten, die Informationen über den Anbau oder das Kaufen und Verkaufen von Drogen enthalten.

- **Glücksspiel**
Darunter fallen beispielsweise Online-Glücksspielseiten oder Lotterieseiten.

- **Waffen**
Darunter fallen beispielsweise Seiten, die Beschreibungen oder Bilder von Waffen sowie Anleitungen zum Bau von Waffen oder Sprengkörpern enthalten.

- **Webmail**
Darunter fallen beispielsweise Seiten, auf denen E-Mail-Konten erstellt werden können, mit deren Hilfe Nachrichten über einen Webbrowser gesendet und empfangen werden können.

- **Soziale Netzwerke**
Darunter fallen beispielsweise Seiten, auf denen ein Mitgliedsprofil erstellt werden kann, um private und berufliche Interessen mit Anderen zu teilen.

- **Forum**
Darunter fallen beispielsweise Diskussionsgruppen, in denen Kommentare angesehen und veröffentlicht werden können oder Programme, mit deren Hilfe Foren erstellt werden können.

- **Blogs**
Darunter fallen beispielsweise Online-Tagebücher, persönliche Webseiten, Blogs und Podcasts.

- **Hass und Gewalt**
Darunter fallen beispielsweise Seiten, die Vorurteile gegenüber Religion, Rasse, Nationalität, Geschlecht, Alter, Behinderung oder sexueller Orientierung zu erkennen geben oder Seiten, auf denen Beschreibungen oder Bilder tätlicher Angriffe auf Menschen, Tiere oder Institutionen zu sehen sind.

- **Anonymisierungen und Proxies**
Darunter fallen beispielsweise Seiten, die versuchen, die Aktivität im Internet nicht zurückverfolgbar zu machen oder Seiten, die Informationen bereitstellen, wie die Filterung umgangen werden kann.

- **Illegale Downloads**
Darunter fallen beispielsweise Seiten, die illegalen oder fragwürdigen Zugriff auf Software anbieten und Seiten, die Programme entwickeln oder vertreiben, die Netzwerke und Systeme möglicherweise gefährden könnten.

- **Shopping**
Darunter fallen beispielsweise Seiten, von denen aus Artikel direkt über das Internet bestellt werden können, Seiten, auf denen Preise verglichen werden oder Online-Auktionsseiten.

- **Sekten**
Darunter fallen beispielsweise Seiten, die an Anhänger fanatischer Gruppen gerichtet sind oder Seiten, die Angriffe auf die Religion oder andere Ideologien fördern.

- **Alkohol und Zigaretten**
Darunter fallen beispielsweise Seiten, die Informationen zu alkoholischen Getränken und Tabakwaren bereitstellen, den Konsum dieser Produkte fördern oder unterstützen.

- **Unbekannt**
Wenn die Art des Inhalts einer Seite nicht verfügbar ist, wird er als unbekannt eingestuft.

4.3 Verwenden der Anwendungskontrolle

Mit der Anwendungskontrolle können Sie die Verwendung von Anwendungen einschränken und unerwünschte Anwendungen entfernen.

Für die Verwendung der Anwendungskontrolle muss die Kindersicherung aktiviert sein. Die folgenden Anweisungen beschreiben, wie Sie die Anwendungskontrolle verwenden:

1. Wählen Sie in der Hauptansicht die Option **Einstellungen.**
2. Wählen Sie **Kindersicherung.**
3. Aktivieren Sie **Kindersicherung.**
4. Aktivieren Sie **Anwendungskontrolle.**
5. Wählen Sie **Eingeschränkte Anwendungen** aus. Die Kindersicherung gibt eine Liste der installierten Anwendungen aus.
6. Damit der Benutzer des Geräts eine bestimmte Anwendung verwenden kann, aktivieren Sie das Kontrollkästchen neben der Anwendung. Um den Zugriff auf die Anwendung zu verhindern, deaktivieren Sie das Kontrollkästchen. Standardmäßig erlaubt die Kindersicherung den Zugriff auf alle Anwendungen.
7. Wenn Sie eine Anwendung vollständig von dem Gerät entfernen möchten, drücken Sie die Anwendung in der Liste so lange, bis die Deinstallationsaufforderung erscheint. Wählen Sie **Deinstallieren**, um die Anwendung zu entfernen.

Beim Versuch, eine über die Anwendungskontrolle gesperrte Anwendung zu öffnen, erscheint eine Sperrseite. Damit verhindert die Kindersicherung den Zugriff auf die Anwendung.

5. Schutz vor ungewollten Anrufen und Nachrichten

5.1 Verwenden von „Anrufsperre“

„Anrufsperre“ sperrt Anrufe und Nachrichten von Nummern der Sperrliste.

Folgen Sie diesen Anweisungen, um Anrufe und Nachrichten von einer neuen Nummer zu sperren:

1. Wählen Sie in der Hauptansicht die Option **Einstellungen.** Die Einstellungsauswahlliste wird geöffnet.
2. Wählen Sie **Anrufsperre** aus der Einstellungsauswahlliste aus.

> **Hinweis**
>
> Als nächstes stellen Sie Ihren Sicherheitscode ein, wenn Sie dies noch nicht getan haben.

3. Stellen Sie sicher, dass **Anrufsperre** aktiviert ist.
4. Wählen Sie **Nummern sperren** aus. Geben Sie Ihren Sicherheitscode ein, um neue Nummern zu sperren. Die Liste mit den gesperrten Nummern öffnet sich.
5. Wählen Sie **Eine Nummer zum Sperren eingeben** aus.
6. Geben Sie den Namen und die Nummer ein, die Sie sperren möchten.
7. Wählen Sie **Speichern** aus, um die Nummer zur Liste mit den gesperrten Nummern hinzuzufügen.

Wenn „Anrufsperre“ aktiviert ist, erhalten Sie keine Anrufe oder Nachrichten mehr von den Nummern aus der Liste mit den gesperrten Nummern. Außerdem sind alle Anrufe an die gesperrten Nummern begrenzt.

5.2 Anzeigen gesperrter Anrufe und Nachrichten

Sie können im Sperrverlauf sehen, welche Anrufe und Nachrichten von „Anrufsperre“ gesperrt wurden.

Folgen Sie diesen Anweisungen, um anzuzeigen, welche Anrufe und Nachrichten von „Anrufsperre“ gesperrt wurden:

1. Wählen Sie in der Hauptansicht die Option **Einstellungen**. Die Einstellungsauswahlliste wird geöffnet.
2. Wählen Sie **Anrufsperre** aus der Einstellungsauswahlliste aus.
3. Wählen Sie **Sperrverlauf anzeigen** aus.

6. Automatische Aktualisierung der Anwendung

6.1 Auswählen des Update-Modus

Nachdem Sie das Produkt aktiviert haben, werden automatische Updates verwendet.

Wenn Sie automatische Updates deaktivieren oder den Echtzeit-Scan-Modus nicht verwenden, müssen Sie die Anwendung manuell aktualisieren.

Gehen Sie wie folgt vor, um den Update-Modus zu ändern:

Wählen Sie einen der folgenden Modi für **Automatische Updates:**

- **Immer**
  die Anwendung lädt in regelmäßigen Abständen automatisch Updates vom Update-Server herunter, um die Virendefinitionsdatenbank auf dem neuesten Stand zu halten (empfohlen).
- **Im Heimnetzwerk**
  die Anwendung lädt automatisch Updates vom Update-Server herunter, sobald Ihr Gerät mit dem Netzwerk Ihres Betreibers verbunden ist.
- **Nie**
  die Virendefinitionen werden nicht automatisch aktualisiert. Es wird nicht empfohlen, automatische Updates zu deaktivieren.

6.2 Manuelle Updates

Sie können das Produkt jederzeit manuell aktualisieren. So aktualisieren Sie das Produkt manuell:

1. Öffnen Sie die Anwendung
2. Tippen Sie im unteren Teil der Benutzeroberfläche auf **Mehr > Updates > Jetzt installieren**

Kundenservice
Telefon: 02735 90 96 99

Technischer Support
Telefon: 02735 90 96 67

Sie erreichen uns
Montag bis Freitag: 9–21 Uhr
Samstag: 9–13 Uhr

Oder online unter
www.buhl.de/mein_konto.html

Online-Support
https://www.buhl.de/kundencenter.html
https://www.buhl.de/wiso-software/forum

Kontakt
Buhl Data Service GmbH
Support Center
Carl-Benz-Str. 2
57299 Burbach

www.buhl.de