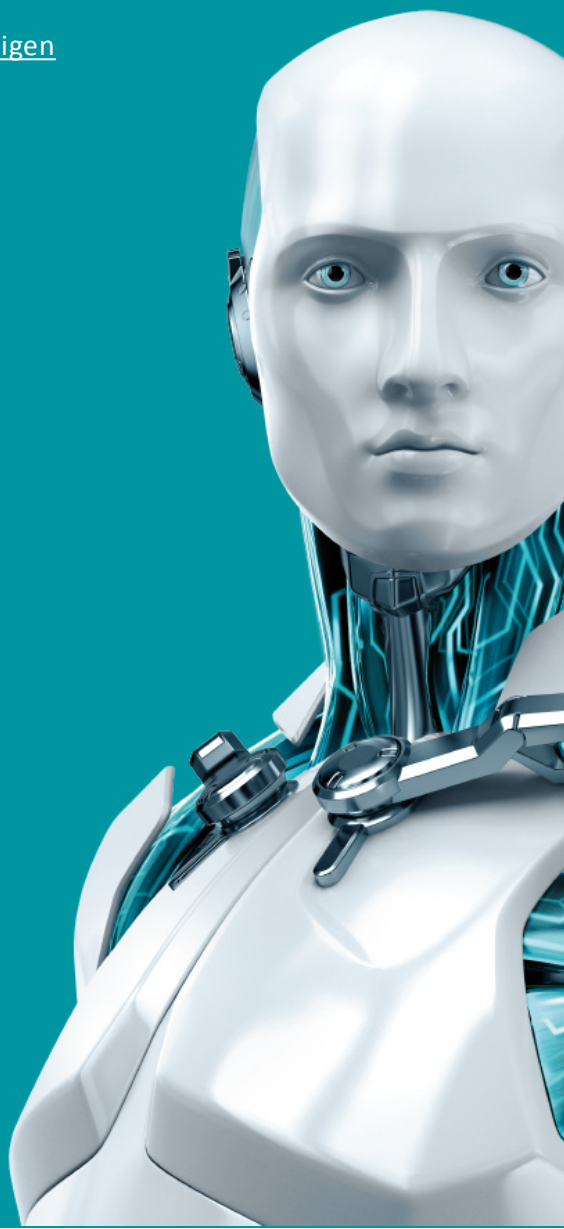
INTERNET SECURITY

BENUTZERHANDBUCH

(für Produktversion 11.0 und höher)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista / Home Server 2011

Klicken Sie hier, um die Onlinehilfe-Version dieses Dokuments anzuzeigen



ENJOY SAFER TECHNOLOGY™

Weltweiter Support: www.eset.de/support

Versionsstand 14.09.2018

Inhalt

1. ESET Internet Security

ESET Internet Security ist ein neuer Ansatz für vollständig integrierte Computersicherheit. Auf diese Weise ist ein intelligentes System entstanden, das permanent vor Angriffen und bösartiger Software schützt, die Ihren Computer gefährden können.

ESET Internet Security ist eine umfassende Sicherheitslösung, die maximalen Schutz mit minimalen Anforderungen an die Systemressourcen verbindet. Die modernen Technologien setzen künstliche Intelligenz ein, um ein Eindringen von Viren, Spyware, Trojanern, Würmern, Adware, Rootkits und anderen Bedrohungen zu vermeiden, ohne dabei die Systemleistung zu beeinträchtigen oder die Computerprozesse zu unterbrechen.

Funktionen und Vorteile

Neu gestaltete Benutzeroberfläche	Die Benutzeroberfläche wurde in dieser Version zu großen Teilen umgestaltet und anhand unserer Tests zur Benutzerfreundlichkeit vereinfacht. Die Texte für Bedienelemente und Benachrichtigungen wurden sorgfältig geprüft, und die Benutzeroberfläche unterstützt jetzt Sprachen mit Schriftbild von rechts nach links, z. B. Hebräisch und Arabisch. **Die Online-Hilfe** ist jetzt in ESET Internet Security integriert und enthält dynamisch aktualisierte Support-Inhalte.
Viren- und Spyware-Schutz	Erkennt und entfernt proaktiv eine Vielzahl bekannter und unbekannter Viren, Würmern, Trojanern und Rootkits. **Advanced Heuristik** erkennt selbst vollkommen neue Malware und schützt Ihren Computer vor unbekannten Bedrohungen, die abgewendet werden, bevor sie Schaden anrichten können. **Web-Schutz** und **Phishing-Schutz** überwachen die Kommunikation zwischen Webbrowsern und Remoteservern (einschließlich SSL-Verbindungen). Der **E-Mail-Schutz** dient der Überwachung eingehender E-Mails, die mit dem POP3(S)- oder dem IMAP(S)-Protokoll übertragen werden.
Reguläre Updates	Aktualisieren Sie die Erkennungsroutine (bisher auch als „Signaturdatenbank“ bezeichnet) und die Programmmodule regelmäßig, um einen optimalen Schutz Ihres Computers sicherzustellen.
ESET LiveGrid® (Cloud-basierter Reputations-Check)	Sie können die Reputation ausgeführter Prozesse und Dateien direkt mit ESET Internet Security überprüfen.
Medienkontrolle	Prüft automatisch alle USB-Speicher, Speicherkarten und CDs/DVDs. Sperrt den Zugriff auf Wechselmedien anhand von Kriterien wie Medientyp, Hersteller, Größe und weiteren Attributen.
HIPS-Funktion	Sie können das Verhalten des Systems detailliert anpassen, Regeln für die Systemregistrierung und für aktive Prozesse und Programme festlegen und Ihre Sicherheitsposition genau konfigurieren.
Gamer-Modus	Unterdrückt Popup-Fenster, Updates und andere systemintensive Aktivitäten, um Systemressourcen für Spiele oder andere Anwendungen im Vollbildmodus zu bewahren.

Die Funktionen von ESET Internet Security arbeiten nur mit einer ordnungsgemäß aktivierten Lizenz. Wir empfehlen, die Lizenz für ESET Internet Security einige Wochen vor dem Ablauf zu verlängern.

1.1 Neuerungen in dieser Version

Die neue Version von ESET Internet Security enthält die folgenden Verbesserungen:

- **Logging mit einem Klick** – Erstellen Sie erweiterte Logs mit nur einem Klicke.
- **Unified Extensible Firmware Interface (UEFI)-Prüfmodul** – Erweitert den Schutz vor Schadsoftware, indem auch Bedrohungen erkannt und entfernt werden, die möglicherweise vor dem Systemstart ausgeführt werden. Weitere Informationen erhalten Sie hier.
- **Starke Leistung und geringe Systembeeinträchtigung** – Diese Version nutzt Ihre Systemressourcen noch effizienter. Sie können Sie die Leistung Ihres Computers voll nutzen und sind gleichzeitig vor neuen Bedrohungen geschützt.
- **Überarbeitete erweiterte Einstellungen** – ESET LiveGrid®-Einstellungen wurden in den Bereich „Erkennungsroutine“ verschoben, das erweiterte Spamschutz-Logging in den Bereich „Diagnose“, usw.
- **Bessere Unterstützung für Sprachausgabeprogramme** – ESET Internet Security unterstützt die beliebtesten Sprachausgabeprogramme (JAWS, NVDA, Narrator).
- **Prüfen per Ziehen und Ablegen** – Sie können eine Datei oder einen Ordner in den markierten Bereich ziehen, um diese manuell zu prüfen.
- **ESET-Produkte an Freunde weiterempfehlen** – ESET Internet Security bietet jetzt Empfehlungsboni an, damit Sie Ihr ESET-Produkterlebnis mit Freunden oder Familienmitgliedern teilen können.
- ESET Internet Security wird jetzt mit einem Minimum an Modulen installiert, um weniger Speicherplatz zu verbrauchen und die Installation zu beschleunigen. Der Download der Module beginnt, nachdem das Produkt installiert und aktiviert wurde.
- ESET Internet Security informiert Sie, wenn Sie sich mit einem gar nicht oder nur schwach geschützten WLAN-Netzwerk verbinden.

Weitere Details zu den neuen Funktionen in ESET Internet Security finden Sie im folgenden ESET Knowledgebase-Artikel:
Neuerungen in dieser Version der ESET Home-Produkte

1.2 Welches Produkt verwende ich?

ESET bietet verschiedene Schutzebenen mit neuen Produkten von einer umfassenden und leistungsstarken Virenschutzlösung bis hin zur All-in-One-Sicherheitslösung mit minimaler Systembelastung:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**

Um herauszufinden, welches Produkt Sie installiert haben, öffnen Sie das Programmfenster (siehe Knowledgebase-Artikel). Dort wird der Name des Produkts am oberen Rand (Kopfzeile) angezeigt.

Die folgende Tabelle enthält die verfügbaren Funktionen der einzelnen Produkte.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Virenschutz	✔	✔	✔
Spyware-Schutz	✔	✔	✔
Exploit-Blocker	✔	✔	✔
Skriptbasierter Angriffsschutz	✔	✔	✔
Phishing-Schutz	✔	✔	✔

Web-Schutz	✔	✔	✔
HIPS (inklusive **Ransomware-Schutz**)	✔	✔	✔
Spam-Schutz		✔	✔
Firewall		✔	✔
Sicheres Heimnetzwerk		✔	✔
Webcam-Schutz		✔	✔
Netzwerkangriffsschutz		✔	✔
Botnetschutz		✔	✔
Online-Banking-Zahlungsschutz		✔	✔
Kindersicherung		✔	✔
Anti-Theft		✔	✔
ESET Password Manager			✔
ESET Secure Data			✔

HINWEIS
Möglicherweise sind nicht alle aufgeführten Produkte für Ihre Sprache oder Region verfügbar.

1.3 Systemanforderungen

Ihr System muss die folgenden Hardware- und Softwareanforderungen erfüllen, um ESET Internet Security mit optimaler Leistung ausführen zu können:

Unterstützte Prozessoren

Intel® oder AMD x86-x64

Unterstützte Betriebssysteme

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7
Microsoft® Windows® Vista
Microsoft® Windows® Home Server 2011 64-Bit

HINWEIS
ESET Anti-Theft ist nicht für den Einsatz auf Microsoft Windows Home Server geeignet.

1.4 Prävention

Bei der Arbeit am Computer und besonders beim Surfen im Internet sollten Sie sich darüber im Klaren sein, dass kein Virenschutz der Welt die mit Infiltrationen und Angriffen einhergehenden Risiken gänzlich ausschließen kann.. Für maximalen Schutz und einen möglichst geringen Aufwand müssen Sie die Virenschutzsoftware richtig einsetzen und dabei einige wichtige Regeln beachten:

Führen Sie regelmäßige Updates durch

Gemäß von ThreatSense erhobenen Statistiken werden täglich tausende neuartige Schadprogramme zur Umgehung bestehender Sicherheitsmaßnahmen entwickelt, die den Entwicklern Vorteile auf Kosten anderer Benutzer verschaffen sollen. Die Experten aus im ESET-Virenlabor analysieren diese Bedrohungen täglich und veröffentlichen Updates zur kontinuierlichen Verbesserung des Virenschutzes. Die richtige Konfiguration der Updates ist von

wesentlicher Bedeutung für die Gewährleistung eines optimalen Schutzes. Weitere Informationen zur Konfiguration von Updates finden Sie im Kapitel Einstellungen für Updates.

Laden Sie Sicherheitspatches herunter

Die Entwickler von Schadsoftware nutzen oft Sicherheitslücken im System aus, um möglichst effektiv Schadcode zu verbreiten. Softwareunternehmen halten daher regelmäßig Ausschau nach neuen Sicherheitslücken in den eigenen Anwendungen und veröffentlichen Sicherheitsupdates zur Bekämpfung potenzieller Bedrohungen. Es ist wichtig, dass Sie diese Updates umgehend nach der Veröffentlichung herunterladen. Microsoft Windows und Webbrowser wie Internet Explorer sind Beispiele für Programme, für die regelmäßig Sicherheitsaktualisierungen veröffentlicht werden.

Sichern wichtiger Daten

Malware-Entwickler missachten die Interessen der Benutzer und legen mit ihrer Software oft das gesamte Betriebssystem lahm bzw. nehmen den Verlust wichtiger Daten bewusst in Kauf. Es ist wichtig, dass Sie Ihre wichtigen und vertraulichen Daten regelmäßig auf einem externen Speichermedium (z. B. einer DVD oder einer externen Festplatte) sichern. So können Sie Ihre Daten bei einem Systemfehler viel einfacher und schneller wiederherstellen.

Scannen Sie Ihren Computer regelmäßig auf Viren

Der Echtzeit-Dateischutz erkennt eine größere Zahl bekannter und unbekannter Viren, Würmer, Trojaner und Rootkits. Jedes Mal, wenn Sie eine Datei öffnen oder auf eine Datei zugreifen, wird die Datei auf Schadcode überprüft. Wir empfehlen jedoch, dass Sie mindestens einmal im Monat eine vollständige Prüfung des Computers ausführen, da Schadcode die verschiedensten Formen annehmen kann und die Erkennungsroutine täglich aktualisiert wird.

Halten Sie grundlegende Sicherheitsregeln ein

Die nützlichste und effektivste Regel von allen ist das Prinzip ständiger Wachsamkeit. Heutzutage erfordert ein Großteil der Schadsoftware zur Ausführung und Ausbreitung ein Eingreifen des Benutzers. Wenn Sie beim Öffnen neuer Dateien achtsam sind, sparen Sie viel Zeit und Aufwand, die Sie andernfalls darauf verwenden müssten, eingedrungene Schadsoftware zu entfernen. Hier finden Sie einige nützliche Richtlinien:

- Besuchen Sie keine zweifelhaften Websites, die durch zahlreiche Popup-Fenster und bunte Werbeanzeigen auffallen.
- Seien Sie vorsichtig bei der Installation von Programmen, Codec-Paketen usw. Verwenden Sie nur sichere Programme, und besuchen Sie ausschließlich sichere Websites.
- Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen, insbesondere wenn es sich um Anhänge von Massen-E-Mails und E-Mail-Nachrichten mit unbekanntem Absender handelt.
- Verwenden Sie für die tägliche Arbeit mit dem Computer kein Administratorkonto.

2. Installation

Zur Installation von ESET Internet Security auf Ihrem Computer stehen verschiedene Methoden zur Verfügung. Die verfügbaren Installationsmethoden unterscheiden sich je nach Land und Vertriebsart:

- Der Live-Installer kann von der ESET-Website heruntergeladen werden. Das Installationspaket gilt für alle Sprachen (wählen Sie die gewünschte Sprache aus). Live-Installer ist eine kleine Datei. Zusätzlich für die Installation von ESET Internet Security erforderliche Dateien werden automatisch heruntergeladen.

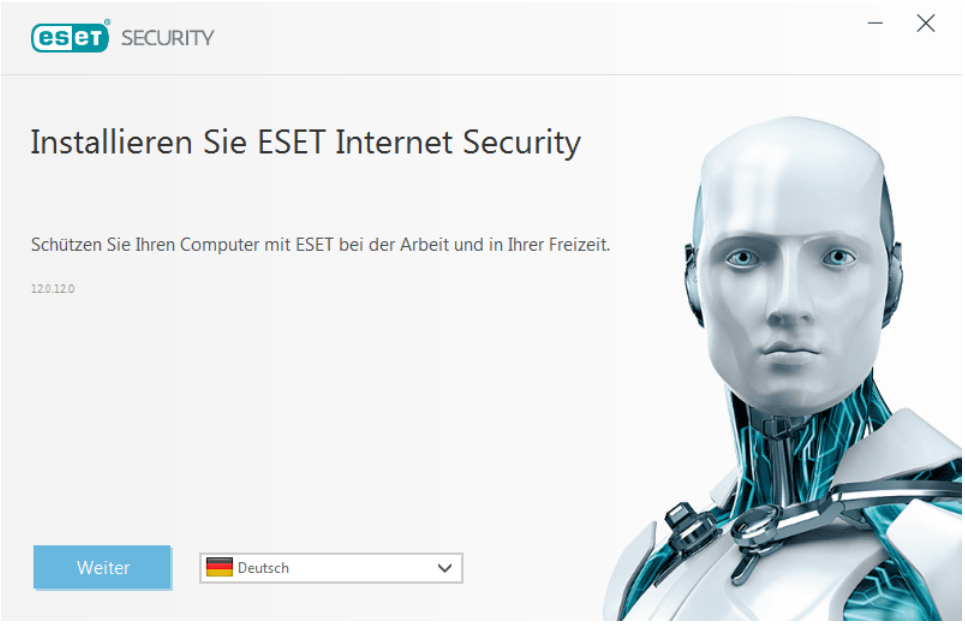
- Offline-Installation – Diese Art der Installation wird beim Installieren von einer CD/DVD verwendet. Die hierbei verwendete *.exe*-Datei ist größer als die Live-Installer-Datei. Zur Installation sind jedoch keine zusätzlichen Dateien und keine Internetverbindung erforderlich.

WICHTIG
Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind, bevor Sie mit der Installation von ESET Internet Security beginnen. Anderenfalls kann es zu Konflikten zwischen den Programmen kommen. Wir empfehlen Ihnen, alle anderen Virusschutzprogramme zu deinstallieren. Eine Liste von Tools zum Deinstallieren üblicher Virenschutzsoftware finden Sie in unserem ESET-Knowledgebase-Artikel (in englischer und in bestimmten weiteren Sprachen verfügbar).

2.1 Live-Installer

Nachdem Sie das *Live-Installer*-Installationspaket heruntergeladen haben, doppelklicken Sie auf die Installationsdatei und befolgen Sie die schrittweisen Anweisungen im Installationsfenster.

WICHTIG
Für diese Art der Installation ist eine Internetverbindung erforderlich.



Wählen Sie im Dropdownmenü Ihre gewünschte Sprache aus und klicken Sie auf **Weiter**. Warten Sie einen Moment, bis die Installationsdateien heruntergeladen wurden.

Wenn Sie die **Endbenutzer-Lizenzvereinbarung** annehmen, werden Sie aufgefordert, **ESET LiveGrid®** und die **Erkennung potenziell unerwünschter Anwendungen** zu konfigurieren. **ESET LiveGrid®** erhält ESET unmittelbar und fortlaufend aktuelle Informationen zu neuen Bedrohungen, um unseren Kunden umfassenden Schutz zu bieten. Das System übermittelt neue Bedrohungen an das ESET-Virenlabor, wo die entsprechenden Dateien analysiert, bearbeitet und zur Erkennungsroutine hinzugefügt werden.

Standardmäßig ist das **ESET LiveGrid®-Feedbacksystem aktiviert (empfohlen)** und die Funktion somit aktiviert.

Im nächsten Schritt der Installation wird die Prüfung auf eventuell unerwünschte Anwendungen konfiguriert. Eventuell unerwünschte Anwendungen sind Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, jedoch negative Auswirkungen auf das Verhalten Ihres Computers haben können. Weitere Details finden Sie im Kapitel Eventuell unerwünschte Anwendungen.

Klicken Sie auf **Installieren**, um die Installation zu beginnen. Dieser Vorgang kann einige Minuten dauern. Klicken Sie auf **Fertig stellen**, um die Einrichtung abzuschließen und mit der Aktivierung zu beginnen.

HINWEIS
Der Download der Module beginnt, nachdem das Produkt installiert und aktiviert wurde. Der Schutz wird gestartet, und ein Teil der Funktionen ist bis zum Abschluss des Downloads unter Umständen nicht vollständig einsatzbereit.

HINWEIS
Falls Ihre Lizenz für andere Versionen eines Produkts gültig ist, können Sie das Produkt gemäß Ihrer Einstellungen auswählen. Weitere Informationen zu den Features der einzelnen Produkte finden Sie hier.

2.2 Offline-Installation

Nachdem Sie die Offline-Installation (.exe) gestartet haben, führt der Installationsassistent Sie durch die Einstellungen.

Wählen Sie im Dropdownmenü Ihre gewünschte Sprache aus und klicken Sie auf **Installieren**.

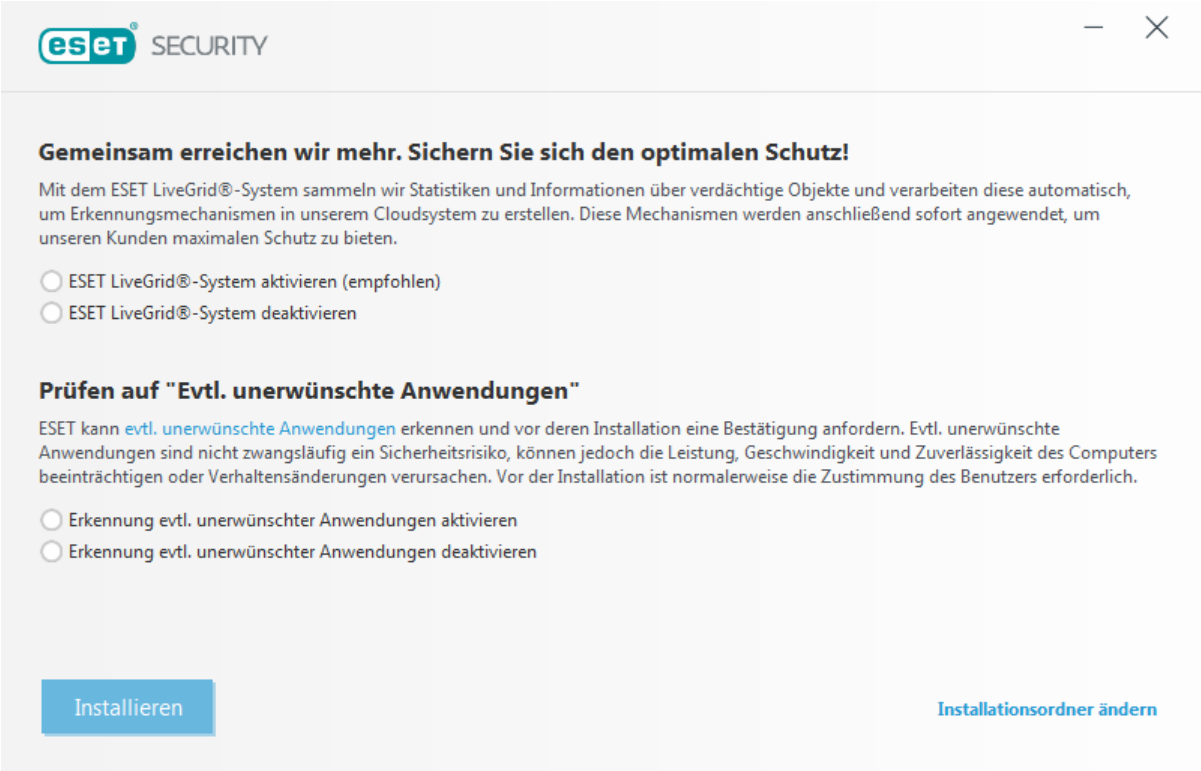
Nach dem Sie die **Endbenutzer-Softwarelizenzvereinbarung** akzeptiert haben, können Sie zwischen den Optionen **Lizenzschlüssel eingeben** und **Lizenzmanager verwenden** auswählen.

Falls Sie noch keine Lizenz haben, wählen Sie **Kostenloser Test** aus, um das ESET-Produkt für begrenzte Zeit zu testen, oder wählen Sie **Lizenz kaufen** aus. Alternativ können Sie die Option **Aktivierung überspringen** auswählen, um die Installation ohne Aktivierung fortzusetzen. In diesem Fall werden Sie später zur Eingabe eines Lizenzschlüssels aufgefordert.

2.2.1 Lizenzschlüssel eingeben

Der Setup-Assistent wählt das zu installierende Produkt anhand Ihres Lizenzschlüssels aus und zeigt den Produktnamen während der Installation an. Klicken Sie auf **Produkt ändern**, um eine Liste aller Produkte anzuzeigen, die mit Ihrer Lizenz aktiviert werden können. Weitere Informationen zu den Features der einzelnen Produkte finden Sie hier.

Klicken Sie auf **Weiter** und wählen Sie Ihre bevorzugten Einstellungen für **ESET LiveGrid®** und die **Erkennung potenziell unerwünschter Anwendungen** aus. **ESET LiveGrid®** erhält ESET unmittelbar und fortlaufend aktuelle Informationen zu neuen Bedrohungen, um unseren Kunden umfassenden Schutz zu bieten. Das System übermittelt neue Bedrohungen an das ESET-Virenlabor, wo die entsprechenden Dateien analysiert, bearbeitet und zur Erkennungsroutine hinzugefügt werden. **Eventuell unerwünschte Anwendungen** sind Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, jedoch negative Auswirkungen auf das Verhalten Ihres Computers haben können. Weitere Details finden Sie im Kapitel Eventuell unerwünschte Anwendungen.



Klicken Sie auf **Installieren**, um die Installation zu beginnen. Dieser Vorgang kann einige Minuten dauern. Klicken Sie auf **Fertig stellen**, um die Einrichtung abzuschließen und mit der Aktivierung zu beginnen.

HINWEIS
Der Download der Module beginnt, nachdem das Produkt installiert und aktiviert wurde. Der Schutz wird gestartet, und ein Teil der Funktionen ist bis zum Abschluss des Downloads unter Umständen nicht vollständig einsatzbereit.

HINWEIS
Falls Ihre Lizenz für andere Produkte gültig ist, können Sie das Produkt gemäß Ihrer Einstellungen auswählen. Weitere Informationen zu den Features der einzelnen Produkte finden Sie hier.

Weitere Anweisungen zu den Installationsschritten, zu **ESET LiveGrid®** und zur Funktion **Prüfen auf eventuell unerwünschte Anwendungen** finden Sie im Abschnitt zum Live-Installer.

2.2.2 Lizenzmanager verwenden

Wenn Sie **Lizenzmanager verwenden** auswählen, werden Sie in einem neuen Fenster aufgefordert, Ihre my.eset.com-Anmeldeinformationen einzugeben. Geben Sie Ihre Anmeldeinformationen für my.eset.com ein und klicken Sie auf **Anmelden**, um eine Lizenz aus Ihrem Lizenzmanager zu verwenden. Wählen Sie eine Lizenz für die Aktivierung aus und klicken Sie auf **Fortfahren**, um Ihr ESET Internet Security zu aktivieren.

HINWEIS
Falls Sie noch kein Konto für my.eset.com haben, klicken Sie auf die Schaltfläche **Konto erstellen**, um sich zu registrieren.

HINWEIS
Falls Sie Ihr Passwort vergessen haben, klicken Sie auf **Ich habe mein Passwort vergessen** und folgen Sie den Schritten auf der Webseite, zu der Sie weitergeleitet werden.

Mit dem ESET-Lizenzmanager können Sie all Ihre ESET-Lizenzen verwalten. Sie können Ihre Lizenz jederzeit erneuern, erweitern oder verlängern und alle wichtigen Lizenzdetails auf einen Blick anzeigen. Geben Sie zunächst Ihren Lizenzschlüssel ein. Anschließend wird das Produkt, das zugeordnete Gerät, die Anzahl der verfügbaren Lizenzen oder das Ablaufdatum angezeigt. Sie können einzelne Geräte deaktivieren oder umbenennen. Wenn Sie auf **Verlängern** klicken, werden Sie zum Online-Shop weitergeleitet. Dort können Sie Ihren Kauf bestätigen und die Verlängerung kaufen.

Falls Sie ein Upgrade für Ihre Lizenz erwerben (z. B. von ESET NOD32 Antivirus auf ESET Smart Security Premium) oder ein ESET-Sicherheitsprodukt auf einem anderen Gerät installieren möchten, werden Sie zum Online-Shop weitergeleitet, um den Kauf abzuschließen.

Im ESET-Lizenzmanager können Sie außerdem weitere Lizenzen hinzufügen, Produkte auf Ihre Geräte herunterladen.

2.2.3 Erweiterte Einstellungen

Nach der Auswahl von **Installationsordner ändern** werden Sie aufgefordert, einen Speicherort für die Installation auszuwählen. Standardmäßig wird das Programm in folgendes Verzeichnis installiert:

C:\Programme\ESET\ESET Internet Security

Klicken Sie auf **Durchsuchen**, um diesen Speicherort zu ändern (nicht empfohlen).

Befolgen Sie zum Abschluss der weiteren Installationsschritte (**ESET LiveGrid®** und **Prüfen auf eventuell unerwünschte Anwendungen**) die Anweisungen im Abschnitt zum Live-Installer.

Klicken Sie auf **Fortsetzen** und auf **Installieren**, um die Installation abzuschließen.

2.3 Bekannte Probleme bei der Installation

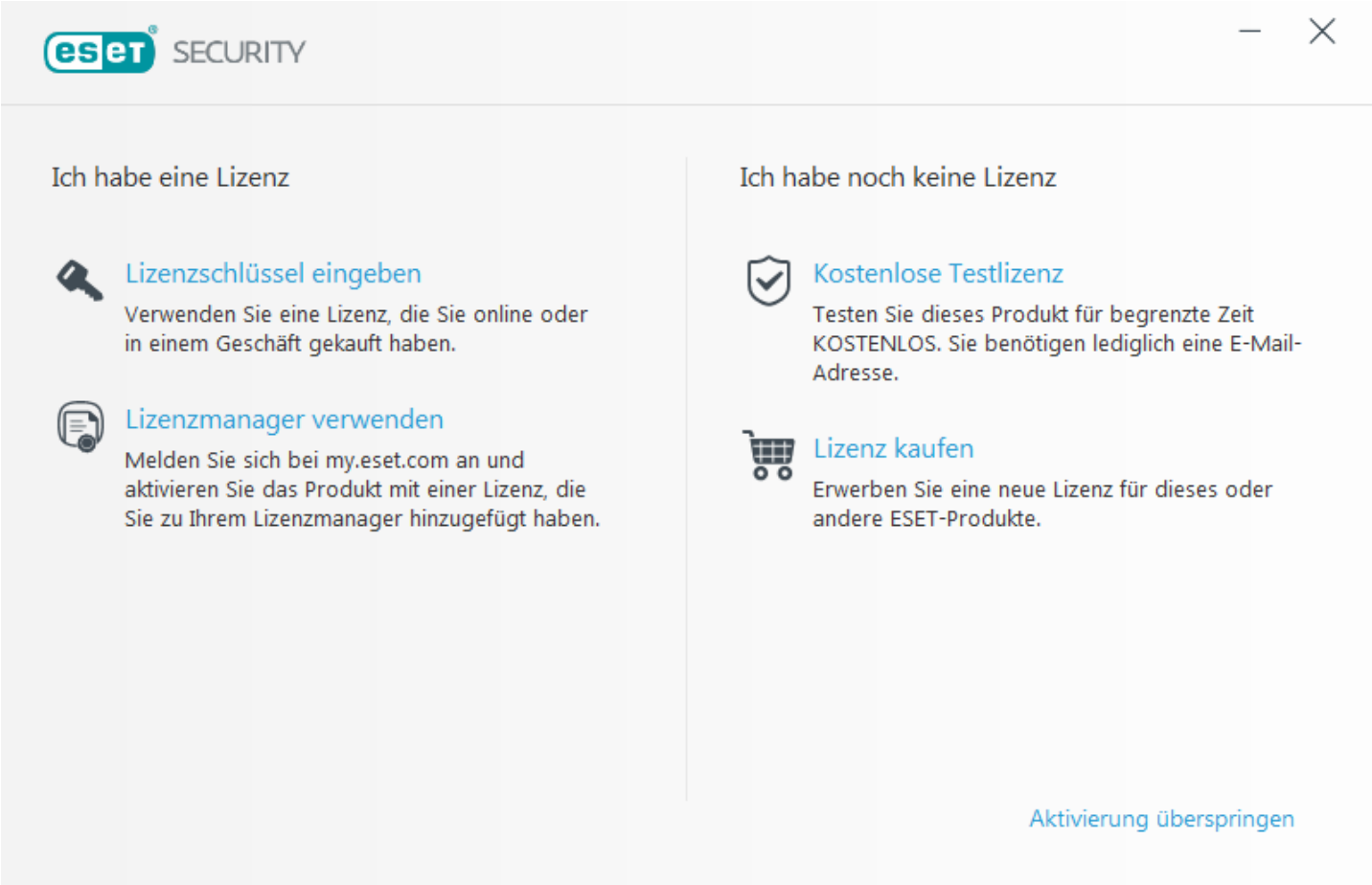
In unserer Liste mit Lösungen für bekannte Probleme bei der Installation finden Sie Hilfestellungen, falls Probleme bei der Installation auftreten.

2.4 Produktaktivierung

Nach Abschluss der Installation werden Sie aufgefordert, Ihr Produkt zu aktivieren.

Für die Aktivierung Ihres Produkts stehen verschiedene Methoden zur Verfügung. Die Verfügbarkeit einzelner Aktivierungsmöglichkeiten im Aktivierungsfenster hängt vom Land und von der Vertriebsart (CD/DVD, ESET-Webseite usw.) ab:

- Wenn Sie das Produkt in einer Einzelhandelsverpackung erworben haben, aktivieren Sie Ihr Produkt mit einem **Lizenzschlüssel**. Den Lizenzschlüssel finden Sie normalerweise in der Produktverpackung oder auf deren Rückseite. Der Lizenzschlüssel muss unverändert eingegeben werden, damit die Aktivierung erfolgreich ausgeführt werden kann. Lizenzschlüssel – Eine eindeutige Zeichenfolge im Format XXXX-XXXX-XXXX-XXXX-XXXX oder XXXX-XXXXXXXX zur Identifizierung des Lizenzinhabers und der Aktivierung der Lizenz.
- Wenn Sie **Lizenzmanager verwenden** auswählen, werden Sie in einem neuen Fenster aufgefordert, Ihre my.eset.com-Anmeldeinformationen einzugeben.
- Wenn Sie ESET Internet Security vor dem Kauf testen möchten, wählen Sie **Kostenloser Test** aus. Geben Sie Ihre E-Mail-Adresse und Ihr Land ein, um ESET Internet Security für begrenzte Zeit zu aktivieren. Sie erhalten die Testlizenz per E-Mail. Eine Testlizenz kann pro Kunde nur ein einziges Mal aktiviert werden.
- Wenn Sie noch keine Lizenz haben und eine erwerben möchten, klicken Sie auf Lizenz kaufen. Hiermit gelangen Sie zur Website Ihres lokalen ESET-Distributors.



2.5 Eingabe Ihres Lizenzschlüssels

Automatische Updates sind wichtig für Ihre Sicherheit. ESET Internet Security erhält erst Updates, nachdem Sie das Produkt mit Ihrem **Lizenzschlüssel** aktiviert haben.

Wenn Sie Ihren Lizenzschlüssel nach der Installation nicht eingegeben haben, wird Ihr Produkt nicht aktiviert. Sie können Ihre Lizenz im Hauptprogrammfenster ändern. Klicken Sie auf **Hilfe und Support** > **Produktaktivierung**. Geben Sie im Produktaktivierungsfenster die Lizenzdaten ein, die Sie für Ihr ESET Security-Produkt erhalten haben.

Geben Sie Ihren **Lizenzschlüssel** unbedingt exakt nach Vorgabe ein:

- Ihr Lizenzschlüssel ist eine eindeutige Zeichenfolge im Format XXXX-XXXX-XXXX-XXXX-XXXX und dient zur Identifizierung des Lizenzinhabers und zur Aktivierung der Lizenz.

Kopieren Sie den Lizenzschlüssel aus der Registrierungs-E-Mail und fügen Sie ihn in das Feld ein, um Tippfehler zu vermeiden.

2.6 ESET-Produkte an Freunde weiterempfehlen

Mit der aktuellen Version von ESET Internet Security wurden Empfehlungsboni eingeführt, damit Sie Ihr ESET-Produkterlebnis mit Freunden oder Familienmitgliedern teilen können. Sie können sogar Empfehlungen von einem Produkt teilen, das mit einer Probelizenz aktiviert wurde. Für jede erfolgreich verschickte Empfehlung, die zu einer Produktaktivierung führt, erhalten Sie und die andere Person den vollständigen Schutz für einen zusätzlichen Monat.

Sie können die Empfehlungen in Ihrem installierten ESET Internet Security verschicken. Die Produkte, die Sie empfehlen können, hängen von dem Produkt ab, das Sie verwenden.

Ihr installiertes Produkt	Produkte, die Sie empfehlen können
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

Empfehlen von Produkten

Um einen Empfehlungslink zu verschicken, klicken Sie auf **Ihrem Freund empfehlen** im Hauptmenü von ESET Internet Security. Klicken Sie auf **Mit Empfehlungslink empfehlen**. Der von Ihrem Produkt generierte Empfehlungslink wird in einem neuen Fenster angezeigt. Kopieren Sie den Link und senden Sie ihn an Freunde und Familienmitglieder. Sie können Ihren Empfehlungslink auf verschiedene Arten teilen: direkt in Ihrem ESET-Produkt, auf **Google+**, an ihre **Gmail-**Kontakte oder auf **Facebook**.

Wenn einer Ihrer Freunde auf Ihren Empfehlungslink klickt, wird die Person auf eine Webseite weitergeleitet, auf der neue Benutzer das Produkt herunterladen oder vorhandene Benutzer ihre Probelizenz um einen Monat verlängern können. Sie erhalten eine Benachrichtigung für jeden erfolgreich aktivierten Empfehlungslink, und Ihre Lizenz wird automatisch um einen Monat verlängert. Sie können die Anzahl der erfolgreich aktivierten Empfehlungslinks im Fenster **Ihrem Freund empfehlen** in Ihrem ESET-Produkt abrufen.

2.7 Upgrade auf eine aktuellere Version

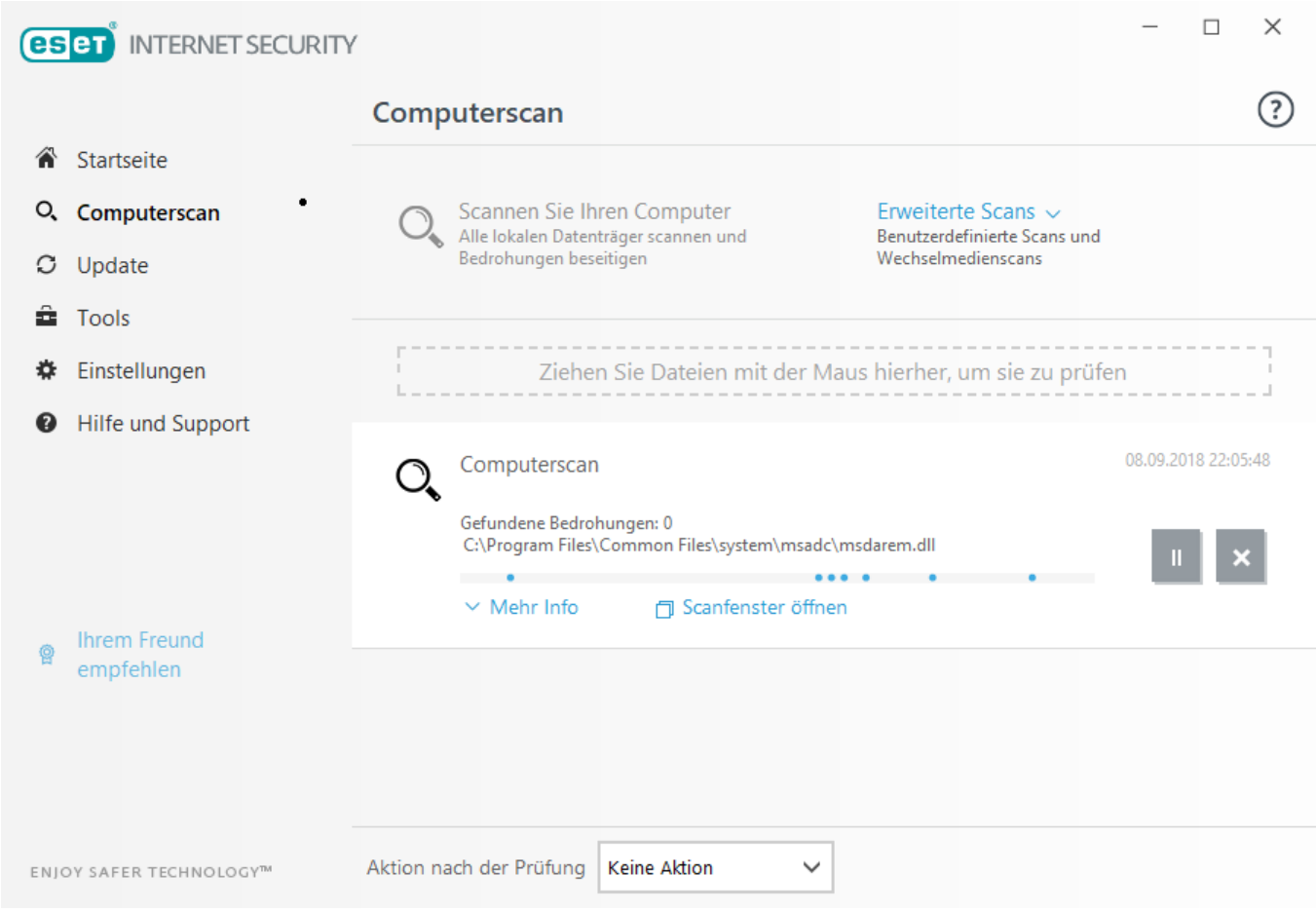
Neuere Versionen von ESET Internet Security werden veröffentlicht, um Verbesserungen oder Patches durchzuführen, die ein automatisches Update der Programmmodule nicht leisten kann. Es gibt verschiedene Möglichkeiten, ein Upgrade auf eine aktuellere Version durchzuführen:

1. Automatische Aktualisierung durch ein Programm-Update
   Da das Programm-Update an alle Benutzer des Programms ausgegeben wird und Auswirkungen auf bestimmte Systemkonfigurationen haben kann, wird es erst nach einer langen Testphase veröffentlicht, wenn sicher ist, dass es in allen möglichen Konfigurationen funktioniert. Wenn Sie sofort nach der Veröffentlichung eines Upgrades auf die neue Version aufrüsten möchten, befolgen Sie eine der nachstehenden Methoden.
2. Manuell im Hauptfenster über **Nach Updates suchen** im Bereich **Update**.
3. Manuelle Aktualisierung durch Herunterladen und Installieren der aktuelleren Version (ohne Deinstallation der vorherigen Version)

2.8 Erstprüfung nach Installation

Nach der Installation von ESET Internet Security und dem ersten erfolgreichen Update wird der Computer auf Schadsoftware geprüft.

Sie können die Prüfung des Computers auch manuell aus dem Haupt-Programmfenster auslösen, indem Sie auf **Computerprüfung** > **Computerprüfung** klicken. Weitere Informationen zur Prüfung des Computers finden Sie im Abschnitt Computerprüfung.



3. Erste Schritte

Dieses Kapitel enthält eine einführende Übersicht zu ESET Internet Security und die Grundeinstellungen des Programms.

3.1 Das Haupt-Programmfenster

Das Hauptprogrammfenster von ESET Internet Security ist in zwei Abschnitte unterteilt. Das primäre Fenster (rechts) zeigt Informationen zu den im Hauptmenü (links) ausgewählten Optionen an.

Im Folgenden werden die Optionen des Hauptmenüs beschrieben:

Startseite - Informationen zum Schutzstatus von ESET Internet Security.

Computerprüfung – Konfigurieren und starten Sie eine Prüfung Ihres Computers oder erstellen Sie eine benutzerdefinierte Prüfung.

Update – Dieser Bereich zeigt Informationen zu Updates der Erkennungsroutine an.

Tools - Zugang zu den Log-Dateien, Schutzstatistiken und den Funktionen „Aktivität beobachten“, „Ausgeführte Prozesse“,Netzwerkverbindungen,, Taskplaner, ESET SysInspector und ESET SysRescue.

Einstellungen - Mit dieser Option können Sie die Sicherheitsebene für Ihren Computer, Ihre Internetverbindung, Netzwerkschutz und Sicherheits-Tools konfigurieren.

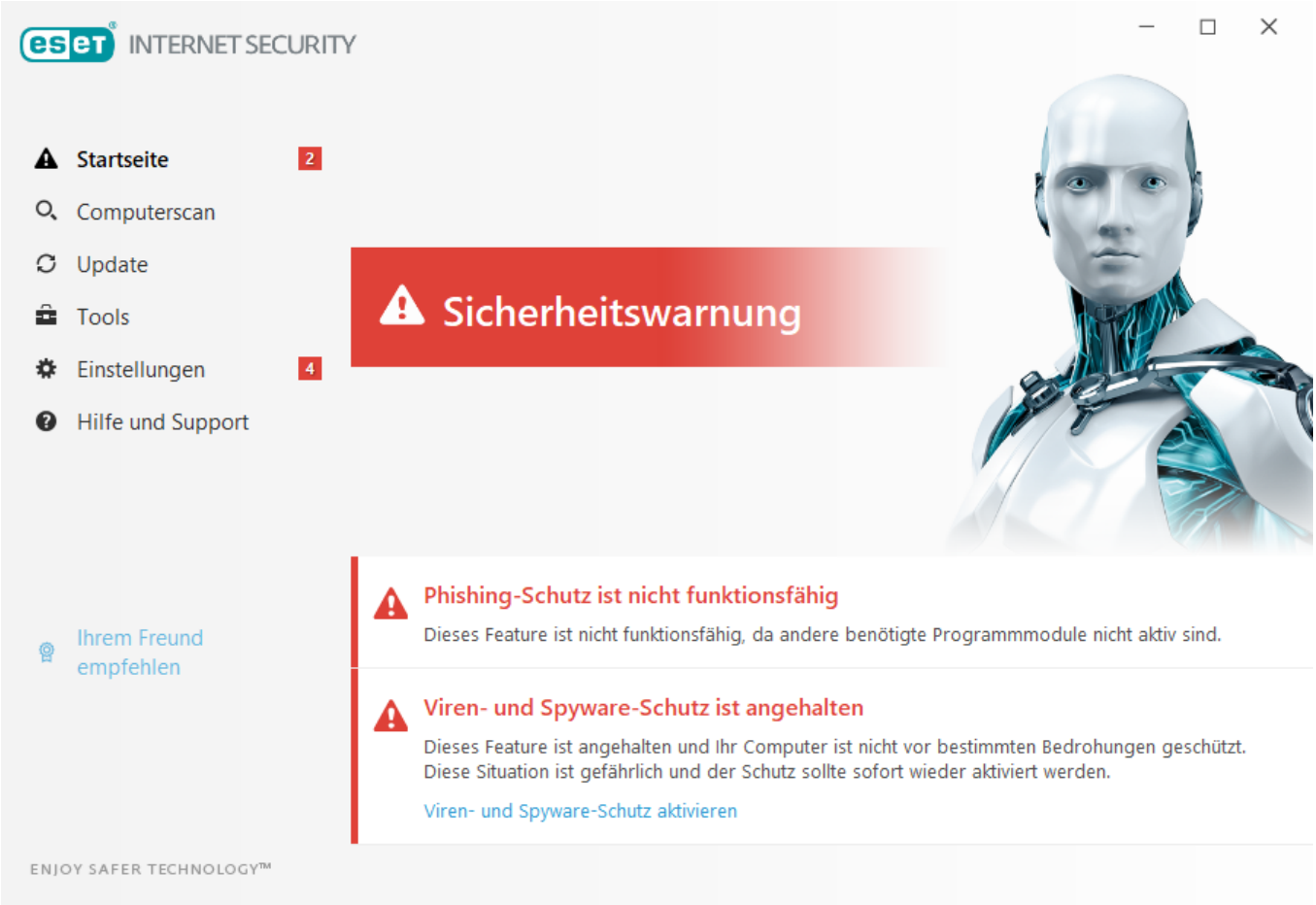
Hilfe und Support - Dieser Bereich bietet Zugriff auf die Hilfedateien, die ESET-Knowledgebase und die ESET-Website und enthält Links zum Übermitteln von Supportanfragen.

Die **Startseite** enthält Informationen über die aktuelle Schutzstufe Ihres Computers. Im Statusfenster werden die am häufigsten verwendeten Funktionen von ESET Internet Security angezeigt. Außerdem finden Sie hier Informationen über das zuletzt ausgeführte Update und das Ablaufdatum Ihrer Lizenz.

Das grüne Schutzstatussymbol zeigt an, dass **Maximaler Schutz** gewährleistet ist.

Vorgehensweise bei fehlerhafter Ausführung des Programms

Wenn ein aktiviertes Schutzmodul ordnungsgemäß arbeitet, wird ein grünes Schutzstatussymbol angezeigt. Ein rotes Ausrufezeichen oder ein orangefarbener Hinweis weisen auf ein nicht optimales Schutzniveau hin. Unter **Startseite** werden zusätzliche Informationen zum Schutzstatus der einzelnen Module und empfohlene Lösungen zum Wiederherstellen des vollständigen Schutzes angezeigt. Um den Status einzelner Module zu ändern, klicken Sie auf **Einstellungen** und wählen Sie das gewünschte Modul aus.



Das rote Symbol und der Status „Maximaler Schutz ist nicht gewährleistet“ weisen auf kritische Probleme hin. Dieser Status kann verschiedene Ursachen haben, zum Beispiel:

- **Produkt nicht aktiviert** – Sie können ESET Internet Security entweder auf der **Startseite** unter **Produkt aktivieren** oder unter Schutzstatus über die Schaltfläche **Jetzt kaufen** aktivieren.
- **Erkennungsroutine ist veraltet** - Dieser Fehler wird angezeigt, wenn die Erkennungsroutine trotz wiederholter Versuche nicht aktualisiert werden konnte. Sie sollten in diesem Fall die Update-Einstellungen überprüfen. Die häufigste Fehlerursache sind falsch eingegebene Lizenzdaten oder fehlerhaft konfigurierte Verbindungseinstellungen.
- **Viren- und Spyware-Schutz deaktiviert** – Sie können den Virenschutz und den Spyware-Schutz wieder aktivieren, indem Sie auf **Viren- und Spyware-Schutz aktivieren** klicken.
- **ESET Firewall deaktiviert** – Dieser Zustand wird durch einen Sicherheitshinweis neben **Netzwerk** auf Ihrem Desktop signalisiert. Sie können den Netzwerkschutz wieder aktivieren, indem Sie auf **Firewall aktivieren** klicken.
- **Lizenz abgelaufen** – Bei diesem Zustand ist das Schutzstatussymbol rot. Bei abgelaufener Lizenz kann das Programm keine Updates mehr durchführen. Führen Sie die in der Warnung angezeigten Anweisungen zur Verlängerung Ihrer Lizenz aus.

Das orangefarbene Symbol deutet auf eingeschränkten Schutz hin. Möglicherweise bestehen Probleme bei der Aktualisierung des Programms, oder Ihre Lizenz läuft demnächst ab.
Dieser Status kann verschiedene Ursachen haben, zum Beispiel:

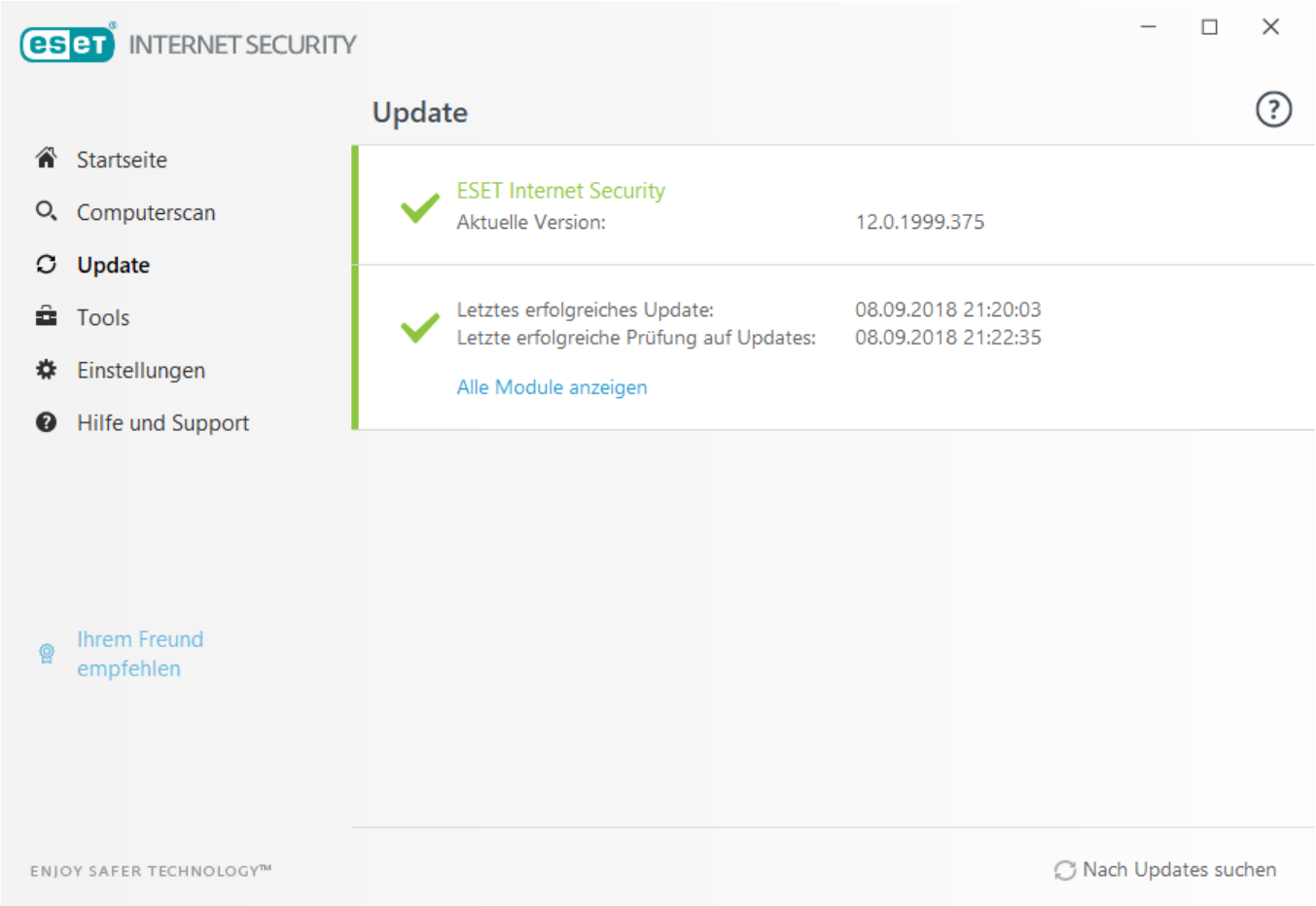
- **Gamer-Modus aktiviert** – Im Gamer-Modus besteht ein erhöhtes Risiko. Aktivieren Sie dieses Feature, um alle Popupfenster zu unterdrücken und alle geplanten Tasks zu beenden.
- **Lizenz läuft bald ab** – Dieser Status wird durch ein Schutzstatussymbol mit einem Ausrufezeichen neben der Systemuhr angezeigt. Nach dem Ablaufen der Lizenz ist kein Programm-Update mehr möglich und das Schutzstatussymbol ist rot.

Wenn Sie ein Problem mit den vorgeschlagenen Lösungen nicht beheben können, klicken Sie auf **Hilfe und Support**, um die Hilfedateien oder die ESET-Knowledgebase zu öffnen. Wenn Sie weiterhin Unterstützung benötigen, können Sie eine Support-Anfrage senden. Unser Support wird sich umgehend mit Ihnen in Verbindung setzen, um Ihre Fragen zu beantworten und Lösungen für Ihr Problem zu finden.

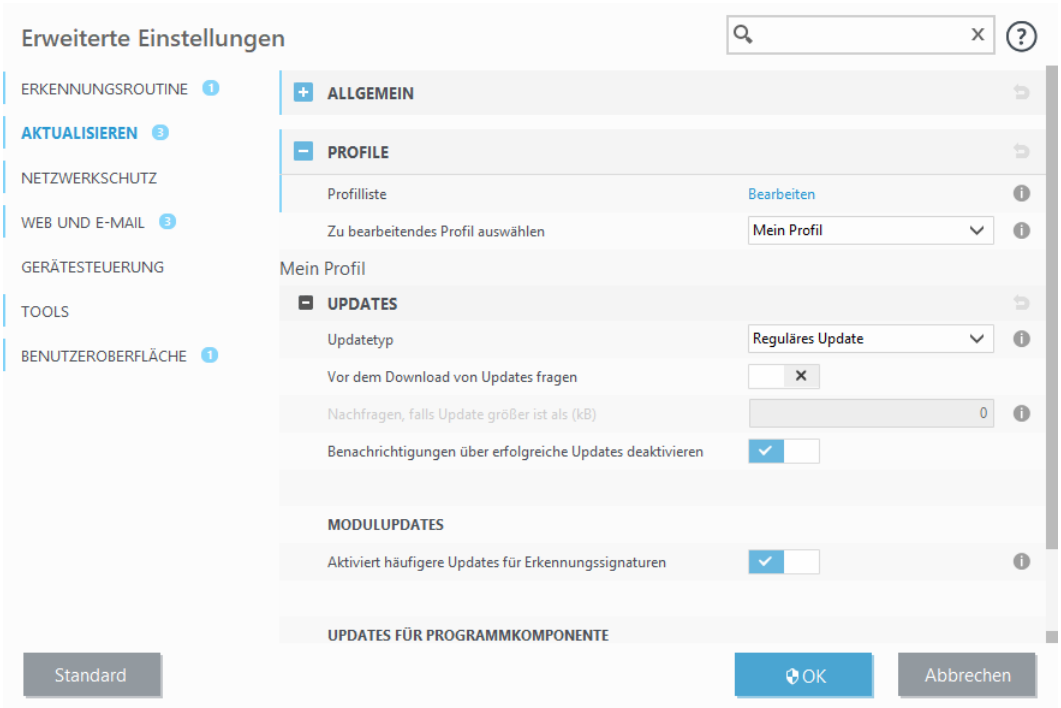
3.2 Updates

Updates der Erkennungsroutine und Updates von Programmkomponenten sind eine wichtige Maßnahmen, um Ihr System vor Schadcode zu schützen. Achten Sie auf eine sorgfältige Konfiguration und Ausführung der Updates. Klicken Sie im Hauptmenü auf **Update** und dann auf **Nach Updates suchen**, um nach einem Update für die Erkennungsroutine zu suchen.

Wenn der Lizenzschlüssel bei der Aktivierung von ESET Internet Security nicht eingegeben wurden, werden Sie nun dazu aufgefordert.



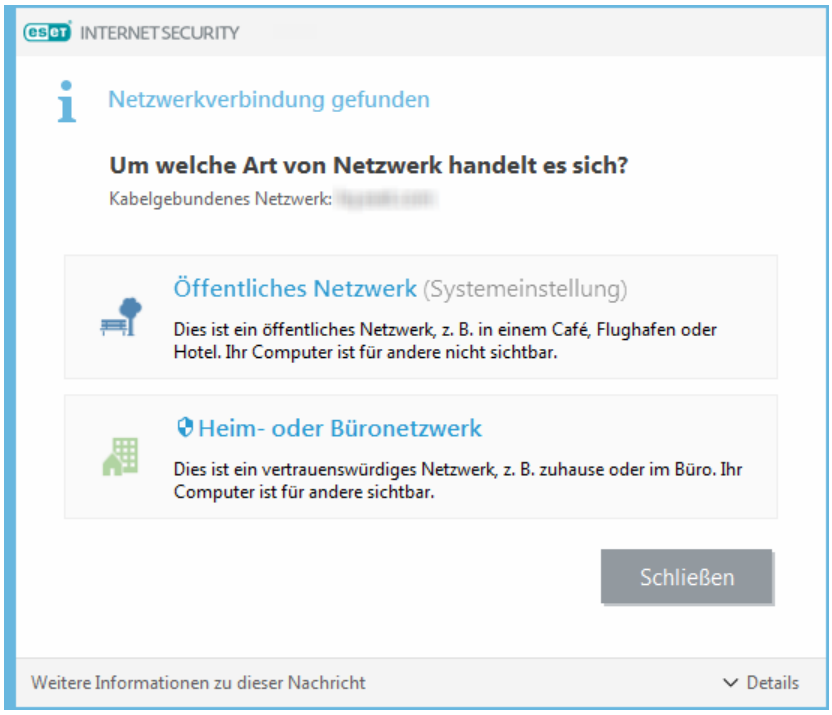
Das Fenster „Erweiterte Einstellungen“ (klicken Sie im Hauptmenü auf **Einstellungen** und dann auf **Erweiterte Einstellungen** oder drücken Sie die Taste **F5**) enthält zusätzliche Update-Optionen. Um erweiterte Update-Optionen wie den Update-Modus, den Proxyserverzugriff und die LAN-Verbindungen zu konfigurieren, klicken Sie auf die entsprechende Registerkarte im **Update**-Fenster.



3.3 Einstellungen vertrauenswürdige Zone

Die Einrichtung vertrauenswürdiger Zonen ist notwendig, um Ihren Computer in einer Netzwerkumgebung zu schützen. Sie können anderen Benutzern Zugriff auf Ihren Computer gewähren, indem Sie eine vertrauenswürdige Zone konfigurieren und Freigaben zulassen. Klicken Sie auf **Einstellungen** > **Netzwerk-Schutz** > **Verbundene Netzwerke**, und klicken Sie anschließend auf den Link unter dem verbundenen Netzwerk. In einem Fenster werden nun Optionen angezeigt, aus denen Sie den gewünschten Schutzmodus Ihres Computers im Netzwerk auswählen können.

Die Erkennung vertrauenswürdiger Zonen erfolgt nach der Installation von ESET Internet Security sowie jedes Mal, wenn Ihr Computer eine Verbindung zu einem neuen Netzwerk herstellt. Daher muss die vertrauenswürdige Zone nicht definiert werden. Standardmäßig wird bei Erkennung einer neuen Zone ein Dialogfenster angezeigt, in dem Sie die Schutzstufe für diese Zone festlegen können.



WARNUNG
Eine falsche Konfiguration der vertrauenswürdigen Zone kann ein Sicherheitsrisiko für Ihren Computer darstellen.

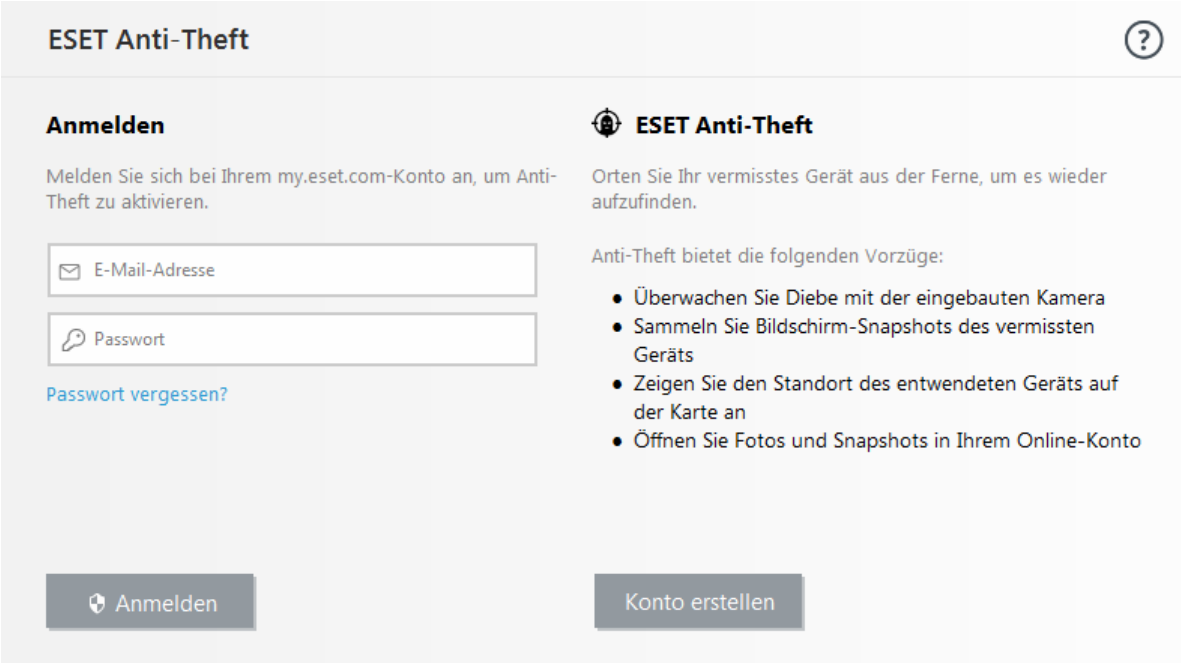
HINWEIS
Computer innerhalb der vertrauenswürdigen Zone erhalten standardmäßig Zugriff auf freigegebene Dateien und Drucker, die RPC-Kommunikation ist aktiviert, und Remotedesktopverbindungen sind möglich.

Weitere Details zu diesem Feature finden Sie im folgenden ESET Knowledgebase-Artikel:
Neue Netzwerkverbindung erkannt in ESET Smart Security

3.4 Anti-Theft

Um Ihren Computer im Falles eines Verlusts oder Diebstahls zu schützen, können Sie ihn über eine der folgenden Optionen beim ESET Anti-Theft-System registrieren.

1. Klicken Sie nach der erfolgreichen Aktivierung auf **Anti-Theft aktivieren**, um die Funktionen von ESET Anti-Theft für den soeben registrierten Computer zu aktivieren.
2. Wenn der Hinweis **ESET Anti-Theft ist verfügbar** auf der **Startseite** von ESET Internet Security angezeigt wird, sollten Sie abwägen, ob Sie diese Funktion für Ihren Computer aktivieren möchten. Klicken Sie auf **ESET Anti-Theft Aktivieren**, um Ihren Computer bei ESET Anti-Theft zu registrieren.
3. Klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Sicherheits-Tools.** Klicken Sie auf neben **ESET Anti-Theft**, und folgen Sie den Anweisungen im Popupfenster.



HINWEIS
ESET Anti-Theft ist nicht für den Einsatz auf Microsoft Windows Home Server geeignet.

Weitere Informationen über das Verknüpfen von Computern mit ESET Anti-Theft finden Sie unter Hinzufügen eines neuen Geräts.

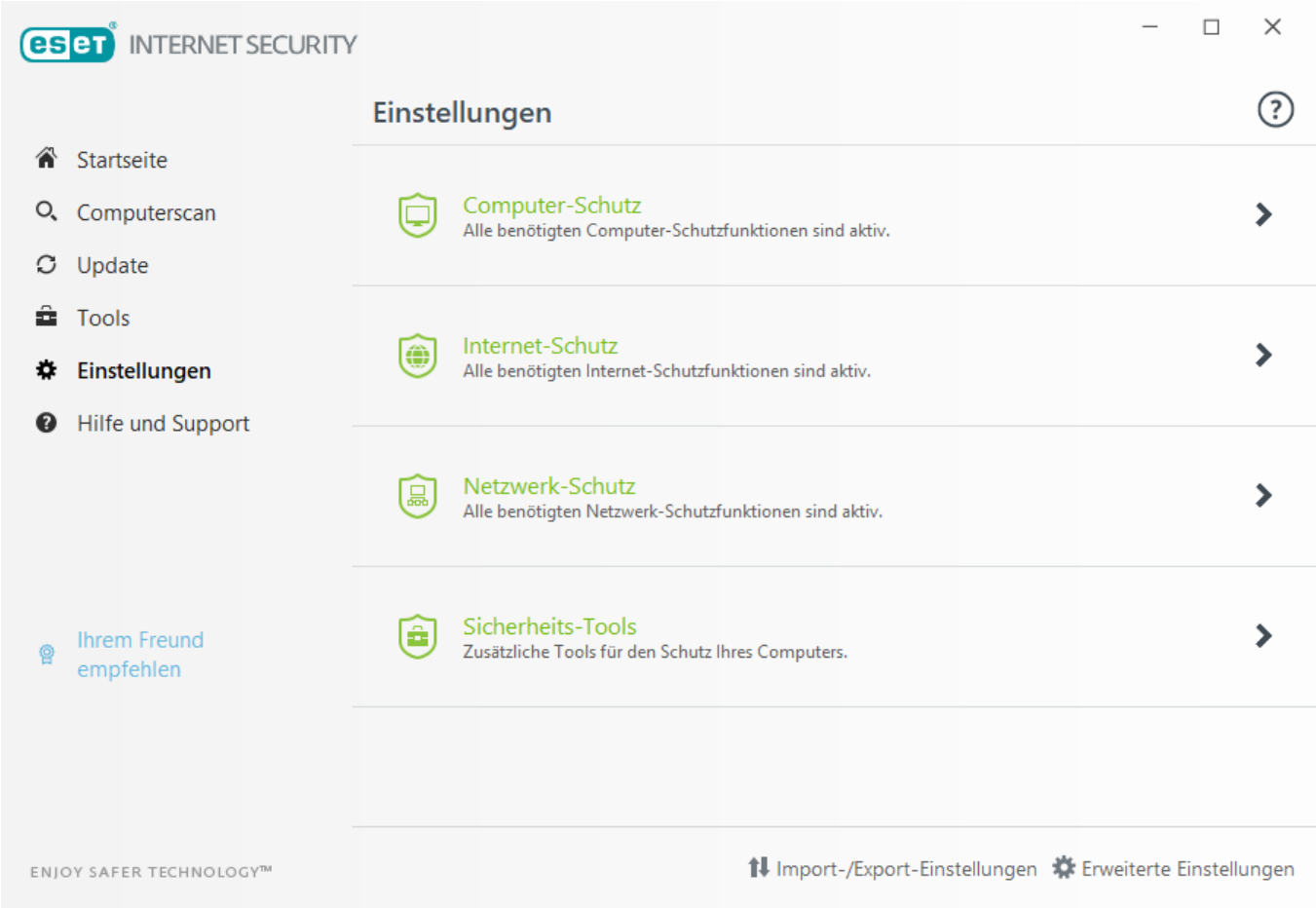
3.5 Kindersicherungs-Tools

Auch wenn Sie die Kindersicherung in ESET Internet Security bereits aktiviert haben, müssen Sie sie für die gewünschten Benutzerkonten konfigurieren, damit sie ordnungsgemäß funktioniert.

Wenn die Kindersicherung aktiviert, jedoch keine Benutzerkonten konfiguriert wurden, wird der Hinweis **Kindersicherung nicht eingerichtet** auf der **Startseite** des Hauptprogrammfensters angezeigt. Klicken Sie auf **Regeln jetzt einrichten** und erstellen Sie Regeln, um Ihre Kinder vor ungeeigneten Inhalten zu schützen. Hinweise zum Erstellen von Regeln finden Sie im Kapitel Kindersicherung.

4. Arbeiten mit ESET Internet Security

ESET Internet Security Mit den Konfigurationsoptionen können Sie Feinabstimmungen rund um den Schutz Ihres Computers vornehmen und das Netzwerk anpassen.



Das Menü **Einstellungen** enthält die folgenden Bereiche:

Computer-Schutz
Internet-Schutz
Netzwerk-Schutz
Sicherheits-Tools

Klicken Sie auf eine Komponente, um die erweiterten Einstellungen des entsprechenden Schutzmoduls anzupassen.

In den Einstellungen für den Computer-Schutz können Sie folgende Komponenten aktivieren oder deaktivieren:

- **Echtzeit-Dateischutz** – Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Ihrem Computer auf Schadcode geprüft.
- **HIPS** – Das HIPS-System überwacht Ereignisse auf Betriebssystemebene und führt Aktionen gemäß individueller Regeln aus.
- **Gamer-Modus** – Aktiviert / deaktiviert den Gamer-Modus. Nach der Aktivierung des Gamer-Modus wird eine Warnung angezeigt (erhöhtes Sicherheitsrisiko) und das Hauptfenster wird orange.
- **Webcam-Schutz** – Kontrolliert Prozesse und Anwendungen, die auf die Webcam Ihres Computers zugreifen. Weitere Informationen erhalten Sie hier.

In den Einstellungen für den Internet-Schutz können Sie folgende Komponenten aktivieren oder deaktivieren:

- **Web-Schutz** – Wenn diese Option aktiviert ist, werden alle Daten geprüft, die über HTTP oder HTTPS übertragen werden.
- **E-Mail-Schutz** – Überwacht eingehende E-Mails, die mit dem POP3- oder dem IMAP-Protokoll übertragen werden.
- **Spam-Schutz** – Prüft unerwünschte E-Mails, also Spam.
- **Phishing-Schutz** – Filtert Websites, für die der Verdacht besteht, dass sie Inhalte enthalten, die den Benutzer zum Einreichen vertraulicher Informationen verleiten.

Im Bereich **Netzwerk-Schutz** können Sie die Funktionen Firewall, Netzwerkangriffsschutz (IDS) und Botnetschutz aktivieren bzw. deaktivieren.

Im Sicherheits-Tools-Setup können Sie die folgenden Module konfigurieren:

- Online-Banking-Zahlungsschutz
- Kindersicherung
- Anti-Theft

Mit der Kindersicherung können Sie Webseiten sperren, die potenziell Unerlaubtes enthalten könnten. Außerdem können Eltern mit dieser Funktion den Zugriff auf über 40 vordefinierte Webseitenkategorien und über 140 Unterkategorien unterbinden.

Zur Reaktivierung des Schutzes dieser Sicherheitskomponente klicken Sie auf den Schieberegler  damit ein grünes Häkchen  angezeigt wird.

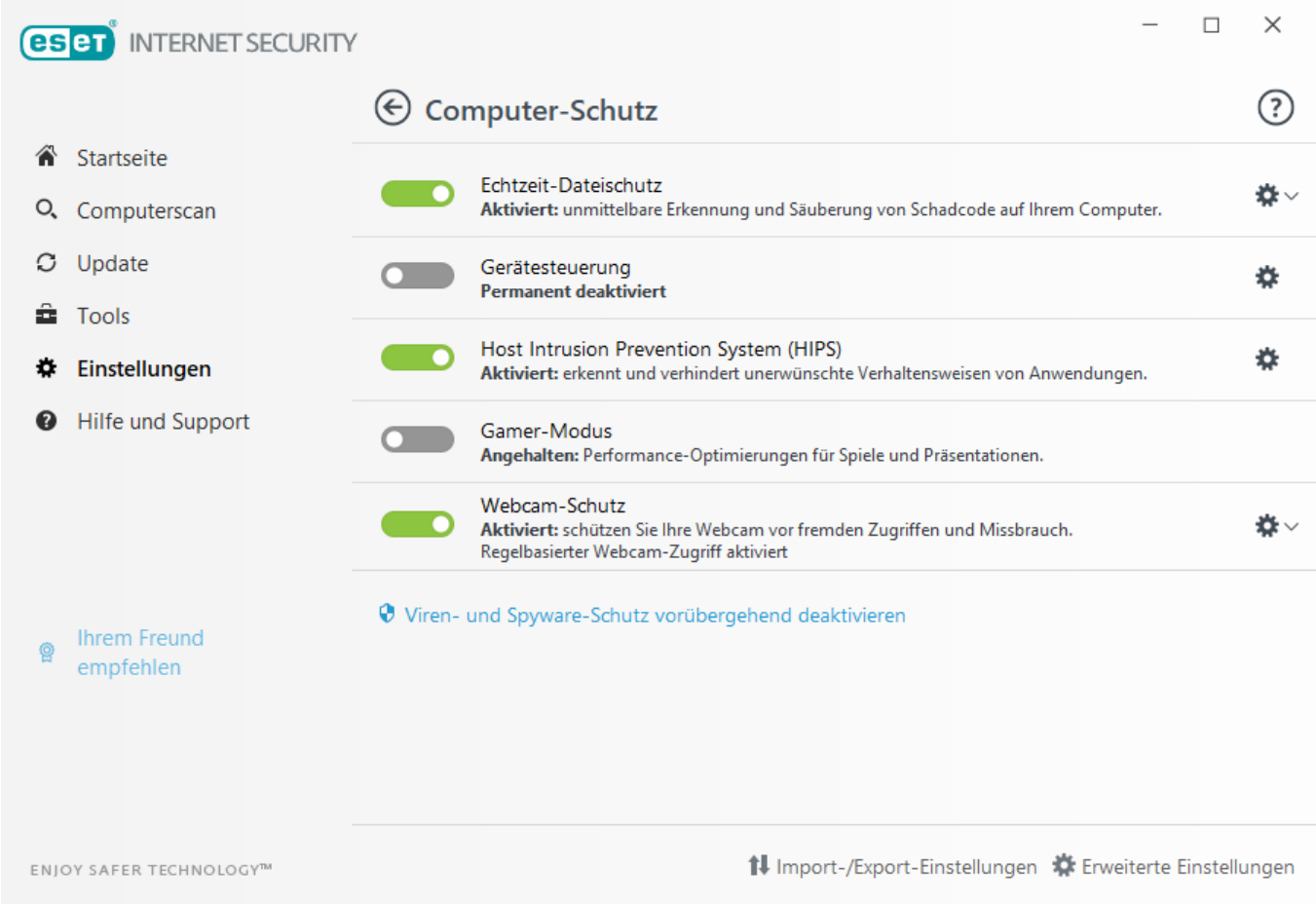
HINWEIS
Wenn Sie den Schutz auf diese Weise deaktivieren, werden alle deaktivierten Schutzmodule nach einem Computerneustart wieder aktiviert.

Am unteren Rand des Fensters „Einstellungen“ finden Sie weitere Optionen. Über den Link **Erweiterte Einstellungen** können Sie weitere Parameter für die einzelnen Module konfigurieren. Unter **Einstellungen importieren/exportieren** können Sie Einstellungen aus einer *.XML*-Konfigurationsdatei laden oder die aktuellen Einstellungen in einer Konfigurationsdatei speichern.

4.1 Computer-Schutz

Klicken Sie im Einstellungsfenster auf „Computer-Schutz“, um eine Übersicht aller Schutzmodule anzuzeigen. Klicken Sie auf , um einzelne Module vorübergehend zu deaktivieren. Beachten Sie, dass dies den Schutz Ihres Computers beeinträchtigen kann. Klicken Sie auf neben einem Schutzmodul, um erweiterte Einstellungen für dieses Modul zu öffnen.

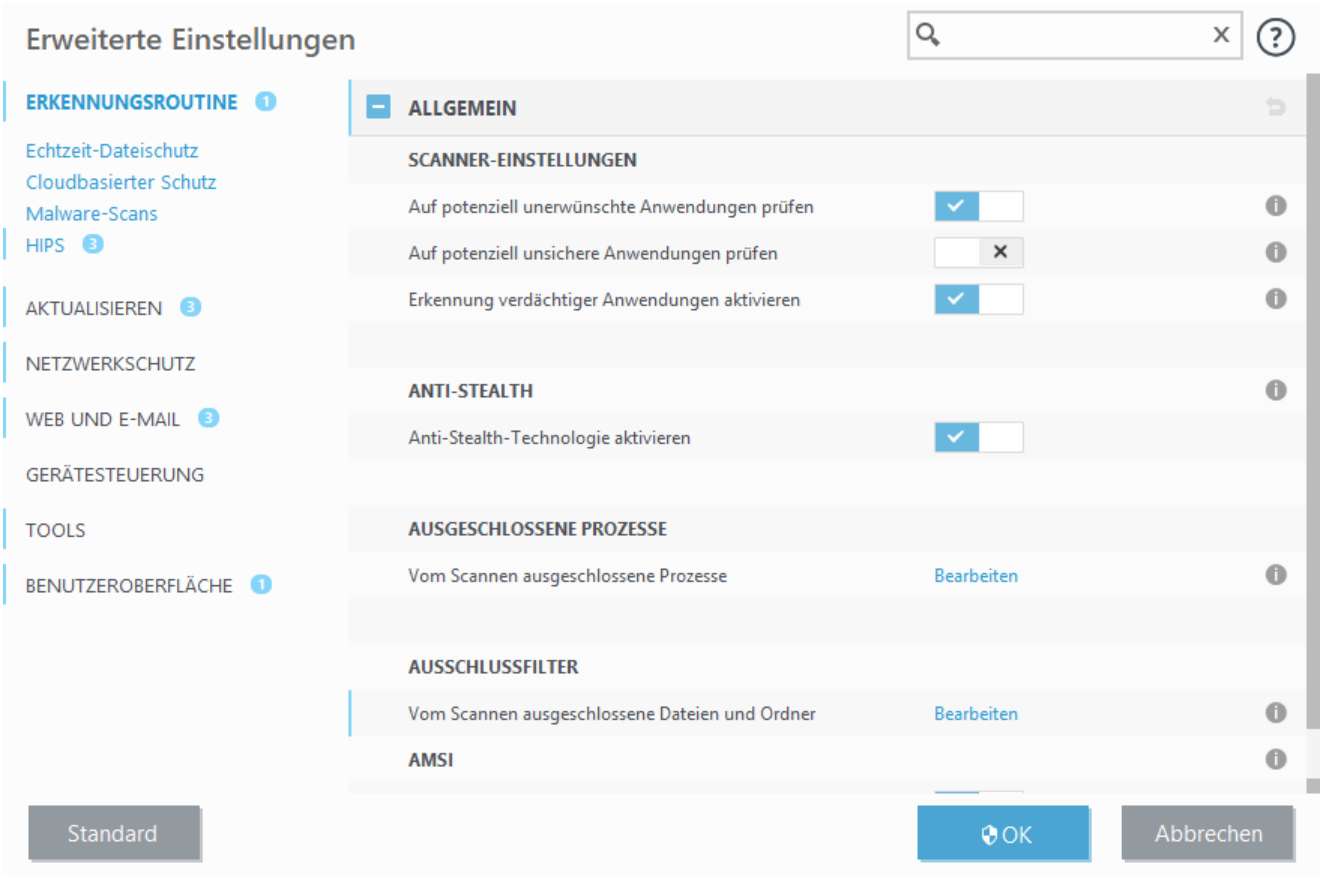
Klicken Sie auf > **Ausschlussfilter bearbeiten** neben **Echtzeit-Dateischutz**, um das Fenster für die Ausschlussfilter-Einstellungen zu öffnen und Dateien und Ordner von der Prüfung auszuschließen.



Viren- und Spyware-Schutz vorübergehend deaktivieren – Deaktiviert alle Viren- und Spyware-Schutzmodule. Wenn Sie den Schutz deaktivieren, wird ein Fenster geöffnet, in dem Sie über das Dropdownmenü **Zeitraum** festlegen können, wie lange der Schutz deaktiviert werden soll. Klicken Sie auf **Übernehmen**, um Ihre Auswahl zu bestätigen.

4.1.1 Erkennungsroutine

Virenschutzlösungen bieten durch Überwachung der Daten-, E-Mail- und Internet-Kommunikation Schutz vor bösartigen Systemangriffen. Wird eine Bedrohung durch Schadcode erkannt, kann das Virenschutz-Modul den Code unschädlich machen, indem es zunächst die Ausführung des Codes blockiert und dann den Code entfernt bzw. die Datei löscht oder in die Quarantäne verschiebt.



Über die Einstellungen für Prüfungen der verschiedenen Schutzmodule (Echtzeit-Dateischutz, Web-Schutz usw.) können Sie die Erkennung folgender Elemente aktivieren und deaktivieren:

- **Eventuell unerwünschte Anwendungen** sind Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, aber auf Leistung und Verhalten Ihres Computers negative Auswirkungen haben können.
  Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.
- **Potenziell unsichere Anwendungen** stellen gewerbliche Software dar, die zu einem böswilligen Zweck missbraucht werden kann. Beispiele für potenziell unsichere Anwendungen sind Programme für das Fernsteuern von Computern (Remotedesktopverbindung), Programme zum Entschlüsseln von Passwörtern und Keylogger (Programme, die aufzeichnen, welche Tasten vom Benutzer gedrückt werden). Diese Option ist in der Voreinstellung deaktiviert.
  Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.
- **Verdächtige Anwendungen** sind Programme, die mit Packprogrammen oder Schutzprogrammen komprimiert wurden. Diese Schutzarten werden oft von Verfassern von Schadcode eingesetzt, um die Erkennung zu umgehen.

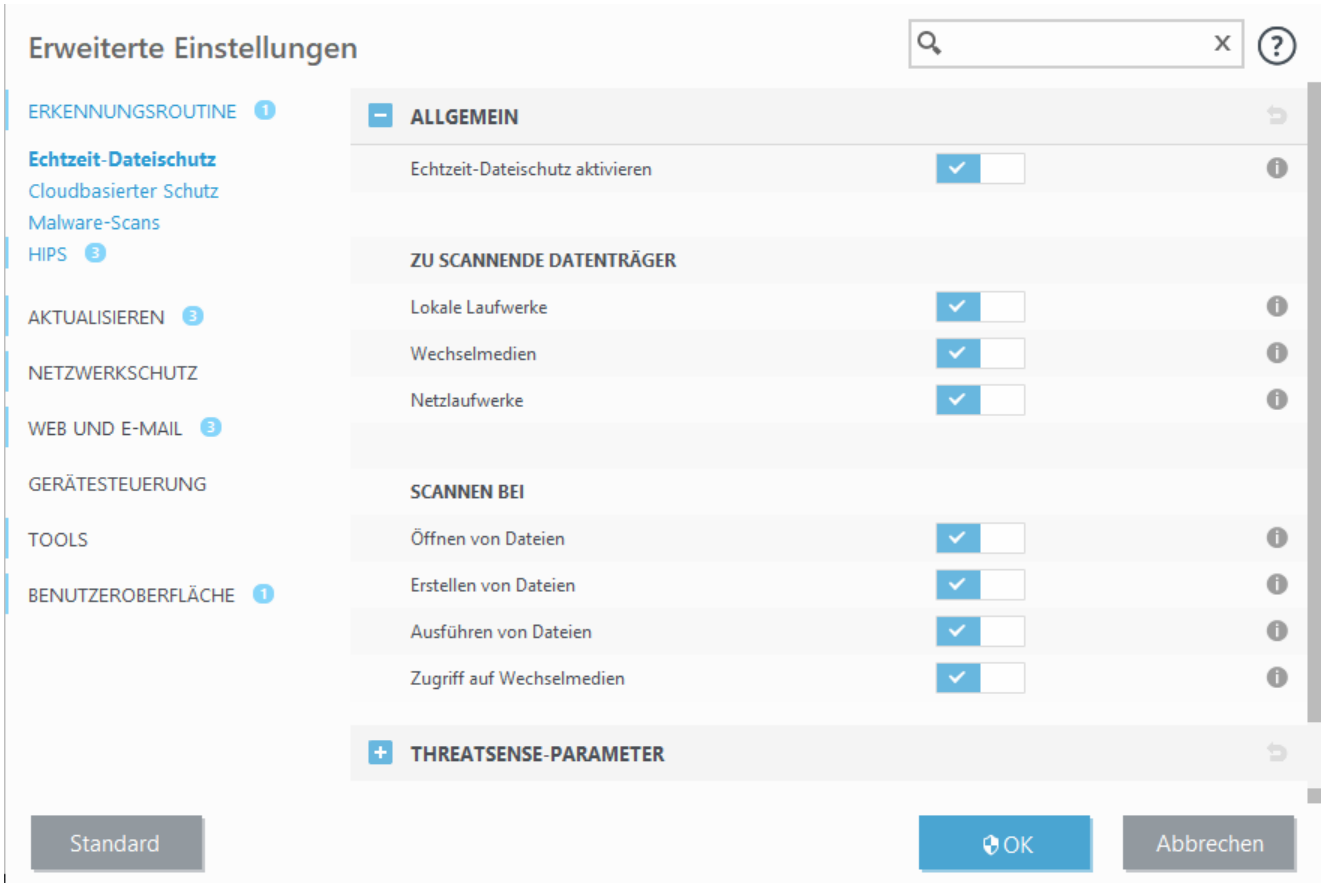
Die **Anti-Stealth-Technologie** ist ein fortschrittliches System zur Erkennung gefährlicher Programme wie Rootkits, die sich vor dem Betriebssystem verstecken können. Aus diesem Grund ist es nahezu unmöglich, sie mit herkömmlichen Prüfmethoden zu erkennen.

Mit dem **Ausschlussfilter** können Sie festlegen, welche Dateien und Ordner von Prüfungen ausgenommen werden sollen. Um zu gewährleisten, dass möglichst alle Objekte auf Bedrohungen geprüft werden, empfehlen wir, nur bei dringendem Bedarf Ausnahmen zu erstellen. In bestimmten Fällen kann es jedoch erforderlich sein, ein Objekt von der Prüfung auszuschließen, beispielsweise bei großen Datenbankeinträgen, deren Prüfung die Computerleistung zu stark beeinträchtigen würde, oder bei Software, die Konflikte mit der Prüfung verursacht. Informationen dazu, wie Sie ein Objekt von Prüfungen ausschließen, finden Sie unter Ausschlussfilter.

Erweiterte AMSI-Prüfung aktivieren – Mit der Anti-Malware-Prüfschnittstelle von Microsoft können Anwendungsentwickler neue Verteidigungsmaßnahmen entwickeln (nur Windows 10).

4.1.1.1 Echtzeit-Dateischutz

Der Echtzeit-Dateischutz überwacht alle für den Virenschutz relevanten Systemereignisse. Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Ihrem Computer auf Schadcode geprüft. Der Echtzeit-Dateischutz wird beim Systemstart gestartet.



Der Echtzeit-Dateischutz wird standardmäßig beim Systemstart gestartet und fortlaufend ausgeführt. In Ausnahmefällen (z. B. bei einem Konflikt mit einer anderen Echtzeitprüfung) kann der Echtzeit-Dateischutz deaktiviert werden. Deaktivieren Sie dazu die Option **Echtzeit-Dateischutz aktivieren** im Bereich **Echtzeit-Dateischutz** > **Einfach** in den **erweiterten Einstellungen**.

Zu scannende Datenträger

In der Standardeinstellung werden alle Datenträger auf mögliche Bedrohungen geprüft:

Lokale Laufwerke – Geprüft werden alle lokalen Laufwerke.
Wechselmedien – Geprüft werden /DVDs, USB-Speichergeräte, Bluetooth-Geräte usw.
Netzlaufwerke – Geprüft werden alle zugeordneten Netzlaufwerke.

Es wird empfohlen, diese Einstellungen nur in Ausnahmefällen zu ändern, z. B. wenn die Prüfung bestimmter Datenträger die Datenübertragung deutlich verlangsamt.

Prüfen bei

Standardmäßig werden alle Dateien beim Öffnen, Erstellen und Ausführen geprüft. Wir empfehlen Ihnen, die Standardeinstellungen beizubehalten. So bietet der Echtzeit-Dateischutz auf Ihrem Computer maximale Sicherheit:

- **Öffnen von Dateien** – Prüfen von Dateien beim Öffnen aktivieren/deaktivieren.
- **Erstellen von Dateien** – Prüfen von Dateien beim Erstellen aktivieren/deaktivieren.
- **Dateiausführung** – Prüfen von Dateien beim Ausführen aktivieren/deaktivieren.
- **Wechselmedienzugriff** – Prüfen beim Zugriff auf Wechselmedien mit Speicherplatz aktivieren/deaktivieren.

Der Echtzeit-Dateischutz überwacht alle Datenträger auf das Eintreten bestimmter Ereignisse wie den Zugriff auf eine Datei. Mit den ThreatSense-Erkennungsmethoden (siehe Abschnitt Einstellungen für ThreatSense) kann der Echtzeit-Dateischutz so konfiguriert werden, dass neu erstellte und vorhandene Dateien unterschiedlich behandelt werden. Sie können den Echtzeit-Dateischutz z. B. so konfigurieren, dass neuere Dateien genauer überwacht werden.

Bereits geprüfte Dateien werden nicht erneut geprüft (sofern sie nicht geändert wurden), um die Systembelastung durch den Echtzeit-Dateischutz möglichst gering zu halten. Nach einem Update der Erkennungsroutine werden die Dateien sofort wieder geprüft. Dieses Verhalten wird mit der **Smart-Optimierung** gesteuert. Wenn die **Smart-Optimierung** deaktiviert ist, werden alle Dateien bei jedem Zugriff geprüft. Um diese Einstellung zu ändern, öffnen Sie die **erweiterten Einstellungen** durch Drücken der Taste **F5** und erweitern Sie anschließend den Eintrag **Erkennungsroutine** > **Echtzeit-Dateischutz**. Klicken Sie auf Einstellungen für **ThreatSense** > **Sonstige** und aktivieren bzw. deaktivieren Sie die Option **Smart-Optimierung aktivieren**.

4.1.1.1.1 Zusätzliche ThreatSense-Parameter

Zusätzliche ThreatSense-Parameter für neu erstellte und geänderte Dateien

Das Infektionsrisiko für neu erstellte oder geänderte Dateien ist vergleichsweise größer als für vorhandene Dateien. Daher prüft das Programm solche Dateien mit zusätzlichen Parametern. ESET Internet Security verwendet Advanced Heuristik zusammen mit signaturbasierten Prüfmethoden, um neue Bedrohungen zu erkennen, bevor ein Update der Erkennungsroutine veröffentlicht wird. Neben neu erstellten Dateien werden auch **selbstentpackende Archive** (SFX) und **laufzeitkomprimierte Dateien** (intern komprimierte, ausführbare Dateien) geprüft. In den Standardeinstellungen werden Archive unabhängig von ihrer tatsächlichen Größe bis zur zehnten Verschachtelungsebene geprüft. Deaktivieren Sie die Option **Standardeinstellungen Archivprüfung**, um die Archivprüfeinstellungen zu ändern.

Zusätzliche ThreatSense-Parameter für ausführbare Dateien

Advanced Heuristik bei der Dateiausführung - Standardmäßig wird bei der Dateiausführung keine Advanced Heuristik verwendet. Wenn diese Option aktiviert ist, sollten Smart-Optimierung und ESET LiveGrid® unbedingt aktiviert bleiben, um die Auswirkungen auf die Systemleistung gering zu halten.

Advanced Heuristik bei der Ausführung von Dateien auf Wechselmedien – Advanced Heuristik emuliert Code in einer virtuellen Umgebung und prüft dessen Verhalten, bevor der Code von einem Wechseldatenträger ausgeführt wird.

4.1.1.1.2 Säuberungsstufen

Für den Echtzeit-Dateischutz stehen drei Säuberungsstufen zur Verfügung. Sie finden diese Stufen unter **Einstellungen für ThreatSense** im Bereich **Echtzeit-Dateischutz** unter **Säubern**.

Nicht säubern – Der in infizierten Objekten erkannte Schadcode wird nicht automatisch entfernt. Eine Warnung wird angezeigt, und der Benutzer wird aufgefordert, eine Aktion auszuwählen. Diese Stufe eignet sich für fortgeschrittene Benutzer, die wissen, wie sie im Falle eingedrungener Schadsoftware vorgehen sollen.

Normale Säuberung – Das Programm versucht, infizierte Dateien automatisch zu säubern oder zu löschen. Es wendet hierzu vordefinierte Aktionen an (je nach Art der Infiltration). Ein Hinweis am unteren rechten Bildschirmrand informiert über die Erkennung und das Löschen infizierter Dateien. Wenn es nicht möglich ist, die angemessene Aktion automatisch zu bestimmen, schlägt das Programm verschiedene Aktionen vor. Dies gilt auch für Fälle, in denen eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden kann.

Immer versuchen, automatisch zu säubern – Das Programm entfernt den Schadcode aus infizierten Dateien oder löscht diese Dateien. Ausnahmen gelten nur für Systemdateien. Wenn es nicht möglich ist, den Schadcode zu entfernen, wird der Benutzer aufgefordert, eine Aktion auszuwählen.

WARNUNG
Wenn infizierte Dateien in einem Archiv gefunden werden, sind zwei Vorgehensweisen möglich. Im Standardmodus (normales Säubern) wird die Archivdatei nur dann gelöscht, wenn alle Dateien im Archiv infiziert sind. Wenn die Option **Immer versuchen, automatisch zu entfernen** aktiviert ist, wird die Archivdatei gelöscht,

sobald eine einzige Datei im Archiv infiziert ist.

4.1.1.1.3 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?

Der Echtzeit-Dateischutz ist die wichtigste Komponente für ein sicheres System. Daher sollte gründlich geprüft werden, ob eine Änderung der Einstellungen wirklich notwendig ist. Es wird empfohlen, seine Parameter nur in einzelnen Fällen zu verändern.

Bei der Installation von ESET Internet Security werden alle Einstellungen optimal eingerichtet, um dem Benutzer die größtmögliche Schutzstufe für das System zu bieten. Wenn Sie die Standardeinstellungen wiederherstellen möchten, klicken Sie neben den Registerkarten im Fenster (**Erweiterte Einstellungen** > **Erkennungsroutine** > **Echtzeit-Dateischutz**) auf .

4.1.1.1.4 Echtzeit-Dateischutz prüfen

Um sicherzustellen, dass der Echtzeit-Dateischutz aktiv ist und Viren erkennt, verwenden Sie eine Testdatei von eicar.com. Diese Testdatei ist harmlos und wird von allen Virenschutzprogrammen erkannt. Die Datei wurde von der Firma EICAR (European Institute for Computer Antivirus Research) erstellt, um die Funktionalität von Virenschutzprogrammen zu testen. Die Datei kann unter http://www.eicar.org/download/eicar.com heruntergeladen werden.

HINWEIS
Bevor Sie eine Prüfung des Echtzeit-Dateischutzes durchführen, müssen Sie die Firewall deaktivieren. Bei aktivierter Firewall wird die Datei erkannt, und die Testdateien können nicht heruntergeladen werden.

4.1.1.1.5 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz

In diesem Kapitel werden mögliche Probleme mit dem Echtzeit-Dateischutz sowie Lösungsstrategien beschrieben.

Echtzeit-Dateischutz ist deaktiviert

Der Echtzeit-Dateischutz wurde versehentlich von einem Benutzer deaktiviert und muss reaktiviert werden. Um den Echtzeit-Dateischutz erneut zu aktivieren, klicken Sie im Hauptprogrammfenster auf **Einstellungen** und dann auf **Computer-Schutz** > **Echtzeit-Dateischutz**.

Wenn der Echtzeit-Dateischutz beim Systemstart nicht initialisiert wird, ist die Option **Echtzeit-Dateischutz aktivieren** vermutlich deaktiviert. Um diese Option zu aktivieren, klicken Sie unter **Erweiterte Einstellungen** (**F5**) auf **Virenschutz** > **Echtzeit-Dateischutz**.

Echtzeit-Dateischutz erkennt und entfernt keinen Schadcode

Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Zwei parallel installierte Antivirenprogramme können Konflikte verursachen. Wir empfehlen Ihnen, vor der Installation von ESET alle anderen Virusschutzprogramme zu deinstallieren.

Echtzeit-Dateischutz startet nicht

Wenn der Echtzeit-Dateischutz beim Systemstart nicht initialisiert wird (und die Option **Echtzeit-Dateischutz aktivieren** aktiviert ist), kann dies an Konflikten mit anderen Programmen liegen. Sollte dies der Fall sein, wenden Sie sich an den ESET-Support.

4.1.1.2 Computerprüfung

Die manuelle Prüfung ist ein wichtiger Teil Ihrer Virenschutzlösung. Sie dient zur Prüfung von Dateien und Ordnern auf dem Computer. Aus Sicherheitsgründen sollten Sie Ihren Computer regelmäßig im Rahmen Ihrer Sicherheitsvorkehrungen prüfen, und nicht nur bei Infektionsverdacht. Es wird empfohlen, regelmäßig eine umfassende Prüfung des Computers vorzunehmen, um Viren zu entdecken, die nicht vom Echtzeit-Dateischutz erfasst wurden, als sie auf die Festplatte gelangten. Dies kommt z. B. vor, wenn der Echtzeit-Dateischutz zu diesem Zeitpunkt deaktiviert oder die Erkennungsroutine nicht auf dem neuesten Stand ist oder die Datei beim Speichern auf dem Datenträger nicht als Virus erkannt wird.

Die hierfür vorgesehene Funktion **Computerprüfung** hat zwei Unterbefehle. **Scannen Sie Ihren Computer** führt eine schnelle Systemprüfung ohne spezielle Prüfparameter durch.Unter **Benutzerdefinierte Prüfung können** Sie eines der vordefinierten Prüfprofile für bestimmte Speicherorte auswählen oder bestimmte zu prüfende Objekte festlegen.

Scannen Sie Ihren Computer

Mit der Option „Scannen Sie Ihren Computer“ können Sie eine schnelle Systemprüfung durchführen und infizierte Dateien entfernen, ohne eingreifen zu müssen. Ihr Vorteil dieser Option ist die einfache Bedienung, bei der Sie keine detaillierten Prüfeinstellungen festlegen müssen. Bei dieser Prüfung werden alle Dateien auf lokalen Laufwerken geprüft, und erkannte eingedrungene Schadsoftware wird automatisch entfernt. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Säuberungstypen finden Sie unter Säubern.

Mit der Funktion **Prüfen per Ziehen und Ablegen** können Sie Dateien und Ordner manuell prüfen. Klicken Sie dazu auf die Datei bzw. den Ordner, bewegen Sie den Mauszeiger bei gedrückter Maustaste über den markierten Bereich, und lassen Sie die Maustaste los. Anschließend wird die Anwendung in den Vordergrund verschoben.

Die folgenden Prüfoptionen sind unter **Erweiterte Prüfungen** verfügbar:

Benutzerdefinierte Prüfung

Bei der Benutzerdefinierten Prüfung können Sie verschiedene Prüfparameter festlegen, z. B. die zu prüfenden Objekte und die Prüfmethoden. Der Vorteil dieser Methode ist die Möglichkeit zur genauen Parameterkonfiguration. Verschiedene Konfigurationen können in benutzerdefinierten Prüfprofilen gespeichert werden. Das ist sinnvoll, wenn Prüfungen wiederholt mit denselben Parametern ausgeführt werden.

Wechselmedien prüfen

Diese Prüfung ähnelt der Option „Computerprüfung“ und ermöglicht ein schnelles Prüfen der aktuell an den Computer angeschlossenen Wechselmedien (wie CD/DVD/USB). Dies ist hilfreich, wenn Sie beispielsweise ein USB-Speichergerät an den Computer anschließen und den Inhalt auf Schadcode und sonstige mögliche Bedrohungen untersuchen möchten.

Sie können diese Prüfung auch über **Benutzerdefinierte Prüfung** starten, indem Sie im Dropdown-Menü **Zu prüfende Objekte** den Eintrag **Wechselmedien** auswählen und auf **Prüfen** klicken.

Letzte Prüfung wiederholen

Mit dieser Option können Sie die zuletzt ausgeführte Prüfung mit denselben Parametern wiederholen.

Weitere Informationen zum Prüfprozess finden Sie im Abschnitt Stand der Prüfung.

HINWEIS
Sie sollten mindestens einmal im Monat eine Prüfung des Computers vornehmen. Sie können die Prüfungen als Task unter **Tools** > **> Weitere Tools** > **Taskplaner**. So planen Sie eine wöchentliche Computerprüfung

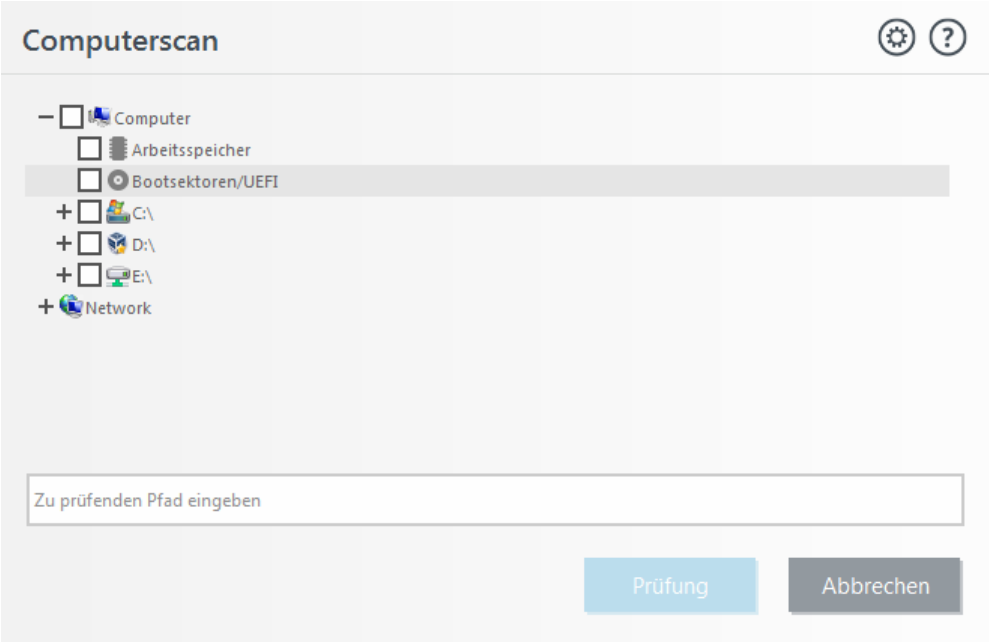
4.1.1.2.1 Benutzerdefinierte Prüfung

Mit der benutzerdefinierten Prüfung können Sie Teile eines Laufwerks anstelle des gesamten Laufwerks überprüfen. Klicken Sie auf **Erweiterte Prüfungen** > **Benutzerdefinierte Prüfung** und wählen Sie eine Option im Dropdownmenü **Prüfziele** aus, oder legen Sie die Prüfziele in der Baumstruktur fest.

Im Dropdown-Menü **Zu prüfende Objekte** können Sie vordefinierte Optionen für die zu prüfenden Objekte auswählen.

- **Nach Profileinstellungen** - Im Prüfprofil festgelegte Prüfziele.
- **Wechselmedien** - Disketten, USB-Speichergeräte, CDs/DVDs.
- **Lokale Laufwerke** - Alle lokalen Systemlaufwerke.
- **Netzlaufwerke** - Alle zugeordneten Netzlaufwerke.
- **Keine Auswahl** - Bricht die Zielauswahl ab.

Geben Sie das Zielverzeichnis in das leere Textfeld unter der Ordnerliste ein, um schnell zu einem Prüfziel zu navigieren oder um Ordner oder Dateien hinzuzufügen. Dies ist nur möglich, wenn keine Objekte aus der Baumstruktur zur Prüfung ausgewählt wurden und im Menü **Prüfziele** die Option **Keine Auswahl** festgelegt ist.



Sie können die Säuberungsparameter für die Prüfung unter **Erweiterte Einstellungen** > **Erkennungsroutine** > **On-Demand-Prüfung** > **ThreatSense-Parameter** > **Säuberung festlegen.** Wählen Sie **Nur prüfen, keine Aktion** aus, um eine Prüfung ohne Säuberungsaktion durchzuführen. Der Prüfungsverlauf wird im Prüfung-Log gespeichert.

Mit der Option **Ausschlüsse ignorieren** werden Dateien mit den zuvor ausgeschlossenen Erweiterungen ohne Ausnahme geprüft.

Im Dropdownmenü **Scan-Profil** können Sie ein Scan-Profil für bestimmte Ziele auswählen. Das Standardprofil ist **Smart-Scan**. Außerdem haben Sie zwei weitere vordefinierte Prüfprofile zur Auswahl: **Tiefen-Scan** und **Kontextmenü-Scan**. Diese Scan-Profile verwenden unterschiedliche ThreatSense-Einstellungen. Sie finden eine Beschreibung der verfügbaren Optionen unter **Erweiterte Einstellungen** > **Erkennungsroutine** > **Schadsoftware-Scans** > **On-demand-Scan** > ThreatSense-Einstellungen.

Klicken Sie auf **Prüfen**, um die Prüfung mit den von Ihnen festgelegten Parametern auszuführen.

Mit der Schaltfläche Als Administrator prüfen können Sie die Prüfung mit dem Administratorkonto ausführen. Verwenden Sie diese Option, wenn der aktuelle Benutzer keine Zugriffsrechte für die zu prüfenden Dateien hat. Diese Schaltfläche ist nur verfügbar, wenn der aktuell angemeldete Benutzer keine UAC-Vorgänge als Administrator aufrufen darf.

HINWEIS
Klicken Sie auf **Logs anzeigen**.

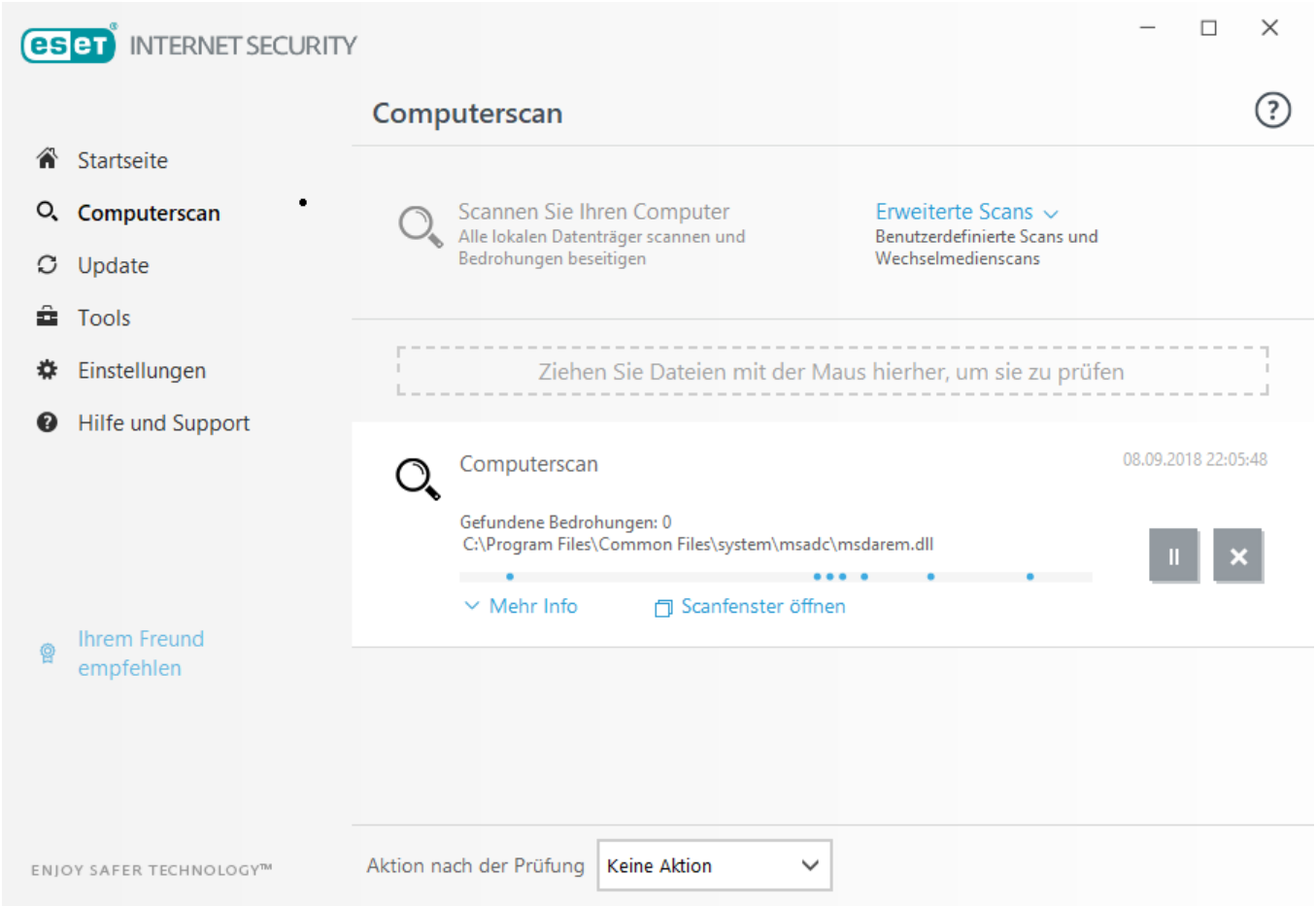
4.1.1.2.2 Stand der Prüfung

Die Fortschrittsanzeige enthält den aktuellen Stand der Prüfung sowie die Anzahl der bisher gefundenen infizierten Dateien.

HINWEIS
Es ist normal, dass u. a. passwortgeschützte Dateien oder Dateien, die ausschließlich vom System genutzt werden (in der Regel sind das *pagefile.sys* und bestimmte Log-Dateien), nicht geprüft werden können. Weitere Informationen finden Sie in unserem Knowledgebase-Artikel.

Stand der Prüfung - Die Fortschrittsanzeige zeigt den Status der bereits geprüften Objekte in Bezug auf die noch zu prüfenden Objekte an. Der Status des Scan-Fortschritts ergibt sich aus der Gesamtzahl der Objekte, die in den Scan einbezogen werden.
Zu prüfende Objekte - Der Name und Speicherort des aktuell geprüften Objekts werden angezeigt.
Bedrohungen erkannt – Zeigt die Gesamtzahl der während der Prüfung geprüften Dateien, gefundenen Bedrohungen und gesäuberten Bedrohungen an.
Anhalten - Unterbrechen der Prüfung.
Fortsetzen - Diese Option wird angezeigt, wenn die Prüfung angehalten wurde. Klicken Sie auf **Fortsetzen**, um mit der Prüfung fortzufahren.
Beenden - Beenden der Prüfung.
Bildlauf in Log-Anzeige aktivieren - Wenn diese Option aktiviert ist, fährt der Bildlauf automatisch nach unten, um die neuesten Einträge der sich verlängernden Liste anzuzeigen.

HINWEIS
Klicken Sie auf die Lupe oder den Pfeil, um Details zur aktuell ausgeführten Prüfung anzuzeigen. Sie können gleichzeitig eine weitere Prüfung ausführen, indem Sie auf **Computerprüfung** oder **Benutzerdefinierte Prüfung** klicken.



Aktion nach der Prüfung – Löst ein geplantes Herunterfahren oder einen geplanten Neustart des Computers nach der Prüfung aus. Nach dem Abschluss der Prüfung wird vor dem Herunterfahren 60 Sekunden lang ein Bestätigungsfenster angezeigt.

4.1.1.2.3 Prüfprofile

Ihre bevorzugten Einstellungen können für zukünftige Prüfungen gespeichert werden. Wir empfehlen Ihnen, für jede regelmäßig durchgeführte Prüfung ein eigenes Profil zu erstellen (mit verschiedenen zu prüfenden Objekten, Prüfmethoden und anderen Parametern).

Um ein neues Profil zu erstellen, öffnen Sie die erweiterten Einstellungen (F5) und klicken auf **Erkennungsroutine** > **Schadsoftware-Prüfungen** > **On-Demand-Prüfung** > **Profilliste**. Im Fenster **Profil-Manager** finden Sie das Dropdownmenü **Ausgewähltes Profil** mit den vorhandenen Prüfprofilen und der Option zum Erstellen eines neuen Profils. Eine Beschreibung der einzelnen Prüfeinstellungen finden Sie im Abschnitt Einstellungen für ThreatSense. So können Sie ein Prüfprofil erstellen, das auf Ihre Anforderungen zugeschnitten ist.

HINWEIS
Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Option **Computerprüfung** eignet sich in gewissem Maße, aber Sie möchten keine laufzeitkomprimierten Dateien oder potenziell unsichere Anwendungen prüfen. Außerdem möchten Sie die Option **Immer versuchen, automatisch zu entfernen** anwenden. Geben Sie den Namen des neuen Profils im **Profilmanager** ein und klicken Sie auf **Hinzufügen**. Wählen Sie das neue Profil im Dropdownmenü **Ausgewähltes Profil** aus, passen Sie die restlichen Parameter nach Ihren Anforderungen an und klicken Sie auf **OK**, um das neue Profil zu speichern.

4.1.1.2.4 Computerprüfungs-Log

Das Computerprüfungs-Log enthält allgemeine Informationen zur Überprüfung, z. B.:

- Abschlusszeit
- Prüfdauer
- Anzahl erkannter Bedrohungen
- Anzahl geprüfter Objekte
- Geprüfte Laufwerke, Ordner und Dateien
- Datum und Uhrzeit der Prüfung
- Version der Erkennungsroutine

4.1.1.3 Leerlauferkennung

Scannen im Leerlaufbetrieb aktivieren – Diese Option führt einen vollständigen Computer-Scan durch, wenn Ihr Computer nicht verwendet wird.

Diese Prüfung wird nur dann ausgeführt, wenn der Computer (Notebook) an die Netzversorgung angeschlossen ist. Sie können diese Einstellung mit der Funktion **Auch ausführen, wenn der Computer im Batteriebetrieb ausgeführt wird** überschreiben.

Aktivieren Sie die Option **Logging aktivieren**, um die Ausgabe eines Computer-Scans in den Log-Dateien abzulegen (Klicken Sie im Hauptprogrammfenster auf **Tools** > **> Weitere Tools** > **Log-Dateien** und wählen Sie **Computer-Scan** im Dropdownmenü **Log** aus).

Die **Prüfung im Leerlaufbetrieb** wird ausgeführt, wenn sich der Computer in einem der folgenden Zustände befindet:

- Bildschirm ausgeschaltet oder Bildschirmschoner
- Computersperre
- Benutzerabmeldung

Klicken Sie auf Einstellungen für ThreatSense, um die Einstellungen (z. B. die Erkennungsmethoden) für die Prüfungen im Leerlaufbetrieb zu ändern.

4.1.1.4 Prüfung der Systemstartdateien

Die automatische Prüfung der Systemstartdateien wird standardmäßig beim Systemstart und beim Update der Erkennungsroutine ausgeführt. Die Ausführung der Prüfung ist abhängig davon, wie der Taskplaner konfiguriert ist und welche Tasks eingerichtet wurden.

Die Option der Systemstartprüfung ist Bestandteil der Task **Prüfung der Systemstartdateien** im Taskplaner. Navigieren Sie zu **Tools** > > **Taskplaner** und klicken Sie auf **Prüfung Systemstartdateien** und anschließend auf **Bearbeiten**. Nach dem letzten Schritt wird das Fenster Prüfung Systemstartdateien angezeigt. (Weitere Informationen finden Sie im nächsten Kapitel.)

Detaillierte Anweisungen zum Erstellen und Verwalten von Tasks im Taskplaner finden Sie unter Erstellen neuer Tasks.

4.1.1.4.1 Prüfung Systemstartdateien

Beim Erstellen eines geplanten Tasks für die Prüfung der Systemstartdateien stehen Optionen zum Anpassen der folgenden Parameter zur Verfügung:

Im Dropdownmenü **Häufig verwendete Dateien** wird die Scan-Tiefe für Systemstartdateien auf Grundlage eines geheimen, komplizierten Algorithmus festgelegt. Die Dateien werden auf Grundlage der folgenden Kriterien in absteigender Reihenfolge sortiert:

- **Alle registrierten Dateien** (größte Anzahl geprüfter Dateien)
- **Selten verwendete Dateien**
- **Von den meisten Benutzern verwendete Dateien**
- **Häufig verwendete Dateien**
- **Nur die am häufigsten verwendeten Dateien** (kleinste Anzahl gescannter Dateien)

Außerdem stehen zwei besondere Gruppen zur Verfügung:

- **Dateien, die vor der Benutzeranmeldung gestartet werden** – Enthält Dateien von Standorten, auf die ohne Benutzeranmeldung zugegriffen werden kann (umfasst nahezu alle Systemstartstandorte wie Dienste, Browserhilfsobjekte, Windows-Anmeldungshinweise, Einträge im Windows-Taskplaner, bekannte DLL-Dateien usw.).
- **Dateien, die nach der Benutzeranmeldung gestartet werden** – Enthält Dateien von Standorten, auf die erst nach einer Benutzeranmeldung zugegriffen werden kann (umfasst Dateien, die nur für einen bestimmten Benutzer ausgeführt werden, üblicherweise im Verzeichnis *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Die Liste der zu prüfenden Dateien ist für jede der zuvor genannten Gruppen unveränderbar.

Prüfpriorität – Prioritätsstufe für den Start der Prüfung:

- **Bei Leerlauf** – Der Task wird nur ausgeführt, wenn das System im Leerlauf ist.
- **Minimal** – bei minimaler Systemlast.
- **Niedrig** – bei geringer Systemlast.
- **Normal** – bei durchschnittlicher Systemlast.

4.1.1.5 Ausschlussfilter

Mit dem Ausschlussfilter können Sie festlegen, welche Dateien und Ordner von Prüfungen ausgenommen werden sollen. Um zu gewährleisten, dass möglichst alle Objekte auf Bedrohungen geprüft werden, empfehlen wir, nur bei dringendem Bedarf Ausnahmen zu erstellen. In bestimmten Fällen kann es jedoch erforderlich sein, ein Objekt von der Prüfung auszuschließen, beispielsweise bei großen Datenbankeinträgen, deren Prüfung die Computerleistung zu stark beeinträchtigen würde, oder bei Software, die Konflikte mit der Prüfung verursacht.

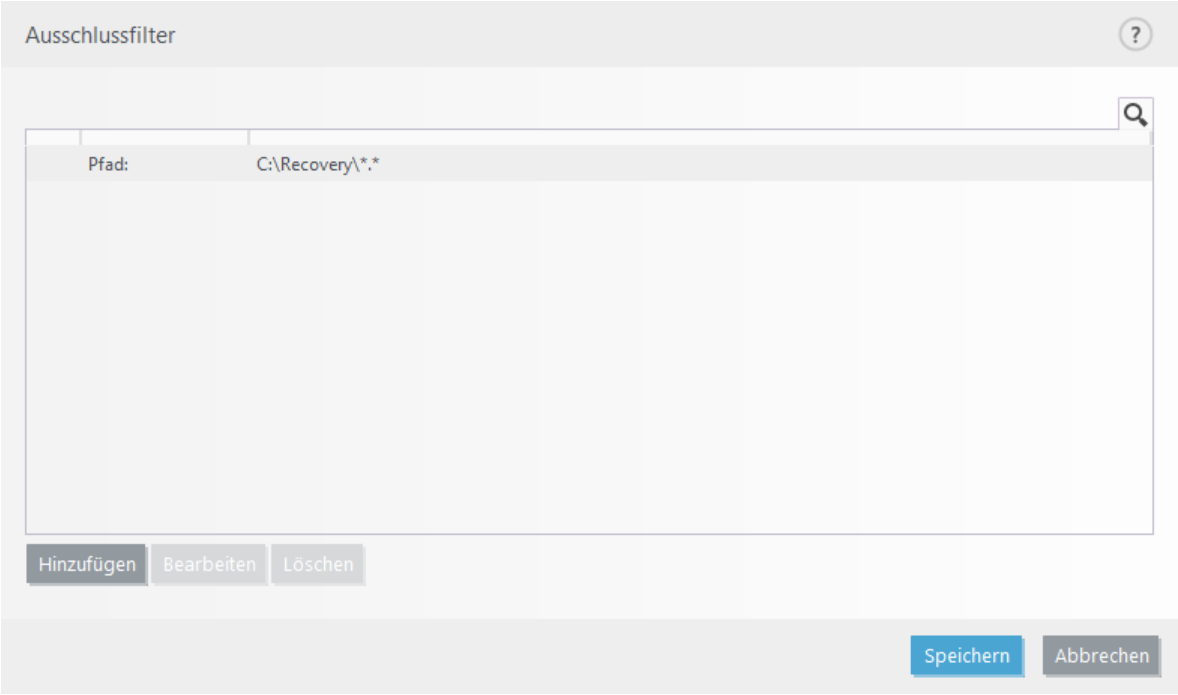
So schließen Sie ein Objekt von Prüfungen aus:

1. Klicken Sie auf **Hinzufügen**,
2. Geben Sie den Pfad des Objekts ein oder wählen Sie es in der Baumstruktur aus.

Mit Hilfe von Platzhaltern können Sie Gruppen von Dateien ausschließen. Dabei steht ein Fragezeichen (?) für genau ein beliebiges Zeichen, ein Sternchen (*) steht für beliebig viele Zeichen oder „kein Zeichen“.

Beispiele

- Wenn Sie alle Dateien in einem bestimmten Ordner ausschließen möchten, geben Sie den Pfad zum Ordner mit der Maske „*.*“ ein.
- Wenn Sie ein gesamtes Laufwerk einschließlich aller Dateien und Unterordner ausschließen möchten, geben Sie den Pfad mit der Maske „D:*“ ein.
- Wenn nur DOC-Dateien ausgeschlossen werden sollen, verwenden Sie die Maske „*.doc“.
- Wenn der Name einer ausführbaren Datei aus einer bestimmten Anzahl von (variierenden) Zeichen besteht und Sie nur den ersten sicher wissen (zum Beispiel „D“), verwenden Sie folgendes Format: „D????.exe“. Die Fragezeichen ersetzen die fehlenden (unbekannten) Zeichen.



HINWEIS
Eine Bedrohung, die sich in einer Datei befindet, die die Kriterien des Ausschlussfilters erfüllt, kann vom Echtzeit-Dateischutz und bei der Prüfung des Computers nicht erkannt werden.

Spalten

Pfad – Pfad zu den auszuschließenden Dateien/Ordnern.

Bedrohung – Steht neben einer ausgeschlossenen Datei der Name einer Bedrohung, so gilt die Ausnahme nicht generell für die Datei, sondern nur für diese bestimmte Bedrohung. Wird die Datei später durch andere Malware infiziert, erkennt der Virenschutz dies. Dieser Ausschlusstyp kann nur bei bestimmten Arten eingedrungener Schadsoftware verwendet werden und wird entweder in dem Warnungsfenster für die Bedrohung erstellt (klicken Sie auf **Erweiterte Einstellungen anzeigen** und dann auf **Von der Erkennung ausschließen**) oder unter **Tools** > > **Weitere Tools** > > **Quarantäne** mit der rechten Maustaste auf die Datei in der Quarantäne klicken und aus dem Kontextmenü den Befehl **Wiederherstellen und von der Erkennung ausschließen** auswählen.

Steuerelemente

Hinzufügen – Objekte von der Prüfung ausnehmen.

Bearbeiten – Ausgewählte Einträge bearbeiten.

Entfernen – Ausgewählte Einträge entfernen.

4.1.1.6 ThreatSense-Parameter

ThreatSense verwendet verschiedene komplexe Methoden zur Bedrohungserkennung. Die Technologie arbeitet proaktiv, d. h. sie schützt das System auch während der ersten Ausbreitung eines neuen Angriffs. Eingesetzt wird eine Kombination aus Code-Analyse, Code-Emulation, allgemeinen Signaturen und Virussignaturen verwendet, die zusammen die Systemsicherheit deutlich erhöhen. Das Prüfmodul kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. Die ThreatSense-Technologie entfernt auch erfolgreich Rootkits.

in den Einstellungen für ThreatSense können Sie verschiedene Prüfparameter festlegen:

- Dateitypen und -erweiterungen, die geprüft werden sollen
- Die Kombination verschiedener Erkennungsmethoden
- Säuberungsstufen usw.

Um das Fenster für die Einstellungen zu öffnen, klicken Sie auf die **ThreatSense-Parameter** , die im Fenster mit erweiterten Einstellungen für alle Module angezeigt werden, die ThreatSense verwenden (siehe unten). Je nach Anforderung sind eventuell verschiedene Sicherheitseinstellungen erforderlich. Dies sollte bei den individuellen ThreatSense-Einstellungen für die folgenden Schutzmodule berücksichtigt werden:

- Echtzeit-Dateischutz
- Prüfen im Leerlaufbetrieb
- Prüfung der Systemstartdateien
- Dokumentenschutz
- E-Mail-Schutz
- Web-Schutz
- Computerprüfung

ThreatSense-Parameter sind für jedes Modul optimal eingerichtet. Eine Veränderung der Einstellungen kann den Systembetrieb spürbar beeinträchtigen. Änderungen an den Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der Advanced Heuristik im Modul „Echtzeit-Dateischutz“ können das System verlangsamen (normalerweise werden mit diesen Methoden nur neu erstellte Dateien geprüft). Es wird empfohlen, die Standard-Parameter für ThreatSense in allen Modulen unverändert beizubehalten. Änderungen sollten nur im Modul „Computer prüfen“ vorgenommen werden.

Zu prüfende Objekte

In diesem Bereich können Sie festlegen, welche Dateien und Komponenten Ihres Computers auf Schadcode geprüft werden sollen.

Arbeitsspeicher - Prüfung auf Bedrohungen für den Arbeitsspeicher des Systems.

Systembereiche (Boot, MBR) - Prüfung der Bootsektoren auf Viren im Master Boot Record.

E-Mail-Dateien - Folgende Erweiterungen werden vom Programm unterstützt: DBX (Outlook Express) und EML.

Archive - Folgende Erweiterungen werden vom Programm unterstützt: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE und viele andere.

Selbstentpackende Archive – Selbstentpackende Archive (SFX) sind Archivdateien, die sich selbst extrahieren können.

Laufzeitkomprimierte Dateien – Im Unterschied zu Standardarchiven werden laufzeitkomprimierte Dateien nach dem Starten im Arbeitsspeicher dekomprimiert. Neben statischen laufzeitkomprimierten Dateiformaten (UPX, yoda, ASPack, FSG usw.) kann die Prüfung durch Code-Emulation viele weitere SFX-Typen erkennen.

Prüfungseinstellungen

Wählen Sie die Methoden aus, mit denen das System auf Infiltrationen gescannt werden soll. Folgende Optionen stehen zur Verfügung:

Heuristik - Als heuristische Methoden werden Verfahren bezeichnet, die (bösartige) Aktivitäten von Programmen analysieren. Auf diese Weise können auch bösartige Programme erkannt werden, die noch nicht in der Erkennungsroutine verzeichnet sind. Nachteilig ist, dass es in Einzelfällen zu Fehlalarmen kommen kann.

Advanced Heuristik/DNA-Signaturen - Advanced Heuristik sind besondere heuristische Verfahren, die von ESET entwickelt wurden, um Würmer, Trojaner und Schadprogramme besser zu erkennen, die in höheren Programmiersprachen geschrieben wurden. Mit Advanced Heuristik werden die Fähigkeiten von ESET-Produkten zur Erkennung von Bedrohungen beträchtlich gesteigert. Mit Hilfe von Signaturen können Viren zuverlässig erkannt werden. Mit automatischen Updates sind Signaturen für neue Bedrohungen innerhalb weniger Stunden verfügbar. Nachteilig an Signaturen ist, dass mit ihrer Hilfe nur bekannte Viren und gering modifizierte Varianten bekannter Viren erkannt werden können.

Potenziell unerwünschte Anwendungen – Grayware (auch als eventuell unerwünscht Anwendung bezeichnet) umfasst verschiedenste Arten von Software, deren Ziel nicht so eindeutig bösartig ist wie bei anderen Arten von Schadsoftware wie Viren oder Trojanern. Diese Art von Software kann jedoch weitere unerwünschte Software installieren, das Verhalten des digitalen Geräts ändern oder Aktionen ausführen, denen der Benutzer nicht zugestimmt hat oder die er nicht erwartet. Weitere Details finden Sie im Kapitel Potenziell unerwünschte Anwendungen.

Potenziell unsichere Anwendungen – Zu den potenziell unsicheren Anwendungen zählen beispielsweise Programme für das Fernsteuern von Computern (Remotedesktopverbindung), Programme zum Entschlüsseln von Passwörtern und Keylogger (Programme, die aufzeichnen, welche Tasten vom Benutzer gedrückt werden), die zwar erwünscht sind, jedoch potenziell gefährliche Funktionen bereitstellen. Diese Option ist in der Voreinstellung deaktiviert.

Die Einstellungen zum Entfernen von Schadcode legen fest, wie beim Entfernen vorgegangen werden soll. Es gibt 3 Arten der Schadcodeentfernung.

Ausschlussfilter

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt einer Datei. In diesem Abschnitt der ThreatSense-Einstellungen können Sie die Dateitypen festlegen, die geprüft werden sollen.

Sonstige

Bei der Konfiguration von ThreatSense für eine On-Demand-Prüfung des Computers sind folgende Optionen im Abschnitt **Sonstige** verfügbar:

Alternative Datenströme (ADS) prüfen - Bei den von NTFS-Dateisystemen verwendeten alternativen Datenströmen (ADS) handelt es sich um Datei- und Ordnerzuordnungen, die mit herkömmlichen Prüftechniken nicht erkannt werden können. Eingedrungene Schadsoftware tarnt sich häufig als alternativer Datenstrom, um nicht erkannt zu werden.

Hintergrundprüfungen mit geringer Priorität ausführen - Jede Prüfung nimmt eine bestimmte Menge von Systemressourcen in Anspruch. Wenn Sie mit Anwendungen arbeiten, welche die Systemressourcen stark beanspruchen, können Sie eine Hintergrundprüfung mit geringer Priorität aktivieren, um Ressourcen für die Anwendungen zu sparen.

Alle Objekte in Log aufnehmen – Wenn Sie diese Option aktivieren, werden alle geprüften Dateien im Log eingetragen. Es werden also auch Dateien eingetragen, bei denen keine Bedrohung erkannt wurde. Wenn beispielsweise in einem Archiv Schadcode gefunden wird, listet das Log auch die in diesem Archiv enthaltenen, nicht infizierten Dateien auf.

Smart-Optimierung aktivieren - Wenn die Smart-Optimierung aktiviert ist, werden die optimalen Einstellungen verwendet, um die effizienteste Prüfung bei höchster Geschwindigkeit zu gewährleisten. Die verschiedenen Schutzmodule führen eine intelligente Prüfung durch. Dabei verwenden sie unterschiedliche Prüfmethoden für die jeweiligen Dateitypen. Wenn die Smart-Optimierung deaktiviert ist, werden nur die benutzerdefinierten Einstellungen im ThreatSense-Kern der entsprechenden Module für die Prüfung verwendet.

Datum für „Geändert am“ beibehalten - Aktivieren Sie diese Option, um den Zeitpunkt des ursprünglichen Zugriffs auf geprüfte Dateien beizubehalten (z. B. für die Verwendung mit Datensicherungssystemen), anstatt ihn zu aktualisieren.

Grenzen

Im Bereich „Grenzen“ können Sie die Maximalgröße von Elementen und Stufen verschachtelter Archive festlegen, die geprüft werden sollen:

Einstellungen für Objektprüfung

Maximale Objektgröße - Definiert die Maximalgröße der zu prüfenden Elemente. Der aktuelle Virenschutz prüft dann nur die Elemente, deren Größe unter der angegebenen Maximalgröße liegt. Diese Option sollte nur von fortgeschrittenen Benutzern geändert werden, die bestimmte Gründe dafür haben, dass größere Elemente von der Prüfung ausgeschlossen werden. Der Standardwert ist: *unbegrenzt*.

Maximale Scanzeit pro Objekt (Sek.) - Definiert die maximale Dauer für die Prüfung eines Elements. Wenn hier ein benutzerdefinierter Wert eingegeben wurde, beendet der Virenschutz die Prüfung eines Elements, sobald diese Zeit abgelaufen ist, und zwar ungeachtet dessen, ob die Prüfung abgeschlossen ist oder nicht. Der Standardwert ist: *unbegrenzt*.

Einstellungen für Archivprüfung

Verschachtelungstiefe bei Archiven - Legt die maximale Tiefe der Virenprüfung von Archiven fest. Der Standardwert ist: *10*.

Maximalgröße von Dateien im Archiv - Hier können Sie die maximale Dateigröße für Dateien in (extrahierten) Archiven festlegen, die geprüft werden sollen. Der Standardwert ist: *unbegrenzt*.

HINWEIS
Die Standardwerte sollten nicht geändert werden; unter normalen Umständen besteht dazu auch kein Grund.

4.1.1.6.1 Säubern

Die Einstellungen zum Entfernen von Schadcode legen fest, wie beim Entfernen vorgegangen werden soll. Es gibt 3 Säuberungsstufen.

4.1.1.6.2 Von der Prüfung ausgeschlossene Dateiendungen

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt einer Datei. In diesem Abschnitt der ThreatSense-Einstellungen können Sie die Dateitypen festlegen, die geprüft werden sollen.

Alle Dateien werden standardmäßig geprüft. Jede Erweiterung kann der Liste ausgeschlossener Dateien hinzugefügt werden.

Der Ausschluss bestimmter Dateien ist dann sinnvoll, wenn die Prüfung bestimmter Dateitypen die Funktion eines Programms beeinträchtigt, das diese Erweiterungen verwendet. So sollten Sie z. B. die Erweiterungen `.edb`, `.eml` und `.tmp` ausschließen, wenn Sie Microsoft Exchange Server verwenden.

Über die Schaltflächen **Hinzufügen** und **Entfernen** können Sie festlegen, welche Erweiterungen geprüft werden sollen. Klicken Sie zum Hinzufügen einer neuen Erweiterung zur Liste auf **Hinzufügen**, geben Sie die Erweiterung in das Feld ein (z. B. `.tmp`), und klicken Sie auf **OK**. Mit der Option **Mehrere Werte eingeben** können Sie mehrere, durch Zeilen, Komma oder Semikolon getrennte Erweiterungen eingeben. Wenn die Mehrfachauswahl aktiviert ist, werden die Erweiterungen in der Liste angezeigt. Wählen Sie eine Erweiterung in der Liste aus und klicken Sie auf **Entfernen**, um die markierte Erweiterung aus der Liste zu entfernen. Wenn Sie eine ausgewählte Erweiterung bearbeiten möchten, klicken Sie auf **Bearbeiten**.

Sie können die Sonderzeichen ? (Fragezeichen) verwenden. Das Fragezeichen ein beliebiges Symbol.

HINWEIS
Um die tatsächliche Erweiterung einer Datei (falls vorhanden) unter Windows anzuzeigen, müssen Sie die Option **Erweiterungen bei bekannten Dateitypen ausblenden** unter **Systemsteuerung** > **Ordneroptionen** > **Ansicht** (Registerkarte) deaktivieren und die Änderung anschließend übernehmen.

4.1.1.7 Eingedrungene Schadsoftware wurde erkannt

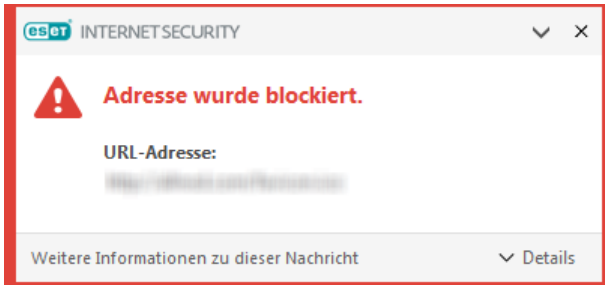
Schadsoftware kann auf vielen Wegen in das System gelangen. Mögliche Eintrittsstellen sind Websites, freigegebene Ordner, E-Mails oder Wechselmedien (USB-Sticks, externe Festplatten, CDs, DVDs, Disketten usw.).

Standardmäßiges Verhalten

ESET Internet Security kann Bedrohungen mit einem der folgenden Module erkennen:

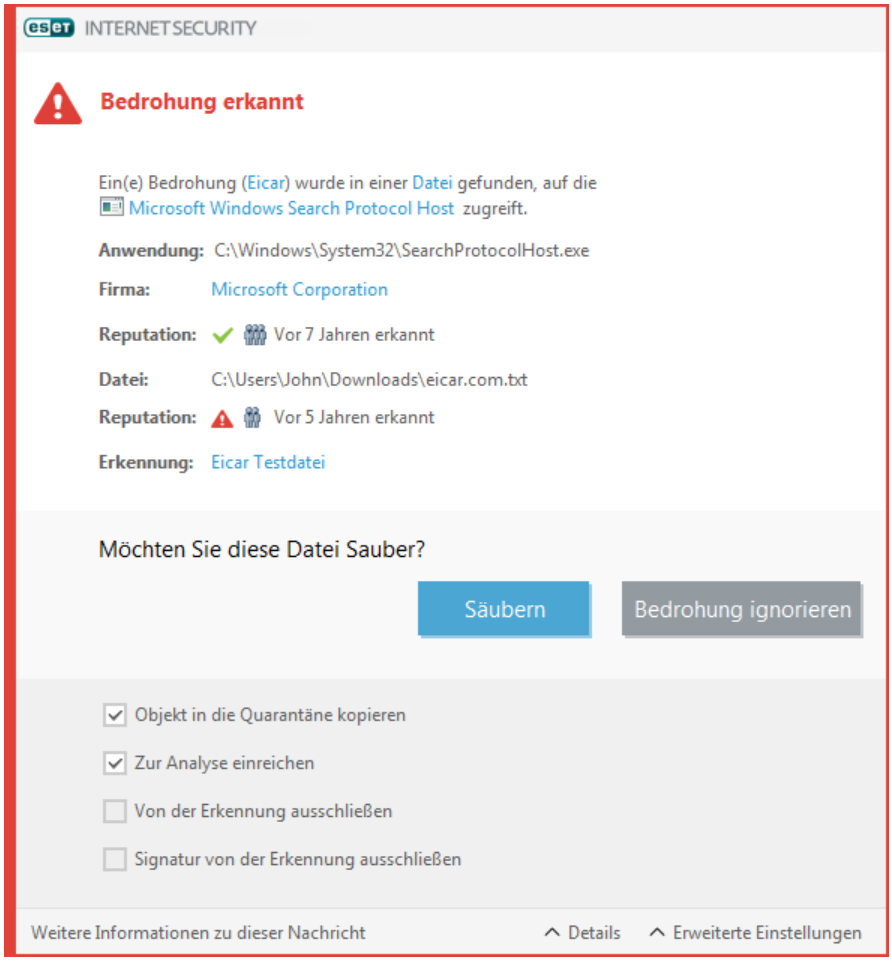
- Echtzeit-Dateischutz
- Web-Schutz
- E-Mail-Schutz
- On-Demand-Prüfung

Standardmäßig wenden die Module die normale Säuberungsstufe an und versuchen, die Datei zu säubern und in die Quarantäne zu verschieben, oder die Verbindung zu beenden. Im Infobereich der Taskleiste rechts unten auf dem Bildschirm wird ein Hinweisfenster angezeigt. Weitere Informationen zu den Säuberungsstufen und zum Verhalten des Produkts finden Sie unter Säubern.



Schadcode entfernen und löschen

Ist für den Echtzeit-Dateischutz keine vordefinierte Aktion angegeben, werden Sie in einem Warnungsfenster aufgefordert, zwischen verschiedenen Optionen zu wählen. In der Regel stehen die Optionen **Säubern**, **Löschen** und **Keine Aktion** zur Auswahl. Die Auswahl der Option **Keine Aktion** ist nicht empfehlenswert, da infizierte Dateien mit dieser Einstellung nicht gesäubert werden. Einzige Ausnahme: Sie sind sich sicher, dass die Datei harmlos ist und versehentlich erkannt wurde.



Wenden Sie die Option „Säubern“ an, wenn eine Datei von einem Virus mit Schadcode infiziert wurde. In einem solchen Fall sollten Sie zuerst versuchen, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.

Wenn eine infizierte Datei „gesperrt“ ist oder von einem Systemprozess verwendet wird, muss die Datei in der Regel erst freigegeben werden (häufig ist dazu ein Systemneustart erforderlich), bevor sie gelöscht werden kann.

Mehrere Bedrohungen

Falls infizierte Dateien während der Prüfung des Computers nicht gesäubert wurden (oder die Säuberungsstufe auf **Nicht säubern** festgelegt wurde), wird in einem Warnfenster nachgefragt, wie mit den Dateien verfahren werden soll. Wählen Sie Aktionen für die Dateien aus (diese werden für jede Datei in der Liste separat festgelegt). Klicken Sie dann auf **Fertig stellen**.

Dateien in Archiven löschen

Im Standard-Säuberungsmodus wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Archive, die auch nicht infizierte Dateien enthalten, werden also nicht gelöscht. Die Option „Immer versuchen, automatisch zu entfernen“ sollten Sie mit Bedacht einsetzen, da in diesem Modus alle Archive gelöscht werden, die mindestens eine infizierte Datei enthalten, und dies unabhängig vom Status der übrigen Archivdateien.

Wenn Ihr Computer die Symptome einer Malware-Infektion aufweist (Computer arbeitet langsamer als gewöhnlich, reagiert häufig nicht usw.), sollten Sie folgendermaßen vorgehen:

- Öffnen Sie ESET Internet Security und klicken Sie auf „Computer prüfen“
- Klicken Sie auf **Computerprüfung** (weitere Informationen siehe Computerprüfung)
- Nachdem die Prüfung abgeschlossen ist, überprüfen Sie im Log die Anzahl der geprüften, infizierten und wiederhergestellten Dateien

Wenn Sie nur einen Teil Ihrer Festplatte prüfen möchten, wählen Sie **Benutzerdefinierte Prüfung** und anschließend die Bereiche, die auf Viren geprüft werden sollen.

4.1.1.8 Dokumentenschutz

Die Dokumentenschutzfunktion überprüft Microsoft Office-Dokumente vor dem Öffnen sowie automatisch von Internet Explorer heruntergeladene Dateien wie Microsoft ActiveX-Elemente. Der Dokumentenschutz bietet eine zusätzliche Schutzebene zum Echtzeit-Dateischutz und kann deaktiviert werden, um die Leistung auf Systemen zu verbessern, die keine große Anzahl an Microsoft Office-Dokumenten verarbeiten müssen.

Um den Dokumentenschutz zu aktivieren, navigieren Sie zu **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **Schadsoftware-Prüfungen** > **Dokumentenschutz**, und klicken Sie auf den Schalter **Systemintegration**.

HINWEIS
Die Funktion wird von Anwendungen aktiviert, die Microsoft Antivirus API verwenden (z. B. Microsoft Office 2000 und höher oder Microsoft Internet Explorer 5.0 und höher).

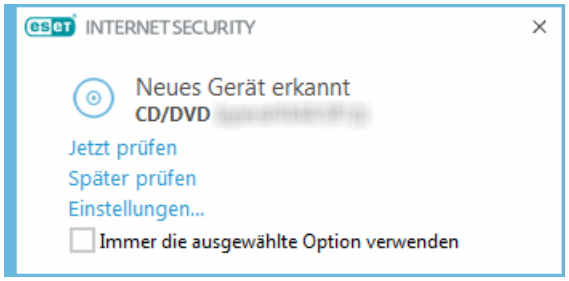
4.1.2 Wechselmedien

ESET Internet Security bietet automatische Prüfmethoden für Wechselmedien (CD/DVD/USB/...). Dieses Modul ermöglicht das Einrichten einer Prüfung für eingelegte Medien. Dies ist sinnvoll, wenn der Administrator verhindern möchte, dass Benutzer Wechselmedien mit unerwünschten Inhalten verwenden.

Aktion nach Einlegen von Wechselmedien - Wählen Sie die Aktion, die standardmäßig ausgeführt werden soll, wenn ein Wechselmedium in den Computer eingelegt wird (CD/DVD/USB). Wenn die Option **Scanoptionen anzeigen** aktiviert ist, wird ein Hinweisfenster angezeigt, in dem Sie eine Aktion wählen können:

- **Nicht prüfen** - Es wird keine Aktion ausgeführt und das Fenster **Neues Gerät erkannt** wird geschlossen.
- **Automatische Geräteprüfung** - Eine On-Demand-Prüfung des eingelegten Wechselmediums wird durchgeführt.
- **Prüfoptionen anzeigen** – Öffnet die Einstellungen für Wechselmedien.

Beim Einlegen eines Wechselmediums wird folgender Dialog angezeigt:



Jetzt prüfen – Dies löst den Wechselmedienscan aus.

Später prüfen – Die Wechselmedienprüfung wird auf einen späteren Zeitpunkt verschoben.

Einstellungen – Öffnet die erweiterten Einstellungen.

Immer die ausgewählte Option verwenden – Wenn diese Option aktiviert ist, wird bei jedem Einlegen eines Wechselmediums die gleiche Aktion ausgeführt.

Zusätzlich bietet ESET Internet Security die Funktion der Medienkontrolle, mit der Sie Regeln für die Nutzung externer Geräte mit einem bestimmten Computer festlegen können. Weitere Informationen zur Medienkontrolle finden Sie im Abschnitt Medienkontrolle.

4.1.3 Medienkontrolle

Medienkontrolle

ESET Internet Security bietet Methoden zur automatischen Prüfung von Geräten (CD/DVD/USB/...). Mit diesem Modul können Sie Medien bzw. Geräte sperren oder erweiterte Filter- und Berechtigungseinstellungen anpassen und definieren, wie ein Benutzer auf diese Geräte zugreifen und mit ihnen arbeiten kann. Dies ist sinnvoll, wenn der Administrator verhindern möchte, dass Benutzer Geräte mit unerwünschten Inhalten verwenden.

Unterstützte externe Geräte:

- Datenträger (Festplatten, USB-Wechselmedien)
- CD/DVD
- USB-Drucker
- FireWire-Speicher
- Bluetooth-Gerät
- Smartcardleser
- Bildverarbeitungsgerät
- Modem
- LPT/COM-Port
- Tragbares Gerät
- Mikrofon
- Alle Gerätetypen

Die Einstellungen für die Medienkontrolle können unter **Erweiterte Einstellungen** (F5) > **Medienkontrolle** geändert werden.

Über das Kontrollkästchen **Systemintegration** aktivieren Sie die Funktion Medienkontrolle in ESET Internet Security. Sie müssen Ihren Computer neu starten, um die Änderungen zu übernehmen. Wenn die Medienkontrolle aktiviert ist, wird die Option **Regeln** verfügbar, über die Sie das Fenster Regel-Editor öffnen können.

HINWEIS
Sie können unterschiedliche Gerätegruppen für Geräte erstellen, auf die jeweils unterschiedliche Regeln angewendet werden sollen. Sie können auch nur eine einzige Gerätegruppe erstellen, auf die die Regel mit der Aktion **Lesen/Schreiben** oder **Schreibgeschützt** angewendet wird. So werden nicht erkannte Geräte durch die Medienkontrolle gesperrt, wenn sie an den Computer angeschlossen werden.

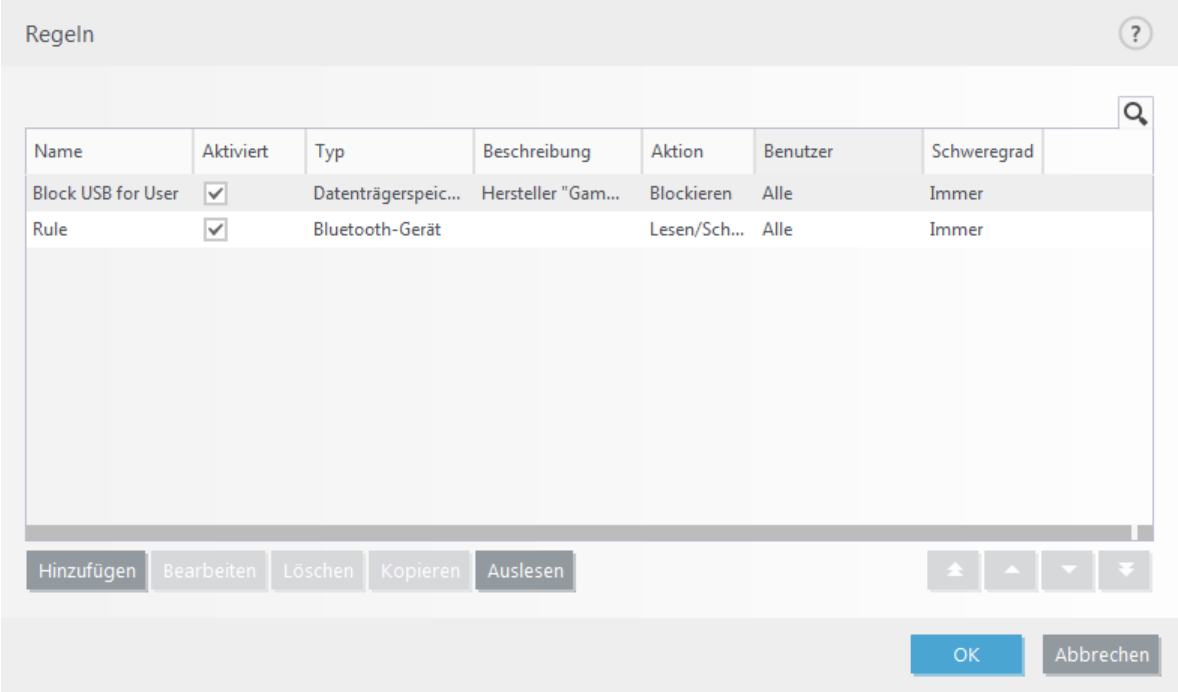
Wenn ein von einer bestehenden Regel blockiertes Gerät eingefügt wird, wird ein Hinweisfenster angezeigt und es wird kein Zugriff auf das Gerät gewährt.

Webcam-Schutz

Mit dem Schalter neben **Systemintegration** können Sie den Webcam-Schutz in ESET Internet Security aktivieren. Wenn Sie den Webcam-Schutz aktivieren, wird die Option **Regeln** aktiviert, mit der Sie das Fenster Regel-Editor öffnen können.

4.1.3.1 Regel-Editor für die Medienkontrolle

Im Fenster **Regel-Editor für die Medienkontrolle** können Sie bestehende Regeln anzeigen und präzise Regeln für Geräte erstellen, die Benutzer an den Computer anschließen.



Bestimmte Gerätetypen können für Benutzer oder Benutzergruppen oder auf Grundlage weiterer, in der Regelkonfiguration festgelegter Parameter zugelassen oder gesperrt werden. Die Liste der Regeln enthält verschiedene Angaben wie Regelname, Art des externen Geräts, auszuführende Aktion beim Anschließen eines externen Geräts und Log-Schweregrad.

Klicken Sie auf **Hinzufügen** oder **Bearbeiten**, um Ihre Regeln zu verwalten. Klicken Sie auf **Kopieren**, um eine neue Regel mit vordefinierten Optionen auf Grundlage der ausgewählten Regel zu erstellen. Die XML-Zeichenketten, die beim Klicken auf eine Regel angezeigt werden, können in den Zwischenspeicher kopiert werden, um den Systemadministrator beim Exportieren/Importieren der Daten zu unterstützen, beispielsweise für ESET Remote Administrator.

Halten Sie die Steuerungstaste (STRG) gedrückt, um mehrere Regeln auszuwählen und Aktionen (Löschen, Verschieben in der Liste) auf alle ausgewählten Regeln anzuwenden. Mit dem Kontrollkästchen **Aktiviert** können Sie eine Regel deaktivieren und aktivieren. Dies ist hilfreich, wenn Sie eine Regel nicht dauerhaft löschen möchten, um sie später wieder verwenden zu können.

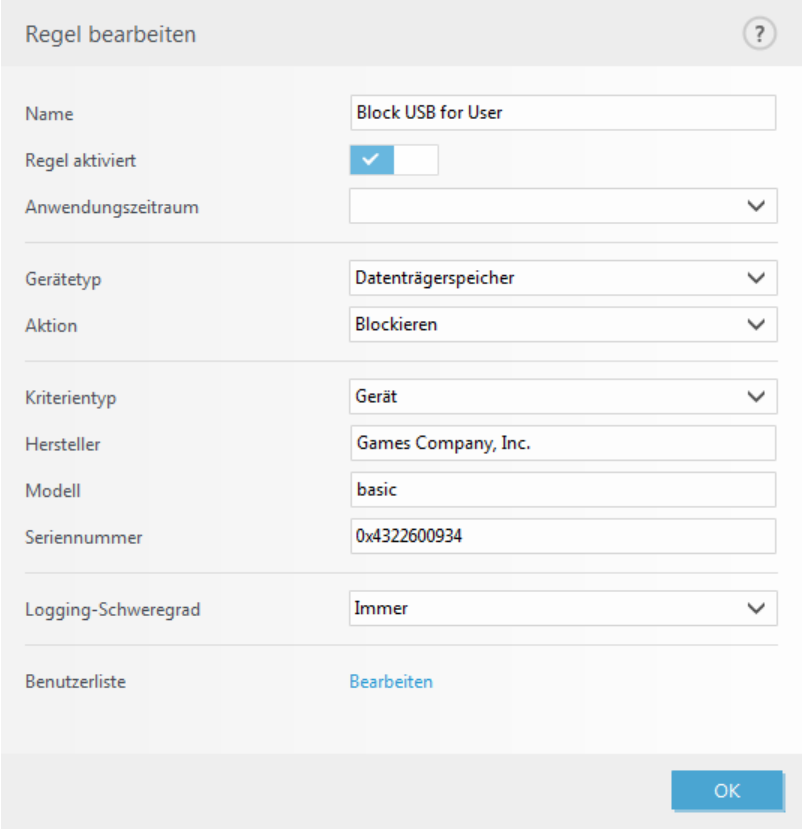
Die Regeln sind in nach absteigender Priorität geordnet (Regeln mit höchster Priorität werden am Anfang der Liste angezeigt).

Um Log-Einträge anzuzeigen, klicken Sie im Hauptfenster von ESET Internet Security auf **Tools** > **Weitere Tools** > **Log-Dateien**.

Im Log der Medienkontrolle werden alle ausgelösten Vorkommnisse der Medienkontrolle aufgezeichnet.

4.1.3.2 Hinzufügen von Regeln für die Medienkontrolle

Eine Regel für die Medienkontrolle definiert die Aktion, die ausgeführt wird, wenn ein Gerät, das die Regelkriterien erfüllt, an den Computer angeschlossen wird.



Geben Sie zur leichteren Identifizierung der Regel im Feld **Name** eine Beschreibung ein. Über den Schalter neben **Regel aktiviert** wird die Regel deaktiviert bzw. aktiviert. Dies ist beispielsweise nützlich, wenn Sie eine Regel deaktivieren, jedoch nicht dauerhaft löschen möchten.

Gerätetyp

Wählen Sie im Dropdown-Menü den Typ des externen Geräts aus (Datenträgerspeicher/tragbares Gerät/Bluetooth/FireWire/...). Die Gerätetypen werden vom Betriebssystem erfasst und können im Geräte-Manager angezeigt werden, sofern ein Gerät an den Computer angeschlossen ist. Speichergeräte umfassen externe Datenträger oder herkömmliche Kartenlesegeräte, die über den USB- oder FireWire-Anschluss an den Computer angeschlossen sind. Smartcard-Lesegeräte umfassen Kartenlesegeräte für Smartcards mit eingebettetem integriertem Schaltkreis, beispielsweise SIM-Karten oder Authentifizierungskarten. Bildverarbeitungsgeräte sind beispielsweise Scanner oder Kameras. Diese Geräte stellen nur Informationen zu den eigenen Aktionen bereit, keine Benutzerinformationen. Daher können diese Geräte nur global blockiert werden.

Aktion

Der Zugriff auf andere Geräte als Speichergeräte kann entweder zugelassen oder gesperrt werden. Im Gegensatz dazu ist es für Speichergeräte möglich, eines der folgenden Rechte für die Regel auszuwählen:

- **Lese-/Schreibzugriff** – Der vollständige Zugriff auf das Gerät wird zugelassen.
- **Sperren** – Der Zugriff auf das Gerät wird gesperrt.
- **Nur Lesezugriff** – Nur Lesezugriff auf das Gerät wird zugelassen.
- **Warnen** – Jedes Mal, wenn ein Gerät angeschlossen wird, erhält der Benutzer eine Benachrichtigung, die angibt, ob das Gerät zugelassen oder gesperrt ist. Außerdem wird ein Log-Eintrag erstellt. Die Geräteinformationen werden nicht gespeichert, d. h. bei einem erneuten, späteren Anschluss des gleichen Geräts wird die Benachrichtigung erneut angezeigt.

Beachten Sie, dass bestimmte Aktionen (Berechtigungen) nur für bestimmte Gerätetypen verfügbar sind. Bei einem Speichergerät sind alle vier Aktionen verfügbar. Für nicht-Speichergeräte sind nur drei Aktionen verfügbar.

(**Schreibgeschützt** ist beispielsweise für Bluetooth-Geräte nicht verfügbar. Bluetooth-Geräte können daher nur entweder gesperrt oder zugelassen werden oder eine Warnung auslösen).

Kriterientyp – Wählen Sie **Gerätegruppe** oder **Gerät** aus.

Weitere Parameter zur Feinanpassung der Regeln und Anpassung an bestimmte Geräte. (die Groß-/Kleinschreibung muss nicht beachtet werden):

- **Hersteller** – Filtern Sie die Liste nach Herstellername oder -ID.
- **Modell** – Die Bezeichnung des Geräts.
- **Seriennummer** – Externe Geräte verfügen üblicherweise über eigene Seriennummern. Bei CDs/DVDs bezieht sich die Seriennummer auf das Exemplar, nicht auf das Laufwerk.

HINWEIS
Wenn diese Parameter nicht definiert werden, ignoriert die Regel dieser Felder bei der Abstimmung. Bei Filterparametern mit Textfeldern braucht die Groß-/Kleinschreibung nicht beachtet zu werden. Platzhalter (*, ?) werden nicht unterstützt.

HINWEIS
Um Informationen zu einem Gerät anzuzeigen, erstellen Sie eine Regel für den entsprechenden Gerätetyp, schließen Sie das Gerät an den Computer an und überprüfen Sie dann die Gerätedetails im Medienkontrolle-Log.

Logging-Schweregrad

ESET Internet Security speichert alle wichtigen Vorgänge in einer Log-Datei, die direkt vom Hauptmenü aus aufgerufen werden kann. Klicken Sie auf **Tools** > **Log-Dateien** und wählen Sie **Medienkontrolle** aus dem Dropdown-Menü **Log** aus.

- **Immer** – Alle Ereignisse werden protokolliert.
- **Diagnose** – Informationen, die für die Feineinstellung des Programms benötigt werden, werden protokolliert.
- **Informationen** – Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnung** – Kritische Fehler und Warnungen werden protokolliert.
- **Keine** – Es werden keine Logs aufgezeichnet.

Die Regeln können auf bestimmte Benutzer oder Benutzergruppen beschränkt werden, indem Sie diese zur **Benutzerliste** hinzufügen:

- **Hinzufügen** – Öffnet das Dialogfenster **Objekttypen: Benutzer oder Gruppen**, in dem Sie bestimmte Benutzer auswählen können.
- **Entfernen** – Entfernt den ausgewählten Benutzer aus dem Filter.

HINWEIS
Alle Geräte können über Benutzerregeln eingeschränkt werden (Bildverarbeitungsgeräte liefern beispielsweise keine Informationen über Benutzer, sondern nur über ausgeführte Aktionen).

4.1.3.3 Regel-Editor für den Webcam-Schutz

In diesem Fenster werden vorhandene Regeln angezeigt. Außerdem können Sie Anwendungen und Prozesse kontrollieren, die gemäß der von Ihnen ausgewählten Aktionen auf die Kamera Ihres Computers zugreifen dürfen.

Folgende Aktionen stehen zur Verfügung:

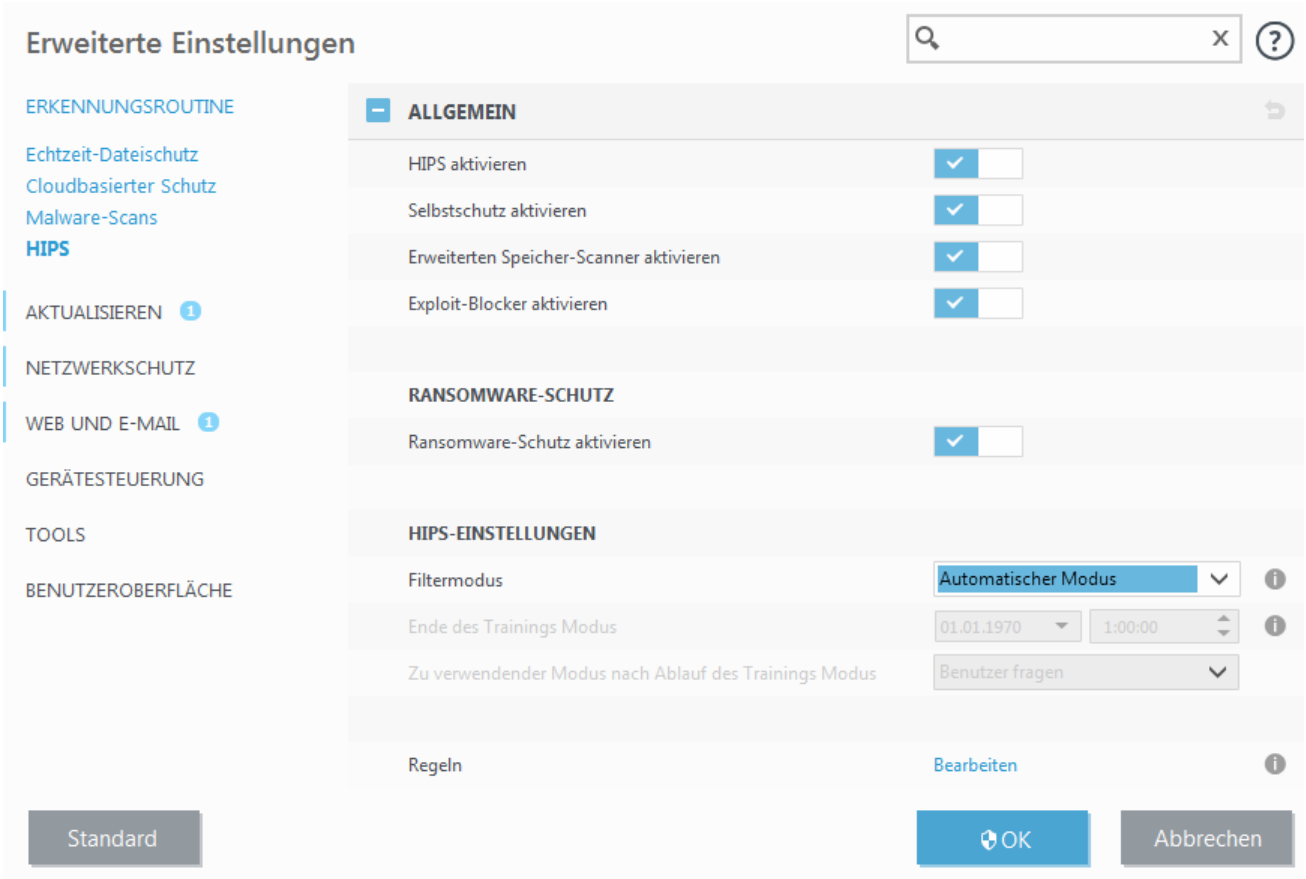
- **Zugriff blockieren**
- **Fragen**
- **Zugriff erlauben**

4.1.4 Host-based Intrusion Prevention System (HIPS)

WARNUNG
Nur erfahrene Benutzer sollten die Einstellungen von HIPS ändern. Eine falsche Konfiguration der HIPS-Einstellungen kann eine Instabilität des Systems verursachen.

Das **Host Intrusion Prevention System** (HIPS) schützt Ihr System vor Schadsoftware und unerwünschten Programmaktivitäten, die negative Auswirkungen auf Ihren Computer haben könnten. HIPS analysiert das Verhalten von Programmen genau und nutzt Netzwerkfilter zur Überwachung von laufenden Prozessen, Dateien und Registrierungsschlüsseln. HIPS stellt eine zusätzliche Funktion zum Echtzeit-Dateischutz dar und ist keine Firewall, da nur die im Betriebssystem ausgeführten Prozesse überwacht werden.

Sie finden die HIPS-Einstellungen unter **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **HIPS** > **Einfach**. Der HIPS-Status (aktiviert/deaktiviert) wird im Hauptprogrammfenster von ESET Internet Security unter **Einstellungen** > **Computer-Schutz** angezeigt.



ESET Internet Security verfügt über einen integrierten **Selbstschutzmechanismus**, der verhindert, dass Schadcode den Viren- und Spyware-Schutz beschädigt oder deaktiviert. Dieser Mechanismus schützt zentrale System- und ESET-Prozesse, Registrierungsschlüssel und Dateien vor Manipulationen.

Protected Service aktivieren – Aktiviert den Kernelschutz (Windows 8.1, 10).

Die Erweiterte Speicherprüfung bietet im Zusammenspiel mit dem Exploit-Blocker einen besseren Schutz vor Malware, die darauf ausgelegt ist, der Erkennung durch Anti-Malware-Produkte mittels Verschleierung oder Verschlüsselung zu entgehen. Die erweiterte Speicherprüfung ist standardmäßig aktiviert. Weitere Informationen zu diesem Schutztyp finden Sie im Glossar.

Der **Exploit-Blocker** sichert besonders anfällige Anwendungstypen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme und MS Office-Komponenten ab. Exploit-Blocker ist standardmäßig aktiviert. Weitere Informationen zu dieser Art des Schutzes finden Sie in unserem Glossar.

Der **Ransomware-Schutz** ist eine weitere Schutzebene im Rahmen der HIPS-Funktion. Sie müssen das LiveGrid®-Reputationssystem aktivieren, um den Ransomware-Schutz verwenden zu können. Weitere Informationen zu

diesem Schutztyp finden Sie hier.

Folgende vier Modi stehen für das Filtern zur Verfügung:

Automatischer Modus - Vorgänge werden ausgeführt, mit Ausnahme der Vorgänge, die durch vorab definierte Regeln zum Schutz Ihres Systems blockiert wurden.

Intelligenter Modus – Der Benutzer wird nur über sehr verdächtige Ereignisse benachrichtigt.

Interaktiver Modus - Der Benutzer wird zur Bestätigung von Vorgängen aufgefordert.

Regelbasierter Modus - Vorgänge werden blockiert.

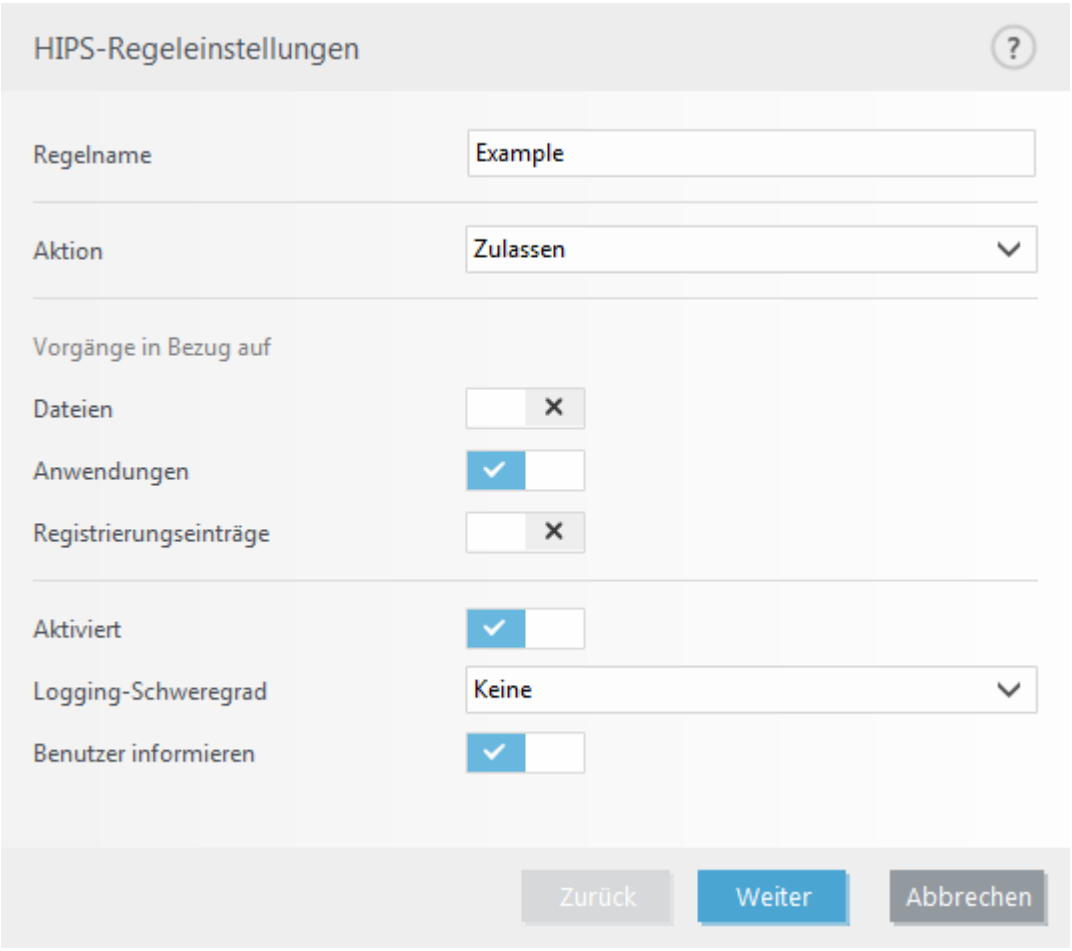
Trainingsmodus - Vorgänge werden ausgeführt und nach jedem Vorgang wird eine Regel erstellt. Die in diesem Modus erstellten Regeln können im Regel-Editor angezeigt werden, doch sie haben geringere Priorität als manuell erstellte Regeln oder Regeln, die im automatischen Modus erstellt wurden. Wenn Sie im Dropdown-Menü für den HIPS-Filtermodus den Trainingsmodus auswählen, wird die Einstellung **Ende des Trainingsmodus** verfügbar. Wählen Sie eine Zeitdauer für den Trainingsmodus aus. Die maximale Dauer beträgt 14 Tage. Wenn die festgelegte Dauer verstrichen ist, werden Sie aufgefordert, die von HIPS im Trainingsmodus erstellten Regeln zu bearbeiten. Sie können auch einen anderen Filtermodus auswählen oder die Entscheidung verschieben und den Trainingsmodus weiterverwenden.

Zu verwendender Modus nach Ablauf des Trainingsmodus – Wählen Sie aus, welcher Filtermodus nach Ablauf des Trainingsmodus verwendet werden soll.

HIPS überwacht Ereignisse auf Betriebssystemebene und führt Aktionen gemäß Regeln aus, die den Regeln für die Firewall ähneln. Klicken Sie auf **Bearbeiten** neben den Regeln, um das Fenster zur HIPS-Regelverwaltung zu öffnen. Im Fenster „HIPS-Regeln“ können Sie Regeln auswählen, hinzufügen, bearbeiten oder entfernen.

Das folgende Beispiel zeigt, wie unerwünschtes Verhalten von Anwendungen beschränkt wird:

1. Benennen Sie die Regel und wählen Sie im Dropdown-Menü **Aktion** die Option **Sperren** aus.
2. Aktivieren Sie die Option **Benutzer informieren**, damit bei jeder Anwendung einer Regel ein Benachrichtigungsfenster angezeigt wird.
3. Wählen Sie mindestens einen Vorgang aus, auf den die Regel angewendet werden soll. Wählen Sie im Fenster **Quellanwendungen** im Dropdownmenü den Eintrag **Alle Anwendungen** aus, um die neue Regel auf alle Anwendungen anzuwenden, die versuchen, einen der ausgewählten Vorgänge auszuführen.
4. Wählen Sie die Option **Zustand anderer Anwendung ändern** (Sämtliche Vorgänge sind in der Produkthilfe beschrieben, die Sie über F1 aufrufen können.).
5. Wählen Sie im Dropdownmenü den Eintrag **Bestimmte Anwendungen** aus und klicken Sie auf **Hinzufügen**, um eine oder mehrere Anwendungen hinzuzufügen, die Sie schützen möchten.
6. Klicken Sie auf **Fertig stellen**, um die neue Regel zu speichern.



4.1.4.1 Erweiterte Einstellungen

Die folgenden Optionen helfen bei der Fehlerbehebung und der Analyse des Verhaltens einer Anwendung:

Treiber dürfen immer geladen werden – Ausgewählte Treiber werden unabhängig vom konfigurierten Filtermodus immer zugelassen, sofern sie nicht durch eine Benutzerregel ausdrücklich blockiert werden.

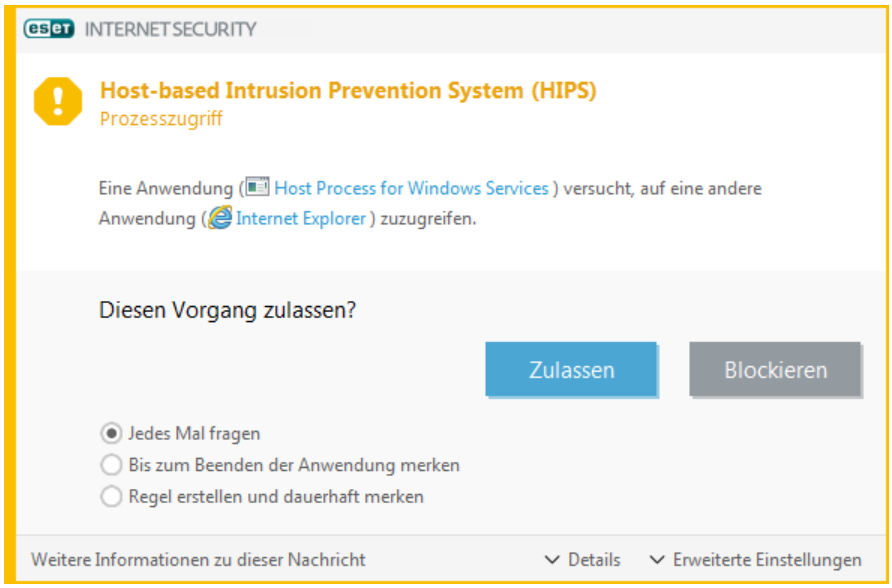
Alle blockierten Vorgänge in Log aufnehmen – Alle blockierten Vorgänge werden in das HIPS-Log geschrieben.

Änderungen an Autostart-Einträgen melden – Zeigt einen Desktophinweis an, wenn eine Anwendung vom Systemstart entfernt bzw. zum Systemstart hinzugefügt wird.

Eine aktualisierte Version dieser Hilfeseite finden Sie im unserem Knowledgebase-Artikel.

4.1.4.2 HIPS-Interaktionsfenster

Wenn **Nachfragen** als Standardaktion für eine Regel eingestellt ist, wird bei jedem Auslösen der Regel ein Dialogfeld angezeigt. Dort können Sie den Vorgang entweder **Verweigern** oder **Zulassen**. Wenn Sie innerhalb des vorgegebenen Zeitrahmens keine Aktion festlegen, wird gemäß den Regeln eine neue Aktion ausgewählt.

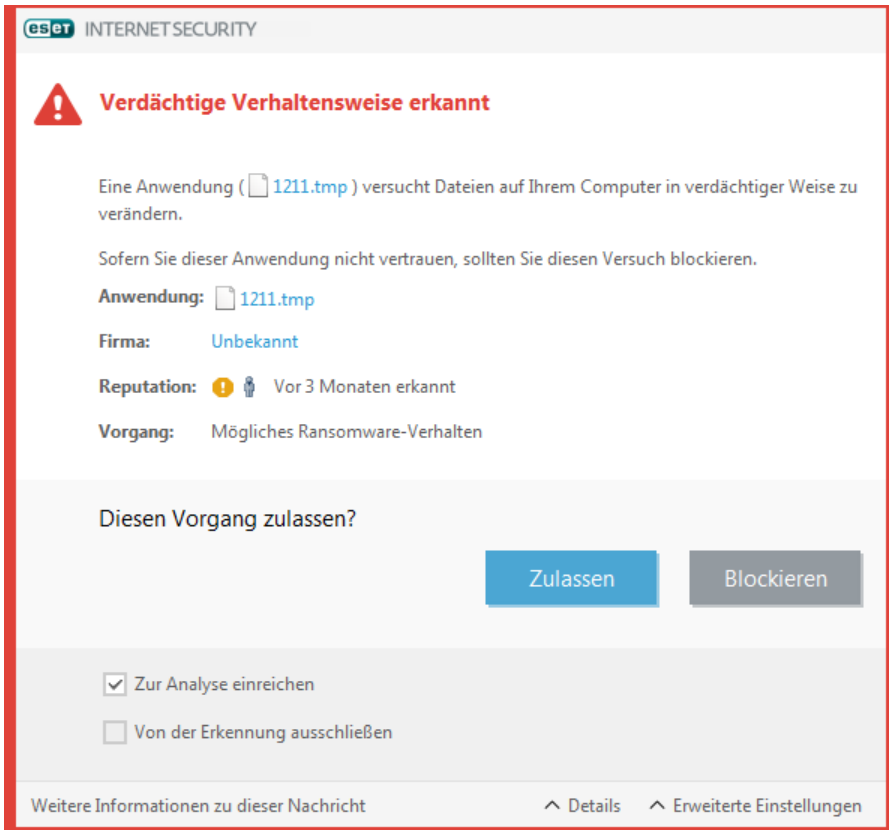


Über das Dialogfenster können Sie eine Regel erstellen, die auf einer beliebigen neuen Aktion basiert, die HIPS erkennt. Definieren Sie dann die Bedingungen, unter denen die Aktion zugelassen oder verweigert werden soll. Sie können die einzelnen Parameter unter **Details** konfigurieren. Auf diese Weise erstellte Regeln und manuell erstellte Regeln sind gleichrangig. Daher können erstere allgemeiner sein als die Regel, die das Dialogfenster ausgelöst hat. Nach dem Erstellen einer solchen Regel kann derselbe Vorgang also die Anzeige desselben Fenster auslösen.

Mit der Option Bis zum Beenden der Anwendung merken wird die Aktion (**Zulassen/Blockieren**) so lange angewendet, bis die Regeln oder der Filtermodus geändert werden, ein Update des HIPS-Moduls ausgeführt wird oder das System neu gestartet wird. Wenn eine dieser drei Aktionen (Regel- oder Filtermodusänderung, Update des HIPS-Moduls oder Neustart des Systems) ausgeführt wird, wird die vorübergehende Regel gelöscht.

4.1.4.3 Mögliches Ransomware-Verhalten erkannt

Dieses interaktive Fenster wird angezeigt, wenn ein potenzielles Ransomware-Verhalten erkannt wird. Dort können Sie den Vorgang entweder **Verweigern** oder **Zulassen**.



Im Dialogfeld können Sie die **Datei zur Analyse einreichen** oder **von der Erkennung ausschließen**. Klicken Sie auf **Details**, um weitere Erkennungsparameter anzuzeigen.

WICHTIG
Für den ordnungsgemäßen Betrieb des Ransomware-Schutzes muss ESET Live Grid aktiviert sein.

4.1.5 Gamer-Modus

Der Gamer-Modus ist eine Funktion für Benutzer, die ihre Software ununterbrochen nutzen, nicht durch Popup-Fenster gestört werden und die CPU-Auslastung reduzieren möchten. Der Gamer-Modus kann auch während Präsentationen verwendet werden, die nicht durch eine Aktion des Virenschutzes unterbrochen werden dürfen. In diesem Modus werden alle Popup-Fenster deaktiviert, und die Aktivität des Taskplaners wird komplett gestoppt. Der Systemschutz läuft weiter im Hintergrund, doch es sind keine Eingaben durch Benutzer erforderlich.

Sie können den Gamer-Modus im Hauptfenster unter **Einstellungen** > **Computer-Schutz** aktivieren, indem Sie auf oder neben **Gamer-Modus** klicken. Im Gamer-Modus besteht ein erhöhtes Risiko. Daher wird das Schutzstatus-Symbol in der Taskleiste orange und mit einer Warnung angezeigt. Diese Warnung wird auch im Hauptprogrammfenster zusammen mit dem orangefarbenen Hinweis **Gamer-Modus aktiviert** angezeigt.

Mit der Option **Gamer-Modus automatisch aktivieren, wenn Anwendungen im Vollbildmodus ausgeführt werden** unter **Erweiterte Einstellungen** (F5) > **Tools** > **Gamer-Modus** wird der Gamer-Modus gestartet, sobald Sie eine Anwendung im Vollbildmodus ausführen und automatisch beendet, sobald Sie die Anwendung beenden.

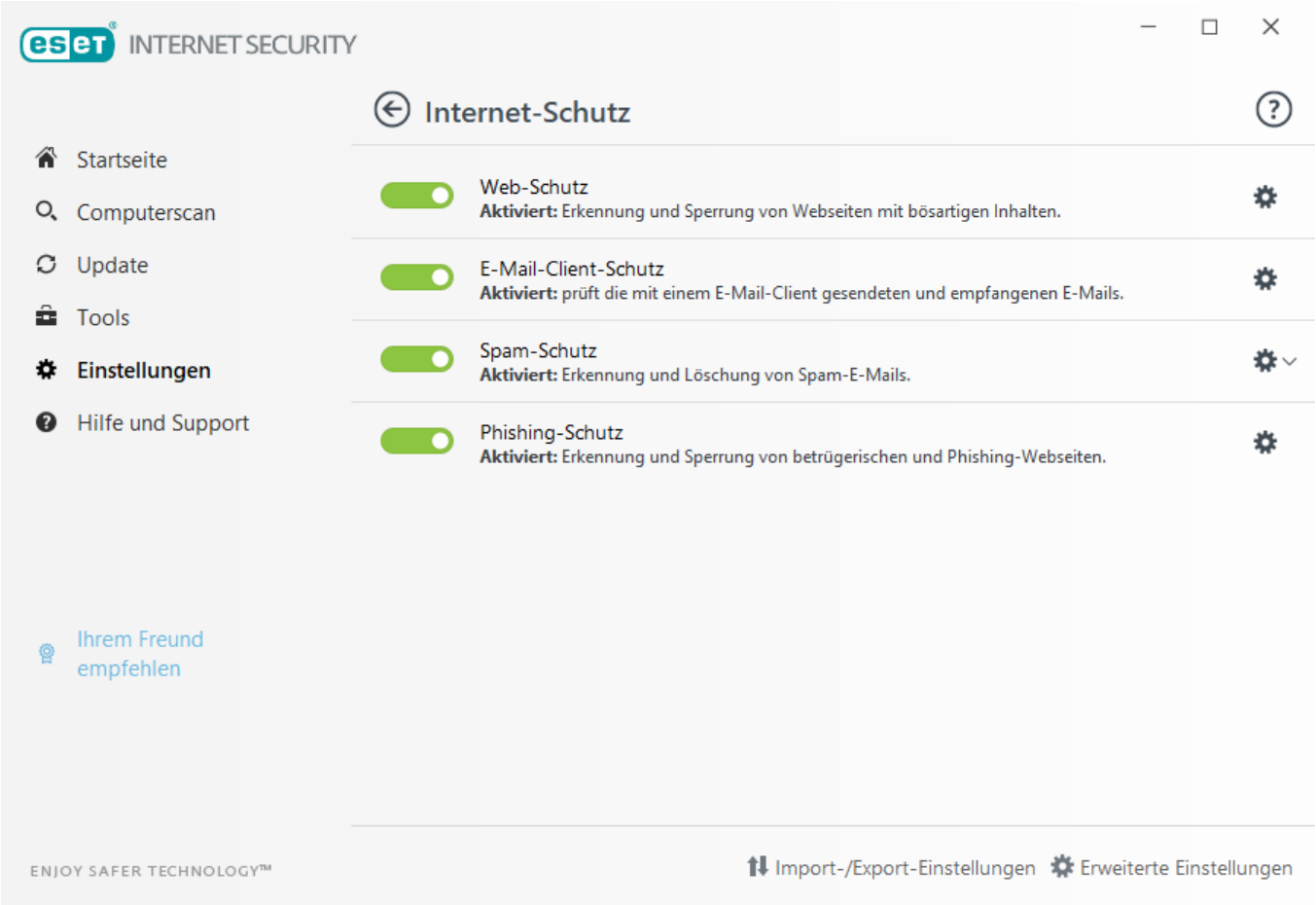
Mit der Option **Gamer-Modus automatisch deaktivieren nach** können Sie außerdem festlegen, nach wie vielen Minuten der Gamer-Modus automatisch deaktiviert werden soll.

HINWEIS
Wenn für die Firewall der interaktive Filtermodus eingestellt ist und der Gamer-Modus aktiviert wird, kann es zu Problemen beim Aufbau einer Internetverbindung kommen. Dies kann beim Ausführen eines Online-Spiels zu

Problemen führen. Üblicherweise müssen Sie eine solche Aktion bestätigen (sofern keine Verbindungsregeln oder -ausnahmen festgelegt wurden), doch im Gamer-Modus kann der Benutzer keine derartigen Eingaben machen. Um die Kommunikation zuzulassen, können Sie eine Kommunikationsregel für alle Anwendungen definieren, bei denen dieses Problem auftritt, oder einen anderen Filtermodus in der Firewall verwenden. Wenn im Gamer-Modus eine Website besucht oder eine Anwendung ausgeführt wird, die möglicherweise Sicherheitsrisiken darstellen, werden Sie möglicherweise nicht darüber benachrichtigt, dass diese blockiert sind. Grund dafür ist die deaktivierte Benutzerinteraktion.

4.2 Internet-Schutz

Sie können die Einstellungen für den Web- und E-Mail-Schutz im Fenster **Einstellungen** konfigurieren, indem Sie auf **Internet-Schutz** klicken. Von hier aus können Sie auf erweiterte Einstellungen des Programms zugreifen.



Der Internetzugang ist eine Standardfunktion von Computern. Leider ist das Internet mittlerweile auch der wichtigste Weg zur Verbreitung von Schadsoftware. Daher müssen Sie die Einstellungen des **Web-Schutzes** sorgfältig auswählen.

Klicken Sie auf ⚙, um die Web-/E-Mail-/Phishing-/Spam- Schutzeinstellungen in den erweiterten Einstellungen zu öffnen.

Der E-Mail-Schutz überwacht eingehende E-Mails, die mit dem POP3- oder IMAP-Protokoll übertragen werden. Mithilfe der Plug-In-Software für Ihr E-Mail-Programm stellt ESET Internet Security Kontrollfunktionen für die gesamte ein- und ausgehende E-Mail-Kommunikation (POP3, MAPI, IMAP, HTTP) bereit.

Der **Spam-Schutz** filtert unerwünschte E-Mails heraus.

Über das Zahnrad ⚙ neben **Spam-Schutz**, haben Sie Zugriff auf die folgenden Optionen:

Konfigurieren... - Öffnet erweiterte Einstellung für den Spam-Schutz von E-Mail-Clients.

Positivliste/Negativliste/Ausnahmeliste des Benutzers – Es wird ein Dialogfenster geöffnet, über das als sicher oder unsicher eingestufte E-Mail-Adressen hinzugefügt, bearbeitet oder gelöscht werden können. Gemäß den an dieser Stelle definierten Regeln werden von diesen Adressen stammende E-Mails nicht geprüft oder als Spam behandelt. Klicken Sie auf die **Ausnahmeliste des Benutzers**, um E-Mail-Adressen hinzuzufügen, zu bearbeiten oder zu löschen, die möglicherweise gefälscht wurden und als Spam-Absender verwendet werden. E-Mails, deren Absender in der Ausnahmeliste stehen, werden immer auf Spam geprüft.

Der Phishing-Schutz blockiert Webseiten, die bekanntermaßen Phishing-Inhalte verbreiten. Es wird dringend empfohlen, den Phishing-Schutz aktiviert zu lassen.

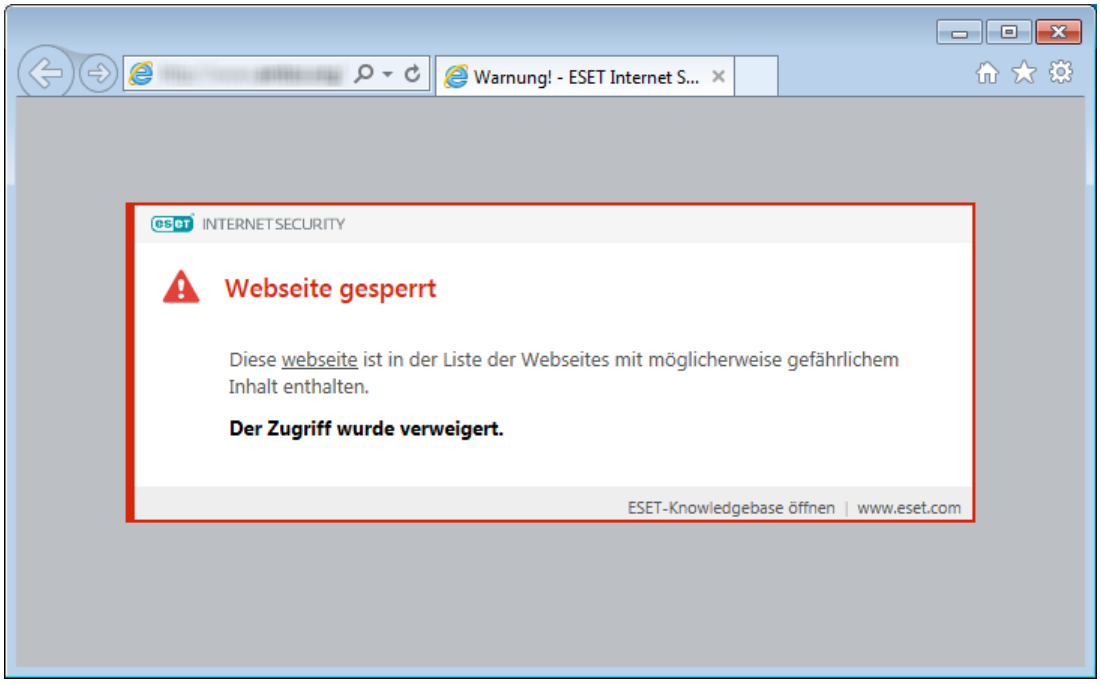
Sie können den Web-/E-Mail-/Phishing/Spam- Schutz kann durch Klicken auf  vorübergehend deaktivieren.

4.2.1 Web-Schutz

Der Internetzugang ist eine Standardfunktion von Computern. Leider ist diese technische Möglichkeit mittlerweile auch der wichtigste Weg zur Verbreitung von Schadsoftware. Der Web-Schutz besteht in der Überwachung der Kommunikation zwischen Webbrowsern und Remoteservern und entspricht den Regeln für HTTP (Hypertext Transfer Protocol) und HTTPS (verschlüsselte Kommunikation).

Der Zugriff auf Webseiten, die bekannterweise Schadcode enthalten, wird vor dem Herunterladen von Inhalt blockiert. Alle anderen Webseiten werden beim Laden vom ThreatSense-Prüfmodul geprüft und blockiert, wenn Schadcode gefunden wird. Der Web-Schutz bietet zwei Schutzebenen: Blockieren nach Negativliste und Blockieren nach Inhalt.

Wir empfehlen dringend, den Web-Schutz zu aktivieren. Sie finden diese Option im Hauptfenster von ESET Internet Security unter **Einstellungen** > **Internet-Schutz** > **Web-Schutz**.



Unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **Web-Schutz** stehen die folgenden Optionen zur Verfügung:

- **Web-Protokolle** – Hier können Sie die Überwachung dieser von den meisten Internetbrowsern verwendeten Standardprotokolle konfigurieren.
- **URL-Adressverwaltung** – Hier können Sie festlegen, welche HTTP-Adressen blockiert, zugelassen oder von der Prüfung ausgeschlossen werden sollen.
- **ThreatSense -Parameter** – In diesem Bereich finden Sie erweiterte Einstellungen für den Virenschutz. Hier können Sie Einstellungen für zu prüfende Objekte (E-Mails, Archive usw.), Erkennungsmethoden für den Web-Schutz usw. festlegen.

4.2.1.1 Einfach

Web-Schutz aktivieren – Wenn diese Option deaktiviert ist, funktionieren Web-Schutz und Phishing-Schutz nicht.

Erweiterte Überprüfung von Browser-Skripts aktivieren – Wenn diese Option aktiviert ist, werden alle in Internet-Browsern ausgeführten JavaScript-Programme vom Virenschutz-Scanner geprüft.

HINWEIS
Der Web-Schutz sollte unbedingt immer aktiviert sein.

4.2.1.2 Webprotokolle

ESET Internet Security ist standardmäßig so konfiguriert, dass das von den meisten Internetbrowsern verwendete HTTP-Protokoll überwacht wird.

Einstellungen für den HTTP-Scanner

Unter Windows Vista und neuer werden HTTP-Verbindungen immer an allen Ports in allen Anwendungen überwacht. Unter Windows XP können Sie die vom **HTTP-Protokoll verwendeten Ports** unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **Web-Schutz** > **Web-Protokolle** ändern. HTTP-Verbindungen werden an den angegebenen Ports in allen Anwendungen sowie an allen Ports zu Anwendungen überwacht, die als Web- und E-Mail-Clients markiert sind.

Einstellungen für den HTTPS-Scanner

ESET Internet Security unterstützt auch die HTTPS-Protokollprüfung. Bei der HTTPS-Kommunikation wird zur Datenübertragung zwischen Server und Client ein verschlüsselter Kanal verwendet. ESET Internet Security überwacht die mit Hilfe der Protokolle SSL (Secure Socket Layer) und TLS (Transport Layer Security) abgewickelte Kommunikation. Unabhängig von der Version des Betriebssystems wird nur Datenverkehr an Ports gescannt, die unter **Vom HTTPS-Protokoll verwendete Ports** definiert wurden.

Verschlüsselter Datenverkehr wird standardmäßig geprüft. Um die Prüfeinstellungen anzuzeigen, navigieren Sie zu SSL/TLS in den erweiterten Einstellungen, klicken Sie auf **Web und E-Mail** > **SSL/TLS**, und aktivieren Sie die Option **SSL/TLS-Protokollfilterung aktivieren**.

4.2.1.3 URL-Adressverwaltung

Im Bereich URL-Adressverwaltung können Sie festlegen, welche HTTP-Adressen blockiert, zugelassen oder von der Prüfung ausgeschlossen werden sollen.

Websites in der **Liste der blockierten Adressen** können nur geöffnet werden, wenn diese sich auch in der **Liste der zulässigen Adressen** befinden. Websites in der **Liste der von der Prüfung ausgenommenen Adressen** werden vor dem Zugriff nicht auf Schadcode gescannt.

Wenn neben HTTP-Webseiten auch HTTPS-Adressen gefiltert werden sollen, muss die Option SSL/TLS-Protokollfilterung aktivieren aktiviert sein. Andernfalls werden nur die Domains besuchter HTTPS-Sites hinzugefügt, nicht aber die URL.

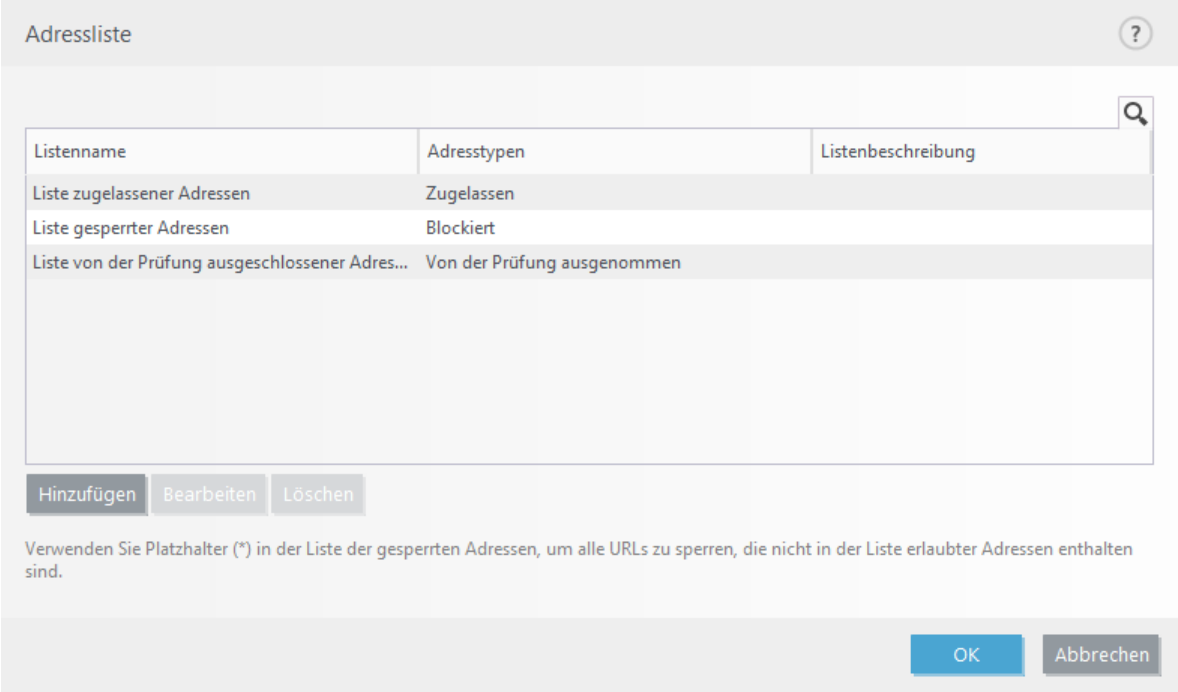
Wenn Sie eine URL-Adresse zur **Liste der von der Prüfung ausgenommenen Adressen** hinzufügen, wird diese von der Prüfung ausgenommen. Sie können auch bestimmte Adressen zulassen oder blockieren, indem Sie sie zur **Liste zugelassener Adressen** oder zur **Liste blockierter Adressen** hinzufügen.

Wenn alle HTTP-Adressen außer denen in der aktiven **Liste zugelassener Adressen** blockiert werden sollen, fügen Sie der aktiven **Liste blockierter Adressen** ein Sternchen (*) hinzu.

Die Sonderzeichen „*“ (Sternchen) und „?“ (Fragezeichen) können in Listen verwendet werden. Das Sternchen ersetzt eine beliebige Zeichenfolge, das Fragezeichen ein beliebiges Symbol. Die Liste der ausgeschlossenen Adressen sollten Sie mit Bedacht zusammenstellen. Geben Sie ausschließlich vertrauenswürdige und sichere Adressen an. Achten Sie darauf, dass die Zeichen „*“ und „?“ korrekt verwendet werden. Unter Maske für HTTP-Adressen/Domains hinzufügen finden Sie Informationen zur sicheren Angabe gesamter Domänen inklusive

Unterdomänen. Um eine Liste zu aktivieren, wählen Sie die Option **Liste aktiv**. Wenn Sie benachrichtigt werden möchten, wenn Sie eine Adresse aus der aktuellen Liste eingeben, wählen Sie **Bei Anwendung benachrichtigen** aus.

HINWEIS
Mit der URL-Adressverwaltung können Sie auch das Öffnen bestimmter Dateitypen beim Internetsurfen blockieren bzw. erlauben. Wenn Sie z. B. das Öffnen ausführbarer Dateien verbieten möchten, wählen Sie im Dropdownmenü die Liste aus, in der Sie diese Dateien sperren möchten, und geben Sie „**.exe“ ein.



Steuerelemente

Hinzufügen – Erstellen einer neuen Liste zusätzlich zu den vordefinierten. Dies kann nützlich sein, wenn Sie verschiedene Gruppen und Adressen auf logische Art und Weise aufteilen möchten. So kann eine Liste blockierter Adressen beispielsweise Adressen aus einer externen öffentlichen Negativliste und eine zweite eigene Negativliste enthalten. Auf diese Weise lässt sich die externe Liste einfacher aktualisieren, während Ihre Liste intakt bleibt.

Bearbeiten – Bearbeiten bestehender Listen. Hiermit können Sie Adressen zu den Listen hinzufügen oder daraus entfernen.

Löschen – Löschen bestehender Listen. Es können nur Listen entfernt werden, die mit der Option **Hinzufügen** erstellt wurden; nicht Standardlisten.

4.2.2 E-Mail-Schutz

4.2.2.1 E-Mail-Programme

Die Integration von ESET Internet Security mit Ihrem E-Mail-Client verbessert den aktiven Schutz vor Schadcode in E-Mail-Nachrichten. Wenn Ihr E-Mail-Programm dies unterstützt, kann die Integration in ESET Internet Security aktiviert werden. Mit der Integration in Ihren E-Mail-Client wird die ESET Internet Security-Symbolleiste direkt im E-Mail-Programm angezeigt und ermöglicht einen effizienteren E-Mail-Schutz (bei neueren Versionen von Windows Live Mail wird die Symbolleiste nicht integriert). Sie finden die Integrationseinstellungen unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **E-Mail-Schutz** > **E-Mail-Programme**.

Integration in E-Mail-Programme

Zu den derzeit unterstützten E-Mail-Programmen gehören Microsoft Outlook, Outlook Express, Windows Mail und Windows Live Mail. Der E-Mail-Schutz ist ein Plug-In für diese Programme. Das Plugin funktioniert unabhängig vom eingesetzten Protokoll. Wenn beim E-Mail-Client eine verschlüsselte Nachricht eingeht, wird

diese entschlüsselt und an das Virenschutz-Prüfmodul weitergeleitet. Eine vollständige Liste der unterstützten E-Mail-Programme und Versionen finden Sie im entsprechenden ESET-Knowledgebase-Artikel.

Auch bei nicht aktivierter Integration ist die E-Mail-Kommunikation durch den E-Mail-Schutz (POP3, IMAP) weiterhin geschützt.

Aktivieren Sie die Option **Prüfen neuer Elemente im Posteingang deaktivieren**, falls bei der Arbeit mit Ihrem E-Mail-Programm die Systemleistung beeinträchtigt wird (nur MS Outlook). Dies kann der Fall sein, wenn Sie E-Mails vom Kerio Outlook Connector Store abrufen.

Zu prüfende E-Mails

E-Mail-Schutz durch Client-Plugins aktivieren – Wenn der E-Mail-Schutz durch Clients deaktiviert ist, bleibt der E-Mail-Schutz durch Protokollfilterung weiterhin aktiv.
Eingehende E-Mails - Aktiviert/deaktiviert die Überprüfung empfangener Nachrichten.
Ausgehende E-Mails - Aktiviert/deaktiviert die Überprüfung ausgehender Nachrichten.
E-Mails, die zum Lesen geöffnet werden - Aktiviert/deaktiviert die Überprüfung gelesener Nachrichten.

Aktion für infizierte E-Mails

Keine Aktion - Infizierte Anhänge werden erkannt, aber es werden keine Aktionen für E-Mails durchgeführt.
E-Mail löschen - Es werden Hinweise zu Bedrohungen angezeigt. Betroffene E-Mails werden gelöscht.
In den Ordner „Gelöschte Objekte“ verschieben - Infizierte E-Mails werden automatisch in den Ordner „Gelöschte Objekte“ verschoben.
In Ordner verschieben - Infizierte E-Mails werden automatisch in den angegebenen Ordner verschoben.

Ordner – Geben Sie den Ordner an, in den erkannte infizierte E-Mails verschoben werden sollen.

Prüfung nach Update der Erkennungsroutine wiederholen - Aktiviert/deaktiviert die erneute Prüfung nach einem Update der Erkennungsroutine.

Prüfergebnisse von anderen Modulen akzeptieren - Wenn diese Option aktiviert ist, nimmt das E-Mail-Schutz-Modul Prüfergebnisse von anderen Modulen entgegen (POP3-, IMAP-Protokollprüfung).

HINWEIS
Die Optionen **E-Mail-Schutz durch Client-Plugins aktivieren** und **E-Mail-Schutz durch Protokollfilterung aktivieren** sollten nach Möglichkeit immer aktiviert sein. Sie finden diese Einstellungen unter Erweiterte Einstellungen (F5) > Web und E-Mail > E-Mail-Schutz > E-Mail-Programme.

4.2.2.2 E-Mail-Protokolle

IMAP und POP3 sind die gängigsten Protokolle für den Empfang von E-Mails in E-Mail-Clientanwendungen. IMAP (Internet Message Access Protocol) ist ein weiteres Internetprotokoll für das Abrufen von E-Mails. IMAP bietet gegenüber POP3 einige Vorteile. Beispielsweise können sich mehrere Clients gleichzeitig beim selben Postfach anmelden und Statusinformationen zu den Nachrichten pflegen, z. B. ob die Nachricht gelesen, beantwortet oder gelöscht wurde. ESET Internet Security bietet Schutz für diese Protokolle, ganz gleich, welcher E-Mail-Client verwendet wird. Dieser braucht auch nicht neu konfiguriert zu werden.

Das Modul für diesen Schutz wird beim Systemstart automatisch gestartet und bleibt danach im Arbeitsspeicher aktiv. Die IMAP-Prüfung wird automatisch ausgeführt, ohne das E-Mail-Programm neu konfigurieren zu müssen. Standardmäßig wird der gesamte Datenverkehr über Port 143 geprüft; weitere Kommunikationsports können bei Bedarf hinzugefügt werden. Mehrfache Portnummern müssen durch ein Komma voneinander getrennt sein.

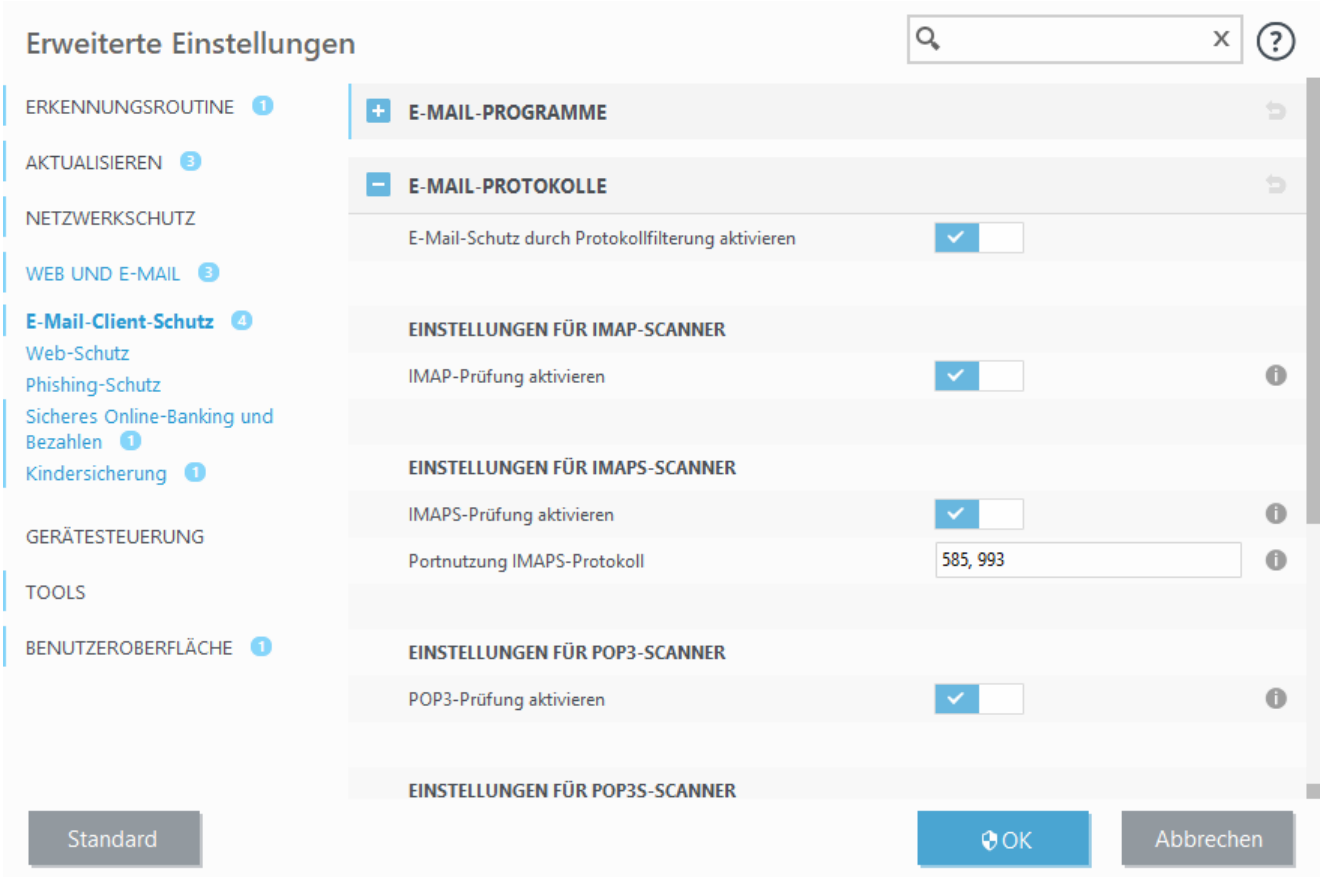
Die IMAP/IMAPS- und POP3/POP3S-Protokollprüfung kann in den erweiterten Einstellungen konfiguriert werden. Sie finden diese Einstellung unter **Web und E-Mail** > **E-Mail-Schutz** > **E-Mail-Protokolle**.

E-Mail-Schutz durch Protokollfilterung aktivieren – Aktiviert die Prüfung von E-Mail-Protokollen.

Unter Windows Vista und neuer werden IMAP- und POP3-Protokolle automatisch erkannt und an allen Ports geprüft. Unter Windows XP werden nur die unter **Portnutzung IMAP-/POP3-Protokoll** konfigurierten Ports für alle Anwendungen gescannt. Außerdem werden alle Ports für Anwendungen gescannt, die als Web- und E-Mail-Clients markiert sind.

ESET Internet Security unterstützt außerdem das Scannen von IMAPS- und POP3S-Protokollen, die Daten zwischen Server und Client über einen verschlüsselten Kanal übertragen. ESET Internet Security überwacht die über die Protokolle SSL (Secure Socket Layer) und TLS (Transport Layer Security) abgewickelte Kommunikation. Unabhängig von der Version des Betriebssystems wird nur Datenverkehr an Ports gescannt, die in **Portnutzung IMAPS-/POP3S-Protokoll** definiert wurden.

Verschlüsselter Datenverkehr wird standardmäßig geprüft. Um die Prüfeinstellungen anzuzeigen, navigieren Sie zu SSL/TLS in den erweiterten Einstellungen, klicken Sie auf **Web und E-Mail** > **SSL/TLS**, und aktivieren Sie die Option **SSL/TLS-Protokollfilterung aktivieren**.



4.2.2.3 Warnungen und Hinweise

Der E-Mail-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3-Protokoll übertragen werden. ESET Internet Security bietet Kontrollfunktionen für die gesamte E-Mail-Kommunikation (POP3, MAPI, IMAP, HTTP) über die Plugins für Microsoft Outlook und andere E-Mail-Clients. Für die Prüfung eingehender Nachrichten verwendet das Programm alle erweiterten ThreatSense-Prüfmethoden. Die Erkennung von Schadcode findet also noch vor dem Abgleich mit der Erkennungsroutine statt. Die Prüfung der POP3-Kommunikation erfolgt unabhängig vom verwendeten E-Mail-Programm.

Die Optionen für diese Funktion finden Sie unter **Erweiterte Einstellungen** unter **Web und E-Mail** > **E-Mail-Schutz** > **Warnungen und Hinweise**.

Nach erfolgter Prüfung kann ein Prüfhinweis zu der E-Mail-Nachricht hinzugefügt werden. Sie haben folgende Optionen: **Prüfhinweis zu eingehenden/gelesenen E-Mails hinzufügen**, **Prüfhinweis an den Betreff empfangener und gelesener infizierter E-Mails anhängen** oder **Prüfhinweis zu ausgehenden E-Mails hinzufügen**. Es kann jedoch nicht ausgeschlossen werden, dass bestimmte Bedrohungen Prüfhinweise in problematischen HTML-Nachrichten fälschen oder löschen. Prüfhinweise können zu empfangenen und gelesenen E-Mails und/oder zu gesendeten E-Mails hinzugefügt werden. Folgende Optionen stehen zur Verfügung:

- **Nie** – Es werden keine Prüfhinweise hinzugefügt.
- **Nur an infizierte E-Mails** - Prüfhinweise werden nur E-Mails hinzugefügt, in denen Schadcode erkannt wurde (Standardeinstellung).
- **Bei allen geprüften E-Mails** - Alle geprüften E-Mails werden mit Prüfhinweisen versehen.

Prüfhinweis an den Betreff gesendeter infizierter E-Mails anhängen - Deaktivieren Sie dieses Kontrollkästchen, wenn keine Prüfhinweise zu den Betreffzeilen infizierter E-Mails hinzugefügt werden sollen. Ohne großen Aufwand können Sie in Ihrem E-Mail-Programm eine Filterregel erstellen, die diesen Prüfhinweis erkennt (falls Ihr E-Mail-Programm Filterregeln unterstützt). Diese Funktion erhöht außerdem die Glaubwürdigkeit beim Empfänger. Wenn eine Infiltration erkannt wird, liefert diese Funktion wertvolle Informationen zur Gefährdung durch eine bestimmte E-Mail oder einen Absender.

Text, der zur Betreffzeile infizierter E-Mails hinzugefügt wird - Geben Sie hier den Text ein, der das Präfix in der Betreffzeile einer infizierten E-Mail ersetzen soll. Mit dieser Funktion wird der Nachrichtenbetreff *„Hallo“* mit dem voreingestellten Präfix *„[virus]“* folgendermaßen gekoppelt: *„[virus] Hallo“*. Dabei repräsentiert die Variable *% VIRUSNAME%* die erkannte Bedrohung.

4.2.2.4 Integration mit E-Mail-Programmen

Die Integration von ESET Internet Security mit E-Mail-Programmen verbessert den aktiven Schutz gegen Schadcode in E-Mail-Nachrichten. Wenn Ihr E-Mail-Programm dies unterstützt, kann die Integration in ESET Internet Security aktiviert werden. Bei aktivierter Integration wird die ESET Internet Security-Symbolleiste vom E-Mail-Programm übernommen, d. h. die Verbindungen werden kontrolliert und die E-Mail-Kommunikation wird dadurch sicherer. Die Integrationseinstellungen befinden sich unter **Einstellungen** > **Erweiterte Einstellungen** > **Web und E-Mail** > **E-Mail-Schutz** > **E-Mail-Clients**.

Zu den derzeit unterstützten E-Mail-Programmen gehören Microsoft Outlook, Outlook Express, Windows Mail und Windows Live Mail. Eine vollständige Liste der unterstützten E-Mail-Programme und Versionen finden Sie im entsprechenden ESET-Knowledgebase-Artikel.

Wählen Sie die Option **Prüfen neuer Elemente im Posteingang deaktivieren**, falls Sie während der Arbeit mit Ihrem E-Mail-Programm eine Systemverlangsamung bemerken. Dies kann der Fall sein, wenn Sie E-Mails vom Kerio Outlook Connector Store abrufen.

Auch bei nicht aktivierter Integration ist die E-Mail-Kommunikation durch den E-Mail-Schutz (POP3, IMAP) weiterhin geschützt.

4.2.2.4.1 Konfiguration des E-Mail-Schutzes

Der E-Mail-Schutz unterstützt folgende E-Mail-Clients: Microsoft Outlook, Outlook Express, Windows Mail und Windows Live Mail. Der E-Mail-Schutz ist ein Plug-In für diese Programme. Das Plugin funktioniert unabhängig vom eingesetzten Protokoll. Wenn beim E-Mail-Client eine verschlüsselte Nachricht eingeht, wird diese entschlüsselt und an das Virenschutz-Prüfmodul weitergeleitet.

4.2.2.5 POP3, POP3S-Prüfung

Das POP3-Protokoll ist das am häufigsten verwendete Protokoll zum Empfangen von E-Mails mit einem E-Mail-Programm. ESET Internet Security bietet POP3-Protokoll-Schutzfunktionen unabhängig vom verwendeten E-Mail-Programm.

Das Modul, das diese Kontrollfunktion bereitstellt, wird automatisch beim Systemstart initialisiert und ist dann im Speicher aktiv. Um das Modul einsetzen zu können, muss es aktiviert sein. Die POP3-Prüfung wird automatisch ausgeführt, ohne dass das E-Mail-Programm neu konfiguriert werden muss. In der Standardeinstellung wird die gesamte Kommunikation über Port 110 geprüft. Bei Bedarf können weitere Kommunikationsports hinzugefügt werden. Mehrfache Portnummern müssen durch ein Komma voneinander getrennt sein.

Verschlüsselter Datenverkehr wird standardmäßig geprüft. Um die Prüfeinstellungen anzuzeigen, navigieren Sie zu SSL/TLS in den erweiterten Einstellungen, klicken Sie auf **Web und E-Mail** > **SSL/TLS**, und aktivieren Sie die Option **SSL/TLS-Protokollfilterung aktivieren**.

In diesem Abschnitt können Sie die Prüfung der Protokolle POP3 und POP3S konfigurieren.

POP3-Prüfung aktivieren – Wenn diese Option aktiviert ist, werden alle Daten geprüft, die über POP3 übertragen werden.

Portnutzung POP3-Protokoll – Eine Liste von Ports, die vom POP3-Protokoll verwendet werden (standardmäßig 110).

ESET Internet Security unterstützt auch die Überwachung von POP3S-Protokollen. Bei dieser Kommunikationsart wird zur Datenübertragung zwischen Server und Client ein verschlüsselter Kanal verwendet. ESET Internet Security überwacht die mit Hilfe der Verschlüsselungsverfahren SSL (Secure Socket Layer) und TLS (Transport Layer Security) abgewickelte Kommunikation.

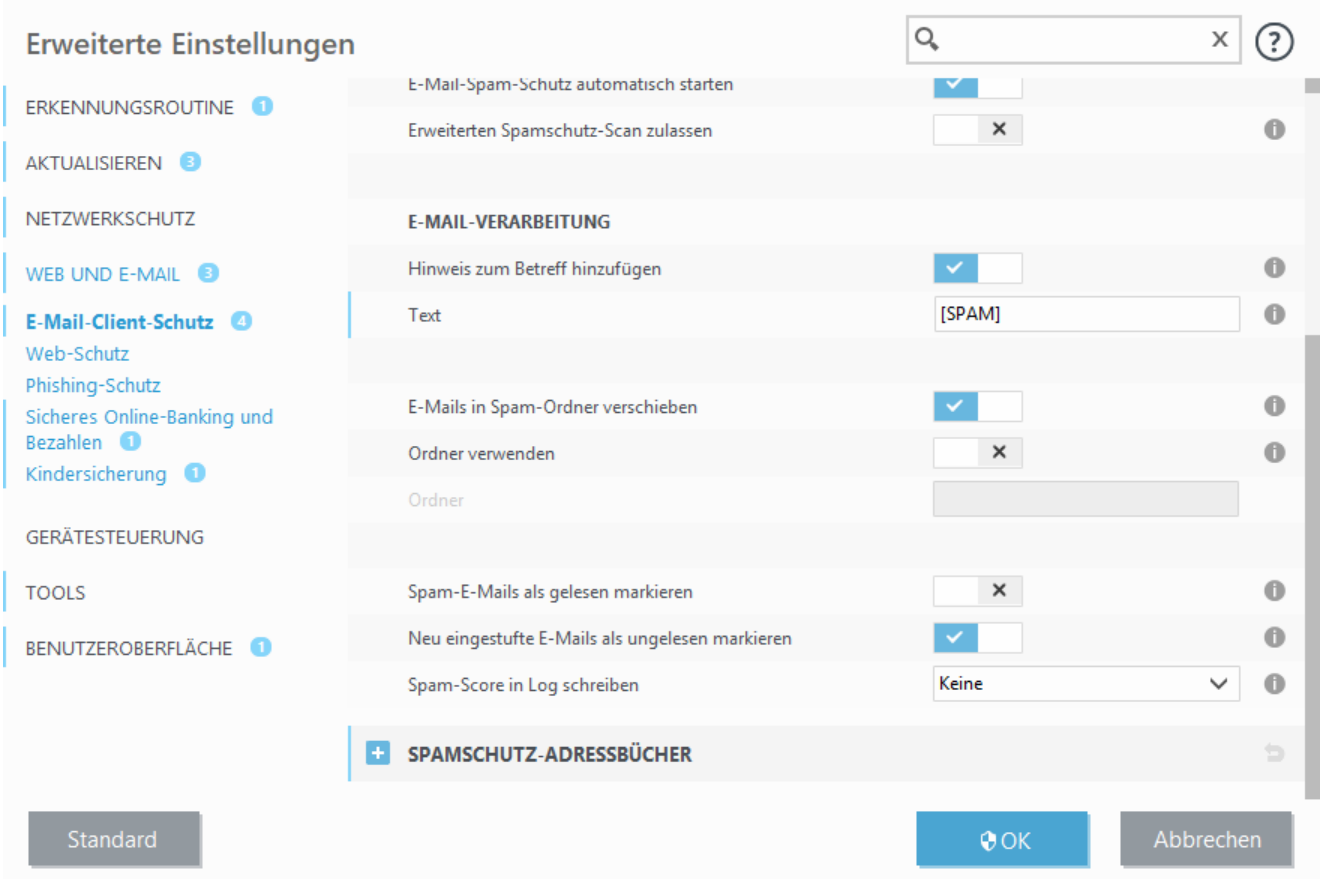
Keine POP3S-Prüfung verwenden – Verschlüsselte Kommunikation wird nicht geprüft.

POP3S-Protokollprüfung für ausgewählte Ports durchführen – Die POP3S-Prüfung wird nur für die unter **Portnutzung POP3-Protokoll** festgelegten Ports durchgeführt.

Portnutzung POP3S-Protokoll – Eine Liste zu prüfender POP3S-Ports (standardmäßig 995).

4.2.2.6 Spam-Schutz

Spam, d. h. unerwünschte E-Mails, stellt ein zentrales Problem der elektronischen Kommunikation dar. Spam macht bis zu 80 Prozent der gesamten E-Mail-Kommunikation aus. Der Spam-Schutz nimmt dieses Problem in Angriff. Verschiedene E-Mail-Sicherheitsverfahren sorgen für ausgezeichnete Filterquoten und halten so Ihren Posteingang frei von Spam.



Ein zentrales Prinzip beim Spam-Schutz ist die Möglichkeit der Erkennung unerwünschter E-Mails über eine Positiv- bzw. eine Negativliste. In der Positivliste werden vertrauenswürdige E-Mail-Adressen, in der Negativliste Spam-Adressen vorab definiert. Alle Adressen in Ihrer Kontaktliste sowie alle vom Benutzer als „sicher“ eingestuften Adressen werden automatisch der Positivliste hinzugefügt.

Die primäre Methode zur Spam-Erkennung ist die Prüfung der E-Mail-Eigenschaften. Empfangene Nachrichten werden anhand grundlegender Spam-Kriterien und mithilfe spezifischer Methoden (Nachrichtendefinitionen, statistische Heuristik, Erkennung von Algorithmen usw.) geprüft. Der sich daraus ergebende Indexwert entscheidet darüber, ob eine Nachricht als Spam eingestuft wird oder nicht.

E-Mail-Spam-Schutz automatisch starten - Aktivieren Sie diese Option, um den Spam-Schutz beim Systemstart automatisch zu starten.

Erweiterte Spamschutz-Prüfung zulassen – Aktivieren Sie diese Option, um regelmäßig zusätzliche Spam-Schutz-Daten herunterzuladen. Dies erweitert den Spam-Schutz und ermöglicht bessere Ergebnisse.

Mit dem Spam-Schutz von ESET Internet Security können Sie für die Verwaltung Ihrer Adresslisten verschiedene Parameter festlegen. Die folgenden Optionen stehen Ihnen zur Verfügung:

Prüfen von E-Mails

Hinweis zum Betreff hinzufügen – Sie können einen Hinweistext festlegen, der zur Betreffzeile von E-Mails hinzugefügt wird, die als Spam eingestuft wurden. Der Standardtext ist „[SPAM]“.

E-Mails in Spam-Ordner verschieben – Wenn diese Option aktiviert ist, werden Spam-Nachrichten in den standardmäßigen Spam-Ordner verschoben. Nachrichten, die als „kein Spam“ neu eingestuft wurden, werden zurück in den Posteingang verschoben. Wenn Sie mit der rechten Maustaste auf eine E-Mail-Nachricht klicken und ESET Internet Security aus dem Kontextmenü auswählen, können Sie aus den zutreffenden Optionen auswählen.

Verschieben in Ordner – Sie können selbst einen Ordner festlegen, in den Spam-E-Mails verschoben werden sollen.

Spam-E-Mails als gelesen markieren - Aktivieren Sie dieses Kontrollkästchen, wenn Spam-E-Mails automatisch als gelesen markiert werden sollen. „Saubere“ Nachrichten sind dann leichter erkennbar.

E-Mails, die vom Benutzer neu eingestuft werden, als ungelesen markieren - Vermeintliche Spam-E-Mails, die Sie manuell als „KEIN Spam“ einstufen, werden als ungelesen markiert.

Spam-Score in Log schreiben – Das Spam-Schutz-Modul von ESET Internet Security berechnet für jede geprüfte Nachricht einen Spam-Score. Die Nachricht wird im Spam-Schutz-Log protokolliert (**ESET Internet Security** > **Tools** > **Log-Dateien** > **Spam-Schutz**).

- **Keine** – Der Score der Spam-Schutz-Prüfung wird nicht aufgezeichnet.
- **Neu eingestuft und als Spam markiert** – Wählen Sie diese Option aus, wenn Sie für als Spam markierte Nachrichten einen Spam-Score aufzeichnen möchten.
- **Alle** - Alle Nachrichten werden im Log mit ihrem Spam-Score protokolliert.

HINWEIS
Wenn Sie im Spam-Ordner auf eine Nachricht klicken, können Sie **Ausgewählte E-Mail(s) als „KEIN Spam“ einstufen**. Die betroffene Nachricht wird dann in den Posteingang verschoben. Wenn Sie im Posteingang auf eine Nachricht klicken, die Sie für Spam halten, klicken Sie auf **E-Mails als Spam einstufen**. Die betroffene Nachricht wird dann in den Spam-Ordner verschoben. Sie können mehrere Nachrichten auswählen und die Aktion gleichzeitig auf alle ausgewählten Nachrichten anwenden.

HINWEIS
ESET Internet Security bietet Spam-Schutz für Microsoft Outlook, Outlook Express, Windows Mail und Windows Live Mail.

4.2.3 Prüfen von Anwendungsprotokollen

Das ThreatSense-Prüfmodul, in dem alle erweiterten Prüfmethoden integriert sind, bietet Virenschutz für Anwendungsprotokolle. Die Protokollprüfung ist unabhängig vom eingesetzten E-Mail-Programm oder Webbrowser. Sie können die Verschlüsselungs-Einstellungen (SSL/TLS) unter **Web und E-Mail** > **SSL/TLS** bearbeiten.

Prüfen von anwendungsspezifischen Protokollen aktivieren – Hiermit kann die Protokollprüfung deaktiviert werden. Bedenken Sie jedoch, dass zahlreiche Komponenten von ESET Internet Security wie Web-Schutz, E-Mail-Schutz, Phishing-Schutz und Web-Kontrolle von dieser Option abhängen und ohne sie nicht ordnungsgemäß funktionieren.

Ausgeschlossene Anwendungen – Ermöglicht das Ausschließen bestimmter Anwendungen von der Protokollprüfung. Diese Option ist nützlich, wenn es aufgrund der Protokollprüfung zu Kompatibilitätsproblemen kommt.

Ausgeschlossene IP-Adressen – Ermöglicht das Ausschließen bestimmter Remote-Adressen von der Protokollprüfung. Diese Option ist nützlich, wenn es aufgrund der Protokollprüfung zu Kompatibilitätsproblemen kommt.

Webbrowser und E-Mail-Programme – Ermöglicht die Auswahl von Anwendungen, deren gesamter Datenverkehr unabhängig von den verwendeten Ports durch die Protokollprüfung geprüft wird (nur Windows XP).

4.2.3.1 Webbrowser und E-Mail-Programme

HINWEIS
Ab Windows Vista Service Pack 1 und Windows Server 2008 wird zur Prüfung der Netzwerkkommunikation die neue Architektur der Windows-Filterplattform (WFP) verwendet. Da bei der WFP-Technologie spezielle Überwachungstechniken verwendet werden, steht hier der Abschnitt **Webbrowser und E-Mail-Programme** nicht zur Verfügung.

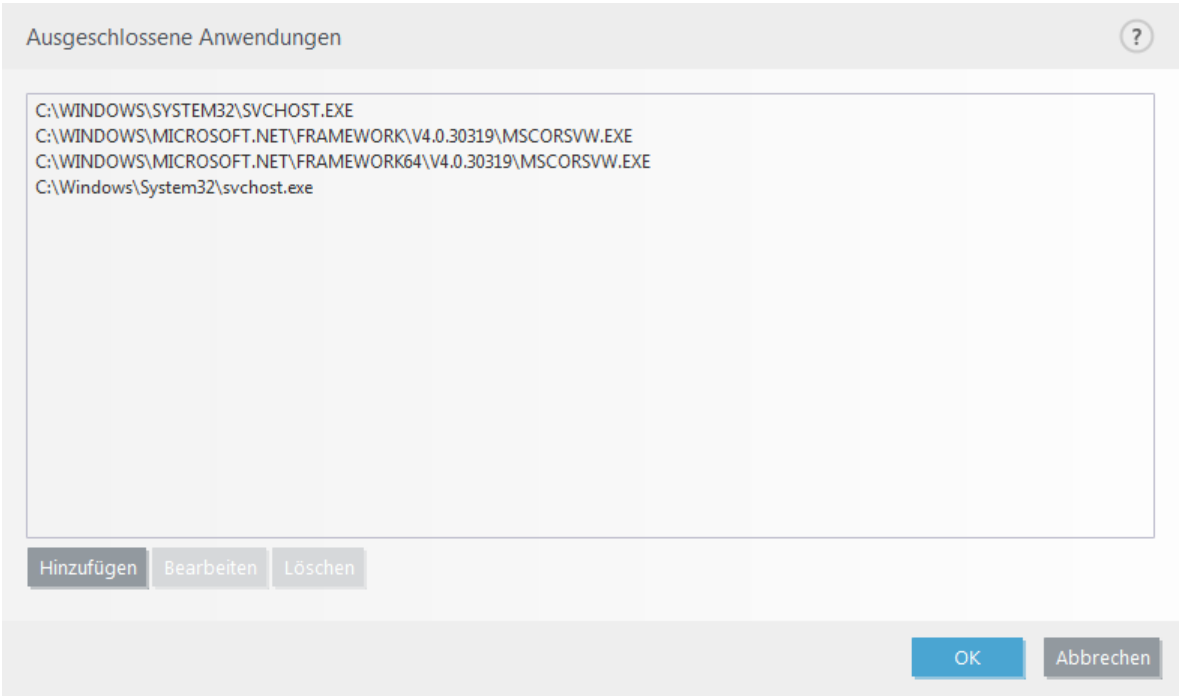
Da im Internet Sicherheitsbedrohungen allgegenwärtig sind, ist sicheres Internetsurfen besonders wichtig. Durch Sicherheitslücken in Webbrowsern und gefälschte Hyperlinks kann Schadcode unbemerkt in Ihr System eindringen. Deshalb bietet ESET Internet Security besondere Funktionen zur Verbesserung der Sicherheit von Webbrowsern an. Sie können beliebige Anwendungen, die auf das Internet zugreifen, als Webbrowser einstufen. Das Kontrollkästchen kann einen der zwei folgenden Status annehmen:

- **Nicht aktiviert** – Die Kommunikation der Anwendungen wird nur für festgelegte Ports gefiltert.
- **Aktiviert** - Die Kommunikation der Anwendungen wird immer geprüft (auch wenn ein anderer Port angegeben ist).

4.2.3.2 Ausgeschlossene Anwendungen

Wählen Sie aus der Liste die Netzwerk-Anwendungen, für deren Datenkommunikation keine Inhaltsprüfung erfolgen soll. Dies schließt die HTTP/POP3/IMAP-Datenkommunikation ausgewählter Anwendungen von der Prüfung auf Bedrohungen aus. Wir empfehlen, diese Option nur für Anwendungen zu aktivieren, deren Datenkommunikation mit aktivierter Prüfung nicht ordnungsgemäß funktioniert.

Aktuell ausgeführte Anwendungen und Dienste stehen hier automatisch zur Verfügung. Klicken Sie auf **Hinzufügen**, um manuell eine Anwendung auszuwählen, die nicht in der Protokollprüfliste angezeigt wird.



4.2.3.3 Ausgeschlossene IP-Adressen

Die in der Liste eingetragenen Adressen werden von der Protokollinhaltsprüfung ausgeschlossen. Die HTTP/POP3/IMAP-Datenkommunikation von/an die ausgewählten Adressen wird nicht auf Bedrohungen geprüft. Wir empfehlen, diese Option nur für Adressen zu aktivieren, die als vertrauenswürdig bekannt sind.

Klicken Sie auf **Hinzufügen**, um eine IP-Adresse, einen Bereich von Adressen oder ein Subnetz für die Gegenstelle zur Liste für die Protokollprüfung hinzuzufügen.

Klicken Sie auf **Entfernen**, um ausgewählte Einträge aus der Liste zu entfernen.

4.2.3.3.1 IPv4-Adresse hinzufügen

Hier können Sie eine IP-Adresse, einen Bereich von Adressen oder ein Subnetz für die Gegenstelle festlegen, die von der Regel erfasst wird. Version 4 ist eine ältere Version des Internetprotokolls. Nach wie vor hat diese Version jedoch die größte Verbreitung.

Einzelne Adresse – Hinzufügen der IP-Adresse eines einzelnen Computers, auf den die Regel angewendet werden soll (zum Beispiel *192.168.0.10*).

Adressbereich – Geben Sie die Start- und Endadresse eines Bereichs von IP-Adressen ein (von mehreren Computern), auf die die Regel angewendet werden soll (z. B. *192.168.0.1* bis *192.168.0.99*).

Subnetz – Hier können Sie durch eine IP-Adresse und eine Maske ein Subnetz (eine Gruppe von Computern) definieren.

255.255.255.0 ist z. B. die Netzwerkmaske für das Präfix *192.168.1.0/24*, also der Adressbereich *192.168.1.1* bis *192.168.1.254*.

4.2.3.3.2 IPv6-Adresse hinzufügen

Hier können Sie eine IPv6-Adresse/ein IPv6-Subnetz für die Gegenstelle festlegen, auf die die Regel angewendet werden soll. IPv6 ist die neueste Version des Internetprotokolls, und wird die bisherige Version 4 ersetzen.

Einzelne Adresse – Hier können Sie die IP-Adresse eines einzelnen Computers eingeben, auf den die Regel angewendet werden soll (z. B. *2001:718:1c01:16:214:22ff:fec9:ca5*).

Subnetz – Hier können Sie durch eine IP-Adresse und eine Maske ein Subnetz definieren. (Beispiel: *2002:c0a8:6301:1::1/64*)

4.2.3.4 SSL/TLS

ESET Internet Security kann Verbindungen, die das SSL-Protokoll verwenden, auf Bedrohungen untersuchen. Für die Untersuchung von durch SSL geschützten Verbindungen gibt es verschiedene Prüfmodi mit vertrauenswürdigen und unbekannten Zertifikaten sowie Zertifikaten, die von der Prüfung SSL-geschützter Verbindungen ausgeschlossen sind.

SSL/TLS-Protokollfilterung aktivieren – Wenn der Protokollfilter deaktiviert ist, werden SSL-Verbindungen nicht geprüft.

Für den SSL/TLS-Protokollfiltermodus sind folgende Optionen verfügbar:

Automatischer Modus – Der Standardmodus prüft nur relevante Anwendungen wie Webbrowser und E-Mail-Clients. Sie können zusätzliche Anwendungen auswählen, deren Kommunikation geprüft werden soll.

Interaktiver Filtermodus – Bei Eingabe einer neuen, durch SSL geschützten Seite (mit unbekanntem Zertifikat) wird ein Dialogfeld mit möglichen Aktionen angezeigt. In diesem Modus können Sie eine Liste von SSL-Zertifikaten und Anwendungen erstellen, die von der Prüfung ausgeschlossen sind.

Policy-Modus – Aktivieren Sie diese Option, um jegliche SSL-geschützte Kommunikation zu prüfen, außer wenn Zertifikate verwendet werden, die von der Prüfung ausgeschlossen sind. Wird eine Verbindung mit einem unbekannten, signierten Zertifikat erstellt, so wird sie ohne gesonderten Hinweis automatisch geprüft. Wenn Sie auf einen Server mit einem nicht vertrauenswürdigen Zertifikat, das sich in der Liste der vertrauenswürdigen Zertifikate befindet und damit als vertrauenswürdig eingestuft wurde, zugreifen, wird die Kommunikation zugelassen und der Inhalt des Kommunikationskanals geprüft.

Liste der vom SSL-Filter betroffenen Anwendungen – Mit dieser Liste können Sie das Verhalten von ESET Internet Security für bestimmte Anwendungen anpassen.

Liste der bekannten Zertifikate – Mit dieser Liste können Sie das Verhalten von ESET Internet Security für bestimmte SSL-Zertifikate anpassen.

Kommunikation mit vertrauenswürdigen Domains ausschließen – Wenn diese Option aktiviert ist, wird die Kommunikation mit vertrauenswürdigen Domänen von der Prüfung ausgeschlossen. Die Vertrauenswürdigkeit von Domains wird anhand einer integrierten Positivliste ermittelt.

Verschlüsselte Kommunikation sperren, die das obsolete Protokoll SSL v2 verwendet – Verbindungen, die die frühere Version des SSL-Protokolls verwenden, werden automatisch blockiert.

Stammzertifikat

Stammzertifikat zu bekannten Browsern hinzufügen – Damit die SSL-Kommunikation in Ihren Browsern/E-Mail-Programmen ordnungsgemäß funktioniert, muss das Stammzertifikat für ESET zur Liste der bekannten Stammzertifikate (Herausgeber) hinzugefügt werden. Mit dieser Option fügt ESET Internet Security das ESET-Stammzertifikat automatisch zu den bekannten Browsern (z. B. Opera, Firefox) hinzu. Wenn ein Browser den Systemzertifizierungsspeicher verwendet, wird das Zertifikat automatisch hinzugefügt (z. B. Internet Explorer).

Um das Zertifikat für nicht unterstützte Browser zu übernehmen, klicken Sie auf **Zertifikat anzeigen** > **Details** > **In Datei kopieren...**, und importieren Sie die Datei anschließend manuell in den Browser.

Gültigkeit des Zertifikats

Falls das Zertifikat nicht über die VSZS-Zertifikatablage geprüft werden kann – In manchen Fällen kann ein Website-Zertifikat nicht über den Speicher vertrauenswürdiger Stammzertifizierungsstellen (VSZS) geprüft werden. Das bedeutet, dass jemand das Zertifikat signiert hat (z. B. der Administrator eines Webservers oder ein Kleinunternehmen). Das Zertifikat als vertrauenswürdig einzustufen, stellt nicht immer ein Risiko dar. Die meisten großen Unternehmen (z. B. Banken) verwenden Zertifikate, die von einer vertrauenswürdigen Stammzertifizierungsstelle signiert sind. Wenn die Option **Gültigkeit des Zertifikats erfragen** ausgewählt ist (Standardeinstellung), muss der Benutzer eine Standardaktion für verschlüsselte Verbindungen festlegen. Aktivieren Sie die Option **Kommunikation blockieren, die das Zertifikat verwendet**, um verschlüsselte Verbindungen zu Sites mit nicht verifizierten Zertifikaten immer zu beenden.

Wenn das Zertifikat ungültig oder beschädigt ist – Dies bedeutet, dass es entweder abgelaufen ist oder fehlerhaft signiert wurde. Verwenden Sie in diesem Fall die Option **Kommunikation blockieren, die das Zertifikat verwendet**.

4.2.3.4.1 Zertifikate

Damit die SSL-Kommunikation in Ihren Browsern/E-Mail-Programmen ordnungsgemäß funktioniert, muss das Stammzertifikat für ESET der Liste der bekannten Stammzertifikate (Herausgeber) hinzugefügt werden. **Bekannten Browsern das Stammzertifikat hinzufügen** sollte aktiviert sein. Wählen Sie diese Option, um das ESET-Stammzertifikat automatisch zu den bekannten Browsern (z. B. Opera, Firefox) hinzuzufügen. Wenn ein Browser den Systemzertifizierungsspeicher verwendet, wird das Zertifikat automatisch hinzugefügt (z. B. Internet Explorer). Um das Zertifikat für nicht unterstützte Browser zu übernehmen, klicken Sie auf **Zertifikat anzeigen** > **Details** > **In die Datei kopieren...**, und importieren Sie es anschließend manuell in den Browser.

In manchen Fällen kann das Zertifikat nicht über den Speicher vertrauenswürdiger Stammzertifizierungsstellen geprüft werden (z. B. VeriSign). Das bedeutet, dass jemand das Zertifikat selbst signiert hat (z. B. der Administrator eines Webservers oder ein Kleinunternehmen). Das Zertifikat als vertrauenswürdig einzustufen, stellt nicht immer ein Risiko dar. Die meisten großen Unternehmen (z. B. Banken) verwenden Zertifikate, die von einer vertrauenswürdigen Stammzertifizierungsstelle signiert sind. Wenn die Option **Gültigkeit des Zertifikats erfragen** ausgewählt ist (Standardeinstellung), muss der Benutzer eine Aktion festlegen, die ausgeführt werden soll, wenn verschlüsselte Verbindungen aufgebaut werden. Dazu wird ein Aktionsauswahl-Dialogfenster angezeigt, in dem Sie das Zertifikat als vertrauenswürdig markieren oder ausschließen können. Wenn das Zertifikat nicht in der Liste vertrauenswürdiger Stammzertifizierungsstellen enthalten ist, ist das Fenster rot hinterlegt, sonst ist es grün.

Sie können die Option **Kommunikation blockieren, die das Zertifikat verwendet** auswählen, um verschlüsselte Verbindungen zu der Site, die das nicht verifizierte Zertifikat verwendet, immer zu beenden.

Wenn das Zertifikat ungültig oder beschädigt ist, ist es entweder abgelaufen oder wurde fehlerhaft selbst signiert. In diesem Fall empfehlen wir, die Verbindung, die das Zertifikat verwendet, zu blockieren.

4.2.3.4.1.1 Verschlüsselte Netzwerkverbindung

Falls der Computer für SSL-Protokollüberprüfung eingerichtet ist, werden Sie in einem Dialogfenster aufgefordert, eine Aktion auszuwählen, die ausgeführt wird, sobald eine verschlüsselte Kommunikation (über ein unbekanntes Zertifikat) angefordert wird.

Folgende Daten werden angezeigt:

- Name der Anwendung, die die Kommunikation gestartet hat
- Name des verwendeten Zertifikats
- Auszuführende Aktion – Angabe, ob die verschlüsselte Kommunikation geprüft werden soll und ob die Aktion für die Anwendung bzw. das Zertifikat gespeichert werden soll.

Wenn sich das Zertifikat nicht im Speicher vertrauenswürdiger Stammzertifizierungsstellen (Trusted Root Certification Authorities, TRCA) befindet, wird es als nicht vertrauenswürdig eingestuft.

4.2.3.4.2 Liste bekannter Zertifikate

Mit der **Liste bekannter Zertifikate** können Sie das Verhalten von ESET Internet Security bei bestimmten SSL-Zertifikaten anpassen und gewählte Aktionen speichern, wenn der **Interaktive Modus** unter **SSL/TLS-Protokollfilterungsmodus** ausgewählt ist. Sie können die Liste unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **SSL/TLS** > **Liste bekannter Zertifikate** anzeigen und bearbeiten.

Das Fenster **Liste bekannter Zertifikate** enthält die folgenden Elemente:

Spalten

Name – Name des Zertifikats.

Zertifikataussteller – Name des Zertifikaterstellers.

Zertifikatbetreff – Das Betrefffeld enthält die Entität, die mit dem öffentlichen Schlüssel verknüpft ist, welcher im entsprechenden Feld des Betreffs gespeichert ist.

Zugriff – Wählen Sie **Zulassen** oder **Blockieren** als **Zugriffsaktion**, um die von diesem Zertifikat gesicherte Verbindung unabhängig von ihrer Vertrauenswürdigkeit zuzulassen oder zu blockieren. Wählen Sie **Autom.**, wenn vertrauenswürdige Zertifikate zugelassen werden sollen und bei nicht vertrauenswürdigen nachgefragt werden soll. Wählen Sie **Nachfragen**, wenn der Benutzer immer gefragt werden soll, welche Maßnahme ergriffen werden soll.

Prüfen – Wählen Sie **Prüfen** oder **Ignorieren** als **Prüfungsaktion** aus, um die von diesem Zertifikat gesicherte Verbindung zu scannen oder zu ignorieren. Wählen Sie **Autom.**, wenn im automatischen Modus geprüft und im interaktiven Modus nachgefragt werden soll. Wählen Sie **Nachfragen**, wenn der Benutzer immer gefragt werden soll, welche Maßnahme ergriffen werden soll.

Steuerelemente

Hinzufügen – Fügen Sie ein neues Zertifikat hinzu und passen Sie die Einstellungen für Zugriffs- und Prüfoptionen an.

Bearbeiten – Wählen Sie das zu konfigurierende Zertifikat aus und klicken Sie auf **Bearbeiten**.

Entfernen – Wählen Sie das zu löschende Zertifikat aus und klicken Sie auf **Entfernen**.

OK/Abbrechen – Klicken Sie auf **OK**, um die Änderungen zu speichern, oder auf **Abbrechen**, um den Vorgang ohne Speichern zu beenden.

4.2.3.4.3 Liste der vom SSL/TLS-Filter betroffenen Anwendungen

Mit der **Liste der vom SSL/TLS-Filter betroffenen Anwendungen** können Sie das Verhalten von ESET Internet Security für bestimmte Anwendungen anpassen und ausgewählte Aktionen speichern, wenn der **Interaktive Modus** als **Filtermodus für das SSL/TLS-Protokoll** ausgewählt ist. Sie können die Liste unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **SSL/TLS** > **Liste der vom SSL/TLS-Filter betroffenen Anwendungen** anzeigen und bearbeiten.

Das Fenster **Liste der vom SSL-Filter betroffenen Anwendungen** enthält die folgenden Elemente:

Spalten

Anwendung – Name der Anwendung.

Prüfaktion – Wählen Sie **Prüfen** oder **Ignorieren** aus, um die Kommunikation zu prüfen oder zu ignorieren. Wählen Sie **Autom.**, wenn im automatischen Modus geprüft und im interaktiven Modus nachgefragt werden soll. Wählen Sie **Nachfragen**, wenn der Benutzer immer gefragt werden soll, welche Maßnahme ergriffen werden soll.

Steuerelemente

Hinzufügen – Gefilterte Anwendung hinzufügen.

Bearbeiten – Wählen Sie das zu konfigurierende Zertifikat aus und klicken Sie auf **Bearbeiten**.

Entfernen – Wählen Sie das zu löschende Zertifikat aus und klicken Sie auf **Entfernen**.

OK/Abbrechen – Klicken Sie auf **OK**, um die Änderungen zu speichern, oder auf **Abbrechen**, um den Vorgang ohne Speichern zu beenden.

4.2.4 Phishing-Schutz

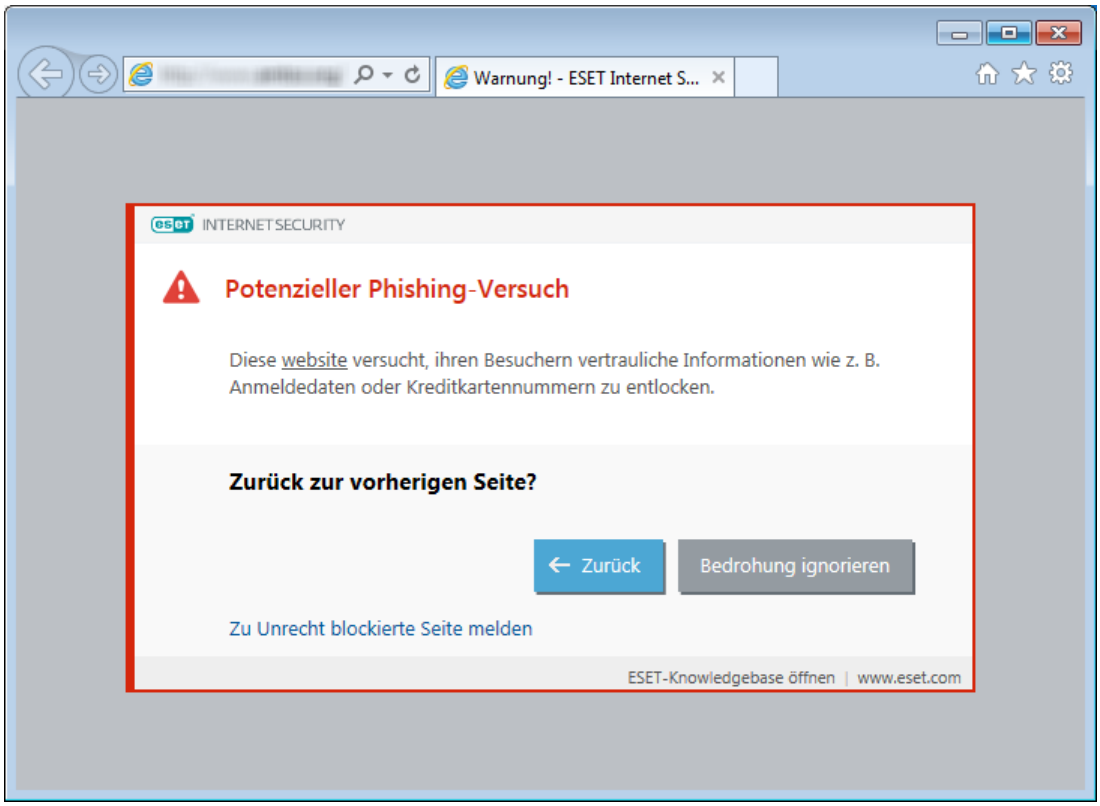
Der Begriff „Phishing“ bezeichnet eine kriminelle Vorgehensweise, die sich Techniken des Social Engineering (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Phishing wird oft eingesetzt, um Zugriff auf vertrauliche Daten zu erlangen, wie Kontonummern oder PIN-Codes. Weitere Informationen zu dieser Aktivität finden Sie im Glossar. ESET Internet Security enthält einen Phishing-Schutz: Webseiten, die dafür bekannt sind, Phishing-Inhalte zu enthalten, können gesperrt werden.

Wir empfehlen, den Phishing-Schutz in ESET Internet Security zu aktivieren. Diese Option finden Sie im Bereich **Erweiterte Einstellungen** (F5) unter **Web und E-Mail** > **Phishing-Schutz**.

In unserem Knowledgebase-Artikel finden Sie weitere Informationen zum Phishing-Schutz von ESET Internet Security.

Zugriff auf eine Phishing-Website

Wenn Sie auf eine erkannte Phishing-Website zugreifen, wird das folgende Dialogfenster im Webbrowser angezeigt. Wenn Sie trotzdem auf die Website zugreifen möchten, klicken Sie auf **Bedrohung ignorieren** (nicht empfohlen).



HINWEIS
Potenzielle Phishing-Websites, die zur Positivliste hinzugefügt wurden, werden standardmäßig nach einigen Stunden wieder von der Liste gelöscht. Verwenden Sie die URL-Adressverwaltung, um eine Website dauerhaft zuzulassen. Klicken Sie unter **Erweiterte Einstellungen** (F5) auf **Web und E-Mail** > **Web-Schutz** > **URL-Adressverwaltung** > **Adressliste**. Klicken Sie anschließend auf **Bearbeiten** und fügen Sie die Website, die Sie bearbeiten möchten, zu dieser Liste hinzu.

Melden einer Phishing-Website

Über den Link Melden können Sie eine Website mit vermutetem Phishing-Inhalt oder anderem Schadcode an ESET melden.

HINWEIS
Auf Websites, die Sie bei ESET melden, sollte mindestens eines der folgenden Kriterien zutreffen:

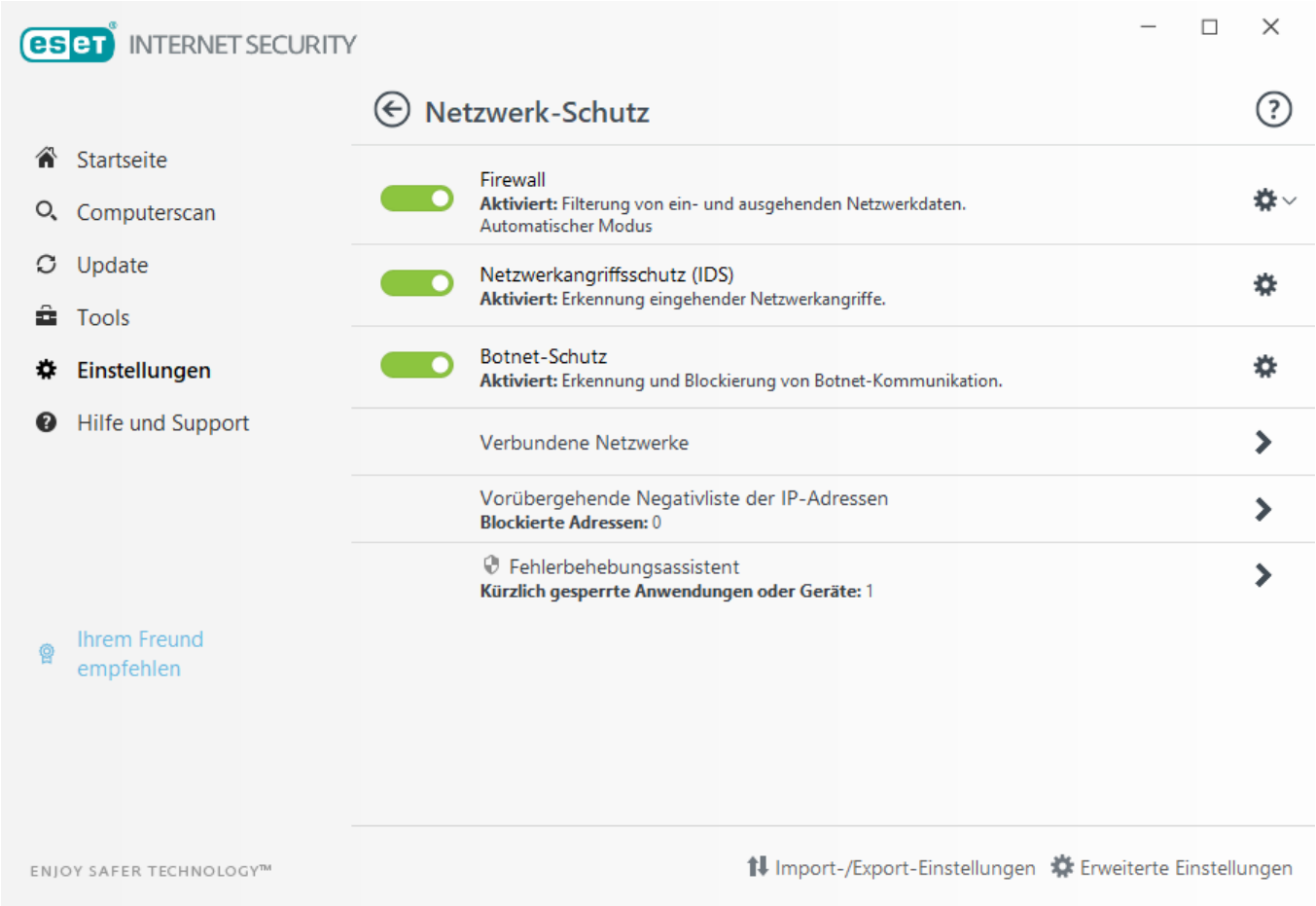
- Die Website wird nicht als Bedrohung erkannt.
- Die Website wird als Bedrohung erkannt, obwohl Sie keinen Schadcode enthält. In diesem Fall können Sie eine Zu Unrecht blockierte Seite melden.

Sie können Websites auch per E-Mail melden. Senden Sie die E-Mail an samples@eset.com. Verwenden Sie einen treffenden Text in der Betreffzeile und liefern Sie möglichst viele Informationen zur Website (wie Sie auf die Website gelangt sind, wo Sie von der Website erfahren haben usw.).

4.3 Netzwerk-Schutz

Die Firewall kontrolliert den gesamten Netzwerkdatenverkehr vom und zum System. Dazu werden einzelne Netzwerkverbindungen anhand zuvor festgelegter Filterregeln zugelassen oder blockiert. Die Firewall bietet Schutz gegen Angriffe von Remotecomputern und blockiert bestimmte Dienste. Sie bietet zudem auch Virenschutz für HTTP-, POP3- und IMAP-Protokolle. Mit diesen Funktionen ist die Personal Firewall ein wirksames Hilfsmittel zum Schutz Ihres Computers. ESET Internet Security informiert Sie, wenn Sie sich mit einem gar nicht oder nur schwach geschützten WLAN-Netzwerk verbinden.

Sie können die Firewall im Fenster **Einstellungen** unter **Netzwerk-Schutz** konfigurieren. Dort können Sie den Filtermodus, Regeln und erweiterte Einstellungen anpassen. Klicken Sie auf das Zahnrad > **Konfigurieren ...** neben **Firewall oder** öffnen Sie die Erweiterten Einstellungen mit der Taste **F5**, um weitere detailliertere Optionen anzuzeigen.



Klicken Sie auf das Zahnrad neben **Firewall**, um die folgenden Einstellungen anzuzeigen:

Konfigurieren... - Öffnet das Fenster „Firewall“ in den Erweiterten Einstellungen, in dem Sie festlegen können, wie die Firewall mit der Netzwerkkommunikation verfahren soll.

Firewall anhalten (gesamten Datenverkehr zulassen) – Die Blockierung des Netzwerkverkehrs wird aufgehoben. Wenn Sie diese Option auswählen, werden alle Filteroptionen der Firewall deaktiviert und alle eingehenden und ausgehenden Verbindungen zugelassen. Klicken Sie auf **Firewall aktivieren** , um die Firewall erneut zu aktivieren, wenn die Prüfung des Netzwerkdatenverkehrs in diesem Modus ist.

Alle Verbindungen blockieren – Alle ein- und ausgehenden Verbindungen werden von der Firewall blockiert. Verwenden Sie diese Option nur, wenn Sie schwerwiegende Sicherheitsrisiken befürchten, die eine Trennung der Netzwerkverbindung erfordern. Wenn die Prüfung des Netzwerkdatenverkehrs im Modus **Alle Verbindungen blockieren** ist, klicken Sie auf **Sämtlichen Datenverkehr zulassen**, um den Normalbetrieb der Firewall wiederherzustellen.

Automatischer Filtermodus – (wenn ein anderer Filtermodus aktiviert ist) – Hiermit wird der automatische Filtermodus mit benutzerdefinierten Regeln aktiviert.

Interaktiver Filtermodus – (wenn ein anderer Filtermodus aktiviert ist) – Hiermit wird der interaktive Filtermodus aktiviert.

Netzwerkangriffsschutz (IDS) - Analysiert den Inhalt des Netzwerkverkehrs und schützt vor Angriffen aus dem Netzwerk. Jeglicher als schädlich erkannter Verkehr wird blockiert.

Botnetschutz – Erkennt Schadsoftware auf Ihrem System schnell und präzise.

Verbundene Netzwerke – Zeigt die Netzwerke an, mit denen die Netzwerkadapter verbunden sind. Klicken Sie auf das Zahnrad unterhalb des Netzwerknamens, um einen Schutztyp für das Netzwerk auszuwählen, mit der entsprechende Netzwerkadapter verbunden ist. Diese Einstellung bestimmt, wie zugänglich Ihr Computer für andere Computer im Netzwerk ist.

Vorübergehende Negativliste der IP-Adressen – Zeigt eine Liste von IP-Adressen an, die als Angriffsquellen identifiziert und zur Negativliste hinzugefügt wurden, um die Verbindung für einen bestimmten Zeitraum zu unterbinden. Für weitere Informationen klicken Sie auf diese Option und drücken Sie die Taste F1.

Fehlerbehebungsassistent – Hilft Ihnen bei der Lösung von Konnektivitätsproblemen, die von der ESET Firewall verursacht wurden. Weitere Informationen finden Sie unter Fehlerbehebungsassistent.

4.3.1 Firewall

Die Firewall kontrolliert den gesamten Netzwerkdatenverkehr vom und zum System. Dabei werden einzelne Netzwerkverbindungen anhand zuvor festgelegter Filterregeln zugelassen oder blockiert. Die Firewall bietet Schutz gegen Angriffe von Remotecomputern und blockiert potenziell gefährliche Dienste. Darüber hinaus bietet sie einen Virenschutz für die Protokolle HTTP, POP3 und IMAP.

Einfach

Firewall aktivieren – Dieses Feature sollte immer aktiviert sein, um die Systemsicherheit zu gewährleisten. Mit aktiver Firewall wird der Netzwerkdatenverkehr in beide Richtungen geprüft.

Windows Firewall-Regeln ebenfalls auswerten – Im automatischen Modus wird eingehender Datenverkehr mit entsprechender Windows Firewall-Regel zugelassen, sofern nicht ausdrücklich durch ESET-Regeln gesperrt.

Filtermodus – Das Verhalten der Firewall hängt vom Filtermodus ab. Die Filtermodi beeinflussen auch den Umfang der erforderlichen Benutzereingaben. Für die ESET Internet Security Firewall stehen drei Filtermodi zur Auswahl:

Automatischer Filtermodus – Standardmodus. Dieser Modus ist für Benutzer geeignet, die eine einfache und komfortable Verwendung der Firewall bevorzugen, bei der keine Regeln definiert werden müssen. Benutzerdefinierte Regeln können erstellt werden, sind im Modus „Automatisch“ jedoch nicht erforderlich. Im automatischen Modus wird der gesamte ausgehende Datenverkehr des angegebenen Systems zugelassen und der meiste eingehende Datenverkehr blockiert (mit Ausnahme für die vertrauenswürdige Zone, die gemäß IDS und erweiterte Optionen/Zugelassene Dienste zugelassen wurde, sowie Antworten auf ausgehende Verbindungen).

Interaktiver Filtermodus – Ermöglicht eine benutzerdefinierte Konfiguration für die Firewall. Bei jeder gefundenen Verbindung, für die noch keine Regel besteht, wird ein Dialogfenster angezeigt, in dem auf die unbekannte Verbindung hingewiesen wird. Der Benutzer kann entscheiden, ob die Verbindung zugelassen oder blockiert werden soll, und diese Auswahl kann als neue Regel für die Firewall übernommen werden. Wenn eine neue Regel erstellt wurde, werden Verbindungen dieser Art beim nächsten Verbindungsversuch entsprechend der Regel automatisch zugelassen oder blockiert.

Regelbasierter Filtermodus – blockiert alle Verbindungen, für die keine Regel besteht, nach der diese zugelassen werden. Mit diesem Modus können erfahrene Benutzer Regeln festlegen, um nur erwünschte und sichere Verbindungen zuzulassen. Alle anderen Verbindungen werden von der Firewall blockiert.

Trainingsmodus – Erstellt und speichert Regeln automatisch. Dieser Modus eignet sich für die Ersteinrichtung der Firewall, sollte jedoch nicht über längere Zeit aktiviert werden. Es ist keine Benutzerinteraktion erforderlich, weil ESET Internet Security Regeln entsprechend der vordefinierten Parameter speichert. Der Trainingsmodus sollte nur so lange verwendet werden, bis alle Regeln für die erforderlichen Verbindungen erstellt wurden, um Sicherheitsrisiken zu vermeiden.

Mit Profilen können Sie das Verhalten der ESET Internet Security Firewall anpassen, indem Sie unterschiedliche Regeln für unterschiedliche Situationen festlegen.

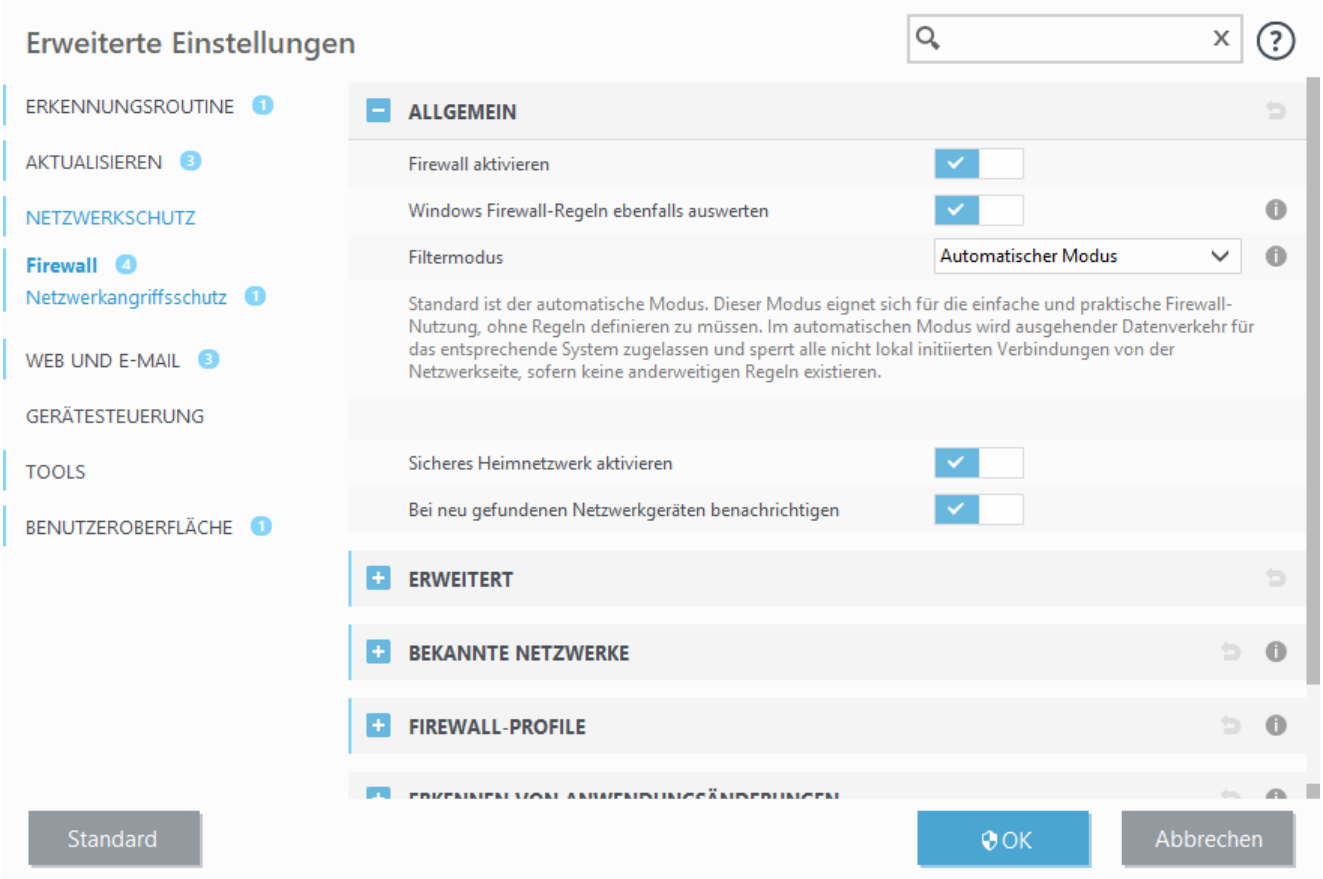
Sicheres Heimnetzwerk aktivieren – Schützt Computer vor eingehenden Netzwerk- bzw. WLAN-Bedrohungen.

Bei neu gefundenen Netzwerkgeräten benachrichtigen – Benachrichtigt Sie, wenn ein neues Gerät in Ihrem Netzwerk erkannt wird.

Erweitert

Regeln – Hier können Sie Regeln hinzufügen und festlegen, wie die Firewall mit dem Datenverkehr umgeht.

Zonen – Hier können Sie Zonen mit einer oder mehreren sicheren IP-Adressen einrichten.



HINWEIS
Sie können IDS-Ausnahmen erstellen, wenn ein Botnetz Ihren Computer angreift. Sie können Ausnahmen bearbeiten, indem Sie unter **Erweiterte Einstellungen** (F5) > **Netzwerk-Schutz** > **Netzwerkangriffsschutz** > **IDS-Ausnahmen** auf **Bearbeiten** klicken.

4.3.1.1 Einstellungen für Trainings Modus

Im Trainingsmodus wird für jede im System hergestellte Verbindung automatisch eine Regel erstellt und gespeichert. Es ist keine Benutzerinteraktion erforderlich, weil ESET Internet Security Regeln entsprechend der vordefinierten Parameter speichert.

Dieser Modus kann Ihr System zusätzlichen Risiken aussetzen und wird daher nur für die Erstinstallation der Firewall empfohlen.

Wählen Sie **Trainingsmodus** im Dropdownmenü unter **Erweiterte Einstellungen** (F5) > **Firewall** > **Einfach** > **Filtermodus** aus, um die **Optionen für den Trainingsmodus** zu aktivieren. Dieser Bereich enthält die folgenden Elemente:

WARNUNG
Während sich die Firewall im Trainingsmodus befindet, wird die Kommunikation nicht geprüft. Alle aus- und eingehenden Verbindungen werden zugelassen. In diesem Modus ist der Computer nicht vollständig durch die Firewall geschützt.

Kommunikationsart – Wählen Sie die jeweiligen Richtlinien zur Regelerstellung für jede Kommunikationsart aus. Es gibt vier Arten von Kommunikation:

Eingehender Datenverkehr aus der vertrauenswürdigen Zone – Ein Beispiel für eine eingehende Verbindung innerhalb der vertrauenswürdigen Zone wäre ein Remotecomputer aus der vertrauenswürdigen Zone, der versucht, eine Verbindung zu einer Anwendung auf Ihrem Computer herzustellen.

Ausgehender Datenverkehr in die vertrauenswürdige Zone – Eine lokale Anwendung versucht, eine Verbindung zu einem anderen Computer im lokalen Netzwerk oder innerhalb der vertrauenswürdigen Zone herzustellen.

Eingehender Datenverkehr aus dem Internet – Ein Remotecomputer versucht, eine Verbindung zu einer Anwendung auf dem Computer herzustellen.

Ausgehender Datenverkehr in das Internet - Eine lokale Anwendung versucht, eine Verbindung zu einem anderen Computer herzustellen.

Sie können in jedem Bereich Parameter festlegen, die den neu erstellten Regeln hinzugefügt werden:

Lokalen Port hinzufügen – Die Nummer des lokalen Ports der Netzwerkkommunikation wird eingeschlossen. Bei ausgehenden Verbindungen werden normalerweise zufällige Nummern generiert. Daher wird empfohlen, diese Option nur für eingehende Verbindungen zu aktivieren.

Anwendung hinzufügen – Der Name der lokalen Anwendung wird eingeschlossen. Diese Option eignet sich für zukünftige Regeln auf Anwendungsebene (Regeln, die die Kommunikation für eine ganze Anwendung festlegen). Sie können beispielsweise nur die Kommunikation eines Webbrowsers oder E-Mail-Programms zulassen.

Remote-Port hinzufügen – Die Nummer des Remote-Ports der Netzwerkkommunikation wird eingeschlossen. Sie können beispielsweise einen bestimmten, mit einer Standardportnummer (HTTP – 80, POP3 – 110 usw.) verbundenen Dienst zulassen oder verweigern.

Remote-IP-Adresse / vertrauenswürdige Zone hinzufügen – Eine Remote-IP-Adresse oder Zone kann als Parameter für neue Regeln verwendet werden, die alle Netzwerkverbindungen zwischen dem lokalen System und diesen Remoteadressen/Zonen bestimmen. Diese Option eignet sich vor allem für die Definition von Aktionen eines bestimmten Computers oder einer Gruppe vernetzter Computer.

Höchstanzahl an unterschiedlichen Regeln für eine Anwendung – Wenn eine Anwendung über verschiedene Ports mit verschiedenen IP-Adressen usw. kommuniziert, erstellt der Trainingsmodus die richtige Anzahl Regeln für diese Anwendung. Diese Option ermöglicht Ihnen, die Anzahl der Regeln zu begrenzen, die für eine Anwendung erstellt werden können.

4.3.1.2 Netzwerkangriffsschutz

Netzwerkangriffsschutz (IDS) aktivieren - Analysiert den Inhalt des Netzwerkverkehrs und schützt vor Angriffen aus dem Netzwerk. Jeglicher als schädlich erkannter Verkehr wird blockiert.

Botnetschutz aktivieren – Erkennt und sperrt die Kommunikation mit schädlichen Steuerungszentralen anhand bekannter Muster, die auftreten, wenn ein Bot versucht, eine Kommunikation herzustellen.

IDS-Ausnahmen – Ermöglicht das Hinzufügen von IDS-Ausnahmen und das Anpassen von Reaktionen auf verdächtige Aktivitäten.

4.3.2 Firewall-Profile

Mit Profilen können Sie das Verhalten der Firewall von ESET Internet Security steuern. Beim Erstellen oder Bearbeiten einer Firewall-Regel können Sie diese Regel einem bestimmten Profil zuordnen oder auf alle Profile anwenden. Wenn ein Profil in einer Netzwerkschnittstelle aktiv ist, werden nur die globalen Regeln (ohne Angabe eines Profils) sowie die Regeln angewendet, die diesem Profil zugeordnet wurden. Sie können mehrere Profile erstellen, denen unterschiedliche Regeln zugeordnet sind, um auf einfache Weise das Verhalten der Firewall zu verändern.

Klicken Sie neben der Profilliste auf **Bearbeiten**, um das Fenster **Firewall-Profile** zum Bearbeiten der Profile zu öffnen.

Ein Netzwerkadapter kann so eingestellt werden, dass er ein für ein bestimmtes Netzwerk konfiguriertes Profil verwendet, wenn er mit diesem Netzwerk verbunden ist. Unter **Erweiterte Einstellungen** (F5) > **Netzwerk-Schutz** > **Firewall** > **Bekannte Netzwerke** können Sie außerdem ein Profil zuweisen, das für Verbindungen zu einem bestimmten Netzwerk verwendet werden soll. Wählen Sie ein Netzwerk aus der Liste **Bekannte Netzwerke** aus und klicken Sie auf **Bearbeiten**, um diesem Netzwerk ein Firewall-Profil aus dem Dropdown-Menü **Firewall-Profil** zuzuweisen. Wenn diesem Netzwerk kein Profil zugewiesen ist, wird das Standardprofil des Adapters verwendet. Wenn der Adapter so eingestellt ist, dass er das Profil des Netzwerks nicht verwenden soll, wird unabhängig davon, mit welchem Netzwerk er verbunden ist, das Standardprofil verwendet. Falls kein Profil für Netzwerk oder Adapter existiert, wird das globale Standardprofil verwendet. Um einem Netzwerkadapter ein Profil zuzuweisen, wählen Sie den Netzwerkadapter aus, klicken Sie neben **An Netzwerkadapter zugewiesene Profile** auf **Bearbeiten**, bearbeiten Sie den ausgewählten Netzwerkadapter und wählen Sie das Profil aus dem Dropdown-Menü **Firewall-Standardprofil** aus.

Wenn die Firewall zu einem anderen Profil wechselt, wird in der rechten unteren Ecke neben der Systemuhr ein Hinweis angezeigt.

4.3.2.1 An Netzwerkadapter zugewiesene Profile

Durch Wechseln der Profile können Sie auf schnelle Art und Weise mehrere Änderungen am Firewall-Verhalten vornehmen. Sie können benutzerdefinierte Regeln für bestimmte Profile festlegen und anwenden. Einträge zu allen Adaptern im Computer werden der Liste **Netzwerkadapter** automatisch hinzugefügt.

Spalten

Name – Name des Netzwerkadapters.

Firewall-Standardprofil – Das Standardprofil wird verwendet, wenn zu dem Netzwerk, mit dem Sie verbunden sind, kein Profil konfiguriert ist oder der Netzwerkadapter so eingestellt ist, dass kein Netzwerkprofil verwendet werden soll.

Netzwerkprofil bevorzugen – Wenn die Option **Firewall-Profil des verbundenen Netzwerks bevorzugen** aktiviert ist, verwendet der Netzwerkadapter nach Möglichkeit das Firewall-Profil, das mit einem verbundenen Netzwerk verknüpft ist.

Steuerelemente

Hinzufügen – Erstellt einen neuen Netzwerkadapter.

Bearbeiten – Ermöglicht das Bearbeiten eines bestehenden Netzwerkadapters.

Entfernen – Wählen Sie einen Netzwerkadapter aus der Liste aus und klicken Sie auf **Entfernen**, um den Netzwerkadapter aus der Liste zu entfernen.

OK/Abbrechen – Klicken Sie auf **OK**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang zu beenden, ohne zu speichern.

4.3.3 Konfigurieren und Verwenden von Regeln

Regeln fassen verschiedene Bedingungen zusammen, die eingesetzt werden, um alle Netzwerkverbindungen und damit verbundenen Aktionen wirksam zu prüfen. Mit den Firewall-Regeln können Sie definieren, welche Aktion ausgeführt wird, wenn verschiedene Netzwerkverbindungen aufgebaut werden. Sie finden die Filtereinstellungen für Regeln unter **Erweiterte Einstellungen** (F5) > **Firewall** > **Einfach**. Einige vordefinierte Regeln sind an die Kontrollkästchen unter **Zugelassene Dienste** (IDS und erweiterte Optionen) gebunden und können nicht direkt, sondern nur über diese Kontrollkästchen deaktiviert werden.

Anders als in der Vorgängerversion von ESET Internet Security werden Regeln von oben nach unten geprüft. Die Aktion zur ersten übereinstimmenden Regel wird auf jede geprüfte Netzwerkverbindung angewandt. Dies stellt eine wichtige Änderung des Verhaltens im Vergleich zur Vorversion dar, in der die Priorität der Regeln automatisch festgelegt wurde und spezifischere Regeln somit Priorität vor allgemeinen Regeln hatten.

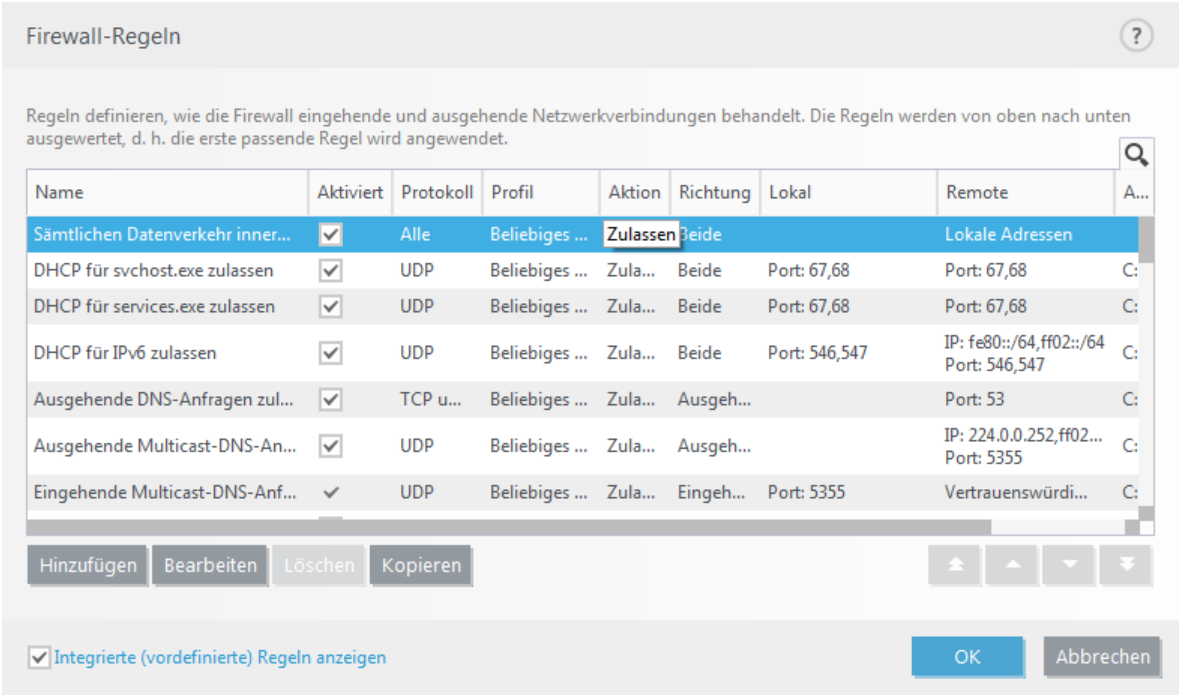
Es gibt zwei Arten von Verbindungen: eingehende und ausgehende. Eingehende Verbindungen gehen von einem Remotecomputer aus, der versucht, eine Verbindung mit dem lokalen System herzustellen. Ausgehende Verbindungen funktionieren umgekehrt – das lokale System nimmt Kontakt mit einem Remotecomputer auf.

Wenn eine neue, unbekannte Verbindung erkannt wird, sollten Sie genau prüfen, ob diese zugelassen oder blockiert werden soll. Unerwünschte, unsichere oder unbekannte Verbindungen können ein Sicherheitsrisiko für Ihren Computer darstellen. Wenn eine solche Verbindung aufgebaut wird, sollten Sie besonders auf die Gegenstelle achten und prüfen, welche Anwendung versucht, mit ihrem Computer zu kommunizieren. Viele Schadprogramme versuchen, persönliche Daten zu erfassen und zu versenden oder weitere schädliche Anwendungen auf den Host-Computer zu laden. Mit der Firewall können Sie solche Verbindungen erkennen und beenden.

4.3.3.1 Firewall-Regeln

Klicken Sie auf der Registerkarte im Abschnitt **Einfach** neben **Regeln** auf **Bearbeiten**, um das Fenster **Firewall-Regeln** zu öffnen, in dem die Liste aller Regeln angezeigt wird. **Mit den Optionen Hinzufügen**, **Bearbeiten** und **Entfernen** können Sie Regeln hinzufügen, konfigurieren oder löschen. Sie können auch die Priorität einer Regel ändern, indem Sie eine Regel auswählen und auf **Oben/Nach oben/Nach unten/Unten** klicken.

TIPP: Über das Feld **Suchen** können Sie eine Regel nach Name, Protokoll oder Port suchen.



Spalten

Name – Der Name der Regel.

Aktiviert – Zeigt an, ob Regeln aktiviert oder deaktiviert sind. Zum Aktivieren einer Regel muss das dazugehörige Kontrollkästchen markiert werden.

Protokoll – Das Protokoll, für das diese Regel gilt.

Profil – Zeigt das Firewall-Profil an, für das diese Regel gilt.

Aktion – Zeigt den Verbindungsstatus an (blockieren/zulassen/nachfragen).

Richtung – Die Verbindungsrichtung (eingehend/ausgehend/beide).

Lokal – IP-Adresse und Port des lokalen Computers.

Remote – IP-Adresse und Port des Remotecomputers.

Anwendungen – Anwendung, auf die die Regel angewendet wird.

Steuerelemente

Hinzufügen – Erstellt eine neue Regel.

Bearbeiten – Ermöglicht das Bearbeiten vorhandener Regeln.

Entfernen – Entfernt vorhandene Regeln.

Integrierte (vordefinierte) Regeln anzeigen – Von ESET Internet Security vordefinierte Regeln, die bestimmte Verbindungen zulassen oder ablehnen. Sie können diese Regeln deaktivieren, jedoch keine vordefinierte Regel löschen.

Oben/Nach oben/Nach unten/Unten – Definieren Sie die Priorität von Regeln (Regeln werden von oben nach unten ausgeführt).

4.3.3.2 Arbeiten mit Regeln

Eine Änderung der Einstellungen ist immer dann erforderlich, wenn sich die überwachten Parameter geändert haben. Wenn Änderungen vorgenommen werden, sodass die Regel nicht die Bedingungen erfüllen und die festgelegte Aktion nicht ausgeführt werden kann, wird die entsprechende Verbindung möglicherweise blockiert. Hierbei können Probleme bei der Ausführung der von der Regel betroffenen Anwendung entstehen. Ein typisches Beispiel hierfür ist eine Änderung der Netzwerkadresse oder Portnummer der Gegenstelle.

Im oberen Teil des Fensters werden drei Registerkarten angezeigt:

- **Allgemein** – Geben Sie einen Regelnamen sowie die Verbindungsrichtung, die Aktion (**Zulassen**, **Verweigern**, **Fragen**), das Protokoll und das Profil an, für das die Regel gelten soll.
- **Lokal** – Zeigt Informationen zur lokalen Seite der Verbindung an, darunter die Nummer des lokalen Ports oder Portbereichs und den Namen der kommunizierenden Anwendung. Hier können Sie eine vordefinierte oder erstellte Zone mit einem IP-Adressbereich hinzufügen. Klicken Sie dazu auf **Hinzufügen**.
- **Remote (Gegenstelle)** – Auf dieser Registerkarte werden Informationen zum Remoteport (Portbereich) angezeigt. Hier können Sie eine Liste mit Remote-IP-Adressen oder Zonen für eine Regel angeben. Außerdem können Sie eine vordefinierte oder erstellte Zone mit einem IP-Adressbereich hinzufügen. Klicken Sie dazu auf **Hinzufügen**.

Beim Erstellen einer neuen Regel müssen Sie im Feld **Name** einen Namen für die Regel eingeben. Wählen Sie im Dropdown-Menü **Richtung** die Verbindungsrichtung aus, auf die die Regel angewendet werden soll. Legen Sie über das Dropdown-Menü **Aktion** fest, welche Aktion ausgeführt werden soll, wenn eine Verbindung mit der Regel übereinstimmt.

Protokoll bezeichnet das Übertragungsprotokoll, das für die Regel verwendet wird. Wählen Sie das für eine Regel zu verwendende Protokoll im Dropdown-Menü aus.

ICMP-Typ/Code stellt eine durch eine Zahl gekennzeichnete ICMP-Meldung dar (Beispiel: 0 steht für „Echo-Antwort“).

Standardmäßig sind alle Regeln Für **jedes Profil** aktiviert. Wählen Sie alternativ ein benutzerdefiniertes Firewall-Profil aus dem Dropdown-Menü **Profil** aus.

Wenn Sie **Log** aktivieren, wird die mit der Regel verbundene Aktivität in einem Log aufgezeichnet. Wenn die Option **Benutzer informieren** aktiviert ist, wird beim Anwenden der Regel ein entsprechender Hinweis angezeigt.

HINWEIS

Nachstehend sehen Sie ein Beispiel für die Erstellung einer neuen Regel, mit der der Webbrowseranwendung der Zugriff auf das Netzwerk erlaubt wird. Die folgenden Voraussetzungen müssen erfüllt sein:

- Aktivieren Sie in der Registerkarte **Allgemein** ausgehende Verbindungen über TCP und UDP.
- Fügen Sie in der Registerkarte **Lokal** Ihre Browseranwendung hinzu (z. B. „iexplore.exe“ für Internet Explorer).
- Aktivieren Sie auf der Registerkarte **Remote** Portnummer 80, wenn Sie Standard-Webbrowser-Aktivitäten zulassen möchten.

HINWEIS

Beachten Sie, dass vordefinierte Regeln nur eingeschränkt geändert werden können.

4.3.4 Konfigurieren von Zonen

Eine Zone besteht aus einer Sammlung von Netzwerkadressen, die zusammen eine logische Gruppe von IP-Adressen bilden. Zonen sind hilfreich, wenn Sie dieselben Adressen in mehreren Regeln verwenden möchten. Jeder Adresse in einer Gruppe werden ähnliche Regeln zugewiesen, die zentral für die Gruppe festgelegt werden können. Ein Beispiel für eine solche Gruppe ist die **vertrauenswürdige Zone**. Die vertrauenswürdige Zone ist eine Gruppe von Netzwerkadressen, die nicht von der Firewall blockiert werden. Sie können diese Zonen unter Erweiterte **Einstellungen** > **Firewall** > **Erweitert** konfigurieren, indem Sie neben **Zonen** auf **Bearbeiten** klicken. Klicken Sie zum Hinzufügen einer neuen Zone auf **Hinzufügen**, und geben Sie einen **Namen** und eine **Beschreibung** für die Zone ein. Geben Sie außerdem eine Remote-IP-Adresse in das Feld **Adresse des Remote-Computers** (IPv4, IPv6, Bereich, Maske) ein.

In den Einstellungen der **Firewall-Zonen** können Sie einen Namen für die Zone, eine Beschreibung und eine Liste mit Netzwerkadressen eingeben (siehe auch Editor für bekannte Netzwerke).

4.3.5 Bekannte Netzwerke

Wenn Sie sich mit Ihrem Computer häufig mit öffentlichen Netzwerken oder Netzwerken außerhalb Ihres normalen Heim- oder Arbeitsnetzwerks verbinden, sollten Sie stets die Vertrauenswürdigkeit neuer Netzwerke überprüfen. Nach der Definition der Netzwerke kann ESET Internet Security vertrauenswürdige Heim- oder Arbeitsnetzwerke mithilfe der unter **Netzwerkidentifikation** konfigurierten Netzwerkparameter erkennen. Computer melden sich oft bei Netzwerken mit IP-Adressen an, die jenen der vertrauenswürdigen Netzwerke gleichen. In solchen Fällen kann es vorkommen, dass ESET Internet Security ein unbekanntes Heim- oder Arbeitsnetzwerk als vertrauensvoll einstuft. Um derartige Situationen zu vermeiden, sollten Sie **Netzwerkauthentifizierung** verwenden.

Wenn ein Netzwerkadapter mit dem Netzwerk verbunden ist oder dessen Netzwerkeinstellungen neu konfiguriert wurden, sucht ESET Internet Security in der Liste der bekannten Netzwerke nach einem Eintrag, der mit dem neuen Netzwerk übereinstimmt. Wenn **Netzwerkidentifikation** und **Netzwerkauthentifizierung** (optional) übereinstimmen, wird das Netzwerk in dieser Schnittstelle als verbunden markiert. Wenn kein bekanntes Netzwerk gefunden wurde, erstellt die Netzwerkidentifikations-Konfiguration eine neue Netzwerkverbindung, um das Netzwerk bei der nächsten Verbindung zu identifizieren. Die neue Netzwerkverbindung verwendet standardmäßig den Schutztyp **Öffentliches Netzwerk**. Im Dialogfeld **Neue Netzwerkverbindung erkannt** werden Sie aufgefordert, einen der Schutztypen **Öffentliches Netzwerk**, **Heimnetzwerk** oder **Windows-Einstellung verwenden** auszuwählen. Wenn ein Netzwerkadapter mit einem bekannten Netzwerk verbunden ist, das als **Heim- oder Arbeitsnetzwerk** markiert ist, werden lokale Subnetze des Adapters zur vertrauenswürdigen Zone hinzugefügt.

Schutztyp für neue Netzwerke – Wählen Sie eine der folgenden Optionen aus: **Windows-Einstellung verwenden**, **Benutzer fragen** oder **Als öffentlich kennzeichnen** wird standardmäßig für neue Netzwerke verwendet.

Unter **Bekannte Netzwerke** können Sie Netzwerknamen und -Identifikation, Schutztyp usw. konfigurieren. Klicken Sie auf **Bearbeiten**, um den Editor für bekannte Netzwerke zu öffnen.

HINWEIS
Wenn Sie die Option **Windows-Einstellung verwenden** auswählen, wird kein Dialogfeld angezeigt, und das Netzwerk, mit dem Sie verbunden sind, wird gemäß Ihrer Windows-Einstellungen gekennzeichnet. Dies hat zur Folge, dass bestimmte Funktionen wie z. B. Dateifreigabe und Remotedesktop von neuen Netzwerken aus nicht zugänglich sind.

4.3.5.1 Editor für bekannte Netzwerke

Sie können die bekannten Netzwerke manuell bearbeiten, indem Sie unter **Erweiterte Einstellungen** > **Netzwerk-Schutz** > **Firewall** > **Bekannte Netzwerke** auf **Bearbeiten** klicken.

Spalten

Name – Name des bekannten Netzwerks.

Schutztyp – Zeigt an, ob das Netzwerk als **Heim- oder Arbeitsnetzwerk**, als **öffentliches Netzwerk** oder über die **Windows-Einstellungen** konfiguriert wurde.

Firewall-Profil – Wählen Sie aus dem Dropdown-Menü **Im Profil verwendete Regeln anzeigen** ein Profil aus, um die Regeln für das Profil anzuzeigen.

Profil aktualisieren – Mit dieser Option können Sie ein erstelltes Updateprofil anwenden, wenn Sie mit diesem Netzwerk verbunden sind.

Steuerelemente

Hinzufügen – Erstellt ein neues bekanntes Netzwerk.

Bearbeiten – Bearbeiten eines bestehenden bekannten Netzwerks.

Entfernen – Wählen Sie ein Netzwerk aus und klicken Sie auf **Entfernen**, um es aus der Liste der bekannten Netzwerke zu entfernen.

Oben/Nach oben/Nach unten/Unten – Ermöglicht das Einstellen der Priorität bekannter Netzwerke (die Netzwerke werden von oben nach unten geprüft).

Sie finden die Netzwerkeinstellungen in den folgenden Registerkarten:

Netzwerk

Hier legen Sie den **Netzwerknamen** und den **Schutztyp** (Öffentliches Netzwerk, Heim- oder Arbeitsnetzwerk oder Windows-Einstellungen verwenden) für das Netzwerk fest. Wählen Sie das Profil für dieses Netzwerk im Dropdown-Menü **Firewall-Profil** aus. Wenn das Netzwerk den Schutztyp **Heim- oder Arbeitsnetzwerk** hat, werden alle direkt angeschlossenen Subnetze als vertrauenswürdig eingestuft. Wenn beispielsweise ein Netzwerkadapter mit der IP-Adresse 192.168.1.5 und der Subnetzmaske 255.255.255.0 an dieses Netzwerk angeschlossen wird, wird das Subnetz 192.168.1.0/24 der vertrauenswürdigen Zone dieses Adapters hinzugefügt. Wenn der Adapter mehrere Adressen/Subnetze aufweist, gelten sie alle unabhängig von der **Netzwerkidentifikations**-Konfiguration des bekannten Netzwerks als vertrauenswürdig.

Außerdem werden unter **Weitere vertrauenswürdige Adressen** hinzugefügte Adressen unabhängig vom Schutztyp des Netzwerks immer zur vertrauenswürdigen Zone der mit diesem Netzwerk verbundenen Adapter hinzugefügt.

Vor unsicherer WLAN-Verschlüsselung warnen – ESET Internet Security informiert Sie, wenn Sie sich mit einem ungeschützten oder schwach geschützten WLAN-Netzwerk verbinden.

Firewall-Profil – Wählen Sie das gewünschte Firewall-Profil für die Verbindung mit diesem Netzwerk aus.

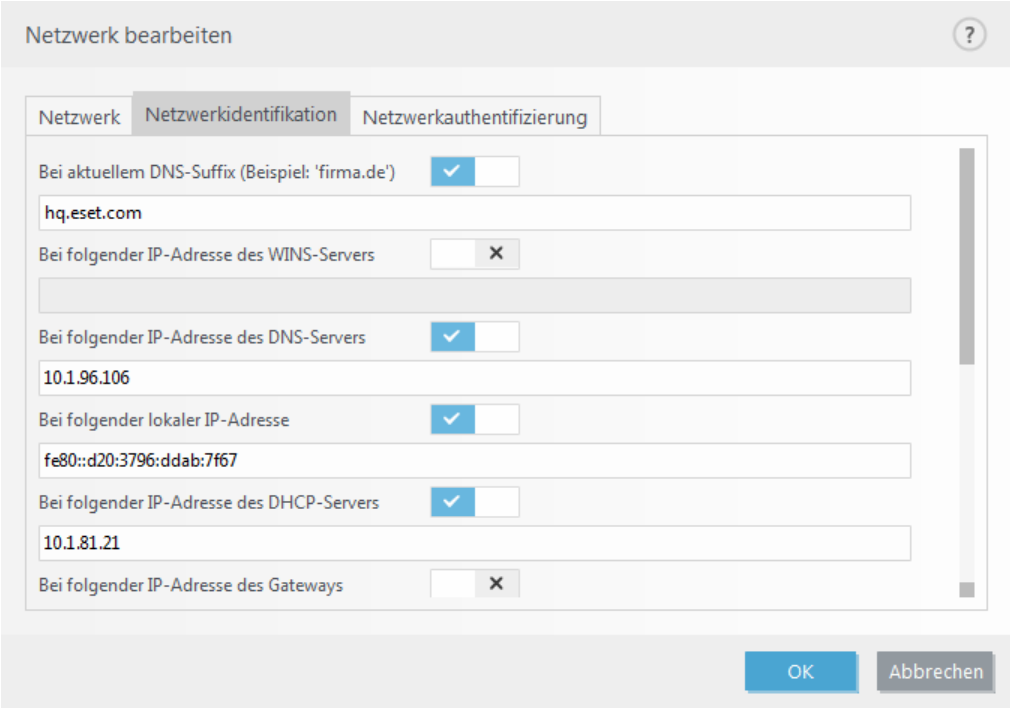
Updateprofil – Wählen Sie das gewünschte Updateprofil für die Verbindung mit diesem Netzwerk aus.

Damit ein Netzwerk in der Liste der angeschlossenen Netzwerke als angeschlossen markiert wird, müssen folgende Bedingungen erfüllt sein:

- Netzwerkidentifikation – Alle eingegebenen Parameter müssen mit aktiven Verbindungsparametern übereinstimmen.
- Netzwerkauthentifizierung – Wenn ein Authentifizierungsserver ausgewählt ist, muss eine erfolgreiche Authentifizierung beim ESET-Authentifizierungsserver erfolgen.
- Netzwerkeinschränkungen (nur Windows XP) – Alle ausgewählten globalen Einschränkungen müssen erfüllt werden.

Netzwerkidentifikation

Die Netzwerkidentifikation erfolgt entsprechend den Parametern einer lokalen Netzwerkkarte. Alle ausgewählten Parameter werden mit den tatsächlichen Parametern aktiver Netzwerkverbindungen verglichen. IPv4- und IPv6-Adressen sind zulässig.



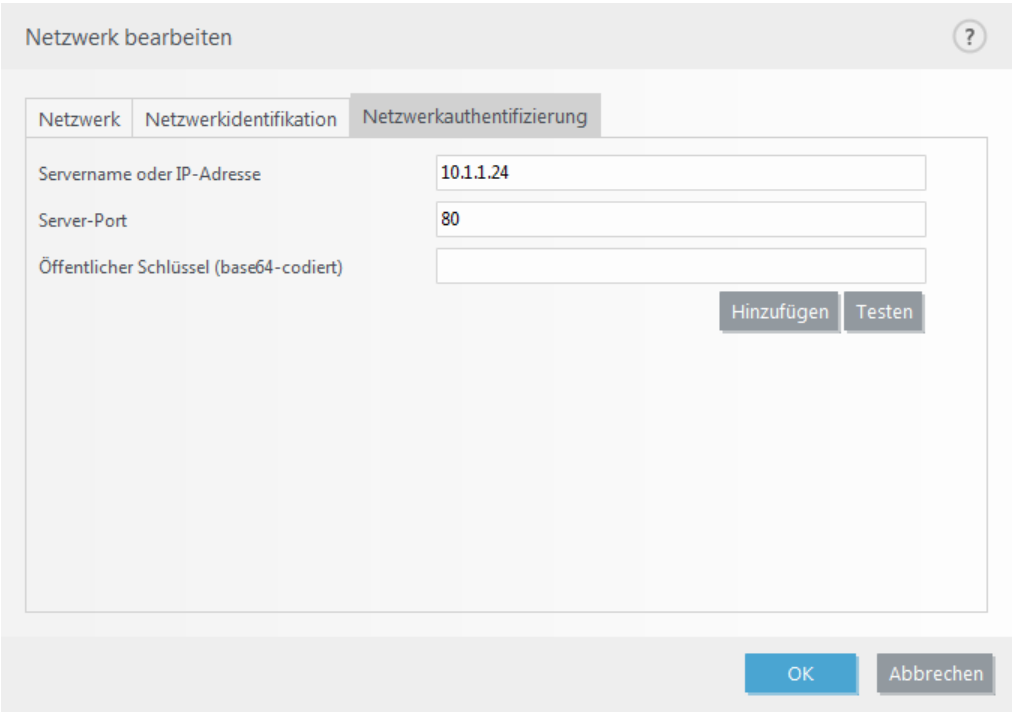
Netzwerkauthentifizierung

Die Netzwerkauthentifizierung sucht nach einem bestimmten Server im Netzwerk und verwendet zur Serverauthentifizierung eine asymmetrische Verschlüsselung (RSA). Der Name des authentifizierten Netzwerks muss mit dem in den Einstellungen des Authentifizierungsservers festgelegten Zonennamen übereinstimmen. Die Groß-/Kleinschreibung des Namens muss beachtet werden. Geben Sie einen Servernamen, einen Listening-Port für den Server und einen öffentlichen Serverschlüssel an, der dem privaten Serverschlüssel entspricht (siehe Abschnitt Netzwerkauthentifizierung – Server-Konfiguration). Der Servername kann in Form einer IP-Adresse oder eines DNS- oder NetBios-Namens gefolgt von einem Pfad eingegeben werden, der den Speicherort des Schlüssels auf dem Server angibt (zum Beispiel „servername/verzeichnis1/verzeichnis2/authentifizierung“). Sie können zu verwendende alternative Server festlegen, die Sie durch Semikolon getrennt an den Pfad anhängen.

Laden Sie den ESET-Authentifizierungsserver herunter.

Der öffentliche Schlüssel kann mit einem der folgenden Dateitypen importiert werden:

- PEM-verschlüsselter öffentlicher Schlüssel (.pem); dieser Schlüssel kann mit dem ESET-Authentifizierungsserver generiert werden (siehe Netzwerkauthentifizierung – Serverkonfiguration).
- Verschlüsselter öffentlicher Schlüssel
- Zertifikat für öffentlichen Schlüssel (.crt)



Klicken Sie auf **Testen**, um Ihre Einstellungen zu testen. Bei erfolgreicher Authentifizierung wird der Hinweis *Serverauthentifizierung war erfolgreich* angezeigt. Wenn die Authentifizierung nicht richtig konfiguriert ist, wird eine der folgenden Fehlermeldungen angezeigt:

Fehler bei der Serverauthentifizierung. Ungültige oder falsche Signatur.
Die Serversignatur stimmt nicht mit dem eingegebenen öffentlichen Schlüssel überein.

Fehler bei der Serverauthentifizierung. Falscher Netzwerkname.
Der konfigurierte Netzwerkname entspricht nicht dem Namen des Authentifizierungsservers. Überprüfen Sie beide Namen, und stellen Sie sicher, dass sie identisch sind.

Fehler bei der Serverauthentifizierung. Ungültige oder keine Antwort vom Server.
Wenn der Server nicht ausgeführt wird oder nicht erreichbar ist, wird keine Antwort empfangen. Wenn ein anderer HTTP-Server unter der angegebenen Adresse ausgeführt wird, wird möglicherweise eine ungültige Antwort empfangen.

Ungültiger öffentlicher Schlüssel eingegeben.
Stellen Sie sicher, dass die eingegebene öffentliche Schlüsseldatei nicht beschädigt ist.

Netzwerkeinschränkungen (nur für Windows XP)

Auf modernen Betriebssystemen (Windows Vista und neuer) hat jeder Netzwerkadapter eine eigene vertrauenswürdige Zone und ein eigenes aktives Firewall-Profil. Unter Windows XP wird dieses Layout nicht unterstützt. Daher verwenden alle Netzwerkadapter ein und dieselbe vertrauenswürdige Zone und ein und dasselbe aktive Firewall-Profil. Dies stellt ein potenzielles Sicherheitsrisiko dar, wenn der Computer gleichzeitig mit mehreren Netzwerken verbunden wird. In solchen Fällen kann Verkehr, der aus einem nicht vertrauenswürdigen Netzwerk stammt, über die vertrauenswürdige Zone und das Firewall-Profil geprüft werden, die für das andere verbundene Netzwerk konfiguriert wurden. Um etwaige Sicherheitsrisiken auszuschließen, können Sie mithilfe der folgenden Beschränkungen verhindern, dass eine Netzwerkkonfiguration global angewendet wird, während ein anderes (potenziell nicht vertrauenswürdiges) Netzwerk angeschlossen ist.

Unter Windows XP werden die Einstellungen für verbundene Netzwerke (vertrauenswürdige Zone und Firewall-Profil) global angewendet, sofern nicht mindestens eine der folgenden Beschränkungen aktiviert ist und nicht erfüllt wird:

a. Nur eine aktive Verbindung
b. Es wird keine Drahtlosverbindung hergestellt
c. Es wird keine unsichere Drahtlosverbindung hergestellt

4.3.5.2 Netzwerkauthentifizierung - Serverkonfiguration

Die Authentifizierung kann durch jeden Computer/Server ausgeführt werden, der mit dem zu authentifizierenden Netzwerk verbunden ist. Die Anwendung für den ESET-Authentifizierungsserver muss auf einem Computer/Server installiert sein, der jederzeit für die Authentifizierung verfügbar ist, wenn ein Client versucht, eine Verbindung mit dem Netzwerk herzustellen. Die Installationsdatei der Anwendung für den ESET-Authentifizierungsserver kann von der ESET-Website heruntergeladen werden.

Nach der Installation der Anwendung für den ESET-Authentifizierungsserver wird ein Dialogfenster angezeigt (Sie können unter **Start** > **Alle Programme** > **ESET** > **ESET-Authentifizierungsserver** auf die Anwendung zugreifen).

Zum Konfigurieren des Authentifizierungsservers geben Sie den Namen der Authentifizierungszone, den Listening-Port für den Server (standardmäßig Port 80) und den Speicherort für den öffentlichen und den privaten Schlüssel ein. Erzeugen Sie dann den öffentlichen und den privaten Schlüssel, die bei der Authentifizierung verwendet werden. Der private Schlüssel verbleibt auf dem Server, während der öffentliche Schlüssel auf Seiten des Clients noch in die Authentifizierungszone importiert werden muss, die bei der Einrichtung der Firewall eingestellt wird.

Weitere Details zu diesem Feature finden Sie in diesem ESET Knowledgebase-Artikel.

4.3.6 Erstellen von Logs

Die ESET Internet Security Firewall speichert alle wichtigen Vorgänge in einer Log-Datei, die direkt vom Hauptmenü aus aufgerufen werden kann. Klicken Sie auf **Tools** > **Log-Dateien** und wählen Sie **Firewall** im Dropdownmenü **Log** aus.

Anhand der Log-Dateien können Sie Fehler und Eindringungsversuche in Ihr System erkennen. Die Log-Dateien der ESET Firewall enthalten folgende Daten:

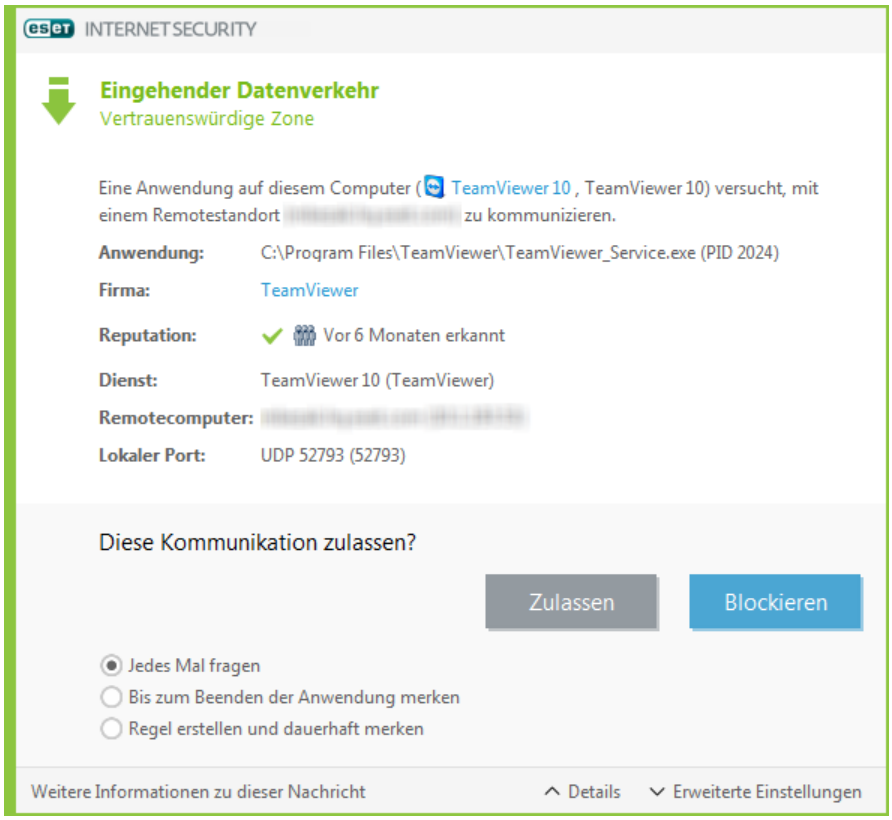
- Datum und Uhrzeit des Ereignisses
- Name des Ereignisses
- Quelle
- Zieladresse
- Netzwerk-Übertragungsprotokoll
- Zugewiesene Regel oder, falls identifiziert, Name des Wurms
- Beteiligte Anwendung
- Benutzer

Eine gründliche Analyse dieser Daten kann wesentlich dazu beitragen, Angriffe auf die Systemsicherheit frühzeitig zu erkennen. Viele andere Faktoren können auf Sicherheitsrisiken hinweisen und sollten beobachtet werden, um mögliche Auswirkungen zu minimieren: häufige Verbindungen von unbekannten Standorten, ungewöhnlich viele Verbindungsversuche, Verbindungen mit unbekannten Anwendungen, Benutzung ungewöhnlicher Portnummern.

4.3.7 Verbindung herstellen – Erkennung

Die Firewall erkennt jede neu erstellte Netzwerkverbindung. Durch den aktivierten Firewall-Modus wird bestimmt, welche Vorgänge für die neue Regel ausgeführt werden. Wenn die Optionen **Automatischer Filtermodus** bzw. **Regelbasierter Filtermodus** aktiviert wurden, führt die Firewall die vordefinierten Aktionen automatisch aus.

Im interaktiven Filtermodus wird bei einer neu erkannten Netzwerkverbindung ein Fenster mit genauen Informationen angezeigt. Sie können dann entscheiden, ob die Verbindung zugelassen oder blockiert werden soll. Wenn dieselbe Verbindung im Dialogfenster mehrmals zugelassen wurde, sollte eine neue Regel erstellt werden. Wählen Sie dazu die Option **Regel erstellen und dauerhaft merken** aus und speichern Sie die Aktion als neue Regel für die Firewall. Wenn die Firewall erneut dieselbe Verbindung erkennt, wird die entsprechende Regel ohne Benutzerinteraktion angewendet.



Seien Sie vorsichtig, wenn Sie neue Regeln erstellen. Lassen Sie nur bekannte, sichere Verbindungen zu. Wenn alle Verbindungen zugelassen werden, kann die Firewall ihren Zweck nicht erfüllen. Die wesentlichen Parameter für Verbindungen sind:

- **Gegenstelle** – Lassen Sie nur Verbindungen mit vertrauenswürdigen und bekannten Adressen zu.
- **Lokale Anwendung** – Es wird davon abgeraten, Verbindungen für unbekannte Anwendungen oder Prozesse zuzulassen.
- **Portnummer** - Verbindungen über übliche Ports (z. B. Web-Daten - Portnummer 80) können im Normalfall zugelassen werden.

Schadsoftware wird häufig über das Internet oder über versteckte Verbindungen verbreitet, um fremde Systeme zu infizieren. Wenn die Regeln richtig konfiguriert werden, ist die Firewall ein wirksames Hilfsmittel zum Schutz vor verschiedensten Schadcode-Angriffen.

4.3.8 Lösen von Problemen mit der ESET Firewall

Wenn bei Computern, auf denen ESET Internet Security installiert ist, Konnektivitätsprobleme auftreten, kann auf mehrere Arten festgestellt werden, ob die ESET Firewall die Ursache dafür ist. Darüber hinaus kann Ihnen die ESET Firewall bei der Erstellung neuer Regeln oder Ausnahmen helfen, um Konnektivitätsprobleme zu vermeiden.

In den folgenden Themen finden Sie Hilfe bei Problemen mit der ESET Firewall:

- Fehlerbehebungsassistent
- Erstellen von Logs und Erstellen von Regeln oder Ausnahmen anhand des Logs
- Erstellen von Ausnahmen von Firewall-Hinweisen
- Erweitertes PCAP-Logging
- Lösen von Problemen bei der Protokollfilterung

4.3.8.1 Fehlerbehebungsassistent

Der Feherbehebungsassistent überwacht im Hintergrund alle blockierten Verbindungen und begleitet Sie durch den Fehlerbehebungsprozess, um Firewall-Probleme bei bestimmten Anwendungen oder Geräten zu lösen. Anschließend schlägt der Assistent eine neue Reihe von Regeln vor, die angewendet werden, wenn Sie sie genehmigen. **Sie finden den Fehlerbehebungsassistenten** im Hauptmenü unter **Einstellungen** > **Netzwerk-Schutz**.

4.3.8.2 Erstellen von Logs und Erstellen von Regeln oder Ausnahmen anhand des Logs

In der ESET Firewall werden standardmäßig nicht alle blockierten Verbindungen in einem Log aufgezeichnet. Um zu sehen, welche Verbindungen von der Firewall blockiert wurden, aktivieren Sie das Logging unter **Erweiterte Einstellungen** > **Tools** > **Diagnose** > **Erweitertes Logging für Firewall aktivieren**. Wenn die Log-Datei Einträge enthält, die die Firewall nicht blockieren soll, können Sie eine Regel oder eine IDS-Ausnahme erstellen. Klicken Sie hierzu mit der rechten Maustaste auf den entsprechenden Eintrag und wählen Sie **Ähnliche Ereignisse zukünftig nicht blockieren** aus. Bedenken Sie, dass das Log aller blockierten Verbindungen möglicherweise Tausende von Einträgen enthält und bestimmte Verbindungen somit schwer zu finden sind. Sie sollten die Log-Erstellung daher deaktivieren, nachdem Sie Ihr Problem gelöst haben.

Weitere Informationen zum Log finden Sie unter Log-Dateien.

HINWEIS
Anhand der Log-Erstellung lässt sich die Reihenfolge erkennen, in der die Firewall bestimmte Verbindungen blockiert hat. Außerdem können Sie anhand des Logs Regeln erstellen, die sich genau so verhalten, wie Sie es wünschen.

4.3.8.2.1 Regel aus Log erstellen

Mit der neuen Version von ESET Internet Security können Sie eine Regel im Log erstellen. Klicken Sie im Hauptmenü auf **Tools** > **Weitere Tools** > **Log-Dateien**. Wählen Sie **Firewall** im Dropdownmenü aus, klicken Sie mit der rechten Maustaste auf den gewünschten Log-Eintrag und wählen Sie **Ähnliche Ereignisse zukünftig nicht blockieren** im Kontextmenü aus. Die neue Regel wird in einem Hinweisfenster angezeigt.

Für die Erstellung neuer Regeln aus dem Log müssen die folgenden Einstellungen in ESET Internet Security vorgenommen werden:

- Stellen Sie die Mindestinformation in Logs unter **Erweiterte Einstellungen** (F5) > **Tools** > **Log-Dateien** auf **Diagnose** ein,
- Aktivieren Sie die Option **Benachrichtigung auch bei eingehenden Angriffen auf Sicherheitslücken anzeigen** unter **Erweiterte Einstellungen** (F5) > **Firewall** > **IDS und erweiterte Optionen** > **Eindringversuche erkennen**.

4.3.8.3 Erstellen von Ausnahmen von Firewall-Hinweisen

Wenn die ESET Firewall schädliche Netzwerkaktivitäten erkennt, wird ein Hinweisfenster mit einer Beschreibung des Ereignisses angezeigt. Dieser Hinweis enthält ein Link, der weitere Informationen zum Ereignis enthält und unter dem Sie ggf. eine Ausnahme für dieses Ereignis erstellen können.

HINWEIS
Wenn eine Netzwerkanwendung oder ein Gerät Netzwerkstandards nicht ordnungsgemäß implementiert, kann dies dazu führen, dass wiederholte IDS-Hinweise zur Firewall angezeigt werden. Damit die ESET Firewall diese Anwendung bzw. dieses Gerät künftig nicht mehr erkennt, können Sie direkt im Hinweis eine Ausnahme erstellen.

4.3.8.4 Erweitertes PCAP-Logging

Diese Funktion dient dazu, komplexere Log-Dateien für den ESET-Kundendienst zu liefern. Verwenden Sie sie nur, wenn Sie vom ESET-Kundendienst dazu aufgefordert werden, da hiermit eine möglicherweise sehr große Log-Datei erstellt wird, die die Leistung Ihres Computers beeinträchtigt.

1. Navigieren Sie zu **Erweiterte Einstellungen** > **Tools** > **Diagnose**, und aktivieren Sie die Option **Erweitertes Firewall-Logging aktivieren**.
2. Versuchen Sie, das aufgetretene Problem zu reproduzieren.
3. Deaktivieren Sie das erweiterte PCAP-Logging.
4. Die PCAP-Log-Datei befindet sich im selben Verzeichnis, in dem Speicherabbilder zur Diagnose erzeugt werden:

- Microsoft Windows Vista oder neuer

  C:\ProgramData\ESET\ESET Internet Security\Diagnostics

- Microsoft Windows XP

  C:\Dokumente und Einstellungen\Alle Benutzer\...

4.3.8.5 Lösen von Problemen bei der Protokollfilterung

Wenn Sie Probleme mit dem Browser oder dem E-Mail-Programm haben, überprüfen Sie als erstes, ob die Ursache dafür möglicherweise die Protokollfilterung ist. Deaktivieren Sie hierfür vorübergehend die Anwendungsprotokollfilterung in den erweiterten Einstellungen. Denken Sie daran, sie anschließend wieder zu aktivieren, da Browser und E-Mail-Programm ansonsten nicht geschützt sind. Wenn das Problem hiermit behoben ist, finden Sie nachstehend eine Liste gängiger Probleme nebst deren Lösung:

Probleme mit Updates oder sicheren Verbindungen

Wenn Ihre Anwendung nicht aktualisiert werden kann oder ein Kommunikationskanal nicht sicher ist:

- Wenn die SSL-Protokollfilterung aktiviert ist, deaktivieren Sie sie vorübergehend. Wenn das Problem damit behoben ist, können Sie die SSL-Filterung aktiviert lassen und das Update durch Ausschließen der problematischen Verbindung anwenden:
  Setzen Sie den SSL-Protokollfiltermodus auf „interaktiv“. Führen Sie das Update erneut aus. Es sollte ein Dialogfeld angezeigt werden, in dem Sie über verschlüsselten Datenverkehr informiert werden. Vergewissern Sie sich, dass die Anwendung mit jener übereinstimmt, bei der Sie Fehler beheben und dass das Zertifikat von dem Server stammt, von dem auch das Update stammt. Speichern Sie anschließend die Aktion zu diesem Zertifikat und klicken Sie auf „Ignorieren“. Wenn weitere Dialogfelder angezeigt werden, können Sie den Filtermodus wieder auf „automatisch“ setzen. Das Problem sollte nun behoben sein.
- Wenn es sich bei der Anwendung nicht um einen Browser oder ein E-Mail-Programm handelt, können Sie sie komplett aus der Protokollfilterung ausschließen (ein Browser oder ein E-Mail-Programm wäre in diesem Fall ungeschützt). Anwendungen, deren Kommunikation bereits in der Vergangenheit gefiltert wurde, sollten sich

bereits in der Liste befinden, die bei Hinzufügen einer Ausnahme angezeigt wird, somit brauchen sie wahrscheinlich nicht manuell hinzugefügt werden.

Problem beim Zugriff auf ein Gerät im Netzwerk

Wenn die Funktionen eines Geräts im Netzwerk nicht genutzt werden können (wenn beispielsweise Webseiten einer Webcam nicht geöffnet oder Videos auf einem Home-Media-Player nicht abgespielt werden können), fügen Sie dessen IPv4- und IPv6-Adressen zur Liste der ausgeschlossenen Adressen hinzu.

Probleme mit einer bestimmten Website

Mithilfe der URL-Adressverwaltung können Sie bestimmte Websites von der Protokollfilterung ausschließen. Wenn Sie beispielsweise nicht auf https://www.gmail.com/intl/en/mail/help/about.html zugreifen können, fügen Sie *gmail.com* zur Liste der ausgeschlossenen Adressen hinzu.

Fehler „Anwendungen, welche das Root-Zertifikat importieren können, sind noch aktiv“

Bei Aktivierung der SSL-Protokollfilterung vergewissert sich ESET Internet Security, dass die installierten Anwendungen der Art und Weise der Filterung von SSL-Protokollen vertrauen, indem ein Zertifikat in ihren Zertifikatspeicher importiert wird. Bei einigen Anwendungen wie Firefox und Opera ist dies nicht möglich, während sie ausgeführt werden. Vergewissern Sie sich, dass keine dieser Anwendungen ausgeführt wird (öffnen Sie hierzu den Taskmanager und stellen Sie sicher, dass sich in der Registerkarte „Prozesse“ keine Einträge mit der Bezeichnung „firefox.exe“ oder „opera.exe“ befinden) und wiederholen Sie den Vorgang.

Fehler aufgrund eines nicht vertrauenswürdigen Ausstellers oder einer ungültigen Signatur

Dies bedeutet in den meisten Fällen, dass der oben beschriebene Zertifikatimport fehlgeschlagen ist. Vergewissern Sie sich, dass keine der genannten Anwendungen ausgeführt wird. Deaktivieren Sie anschließend die SSL-Protokollfilterung und aktivieren Sie sie erneut. Hiermit wird der Import erneut durchgeführt.

4.4 Sicherheits-Tools

Im Sicherheits-Tools-Setup können Sie die folgenden Module konfigurieren:

- Online-Banking-Zahlungsschutz
- Kindersicherung
- Anti-Theft

4.4.1 Kindersicherung

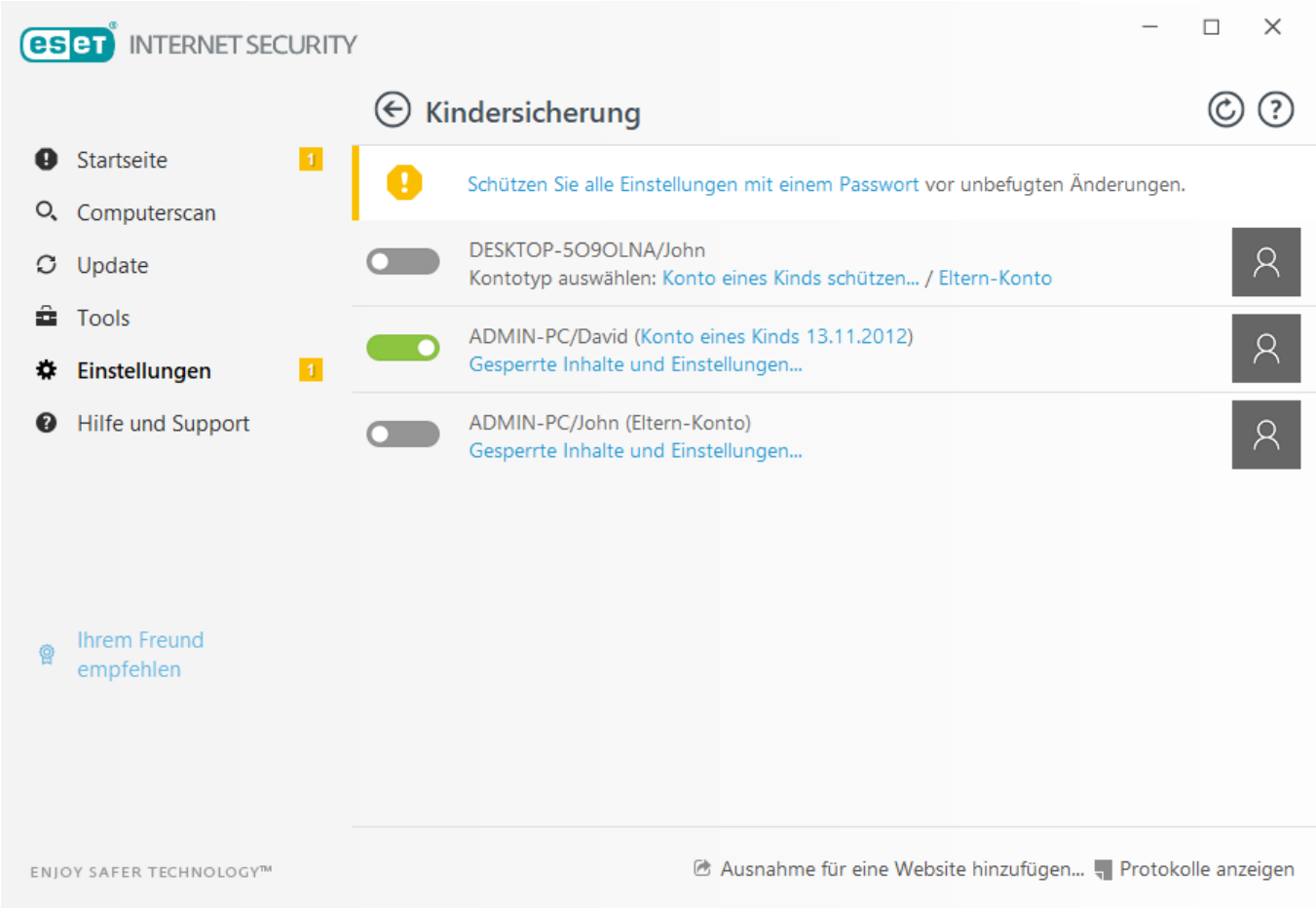
Im Modul „Kindersicherung“ können Sie die Einstellungen für diese Option wählen. So haben Eltern die Möglichkeit, ihre Kinder mit automatisierten Funktionen zu schützen und die Nutzung von Geräten und Diensten einzuschränken. Ziel ist es, dass Kinder und Jugendliche keinen Zugriff auf Websites mit ungeeigneten oder schädlichen Inhalten erhalten.

Mit der Kindersicherung können Sie Webseiten sperren, die potenziell Unerlaubtes enthalten könnten. Außerdem können Eltern mit dieser Funktion den Zugriff auf über 40 vordefinierte Webseitenkategorien und über 140 Unterkategorien unterbinden.

Befolgen Sie die nachstehenden Schritte, um die Kindersicherung für ein bestimmtes Benutzerkonto zu aktivieren:

1. Standardmäßig ist die Kindersicherung in ESET Internet Security deaktiviert. Zur Aktivierung der Kindersicherung stehen zwei Methoden zur Verfügung:
   - Klicken Sie auf  unter **Einstellungen** > **Sicherheits-Tools** > **Kindersicherung** im Hauptprogrammfenster, und ändern Sie den Status der Kindersicherung zu Aktiviert.
   - Drücken Sie F5, um die **Erweiterten Einstellungen** zu öffnen. Navigieren Sie anschließend zu **Web und E-Mail** > **Kindersicherung**, und aktivieren Sie das Kontrollkästchen neben **Systemintegration**.
2. Klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Sicherheits-Tools** > **Kindersicherung**. Auch wenn neben dem Eintrag **Kindersicherung** bereits **Aktiviert** angezeigt wird, müssen Sie die Kindersicherung für das

gewünschte Konto konfigurieren, indem Sie auf **Konto eines Kinds schützen** bzw. auf **Eltern-Konto** klicken. Geben Sie im nächsten Fenster ein Geburtsdatum ein, um die Zugriffsebene und empfohlene, altersangemessene Webseiten zu bestimmen. Die Kindersicherung wird nun für das angegebene Benutzerkonto aktiviert. Klicken Sie unter dem Kontonamen auf **Gesperrte Inhalte und Einstellungen...**, um auf der Registerkarte Kategorien festzulegen, welche Kategorien Sie blockieren bzw. zulassen möchten. Um Webseiten ohne Kategorie zu blockieren bzw. zuzulassen, klicken Sie auf die Registerkarte Ausnahmen.



Klicken Sie im Hauptfenster von ESET Internet Security auf **Erweiterte Einstellungen** > **Sicherheits-Tools** > **Kindersicherung**, um ein Fenster mit dem folgenden Inhalt zu öffnen:

Windows-Benutzerkonten

Wenn Sie eine Rolle für ein vorhandenes Konto erstellt haben, wird es hier angezeigt. Klicken Sie auf den Schieberegler, damit ein grünes Häkchen neben dem Eintrag „Kindersicherung“ für das entsprechende Konto angezeigt wird. Klicken Sie unter einem aktiven Konto auf Gesperrte Inhalte und Einstellungen... , um die Liste der zugelassenen Webseiten-Kategorien sowie die gesperrten und die zugelassenen Webseiten für das Konto anzuzeigen.

WICHTIG
Führen Sie folgende Schritte aus, um unter Windows 7 oder Windows Vista ein neues Konto (z. B. für ein Kind) zu erstellen:

1. Öffnen Sie das Fenster Benutzerkonten. Klicken Sie hierzu auf die Schaltfläche **Start** (am unteren linken Bildschirmrand), auf den Eintrag **Systemsteuerung** und dann auf **Benutzerkonten**.
2. Klicken Sie auf **Benutzerkonto verwalten**. Wenn Sie zur Eingabe des Administratorpassworts oder zu einer Bestätigung aufgefordert werden, geben Sie das Passwort ein bzw. bestätigen Sie.
3. Klicken Sie auf **Neues Konto erstellen**.
4. Geben Sie den gewünschten Namen für das Benutzerkonto an, klicken Sie auf den gewünschten Kontotyp und klicken Sie dann auf **Konto erstellen**.
5. Öffnen Sie erneut den Bereich „Kindersicherung“, indem Sie im Hauptprogrammfenster von ESET Internet Security auf **Erweiterte Einstellungen** > **Sicherheits-Tools** > **Kindersicherung** klicken.

Der untere Teil des Fensters enthält

Ausnahme für eine Website hinzufügen... – Sie können einzelne Websites anhand Ihrer Einstellungen für die einzelnen Elternkonten separat sperren oder erlauben.

Logs anzeigen - Öffnet wird ein detailliertes Log über die Aktivitäten der Kindersicherung (gesperrte Webseiten, das Konto, dem der Zugriff auf die Webseite verweigert wurde, die Kategorie usw.). Sie können dieses Log auch nach Kriterien filtern, indem Sie auf **Filter...** klicken.

Kindersicherung

Wenn Sie die Kindersicherung deaktivieren, wird das Fenster **Kindersicherung deaktivieren** geöffnet. In diesem Fenster können Sie den Zeitraum festlegen, für den der Schutz deaktiviert werden soll. Die Option wechselt anschließend zu **Angehalten** oder **Permanent deaktiviert**.

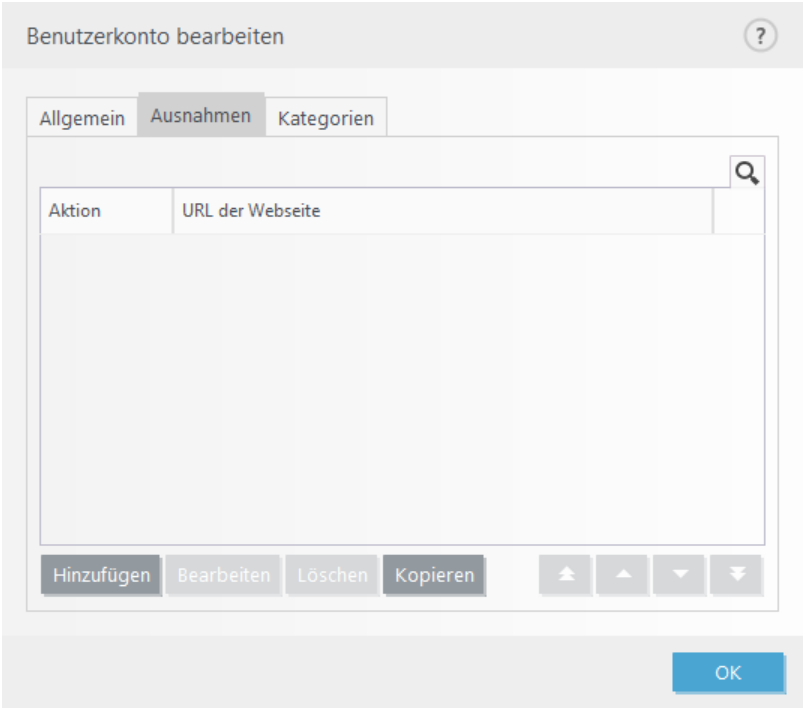
Es ist wichtig, die Einstellungen von ESET Internet Security mit einem Passwort zu schützen. Dieses Passwort können Sie im Bereich Einstellungen für den Zugriff festlegen. Wenn kein Passwort eingerichtet ist, wird die Warnung **Schützen Sie alle Einstellungen mit einem Passwort** angezeigt, um unbefugte Änderungen zu vermeiden. Die in der Kindersicherung festgelegten Einschränkungen betreffen nur die Konten von Standardbenutzern. Auf Administratorkonten haben sie keine Auswirkungen, da diese umfassende Rechte haben.

Standardmäßig wird HTTPS (SSL)-Kommunikation nicht gefiltert. Daher kann keine Sperre für Webseiten festgelegt werden, deren Adresse mit *https://* beginnt. Aktivieren Sie dieses Feature über die Einstellung **SSL/TLS-Protokollfilterung aktivieren** in den **Erweiterten Einstellungen** unter **Web und E-Mail** > **SSL/TLS**.

HINWEIS
Für die optimale Funktion der Kindersicherung müssen die Optionen Prüfen von anwendungsspezifischen Protokollen und HTTP-Prüfung sowie die Systemintegration der Firewall aktiviert sein. Diese Funktionen sind standardmäßig aktiviert.

4.4.1.1 Kategorien

Aktivieren Sie den Schalter neben einer Kategorie, um diese zuzulassen. Wenn der Schalter deaktiviert ist, wird die Kategorie für das Konto nicht zugelassen.

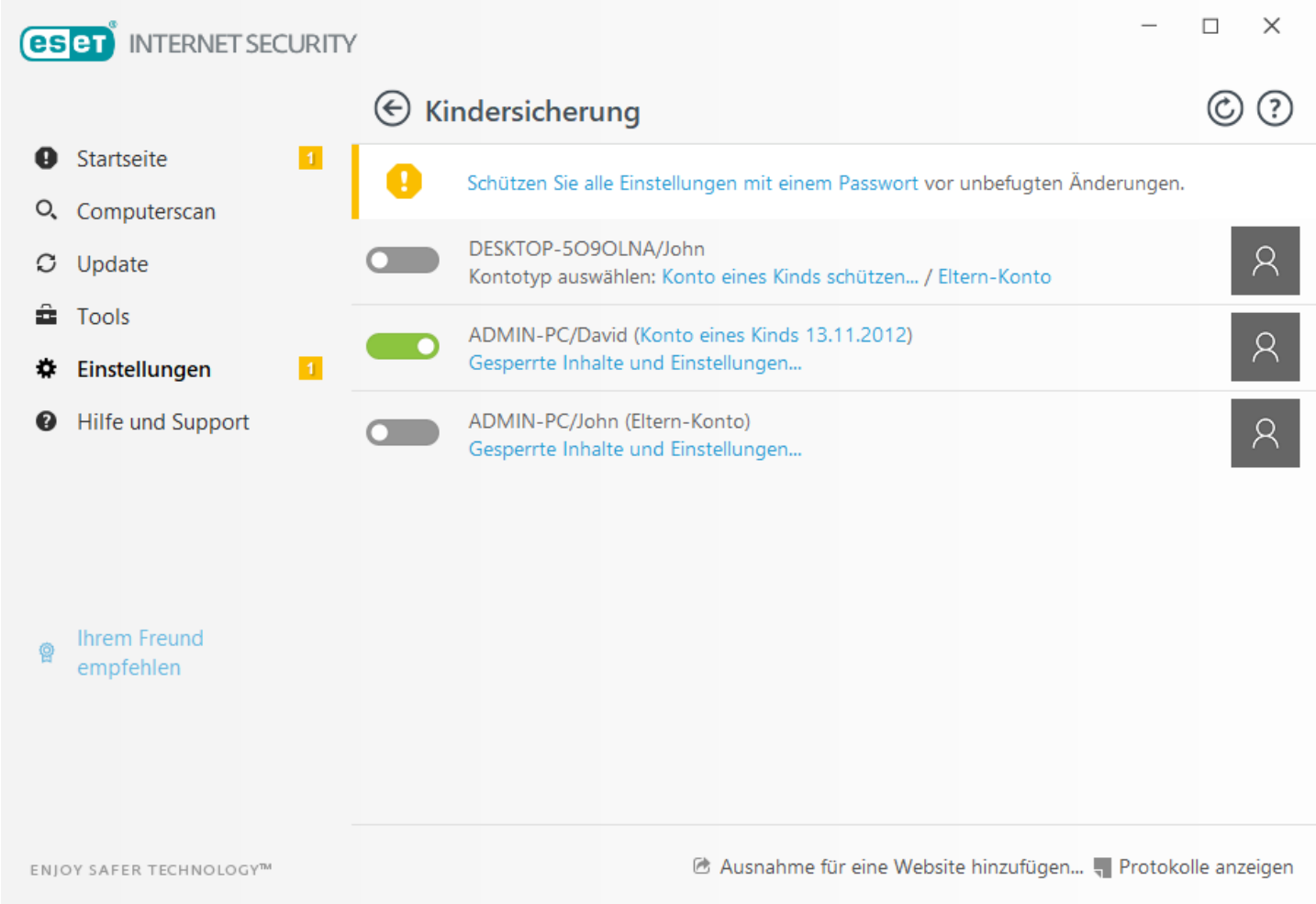


Nachfolgend finden Sie einige Beispiele für Kategorien (Gruppen), mit denen der Benutzer möglicherweise nicht vertraut ist.

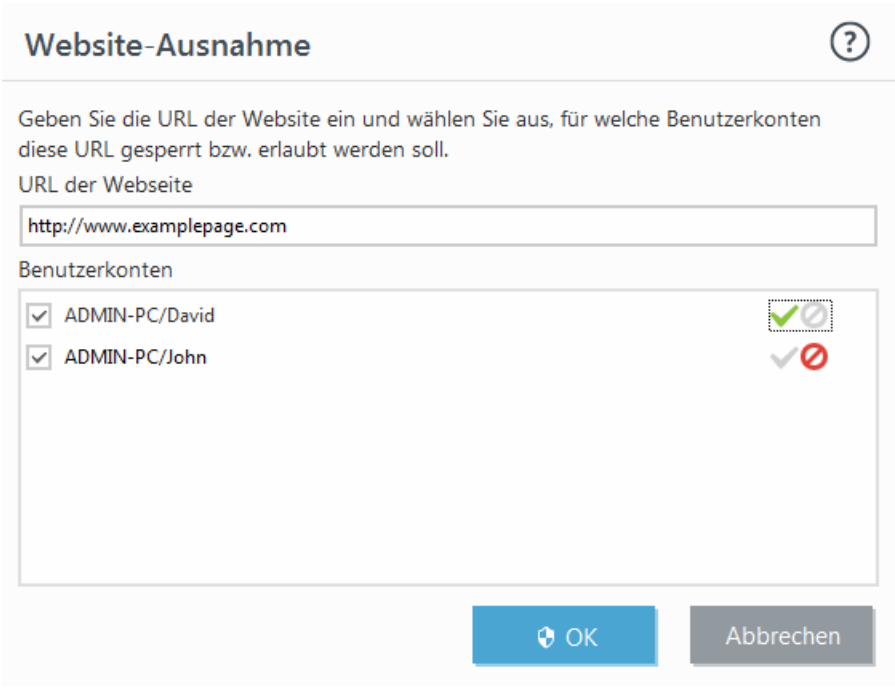
- **Allgemein** – Üblicherweise private (lokale) IP-Adressen, z. B. Intranet, 127.0.0.0/8, 192.168.0.0/16 usw. Bei einem Fehlercode 403 oder 404 wird die Website ebenfalls in diese Kategorie eingestuft.
- **Nicht aufgelöst** – Diese Kategorie enthält Webseiten, die aufgrund eines Fehlers bei der Verbindung zur Datenbank-Engine der Kindersicherung nicht aufgelöst werden konnten.
- **Nicht kategorisiert** – Unbekannte Webseiten, die noch nicht in der Datenbank der Kindersicherung enthalten sind.
- **Dynamisch** – Webseiten, die auf andere Seiten auf anderen Webseiten weiterleiten.

4.4.1.2 Website-Ausnahmen

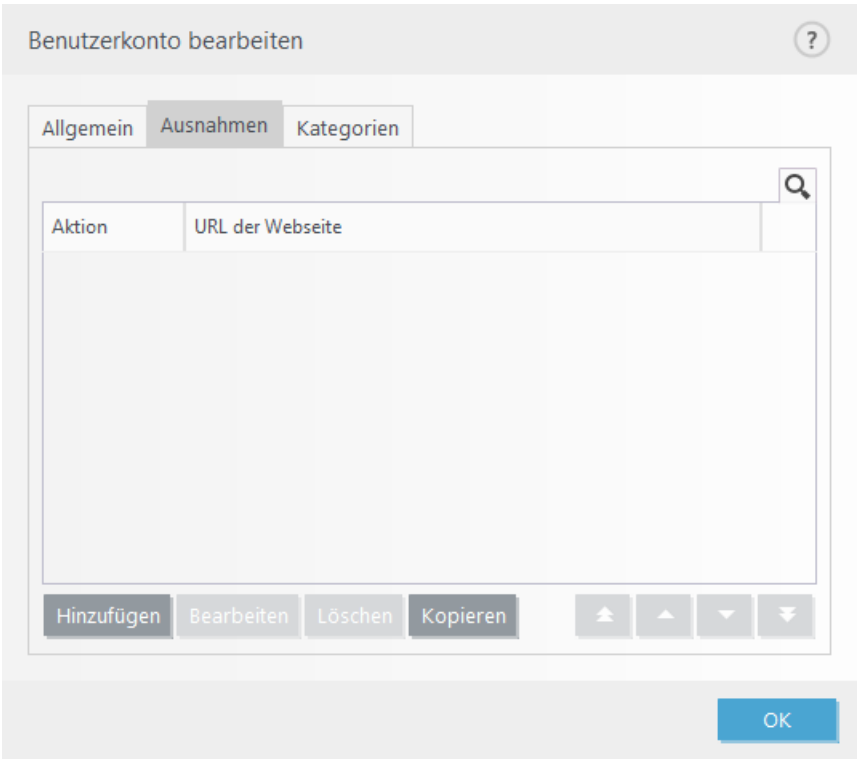
Um eine Ausnahme für eine Webseite hinzuzufügen, klicken Sie auf **Einstellungen** > **Sicherheits-Tools** > **Kindersicherung**, und dann auf **Ausnahme für eine Website hinzufügen**.



Geben Sie eine URL in das Feld **URL der Webseite** ein, wählen Sie ✔ (erlaubt) oder ⊘ (blockiert) für die einzelnen Benutzerkonten aus, und klicken Sie auf **OK**, um die URL zur Liste hinzuzufügen.



Um eine URL aus der Liste zu löschen, klicken Sie auf **Einstellungen** > **Sicherheits-Tools** > **Kindersicherung**, dann auf **Gesperrte Inhalte und Einstellungen** für das gewünschte Benutzerkonto. Klicken Sie auf die Registerkarte **Ausnahme**, wählen Sie die gewünschte Ausnahme aus, und klicken Sie auf **Entfernen**.



In der Liste der URL-Adressen können Sie die Sonderzeichen * (Sternchen) und ? (Fragezeichen) nicht verwenden. Webseitenadressen mit mehreren TLDs müssen beispielsweise manuell eingegeben werden *(beispielseite.com*, *beispielseite.sk* usw.). Wenn Sie eine Domäne zur Liste hinzufügen, werden alle Inhalte der Domäne und der Unterdomänen (z. B. *unterdomäne.beispielseite.com*) je nach gewählter URL-basierter Aktion gesperrt bzw. zugelassen.

HINWEIS

Eine bestimmte Webseite zu sperren bzw. zuzulassen kann effizienter sein, als dies für eine ganze Kategorie von Webseiten zu tun. Seien Sie vorsichtig, wenn Sie diese Einstellungen ändern oder eine Kategorie/Webseite zu einer Liste hinzufügen.

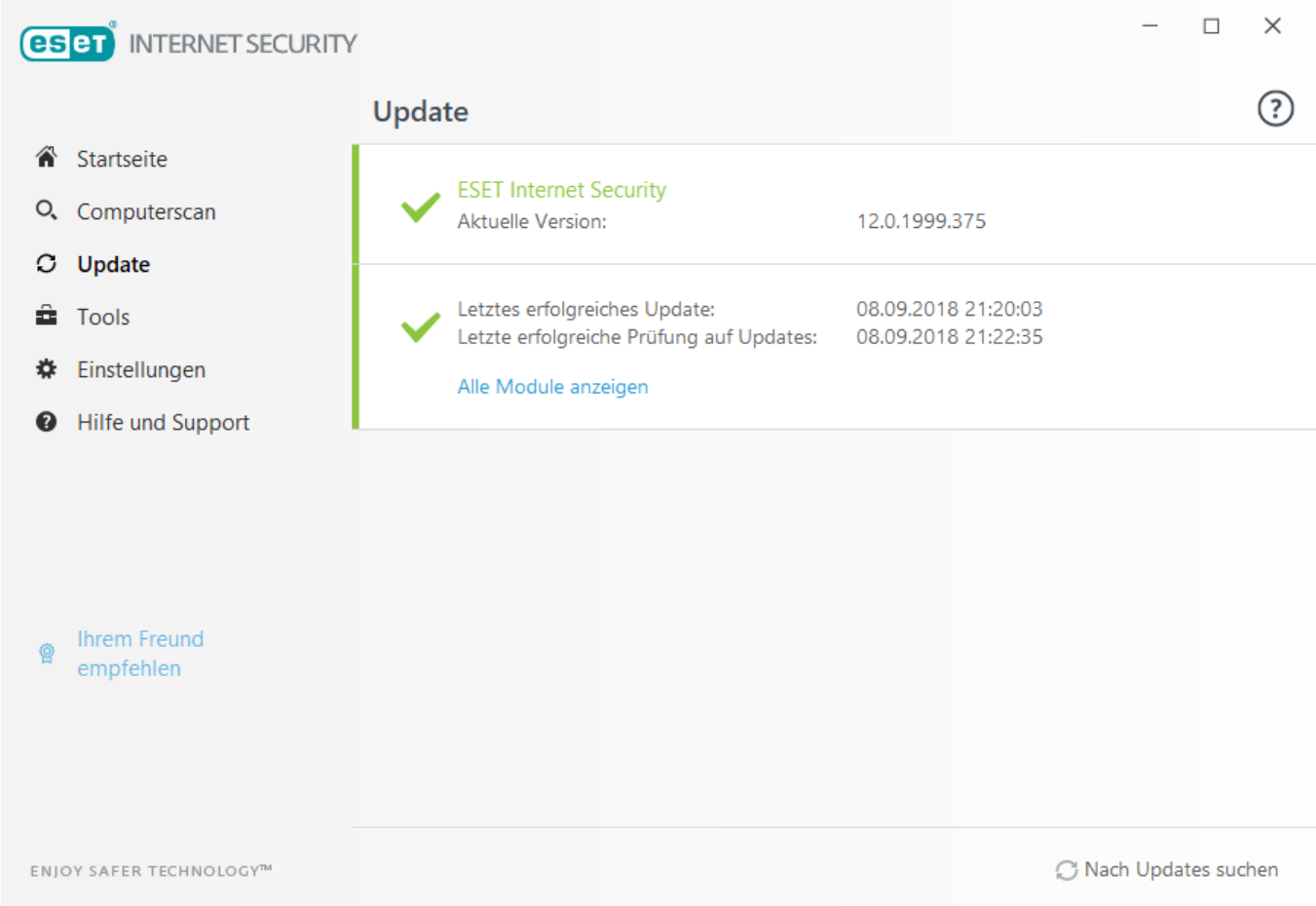
4.5 Aktualisieren des Programms

Den optimalen Schutz Ihres Computers gewährleisten Sie, indem Sie ESET Internet Security regelmäßig aktualisieren. Das Updatemodul hält Programmmodule und Systemkomponenten fortlaufend auf dem neuesten Stand.

Über den Punkt **Update** im Hauptprogrammfenster können Sie sich den aktuellen Update-Status anzeigen lassen. Sie sehen hier Datum und Uhrzeit des letzten Updates und können feststellen, ob ein Update erforderlich ist.

Zusätzlich zu automatischen Updates können Sie auf **Nach Updates suchen** klicken, um ein manuelles Update auszulösen. Regelmäßige Updates von Programmmodulen und Komponenten sind ein wichtiger Aspekt der Maßnahmen für einen möglichst umfassenden Schutz vor Schadcode. Seien Sie deshalb bei Konfiguration und Ausführung besonders sorgfältig. Aktivieren Sie Ihr Produkt mit Ihrem Lizenzschlüssel, um Updates zu erhalten. Falls Sie dies bei der Installation nicht erledigt haben, können Sie Ihr Produkt vor dem Update mit Ihrem Lizenzschlüssel aktivieren und auf die ESET-Update-Server zuzugreifen.

HINWEIS
Sie erhalten den Lizenzschlüssel per E-Mail von ESET nach dem Kauf von ESET Internet Security.



Aktuelle Version – Zeigt die Nummer der aktuell installierten Version an.

Letztes erfolgreiches Update – Zeigt das Datum des letzten erfolgreichen Updates an. Wenn das angezeigte Datum bereits einige Zeit zurückliegt, ist Ihr Produkt möglicherweise nicht auf dem neuesten Stand.

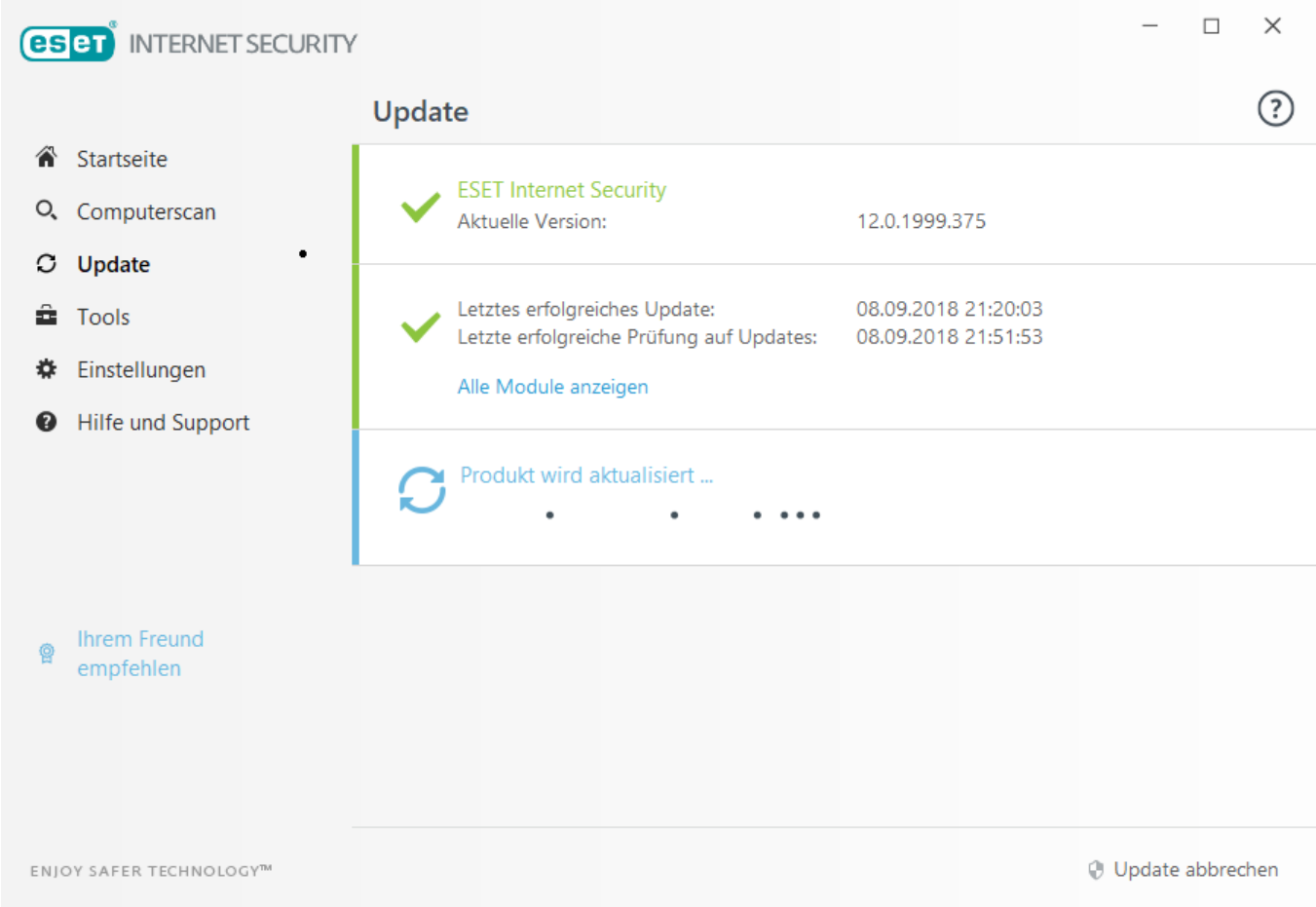
Letzte erfolgreiche Prüfung auf Updates – Zeigt das Datum der letzten erfolgreichen Prüfung auf Updates an.

Alle Module anzeigen – Zeigt Informationen zur Liste der installierten Programmmodule an.

Klicken Sie auf **Nach Updates suchen**, um die neueste verfügbare Version ESET Internet Security zu ermitteln.

Update-Vorgang

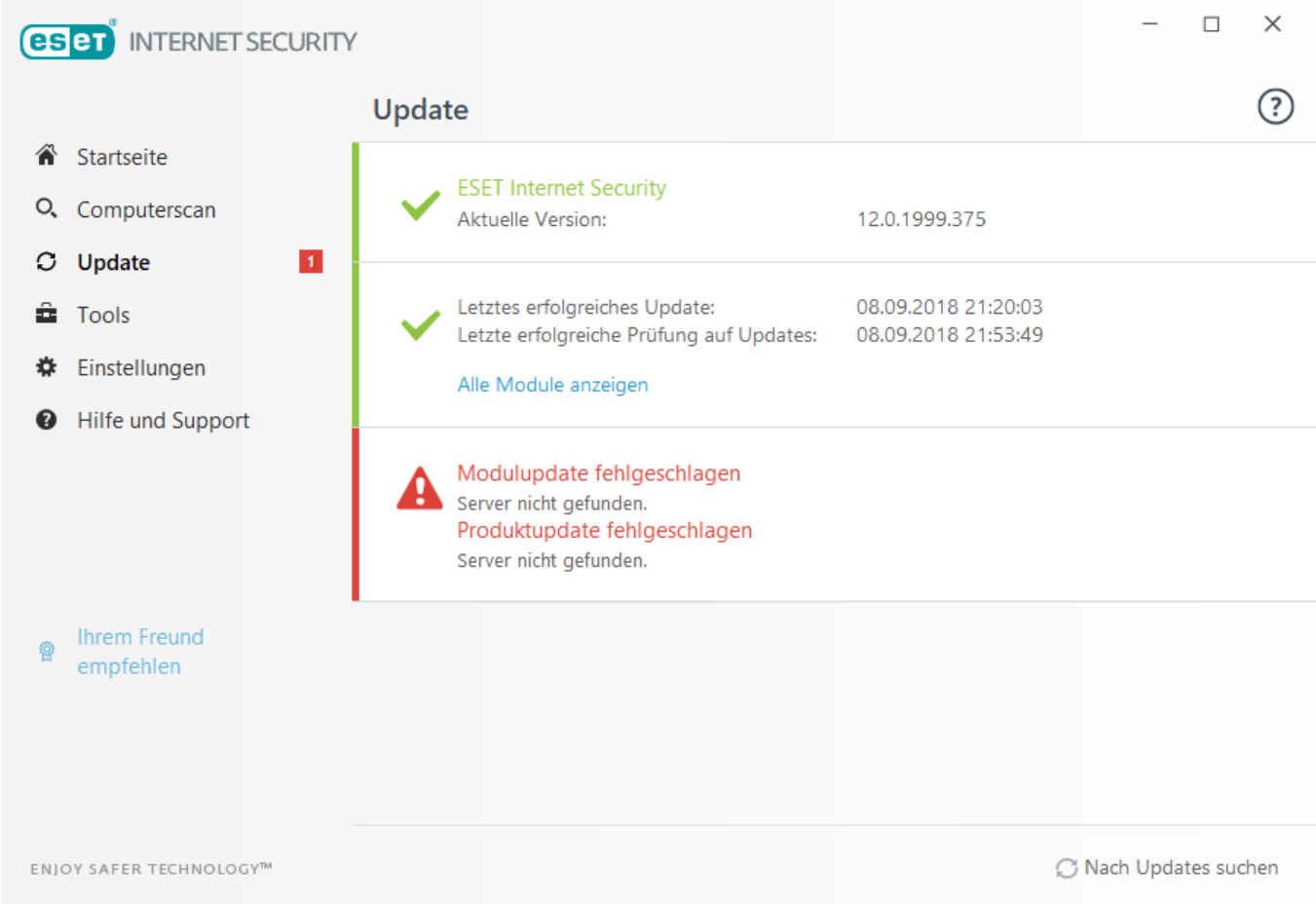
Klicken Sie auf **Nach Updates suchen**, um den Download zu starten. Eine Fortschrittsanzeige und die verbleibende Zeit wird angezeigt. Um den Update-Vorgang abzubrechen, klicken Sie auf **Update abbrechen**.



WICHTIG
Unter normalen Umständen weist ein grünes Häkchen im Fenster **Update** darauf hin, dass das Programm auf dem neuesten Stand ist. Andernfalls ist das Programm nicht auf dem neuesten Stand und anfälliger für Infektionen. Aktualisieren Sie die Module in diesem Fall so schnell wie möglich.

Falls ein Update fehlschlägt, ist möglicherweise eine der folgenden Ursachen verantwortlich:

1. **Ungültige Lizenz** – Der Lizenzschlüssel wurde falsch in den Update-Einstellungen eingegeben. Überprüfen Sie die richtige Eingabe der Lizenzdaten. Im Fenster „Erweiterte Einstellungen“ (klicken Sie im Hauptmenü auf **Einstellungen** und dann auf **Erweiterte Einstellungen**, oder drücken Sie **F5**) finden Sie zusätzliche Update-Optionen. Klicken Sie im Hauptmenü auf **Hilfe und Support** > **Lizenzen verwalten**, um einen neuen Lizenzschlüssel einzugeben.
2. **Fehler beim Herunterladen der Update-Dateien** - Ein Grund für den Fehler könnten falsche Einstellungen der Internetverbindung sein. Überprüfen Sie die Internetverbindung, z. B. indem Sie eine beliebige Internetseite im Webbrowser aufrufen. Wenn die Website nicht aufgerufen werden kann, besteht mit ziemlicher Sicherheit keine Internetverbindung. Falls dies der Fall ist, wenden Sie sich an Ihren Internetdienstanbieter.



WICHTIG
Starten Sie Ihren Computer nach einem erfolgreichen Update nach Möglichkeit neu, um sicherzustellen, dass alle Programmmodule korrekt aktualisiert wurden.

HINWEIS
Weitere Informationen finden Sie in diesem Artikel in der ESET-Knowledgebase.

4.5.1 Update-Einstellungen

Die Optionen für die Update-Einstellungen finden Sie im Fenster **Erweiterte Einstellungen** (F5) unter **Update** > **Einfach**. In diesem Bereich finden Sie Informationen zum Abruf von Updates, z. B. die Liste der Update-Server und die Anmeldedaten für diese Server.

Einfach

Das aktuell verwendete Updateprofil (sofern nicht unter **Erweiterte Einstellungen** > **Firewall** > **Bekannte Netzwerke** ein spezielles Profil festgelegt wurde) wird im Dropdownmenü **Standardprofil für Updates auswählen** angezeigt.

Automatischer Profilwechsel – Mit dieser Option können Sie das Profil für ein bestimmtes Netzwerk ändern.

Wenn beim Download der Updates für die Erkennungsroutine Fehler auftreten, klicken Sie auf **Löschen**, um temporäre Update-Dateien und Cache zu löschen.

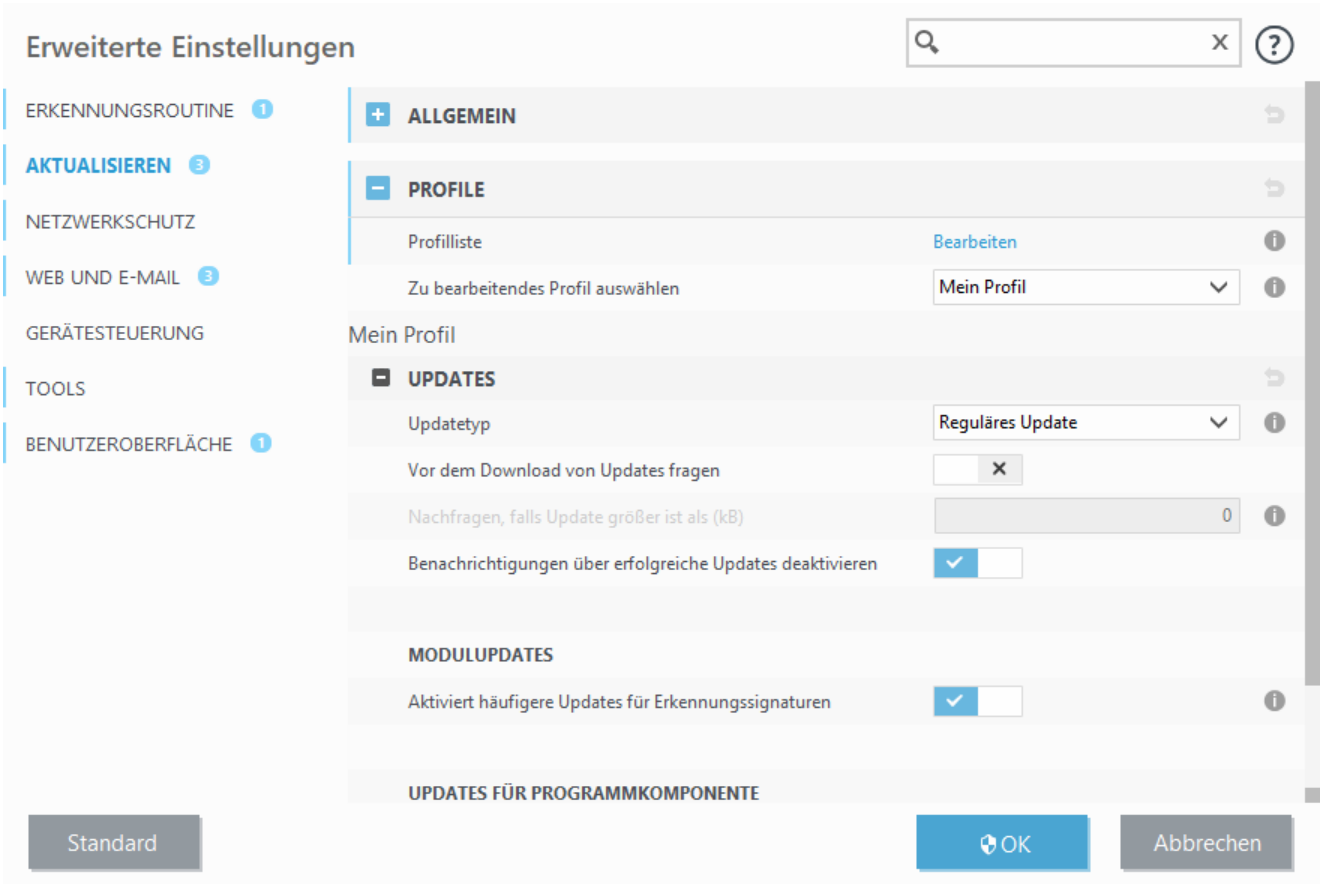
Modul-Rollback

Wenn Sie befürchten, dass ein neues Update der Erkennungsroutine oder eines Programmmoduls korrupt oder nicht stabil ist, können Sie einen Rollback zur vorigen Version ausführen und Updates für einen bestimmten Zeitraum deaktivieren. Hier können Sie auch zuvor für einen unbegrenzten Zeitraum deaktivierte Updates wieder aktivieren.

ESET Internet Security zeichnet Snapshots der Erkennungsroutine und der Programmmodule zur späteren Verwendung mit der *Rollback*-Funktion auf. Um Snapshots der Erkennungsroutine zu erstellen, lassen Sie das

Kontrollkästchen **Snapshots der Update-Dateien erstellen** aktiviert. Das Feld **Zahl der lokal gespeicherten Snapshots** legt fest, wie viele vorige Snapshots der Erkennungsroutine gespeichert werden.

Wenn Sie auf **Rollback ausführen** (**Erweiterte Einstellungen** (F5) > **Update** > **Einfach**) klicken, müssen Sie im Dropdownmenü einen Zeitraum auswählen, um festzulegen, wie lange die Updates der Erkennungsroutine und der Programmkomponenten ausgesetzt werden.



Damit Updates fehlerfrei heruntergeladen werden können, müssen Sie alle Update-Einstellungen ordnungsgemäß eingeben. Falls Sie eine Firewall verwenden, stellen Sie sicher, dass das ESET-Programm Verbindungen mit dem Internet herstellen darf (zum Beispiel HTTP-Verbindungen).

Profile

Update-Profile können für verschiedene Update-Konfigurationen und -Tasks erstellt werden. Besonders sinnvoll ist das Erstellen von Update-Profilen für mobile Benutzer, die auf regelmäßige Änderungen bei der Internetverbindung mit entsprechenden Profilen reagieren können.

Im Dropdownmenü **Zu bearbeitendes Profil auswählen** wird das aktuell ausgewählte Profil angezeigt. Standardmäßig ist hier **Mein Profil** ausgewählt. Um ein neues Profil zu erstellen, klicken Sie neben **Profilliste** auf **Bearbeiten**. Geben Sie den **Namen des Profils** ein und klicken Sie auf **Hinzufügen**.

Updates

Standardmäßig ist der **Update-Typ** auf **Reguläres Update** eingestellt. So werden Updates automatisch von dem ESET-Server heruntergeladen, der am wenigsten belastet ist. Der Testmodus (Option **Testmodus**) stellt Updates bereit, die intern umfangreich geprüft wurden und in absehbarer Zeit allgemein verfügbar sein werden. Wenn Sie den Testmodus aktivieren, können Sie früher von den neuesten Erkennungsmethoden und Fehlerkorrekturen profitieren. Da jedoch letzte Fehler nicht ausgeschlossen werden können, sind diese Updates ausdrücklich NICHT für Rechner im Produktivbetrieb vorgesehen, die durchgängig stabil und verfügbar laufen müssen.

Vor dem Download von Updates fragen – Das Programm zeigt eine Benachrichtigung an, und Sie können auswählen, ob Sie die Updatedateien herunterladen oder ablehnen möchten.

Nachfragen, falls Update größer ist als (kB) – Das Programm zeigt eine Benachrichtigung an, wenn die Größe der Updatedatei den angegebenen Wert überschreitet.

Benachrichtigungen über erfolgreiche Updates deaktivieren – Deaktiviert die Benachrichtigungen im Infobereich der Taskleiste rechts unten auf dem Bildschirm. Diese Option ist sinnvoll, wenn eine Anwendung im Vollbildmodus oder ein Spiel ausgeführt wird. Beachten Sie, dass die Anzeige von Meldungen im Gamer-Modus deaktiviert ist.

Modul-Updates

Aktiviert häufigere Updates für Erkennungssignaturen – Die Erkennungssignaturen werden in kürzeren Abständen aktualisiert. Das Deaktivieren dieser Einstellung kann die Erkennungsrate beeinträchtigen.

Updates für Programmkomponenten

Anwendungsupdate – Ein Bestätigungsdialog wird angezeigt, falls eine erneute Installation erforderlich ist.

4.5.1.1 Erweiterte Einstellungen für Updates

Zu den erweiterten Einstellungen für Updates zählen Konfigurationsoptionen für **Update-Modus** und **HTTP-Proxy**.

4.5.1.1.1 Update-Modus

Die Registerkarte **Update-Modus** enthält Optionen für regelmäßige Softwareupdates. Mit diesen Einstellungen können Sie festlegen, wie das Programm reagieren soll, wenn neue Erkennungsroutinen oder Updates für Programmkomponenten verfügbar sind.

Updates für Programmkomponenten enthalten neue Features oder Änderungen an vorhandenen Features und sind Teil der regelmäßigen Updates der Erkennungsroutine. Nach der Installation von Updates der Programmkomponenten muss der Computer möglicherweise neu gestartet werden.

Die folgenden Einstellungen stehen zur Verfügung:

Anwendungsupdate – Mit dieser Option werden sämtliche Updates von Programmkomponenten automatisch und unbeaufsichtigt ausgeführt, ohne das gesamte Produkt zu aktualisieren.

Manuelle Updates von Programmkomponenten aktivieren – Standardmäßig deaktiviert. Wenn diese Option aktiviert ist und eine neue Version von ESET Internet Security verfügbar ist, können Sie im Bereich **Update** nach Updates suchen und die neuere Version **installieren**.

Vor dem Download von Updates fragen – Mit dieser Option wird ein Hinweis angezeigt, und Sie müssen den Download verfügbarer Updates bestätigen, bevor diese installiert werden.

Fragen, falls Update größer ist als (KB) – Wenn das Update größer als der hier angegebene Wert ist, wird ein Hinweis angezeigt, und Sie müssen den Download verfügbarer Updates bestätigen, bevor diese installiert werden.

4.5.1.1.2 Verbindungsoptionen

Um die Proxyserver-Einstellungen für ein bestimmtes Updateprofil zu öffnen, klicken Sie auf **Update** unter **Erweiterte Einstellungen** (F5) und dann auf **Profile** > **Updates** > **Verbindungsoptionen**. Klicken Sie auf das Dropdownmenü **Proxy-Modus** und wählen Sie eine dieser drei Optionen:

- Keinen Proxyserver verwenden
- Verbindung über Proxyserver
- In Systemsteuerung eingestellten Proxy verwenden

Wählen Sie die Option **Globale Proxyeinstellungen verwenden** aus, um die unter „Erweiterte Einstellungen“ (**Tools** > **Proxyserver**) festgelegte Proxyserver-Konfiguration zu übernehmen.

Mit der Option **Keinen Proxyserver verwenden** legen Sie fest, dass kein Proxyserver für Updates von ESET Internet Security genutzt wird.

Wählen Sie die Option Verbindung über Proxyserver in den folgenden Fällen aus:

- Für Updates von ESET Internet Security wird ein anderer Proxyserver als der unter **Einstellungen** > **Proxyserver** konfigurierte Server verwendet. In dieser Konfiguration werden die Informationen für den neuen Proxy unter **Proxyserver**-Adresse, Kommunikations-**Port** (standardmäßig 3128) sowie bei Bedarf **Benutzername** und **Passwort** für den Proxyserver angegeben.
- Die Proxyserver-Einstellungen werden nicht global festgelegt, allerdings lädt ESET Internet Security Updates über einen Proxyserver herunter.
- Ihr Computer über einen Proxyserver mit dem Internet verbunden ist. Bei der Installation werden die Einstellungen aus Internet Explorer übernommen. Falls Sie später Änderungen vornehmen (wenn Sie z. B. den Internetanbieter wechseln), müssen Sie diese HTTP-Proxy-Einstellungen prüfen und ggf. anpassen. Andernfalls kann keine Verbindung zu den Update-Servern hergestellt werden.

Die Standardeinstellung für den Proxyserver ist **In Systemsteuerung eingestellten Proxy verwenden**.

Direktverbindung verwenden, wenn der Proxy nicht verfügbar ist – Der Proxy wird bei der Aktualisierung umgangen, wenn er nicht erreichbar ist.

HINWEIS
Die Felder **Benutzername** und **Passwort** in diesem Bereich gelten nur für den Proxyserver. Füllen Sie diese Felder nur aus, wenn für den Zugriff auf den Proxyserver ein Benutzername und ein Passwort benötigt werden. Tragen Sie in diese Felder nicht das Passwort und den Benutzernamen für ESET Internet Security ein. Füllen Sie diese Felder nur aus, wenn Sie für die Internetverbindung über den Proxyserver ein Passwort benötigen.

4.5.2 Update-Rollback

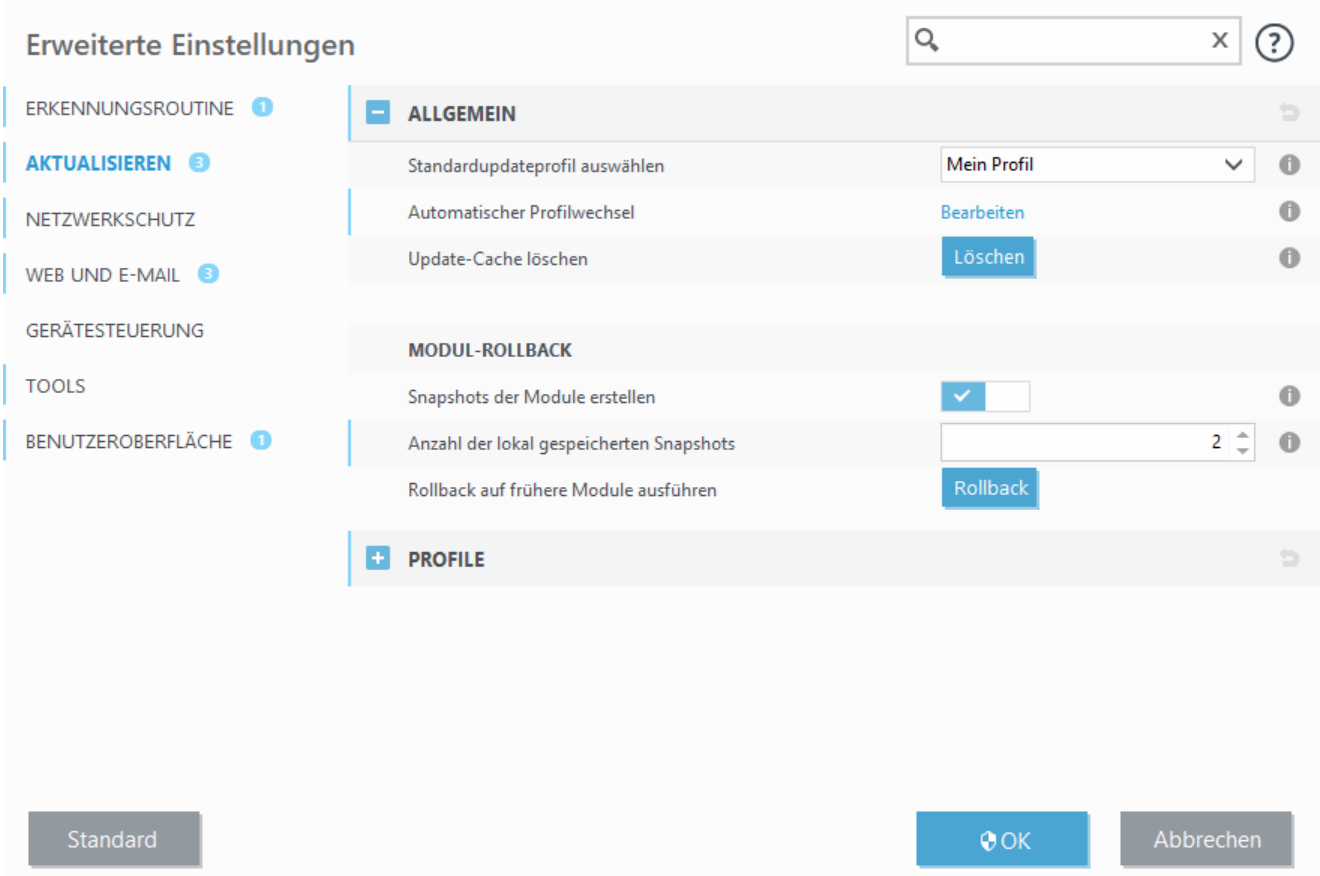
Wenn Sie befürchten, dass ein neues Update der Erkennungsroutine oder eines Programmmoduls beschädigt oder nicht stabil ist, können Sie einen Rollback zur vorigen Version ausführen und Updates für einen bestimmten Zeitraum deaktivieren. Hier können Sie auch zuvor für einen unbegrenzten Zeitraum deaktivierte Updates wieder aktivieren.

ESET Internet Security zeichnet Snapshots der Erkennungsroutine und der Programmmodule zur späteren Verwendung mit der *Rollback*-Funktion auf. Um Snapshots der Erkennungsroutine zu erstellen, lassen Sie das Kontrollkästchen **Snapshots der Update-Dateien erstellen** aktiviert. Das Feld **Zahl der lokal gespeicherten Snapshots** legt fest, wie viele vorige Snapshots der Erkennungsroutine gespeichert werden.

Wenn Sie auf **Rollback ausführen** (**Erweiterte Einstellungen** (F5) > **Update** > **Einfach**) klicken, müssen Sie im Dropdownmenü **Dauer** festlegen, wie lange die Updates der Erkennungsroutine und der Programmkomponenten ausgesetzt werden.

Wählen Sie **bis zum Widerrufen**, um keine regelmäßigen Updates auszuführen, bis die Update-Funktion manuell wieder aktiviert wird. Das Aktivieren dieser Option ist mit einem Sicherheitsrisiko verbunden und daher nicht empfehlenswert.

Wenn ein Rollback durchgeführt wird, wechselt die Schaltfläche **Rollback** zu **Updates erlauben**. Für die im Dropdown-Menü **Updates anhalten** angegebene Dauer werden keine Updates zugelassen. Die Version der Erkennungsroutine wird auf die älteste verfügbare Version herabgestuft und als Snapshot im lokalen Dateisystem des Computers gespeichert.



HINWEIS

Angenommen, die aktuellste Version der Erkennungsroutine ist 6871. Die Versionen 6870 und 6868 sind als Snapshots der Erkennungsroutine gespeichert. Die Version 6869 ist nicht verfügbar, weil der Computer beispielsweise eine Zeit lang heruntergefahren war und ein aktuelleres Update verfügbar war, bevor Version 6869 heruntergeladen wurde. Wenn Sie im Feld **Zahl der lokal gespeicherten Snapshots** den Wert 2 eingegeben haben und auf **Rollback** klicken, wird die Version 6868 der Erkennungsroutine (und Programmmodule) wiederhergestellt. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Überprüfen Sie, ob die Version der Erkennungsroutine im Hauptprogrammfenster von ESET Internet Security im Abschnitt Update herabgestuft wurde.

4.5.3 So erstellen Sie Update-Tasks

Updates können manuell ausgeführt werden. Klicken Sie dazu im Hauptmenü auf **Update**, und wählen Sie im daraufhin angezeigten Dialogfenster die Option **Nach Updates suchen** aus.

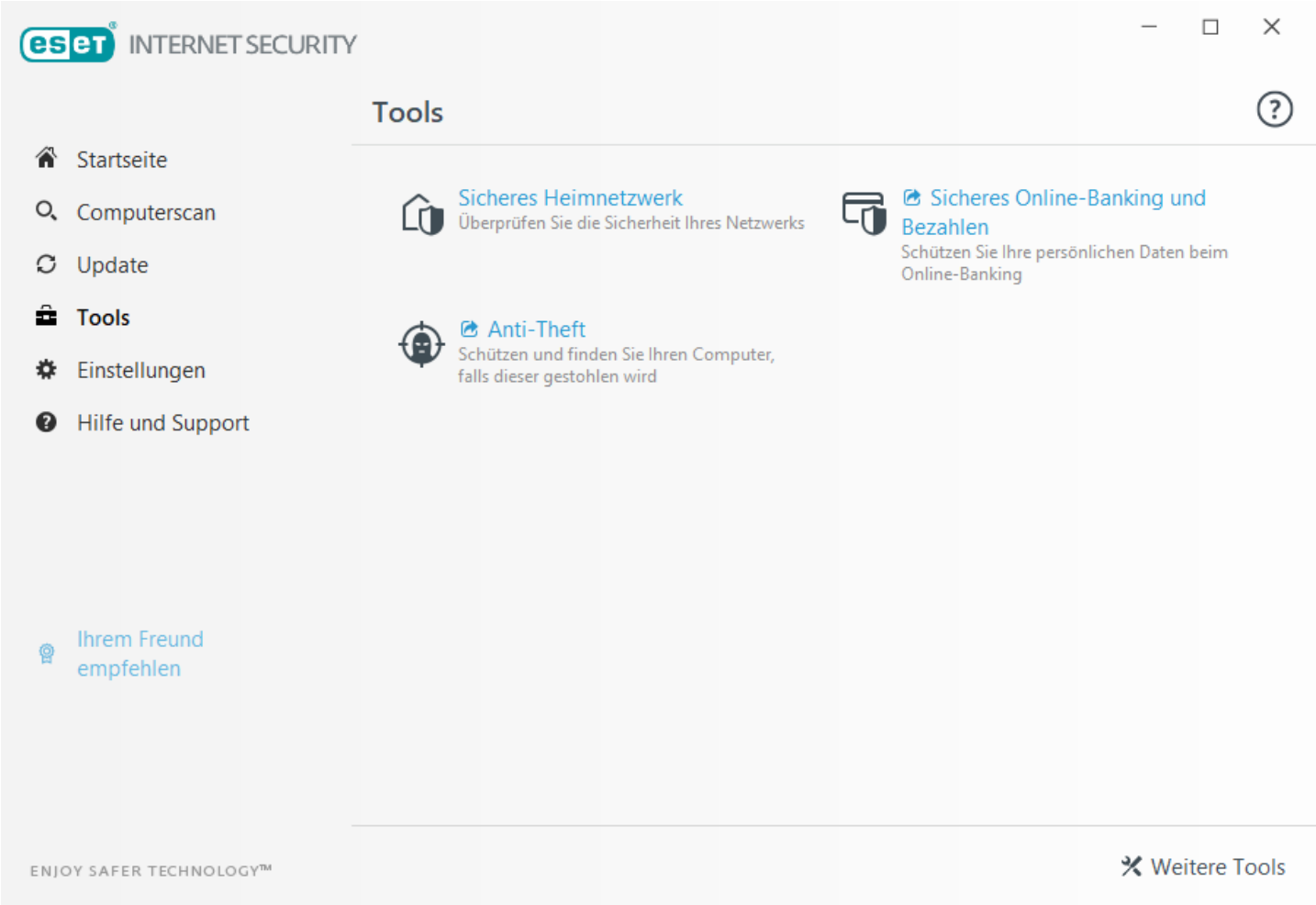
Darüber hinaus können Sie Updates auch als geplante Tasks einrichten. Um einen Task zu konfigurieren, klicken Sie auf **Tools** > **Taskplaner**. Standardmäßig sind in ESET Internet Security folgende Tasks aktiviert:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Herstellen von DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**

Jeder Update-Task kann bei Bedarf angepasst werden. Neben den standardmäßig ausgeführten Update-Tasks können zusätzliche Update-Tasks mit benutzerdefinierten Einstellungen erstellt werden. Weitere Informationen zum Erstellen und Konfigurieren von Update-Tasks finden Sie im Abschnitt Taskplaner.

4.6 Tools

Das Menü **Tools** enthält Module, die die Verwaltung des Programms vereinfachen und zusätzliche Optionen für erfahrene Benutzer bereitstellen.



Sicheres Heimnetzwerk – Schützt Sie vor Sicherheitsproblemen, wenn Sie mit einem Netzwerk verbunden sind. Weitere Informationen erhalten Sie hier.

Online-Banking-Zahlungsschutz – ESET Internet Security schützt Ihre Kreditkartennummern und andere persönliche Daten beim Onlinebanking und auf Bezahlungswebsites. Sie können Ihre Banktransaktionen gesichert in einem Spezialbrowser durchführen. Weitere Informationen finden Sie in diesem Artikel in der ESET-Knowledgebase.

Klicken Sie auf Weitere Tools, um weitere Tools zum Schutz Ihres Computers anzuzeigen.

4.6.1 Sicheres Heimnetzwerk

Das **sichere Heimnetzwerk** identifiziert Schwachstellen wie offene Ports oder ein unsicheres Routerpasswort in Ihrem Heimnetzwerk. Dieses Feature umfasst eine Liste der verbundenen Geräte kategorisiert nach Gerätetyp (Drucker, Router, Mobilgerät usw.), damit Sie jederzeit überprüfen können, wer mit Ihrem Heimnetzwerk verbunden ist. Diese Funktion nimmt keine Änderungen an der Konfiguration Ihres Routers vor. Sie müssen die Änderungen in der Benutzeroberfläche Ihres Routers selbst durchführen. Privatrouter sind besonders anfällig für Schadsoftware, die für Distributed-Denial-of-Service (DDoS)-Angriffe eingesetzt wird. Wenn Sie das standardmäßige Routerpasswort nicht geändert haben, können sich Hacker bei Ihrem Router anmelden und dessen Konfiguration ändern oder Ihr Netzwerk angreifen.

WARNUNG

Wir empfehlen dringend die Verwendung eines sicheren Passworts, das lang genug ist und Zahlen, Sonderzeichen oder Großbuchstaben enthält. Verwenden Sie eine Mischung aus verschiedenen Zeichentypen, um Angreifern das Leben zu erschweren.

Alle mit Ihrem Netzwerk verbundenen Geräte werden in der Sonar-Ansicht angezeigt. Bewegen Sie den Mauszeiger über ein Gerätesymbol, um grundlegende Informationen wie Netzwerkname und letztes Erkennungsdatum anzuzeigen. Klicken Sie auf das Gerätesymbol, um ausführliche Informationen über das Gerät anzuzeigen.

Klicken Sie auf  , um Informationen über alle verbundenen Geräte in der Listenansicht anzuzeigen. Die Listenansicht enthält dieselben Daten wie die Sonar-Ansicht, jedoch in einem Listenformat. Mit dem Dropdownmenü können Sie die Geräte anhand der folgenden Kriterien filtern:

- Nur Geräte, die mit dem aktuellen Netzwerk verbunden sind
- Geräte ohne Kategorie
- Geräte, die mit einem beliebigen Netzwerk verbunden sind

Das Modul „Sicheres Heimnetzwerk“ zeigt zwei Arten von Benachrichtigungen an:

Neues Netzwerkgerät ist mit dem Netzwerk verbunden – Wird angezeigt, wenn sich ein bisher unbekanntes Gerät mit dem Netzwerk verbindet, während der Benutzer verbunden ist.
Neue Netzwerkgeräte gefunden – Wird angezeigt, wenn Sie sich mit Ihrem Heimnetzwerk verbinden und ein bisher unbekanntes Gerät vorhanden ist.

HINWEIS
Beide Benachrichtigungen weisen Sie darauf hin, dass ein nicht autorisiertes Gerät versucht, sich mit Ihrem Netzwerk zu verbinden.

HINWEIS
Neu verbundene Geräte werden näher am Router angezeigt, um die Sichtbarkeit zu verbessern.

Mit der **Sicheres Heimnetzwerk** können Sie Schwachstellen in Ihrem Router identifizieren und Ihren Schutz in fremden Netzwerken verbessern.

Klicken Sie auf **Netzwerk prüfen**, um eine manuelle Überprüfung des Netzwerks durchzuführen, mit dem Sie momentan verbunden sind.

Sie haben die folgenden Prüfoptionen zur Auswahl:

- Alles prüfen
- Nur Router prüfen
- Nur Geräte prüfen

WARNUNG
Führen Sie Netzwerküberprüfungen nur in Ihrem Heimnetzwerk durch! Machen Sie sich die Gefahren bewusst, wenn Sie diese Überprüfung in fremden Netzwerken durchführen.

Nach Abschluss der Prüfung wird eine Benachrichtigung mit einem Link zu grundlegenden Informationen über das Gerät angezeigt. Alternativ können Sie auf das verdächtige Gerät in der Listen- oder Sonaransicht doppelklicken. Klicken Sie auf **Fehlerbehebung**, um kürzlich gesperrte Kommunikationen anzuzeigen.

HINWEIS
Weitere Informationen zur Fehlerbehebung für die Firewall finden Sie hier.

4.6.1.1 Netzwerkgerät

Hier finden Sie ausführliche Informationen zum Gerät, inklusive der folgenden Daten:

- Gerätename
- Gerätetyp
- Zuletzt gesehen
- Netzwerkname
- IP-Adresse
- MAC-Adresse

Das Stiftsymbol gibt an, dass Sie den Gerätenamen oder den Gerätetyp bearbeiten können.

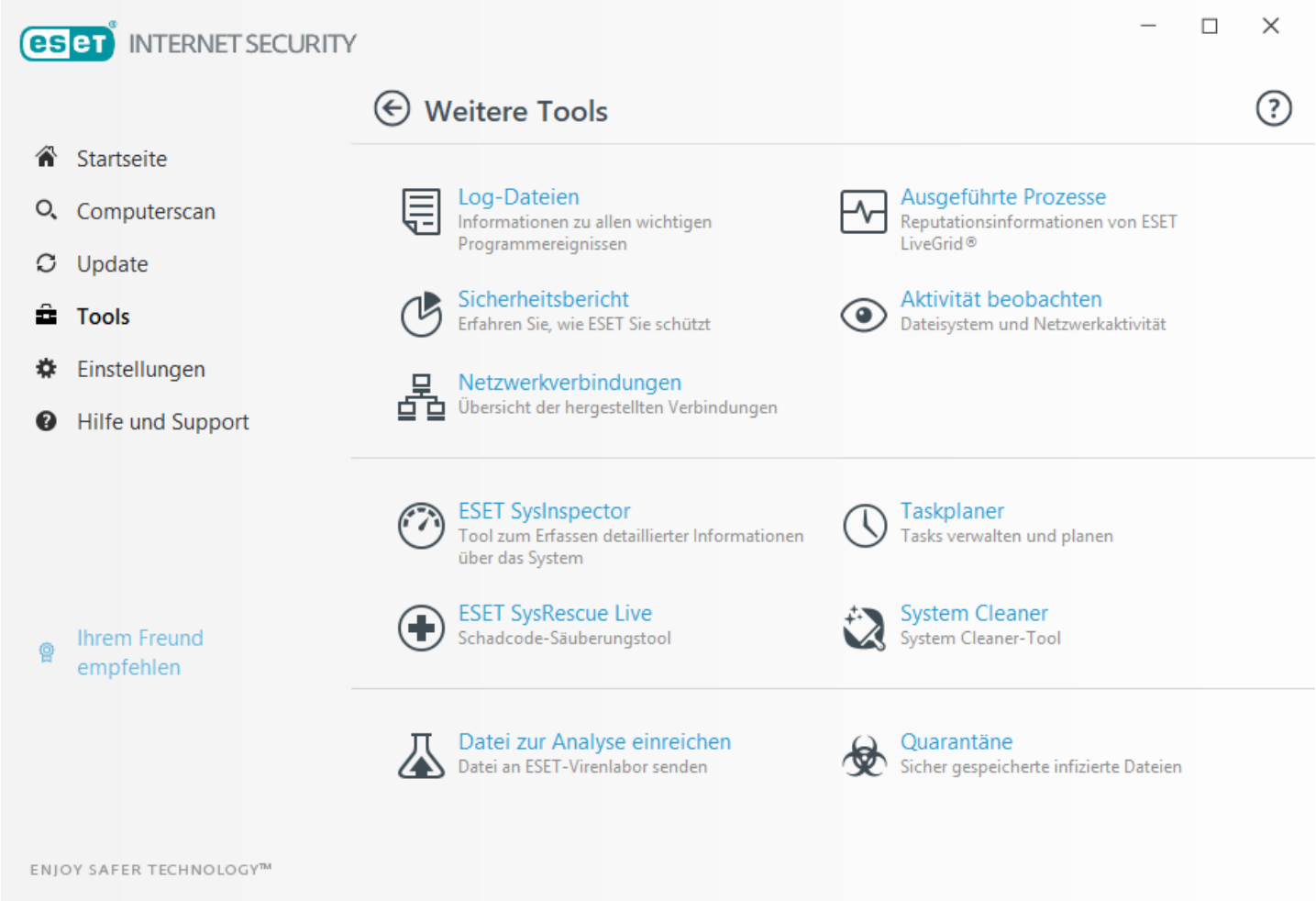
Gerät entfernen – Sie können ein zuvor verbundenes Gerät aus Ihrem Netzwerk entfernen, falls es nicht mehr vorhanden ist.

4.6.2 Webcam-Schutz

Webcam-Schutz – Zeigt Prozesse und Anwendungen an, die auf die Webcam Ihres Computers zugreifen. Ein Benachrichtigungsfenster wird angezeigt, wenn eine unerwünschte Anwendung versucht, auf Ihre Kamera zuzugreifen. Sie können den Zugriff einzelner Prozesse oder Anwendungen auf die Kamera **erlauben** oder **blockieren**.

4.6.3 Tools in ESET Internet Security

Am **Weitere Tools** enthält Module zur einfacheren Verwaltung des Programms und zusätzliche Optionen für fortgeschrittene Benutzer.



Dieser Bereich enthält die folgenden Elemente:

 Log-Dateien

 Sicherheitsbericht

 Aktivität beobachten

 Ausgeführte Prozesse (wenn ESET LiveGrid® in ESET Internet Security aktiviert ist)

 Netzwerkverbindungen (wenn Firewall in ESET Internet Security aktiviert ist)

 ESET SysInspector

 ESET SysRescue Live – Leitet Sie zur ESET SysRescue Live-Seite weiter, auf der Sie das Live-Abbild von ESET SysRescue oder den „Live CD/USB Creator“ für Microsoft Windows-Betriebssysteme herunterladen können.

 Taskplaner

 System Cleaner – Ein Tool, mit dem Sie den Computer nach der Säuberung der Bedrohung auf einen nutzbaren Zustand wiederherstellen können.

 Datei zur Analyse einreichen - Ermöglicht Ihnen, eine verdächtige Datei zur Analyse bei ESET einzureichen. Das Dialogfenster, das nach dem Klicken auf diese Option angezeigt wird, wird in diesem Abschnitt beschrieben.

 Quarantäne

HINWEIS
ESET SysRescue ist in älteren Versionen von ESET-Produkten möglicherweise nicht für Windows 8 verfügbar. In diesem Fall sollten Sie ein Produkt-Upgrade durchführen oder einen ESET SysRescue-Datenträger unter einer anderen Version von Microsoft Windows erstellen.

4.6.3.1 Log-Dateien

Die Log-Dateien enthalten Informationen zu wichtigen aufgetretenen Programmereignissen und bieten einen Überblick über erkannte Bedrohungen. Das Erstellen von Logs ist unabdingbar für die Systemanalyse, die Erkennung von Bedrohungen sowie die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Welche Informationen aufgezeichnet werden, ist abhängig von den aktuellen Einstellungen für die Mindestinformation in Logs. Textnachrichten und Logs können direkt aus ESET Internet Security heraus angezeigt werden. Das Archivieren von Logs erfolgt ebenfalls direkt über das Programm.

Sie können die Log-Dateien abrufen, indem Sie im Hauptprogrammfenster auf **Tools** > > **Weitere Tools** > > **Log-Dateien** klicken. Wählen Sie im Dropdown-Menü **Log** den gewünschten Log-Typ aus. Folgende Logs sind verfügbar:

- **Erkannte Bedrohungen** – Das Bedrohungs-Log enthält detaillierte Informationen über eingedrungene Schadsoftware, die von ESET Internet Security entdeckt wurde. Zu den Informationen gehören die Zeit der Erkennung, der Name der eingedrungenen Schadsoftware, deren Ort, die ausgeführte Aktion und der Name des Benutzers, der zur Zeit der Entdeckung der Schadsoftware angemeldet war. Doppelklicken Sie auf einen Log-Eintrag, um die Details in einem eigenen Fenster anzuzeigen.
- **Ereignisse** – Alle von ESET Internet Security ausgeführten wichtigen Aktionen werden im Ereignis-Log aufgezeichnet. Das Ereignis-Log enthält Informationen über Ereignisse und im Programm aufgetretene Fehler. Es unterstützt Systemadministratoren und Benutzer bei der Fehlerbehebung. Die hier aufgeführten Informationen sind oftmals hilfreich, um ein im Programm aufgetretenes Problem zu beheben.
- **Computerprüfung** - In diesem Fenster werden die Ergebnisse aller manuell durchgeführten oder geplanten Prüfungen angezeigt. Jede Zeile entspricht der Überprüfung eines einzelnen Computers. Durch Doppelklicken auf einen Eintrag können Sie Einzelheiten zu der entsprechenden Prüfung anzeigen.

- **HIPS** – Enthält Einträge spezifischer HIPS-Regeln, die zum Aufzeichnen markiert wurden. Das Protokoll zeigt die Anwendung an, die den Vorgang ausgelöst hat, das Ergebnis (ob der Vorgang zugelassen oder blockiert wurde) sowie den Regelnamen.
- **Netzwerk-Schutz** – Das Netzwerk-Schutz-Log zeigt alle von der Firewall entdeckten Angriffe von anderen Computern an. Hier finden Sie Informationen über alle Angriffe auf Ihren Computer. In der Spalte *Ereignis* werden die entdeckten Angriffe angezeigt. Unter *Quelle* erfahren Sie mehr über den Angreifer. Die Spalte *Protokoll* zeigt das für den Angriff verwendete Datenübertragungsprotokoll an. Analysieren Sie das Netzwerk-Schutz-Log, um Eindringversuche von Schadsoftware rechtzeitig zu erkennen und den unerlaubten Zugriff auf Ihr System zu verhindern.
- **Gefilterte Websites** - Diese Liste enthält die durch den Web-Schutz oder die Kindersicherung gesperrten Websites. Jedes Log enthält die Uhrzeit, die URL-Adresse, den Benutzer und die Anwendung, die sich mit einer bestimmten Website verbunden hat.
- **Spam-Schutz** – Enthält Einträge zu E-Mails, die als Spam eingestuft wurden.
- **Kindersicherung** – Zeigt die Webseiten an, die über die Kindersicherung zugelassen bzw. gesperrt wurden. Die Spalten *Übereinstimmungstyp* und *Übereinstimmungswerte* geben an, wie die Filterregeln angewendet wurden.
- **Medienkontrolle** – Enthält Datensätze zu Wechselmedien oder externen Geräten, die an den Computer angeschlossen wurden. Nur Geräte mit einer entsprechenden Regel für die Medienkontrolle werden in die Log-Datei aufgenommen. Wenn auf ein angeschlossenes Gerät keine Regel zutrifft, wird für das Gerät kein Log-Eintrag erstellt. Außerdem können Sie Details wie Gerätetyp, Seriennummer, Herstellername und Mediengröße (je nach Verfügbarkeit der Informationen) anzeigen.
- **Webcam-Schutz** – Enthält Einträge zu Anwendungen, die vom Webcam-Schutz blockiert wurden.

Wählen Sie den Inhalt eines Logs aus und drücken Sie **Strg + C**, um die Daten in die Zwischenablage zu kopieren. Halten Sie **Strg** und **Umschalt** gedrückt, um mehrere Einträge auszuwählen.

Klicken Sie auf **Filter**, um das Fenster **Log-Filter** zu öffnen, in dem Sie Filterkriterien definieren können.

Klicken Sie mit der rechten Maustaste auf einen Eintrag, um das Kontextmenü zu öffnen. Im Kontextmenü stehen folgende Optionen zur Verfügung:

- **Anzeigen** – Zeigt weitere detaillierte Informationen zum ausgewählten Log in einem neuen Fenster an.
- **Gleiche Datensätze filtern** – Wenn Sie diesen Filter aktivieren, werden nur Einträge desselben Typs angezeigt (Diagnose, Warnungen, ...).
- **Filter/Suchen** – Wenn Sie diese Option anklicken, können Sie im Fenster Log durchsuchen Filterkriterien zu bestimmten Log-Einträgen festlegen.
- **Filter aktivieren** – Aktiviert die Filtereinstellungen.
- **Filter deaktivieren** – Setzt alle Filtereinstellungen (wie oben beschrieben) zurück.
- **Kopieren/Alles kopieren** – Kopiert die Informationen zu allen im Fenster angezeigten Einträgen.
- **Löschen/Alle löschen** – Löscht die ausgewählten oder alle angezeigten Einträge; für diese Option sind Administratorrechte erforderlich.
- **Exportieren...** - Exportiert Informationen zu den Einträgen im XML-Format.
- **Alle exportieren...** - Exportiert Informationen zu allen Einträgen im XML-Format.
- **Bildlauf für Log** – Wenn diese Option aktiv ist, wandern alte Logs automatisch aus der Anzeige, sodass im Fenster **Log-Dateien** die neuesten Einträge sichtbar sind.

4.6.3.1.1 Log-Dateien

Die Log-Konfiguration für ESET Internet Security können Sie aus dem Hauptprogrammfenster aufrufen. Klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen** > **Tools** > **Log-Dateien**. In diesem Bereich können Sie Einstellungen für Logs festlegen. Um den Speicherbedarf zu reduzieren, werden ältere Logs automatisch gelöscht. Für Log-Dateien können die folgenden Einstellungen vorgenommen werden:

Mindestinformation in Logs - Hier können Sie festlegen, welche Ereignistypen in Logs aufgezeichnet werden sollen.

- **Diagnose** – Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.
- **Informationen** - Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen** - Kritische Fehler und Warnungen werden protokolliert.
- **Fehler** – Fehler wie *Fehler beim Herunterladen der Datei* und kritische Fehler werden aufgezeichnet.
- **Kritische Warnungen** – Nur kritische Warnungen (z. B. bei einem Fehler beim Start des Virenschutz-Moduls,, Firewallusw.) werden protokolliert.

Log-Einträge, die älter sind als die unter **Einträge automatisch löschen nach (Tage)** angegebene Anzahl an Tagen werden automatisch gelöscht.

Log-Dateien automatisch optimieren - Ist diese Option aktiviert, werden die Log-Dateien automatisch defragmentiert, wenn die Prozentzahl höher ist als der unter **Wenn ungenutzte Einträge größer als (%)** angegebene Wert.

Klicken Sie zum Defragmentieren der Log-Dateien auf **Optimieren**. Um die Systemleistung und -geschwindigkeit beim Verarbeiten der Log-Dateien zu erhöhen, werden alle leeren Log-Einträge entfernt. Eine starke Verbesserung ist insbesondere dann erkennbar, wenn die Logs eine große Anzahl an Einträgen enthalten.

Mit der Option Textprotokoll aktivieren wird die Speicherung von Logs in einem anderen, von Log-Dateien getrennten Format aktiviert:

- **Zielverzeichnis** – Das Verzeichnis, in dem Log-Dateien gespeichert werden (nur für Text/CSV). Jeder Log-Bereich verfügt über eine eigene Datei mit einem vordefinierten Dateinamen (z. B. *virlog.txt* für den Bereich **Erkannte Bedrohungen** von Log-Dateien, wenn Logs im Nur-Text-Format gespeichert werden).

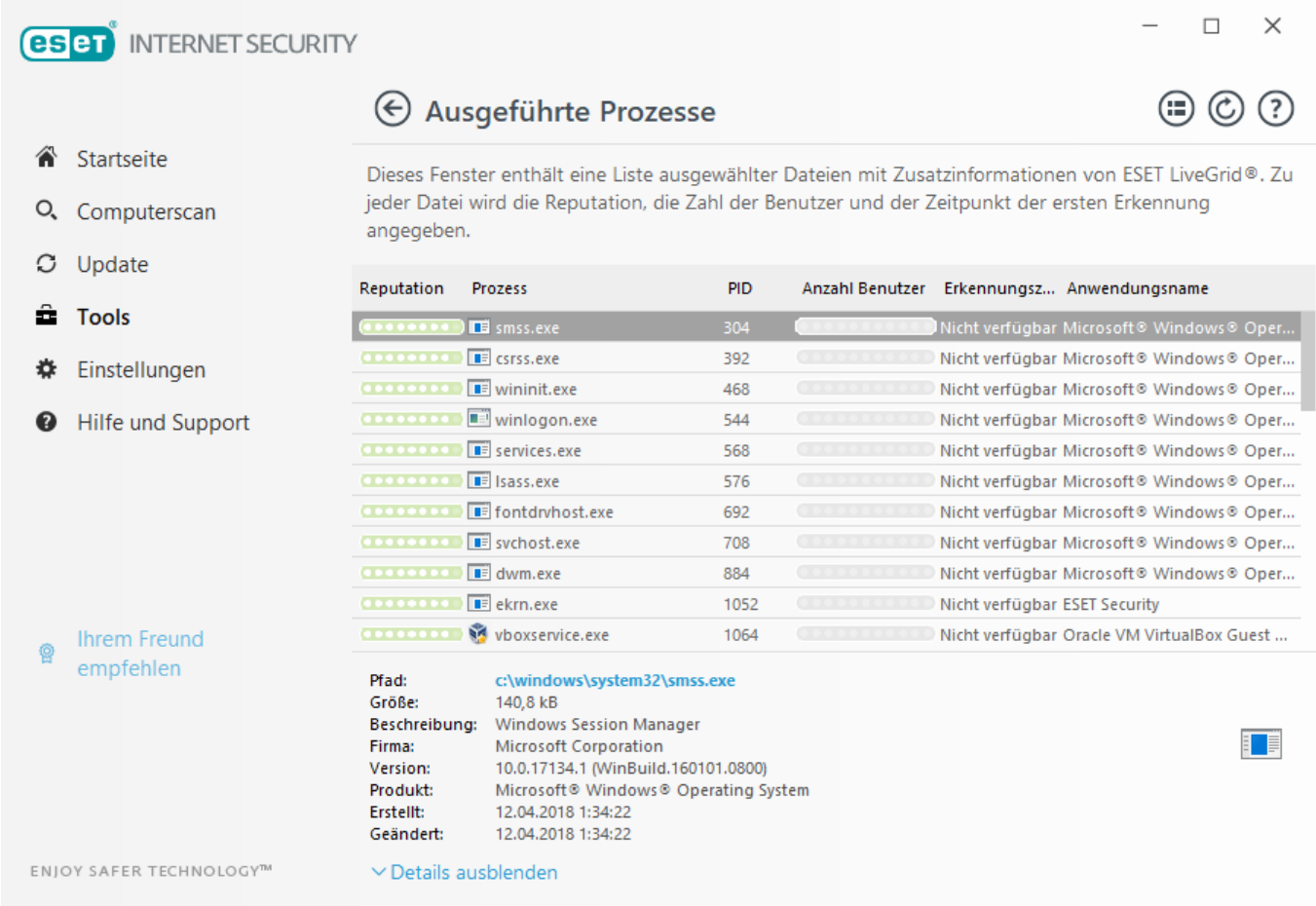
- **Typ** – Mit dem Dateiformat **Text** werden Logs in einer Textdatei gespeichert, wobei die Daten durch Tabulatorzeichen getrennt werden. Gleiches gilt für das kommagetrennte Dateiformat **CSV**. Mit der Option **Ereignis** werden die Logs im Windows-Ereignis-Log anstatt in einer Datei gespeichert (dieses kann in der Ereignisanzeige in der Systemsteuerung eingesehen werden).

Mit der Option **Alle Log-Dateien löschen** werden alle aktuell im Dropdownmenü **Typ** ausgewählten Logs gelöscht. Eine Benachrichtigung über das erfolgreiche Löschen der Logs wird angezeigt.

HINWEIS
Zum Zwecke der schnellen Problemlösung werden Sie von ESET möglicherweise gebeten, Logs von Ihrem Computer bereitzustellen. Mit dem ESET Log Collector können Sie die benötigten Informationen ganz einfach sammeln. Weitere Informationen zum ESET Log Collector finden Sie in diesem Artikel in der ESET Knowledgebase.

4.6.3.2 Ausgeführte Prozesse

Die Informationen zu ausgeführten Prozessen zeigen die auf dem Computer ausgeführten Programme und Prozesse an und stellen dem ESET-Produkt laufend aktuelle Informationen zu neuen Infiltrationen bereit. ESET Internet Security bietet ausführliche Informationen zu ausgeführten Prozessen, um den Benutzern den Schutz der ESET LiveGrid®-Technologie zu bieten.



Prozess – Zeigt den Namen des Programms oder Prozesses an, das/der derzeit auf dem Computer ausgeführt wird. Sie können alle auf Ihrem Computer ausgeführten Prozesse auch über den Windows-Taskmanager anzeigen. Öffnen Sie den Taskmanager, indem Sie mit der rechten Maustaste auf einen leeren Bereich in der Taskleiste und dann auf **Taskmanager** klicken, oder indem Sie **Strg**+**Umschalt**+**Esc** auf Ihrer Tastatur drücken.

Risikostufe – Um Objekten wie Dateien, Prozessen, Registrierungsschlüsseln usw. eine Risikostufe zuzuordnen, verwenden ESET Internet Security und die ThreatSense-Technologie in der Regel einen Satz heuristischer Regeln, mit denen die Merkmale des Objekts untersucht werden, um anschließend nach entsprechender Gewichtung das Potenzial für schädliche Aktivitäten abzuschätzen. Auf der Grundlage dieser Heuristik wird den Objekten so eine Risikostufe von 1 – In Ordnung (grün) bis 9 – Risikoreich (rot) zugeordnet.

HINWEIS
Bekannte Anwendungen, die als In Ordnung (grün) markiert sind und bekanntermaßen keinen Schadcode enthalten (Positivliste), werden von der Prüfung ausgeschlossen, um die Prüfung zu beschleunigen.

PID – Die Prozesskennung kann als Parameter in verschiedenen Funktionsaufrufen verwendet werden, z. B. um die Priorität des Prozesses anzupassen.

Anzahl Benutzer – Die Anzahl der Benutzer, die eine bestimmte Anwendung verwenden. Diese Informationen werden von der ThreatSense-Technologie gesammelt.

Erkennungszeitpunkt – Zeitspanne seit der Erkennung der Anwendung durch die ThreatSense-Technologie.

HINWEIS

Eine als Unbekannt (gelb) eingestufte Anwendung enthält nicht unbedingt Schadcode. In der Regel ist es einfach eine neuere Anwendung. Wenn Sie sich bei einer Datei unsicher sind, können Sie diese über die Funktion Dateien zur Analyse einreichen an das ESET-Virenlabor schicken. Falls die Datei tatsächlich Schadcode enthält, wird die Erkennung der entsprechenden Signatur in einem zukünftigen Update hinzugefügt.

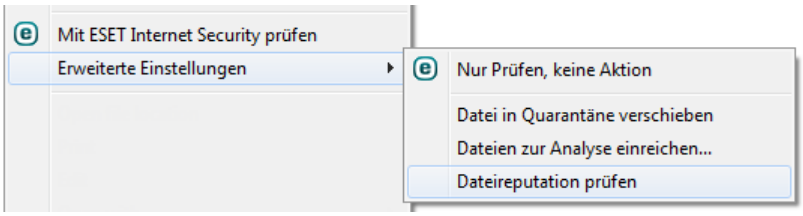
Anwendungsname – Der Name eines Programms oder Prozesses.

In neuem Fenster anzeigen – Die Informationen zu den ausgeführten Prozessen werden in einem neuen Fenster angezeigt.

Klicken Sie auf eine Anwendung, um die folgenden Details zu dieser Anwendung anzuzeigen:

- **Pfad** – Speicherort einer Anwendung auf Ihrem Computer.
- **Größe** – Dateigröße in B (Byte).
- **Beschreibung** – Dateieigenschaften auf Basis der Beschreibung des Betriebssystems.
- **Firma** – Name des Herstellers oder des Anwendungsprozesses.
- **Version** – Information vom Herausgeber der Anwendung.
- **Produkt** – Name der Anwendung und/oder Firmenname.
- **Erstellt/Geändert** – Datum und Uhrzeit der Erstellung bzw. der letzten Änderung.

HINWEIS
Sie können auch die Reputation von Dateien überprüfen, die nicht als Programme oder Prozesse ausgeführt werden. Klicken Sie dazu eine Datei mit der rechten Maustaste an, und wählen Sie **Erweiterte Einstellungen** > **Dateireputation prüfen** aus.



4.6.3.3 Sicherheitsbericht

Diese Funktion enthält eine Übersicht über die Statistiken für die folgenden Kategorien:

Blockierte Webseiten – Die Anzahl der blockierten Webseiten (URL in Negativliste für eventuell unerwünschte Anwendung, Phishing, gehackter Router, IP oder Zertifikat).
Infizierte E-Mail-Objekte erkannt – Die Anzahl der erkannten infizierten E-Mail-Objekte.
Blockierte Webseiten in der Kindersicherung – Die Anzahl der blockierten Webseiten in der Kindersicherung.
Eventuell unerwünschte Anwendung erkannt – Die Anzahl der eventuell unerwünschten Anwendungen.
Spam-E-Mails erkannt – Die Anzahl der erkannten Spam-E-Mails.
Zugriff auf Webcam blockiert – Die Anzahl der blockierten Zugriffe auf die Webcam.
Zugriff auf Internetbanking geschützt – Die Anzahl der geschützten Zugriffe auf Internetbanking-Webseiten.
Überprüfte Dokumente – Die Anzahl der gescannten Dokumentobjekte.
Überprüfte Apps – Die Anzahl der gescannten ausführbaren Objekte.
Überprüfte sonstige Objekte – Die Anzahl der sonstigen gescannten Objekte.
Überprüfte Webseitenobjekte – Die Anzahl der gescannten Webseitenobjekte.
Überprüfte E-Mail-Objekte – Die Anzahl der gescannten E-Mail-Objekte.

Diese Kategorien werden vom höchsten zum niedrigsten numerischen Wert geordnet. Kategorien mit Nullwert werden nicht angezeigt. Klicken Sie auf „Mehr anzeigen“, um ausgeblendete Kategorien zu erweitern und anzuzeigen.

Unter den Kategorien wird die aktuelle Virenlage mit einer Weltkarte angezeigt. Das Vorhandensein von Viren in einzelnen Ländern wird farblich markiert (dunklere Farben bedeuten höhere Zahlen). Länder ohne Daten sind ausgegraut. Bewegen Sie die Maus über ein Land, um Daten für das jeweilige Land anzuzeigen. Wählen Sie einen Kontinent aus, um automatisch zu zoomen.

Im letzten Teil des Sicherheitsberichts können Sie die folgenden Funktionen aktivieren:

- Password Manager
- Sichere Daten
- Kindersicherung
- Anti-Theft

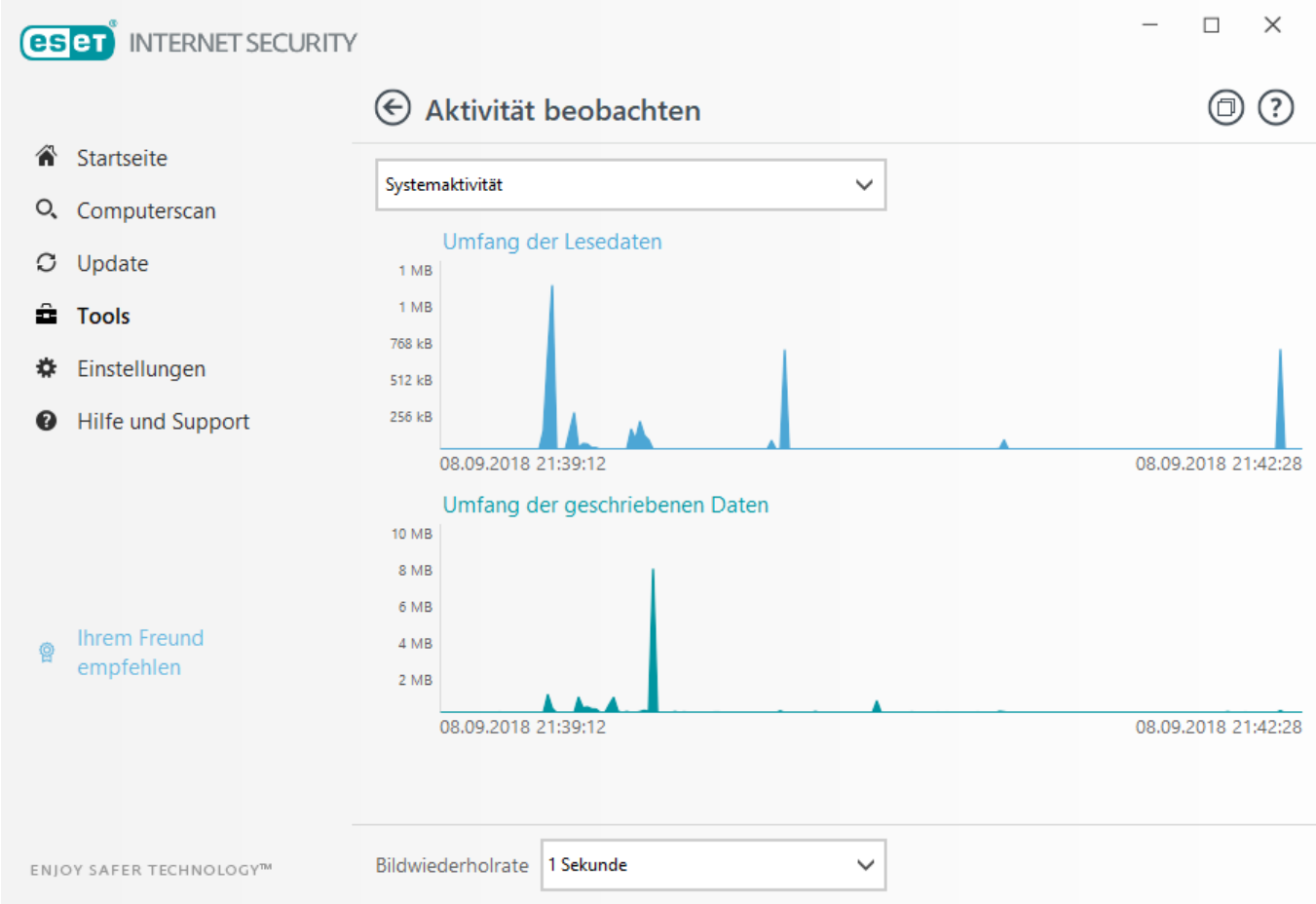
Aktivierte Funktionen werden im Sicherheitsbericht nicht mehr als „nicht funktionsfähig“ angezeigt.

Über das Zahnrad in der oberen rechten Ecke können Sie **Benachrichtigungen für Sicherheitsberichte aktivieren/deaktivieren** oder auswählen, ob die Daten für die letzten 30 Tage oder seit der Produktaktivierung angezeigt werden sollen. Falls ESET Internet Security vor weniger als 30 Tagen installiert wurde, können Sie nur die Anzahl der Tage seit der Installation auswählen. Der Zeitraum von 30 Tagen ist standardmäßig vorausgewählt.

Mit **Daten zurücksetzen** können Sie alle Statistiken löschen und die vorhandenen Daten für den Sicherheitsbericht zurücksetzen. Diese Aktion muss bestätigt werden, es sei denn, Sie haben die Option **Vor dem Zurücksetzen von Statistiken nachfragen** unter **Erweiterte Einstellungen** > **Benutzeroberfläche** > **Warnungen und Benachrichtigungen** > **Bestätigungsnachrichten** deaktiviert.

4.6.3.4 Aktivität beobachten

Um die aktuelle **Systemaktivität** als Diagramm anzuzeigen, klicken Sie auf **Tools** > > **Weitere Tools** > > **Aktivität beobachten**. Im unteren Bereich des Diagramms befindet sich eine Zeitleiste, welche die Systemaktivität in Echtzeit innerhalb des gewählten Zeitraums aufzeichnet. Um die Zeitleiste zu ändern, wählen Sie im Dropdownmenü **Bildwiederholrate** einen Wert aus.



Folgende Optionen stehen zur Verfügung:

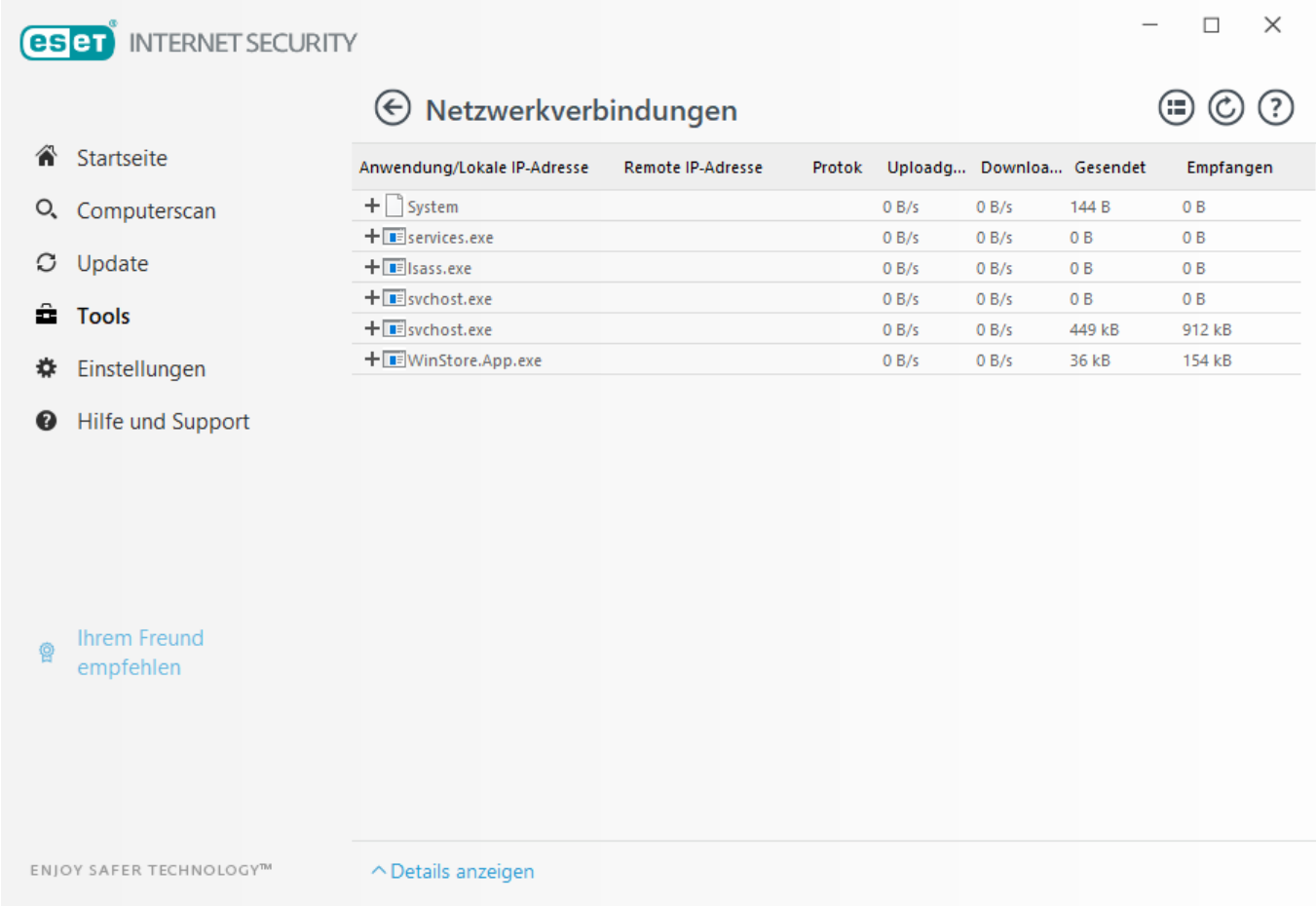
- **Schritt: 1 Sekunde** – Das Diagramm wird jede Sekunde aktualisiert, und die Zeitleiste umfasst die letzten 10 Minuten.
- **Schritt: 1 Minute (letzte 24 Stunden)** – Das Diagramm wird jede Minute aktualisiert. Die Zeitleiste deckt die letzten 24 Stunden.
- **Schritt: 1 Stunde (letzter Monat)** – Das Diagramm wird jede Stunde aktualisiert. Die Zeitleiste deckt den letzten Monat.
- **Schritt: Schritt: 1 Stunde (ausgewählter Monat)** – Das Diagramm wird jede Stunde aktualisiert. Die Zeitleiste deckt die X letzten, ausgewählten Monate.

Die vertikale Achse im **Systemaktivitätsdiagramm** bildet die gelesenen (blau) und geschriebenen Daten (rot) ab. Beide Werte werde in KB (Kilobyte)/MB/GB angegeben. Wenn Sie mit dem Mauszeiger über die gelesenen oder geschriebenen Daten in der Legende unterhalb des Diagramms fahren, werden im Diagramm nur die Daten für diesen Aktivitätstyp angezeigt.

Alternativ können Sie **Netzwerkaktivität** im Dropdownmenü auswählen. Die Anzeige und die Einstellungen der Diagramme für **Systemaktivität** und **Netzwerkaktivität** sind fast identisch. Bei der Netzwerkaktivität werden empfangene (rot) und gesendete Daten (blau) dargestellt.

4.6.3.5 Netzwerkverbindungen

Im Abschnitt „Netzwerkverbindungen“ wird eine Liste der aktiven und der ausstehenden Verbindungen angezeigt. Auf diese Weise behalten Sie die Übersicht über alle Anwendungen, die ausgehende Verbindungen herstellen.



In der ersten Zeile werden der Name der Anwendung und die Geschwindigkeit der Datenübertragung angezeigt. Klicken Sie auf **+**, um eine Liste der von der Anwendung hergestellten Verbindungen (und weiterer Informationen) anzuzeigen.

Spalten

Anwendung/Lokale IP-Adresse – Name der Anwendung, lokale IP-Adressen und für die Datenübertragung verwendete Ports.

Remote IP-Adresse – IP-Adresse und Portnummer eines bestimmten Remotecomputers.

Protokoll – Verwendetes Übertragungsprotokoll.

Uploadgeschwindigkeit/Downloadgeschwindigkeit – Aktuelle Übertragungsgeschwindigkeit eingehender bzw. ausgehender Daten.

Gesendet/Empfangen – Über die Verbindung übertragene Datenmenge.

Details anzeigen – Durch Aktivieren dieser Option werden weitere Informationen zur ausgewählten Verbindung angezeigt.

Klicken Sie mit der rechten Maustaste auf eine Verbindung. Es werden Ihnen zusätzliche Optionen angezeigt:

Hostnamen auflösen – Falls möglich, werden anstelle der IP-Adressen die DNS-Namen von Gegenstellen angezeigt.

Nur TCP-Verbindungen anzeigen – Die Liste enthält nur Verbindungen, die ein TCP-Protokoll verwenden.

Offene Ports anzeigen – Aktivieren Sie diese Option, um nur Verbindungen anzuzeigen, über die zurzeit keine Daten übertragen werden, bei denen das System für die ausstehende Übertragung jedoch bereits einen Port geöffnet hat.

Verbindungen innerhalb des Computers anzeigen – Aktivieren Sie diese Option, um nur Verbindungen anzuzeigen, bei denen die Gegenstelle der eigene Computer ist (sogenannte *Localhost*-Verbindungen).

Aktualisierungsintervall – Wählen Sie das Intervall für die Aktualisierung der aktiven Verbindungen.

Jetzt aktualisieren – Lädt das Fenster „Netzwerkverbindungen“ neu.

Die folgenden Optionen stehen erst zur Verfügung, nachdem Sie eine Anwendung oder einen Prozess angeklickt haben, d. h. nicht eine aktive Verbindung:

Kommunikation für Prozess vorübergehend blockieren – Verbindungen für diese Anwendung werden vorübergehend blockiert. Wenn eine neue Verbindung hergestellt wird, verwendet die Firewall eine vordefinierte Regel. Eine Beschreibung der Einstellungen finden Sie im Abschnitt Konfigurieren und Verwenden von Regeln.

Kommunikation für Prozess vorübergehend zulassen – Verbindungen für diese Anwendung werden vorübergehend zugelassen. Wenn eine neue Verbindung hergestellt wird, verwendet die Firewall eine vordefinierte Regel. Eine Beschreibung der Einstellungen finden Sie im Abschnitt Konfigurieren und Verwenden von Regeln.

4.6.3.6 ESET SysInspector

ESET SysInspector ist eine Anwendung, die Ihren Computer gründlich durchsucht und eine genaue (Risikostufen-) Analyse Ihrer Systemkomponenten erstellt. Hierzu zählen u. a. Treiber und Anwendungen, Netzwerkverbindungen oder wichtige Registrierungseinträge. Diese Informationen helfen Ihnen beim Aufspüren der Ursache für verdächtiges Systemverhalten, welches möglicherweise durch Software- oder Hardwareinkompatibilität oder eine Infektion mit Schadcode hervorgerufen wurde.

Das Fenster „SysInspector“ zeigt folgende Informationen zu erstellten Logs an:

- **Zeit** - Zeitpunkt der Log-Erstellung.
- **Kommentar** - Eine kurze Beschreibung.
- **Benutzer** - Der Name des Benutzers, der das Log erstellt hat.
- **Status** - Status bei der Log-Erstellung.

Folgende Aktionen stehen zur Verfügung:

- **Anzeigen** – Öffnet das erstellte Log. Sie können auch mit der rechten Maustaste auf die Log-Datei klicken und im Kontextmenü **Anzeigen** auswählen.
- **Vergleichen** - Vergleicht zwei vorhandene Logs.
- **Erstellen...** - Erstellen eines neuen Logs Warten Sie, bis ESET SysInspector die Erstellung abgeschlossen hat (Log-Status „Erstellt“), bevor Sie versuchen, die Log-Datei zu öffnen.
- **Löschen** - Löschen der ausgewählten Logs aus der Liste.

Die folgenden Einträge sind im Kontextmenü verfügbar, wenn eine oder mehrere Log-Dateien ausgewählt sind:

- **Anzeigen** - Anzeige des ausgewählten Logs in ESET SysInspector (entspricht einem Doppelklick auf einen beliebigen Eintrag).
- **Vergleichen** - Vergleicht zwei vorhandene Logs.
- **Erstellen...** - Erstellen eines neuen Logs Warten Sie, bis ESET SysInspector die Erstellung abgeschlossen hat (Log-Status „Erstellt“), bevor Sie versuchen, die Log-Datei zu öffnen.
- **Löschen** - Löschen der ausgewählten Logs aus der Liste.
- **Alle löschen** – Löschen aller Logs.
- **Exportieren** - Exportieren des Logs in eine *.xml*-Datei oder eine komprimierte *.xml*-Datei.

4.6.3.7 Taskplaner

Der Taskplaner verwaltet und startet Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften.

Um ihn zu öffnen, klicken Sie im Hauptprogrammfenster von ESET Internet Security auf **Tools** > **Weitere Tools** > **Taskplaner**. Der **Taskplaner** umfasst eine Liste aller geplanten Tasks sowie deren Konfigurationseigenschaften, inklusive des vordefinierten Datums, der Uhrzeit und des verwendeten Prüfprofils.

Er dient zur Planung der folgenden Vorgänge: Module aktualisieren, Prüftask, Prüfung Systemstartdateien und Log-Wartung. Tasks können direkt über das Fenster „Taskplaner“ hinzugefügt oder gelöscht werden. (Klicken Sie dazu unten auf **Task hinzufügen** oder **Löschen**). Sie können die Liste der geplanten Tasks auf den Standard zurücksetzen und alle Änderungen löschen, indem Sie auf **Standard** klicken. Klicken Sie an einer beliebigen Stelle mit der rechten Maustaste in das Fenster „Taskplaner“, um folgende Aktionen auszuführen: Anzeigen ausführlicher Informationen, sofortige Ausführung des Vorgangs, Hinzufügen eines neuen Vorgangs und Löschen eines vorhandenen Vorgangs. Verwenden Sie die Kontrollkästchen vor den einzelnen Einträgen zum Aktivieren oder Deaktivieren der jeweiligen Vorgänge.

Standardmäßig werden im **Taskplaner** die folgenden Tasks angezeigt:

- **Log-Wartung**
- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Herstellen von DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**
- **Regelmäßige Überprüfung auf aktuelle Produktversion** (siehe Update-Modus)
- **Prüfung Systemstartdateien** (nach Benutzeranmeldung)
- **Prüfung Systemstartdateien** (nach Update der Erkennungsroutine)

Um die Konfiguration eines vorhandenen Standardtasks oder eines benutzerdefinierten Tasks zu ändern, klicken Sie mit der rechten Maustaste auf den Task und dann auf **Bearbeiten**, oder wählen Sie den Task aus, den Sie ändern möchten, und klicken Sie auf **Bearbeiten**.

Hinzufügen eines neuen Tasks

1. Klicken Sie am unteren Fensterrand auf **Task hinzufügen**.
2. Geben Sie einen Namen für den Task ein.

3. Wählen Sie dann den gewünschten Task aus der Liste:

- **Start externer Anwendung** – Planen der Ausführung einer externen Anwendung.
- **Log-Wartung** – Log-Dateien enthalten auch unbenutzte leere Einträge von gelöschten Datensätzen. Dieser Task optimiert regelmäßig die Einträge in Log-Dateien.
- **Prüfung Systemstartdateien** - Prüft Dateien, die während des Systemstarts oder der Anmeldung ausgeführt werden.
- **Snapshot des Computerstatus erstellen** - Erstellt einen ESET SysInspector-Snapshot und eine genaue Risikoanalyse Ihrer Systemkomponenten (z. B. Treiber und Anwendungen).
- **On-Demand-Prüfung** - Prüft die Dateien und Ordner auf Ihrem Computer.
- **Update** – Erstellt einen Update-Task zur Aktualisierung der Module.

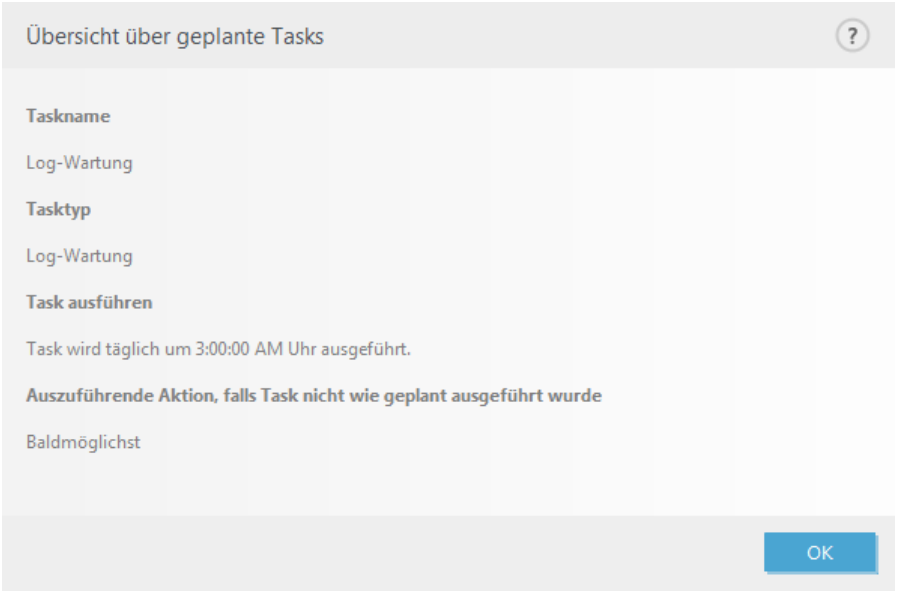
4. Aktivieren Sie den Task mit der Option **Aktivieren** (Sie können dies auch später tun, indem Sie das Kontrollkästchen in der Liste der geplanten Tasks markieren oder die Markierung daraus entfernen), klicken Sie auf **Weiter** und wählen Sie eine Zeitangabe aus:

- **Einmalig** – Der Task wird nur einmalig zu einem festgelegten Zeitpunkt ausgeführt.
- **Wiederholt** – Der Task wird in dem angegebenen Zeitabstand ausgeführt.
- **Täglich** - Der Task wird wiederholt täglich zur festgelegten Uhrzeit ausgeführt.
- **Wöchentlich** - Der Task wird am festgelegten Wochentag zur angegebenen Uhrzeit ausgeführt.
- **Bei Ereignis** - Der Task wird ausgeführt, wenn ein bestimmtes Ereignis eintritt.

5. Wählen Sie **Task im Akkubetrieb überspringen** aus, um die Systembelastung für einen Laptop während des Akkubetriebs möglichst gering zu halten. Der angegebene Task wird zum angegeben Zeitpunkt in den Feldern **Taskausführung** ausgeführt. Wenn der Vorgang nicht zur festgelegten Zeit ausgeführt werden konnte, können Sie einen Zeitpunkt für die nächste Ausführung angeben:

   - **Zur nächsten geplanten Ausführungszeit**
   - **Baldmöglichst**
   - **Sofort ausführen, wenn Intervall seit letzter Ausführung überschritten** (das Intervall kann über das Feld **Zeit seit letzter Ausführung** festgelegt werden)

Sie können den geplanten Task durch Klicken mit der rechten Maustaste und Auswählen der Option **Task-Eigenschaften** überprüfen.



4.6.3.8 System Cleaner

System Cleaner ist ein Tool, mit dem Sie den Computer nach der Säuberung der Bedrohung auf einen nutzbaren Zustand wiederherstellen können. Schadsoftware kann Systemprogramme wie den Registrierungs-Editor, den Task-Manager oder Windows Update deaktivieren. System Cleaner stellt die Standardwerte und -Einstellungen für das jeweilige System mit einem Klick wieder her.

System Cleaner meldet Probleme aus fünf verschiedenen Einstellungskategorien:

- **Sicherheitseinstellungen**: Änderungen an Einstellungen, die sich auf die Anfälligkeit Ihres Computers auswirken können, z. B. Windows Update.
- **Systemeinstellungen**: Änderungen an Systemeinstellungen, die sich auf das Verhalten Ihres Computers auswirken können, z. B. Dateizuordnungen.
- **Systemdarstellung**: Einstellungen, die das Erscheinungsbild Ihres Systems bestimmen, z. B. Ihr Desktophintergrund.
- **Deaktivierte Funktionen**: Wichtige Funktionen und Anwendungen, die möglicherweise deaktiviert sind.
- **Windows-Systemwiederherstellung**: Einstellungen für die Windows-Systemwiederherstellung, mit der Sie Ihr System auf einen früheren Zeitpunkt zurücksetzen können.

Die Ausführung von System Cleaner wird in den folgenden Fällen angefordert:

- Wenn eine Bedrohung gefunden wird
- Wenn ein Benutzer auf **Zurücksetzen** klickt

Sie können die Änderungen überprüfen und die Einstellungen bei Bedarf zurücksetzen.

HINWEIS
Die System Cleaner-Aktionen können nur von Benutzern mit Administratorrechten ausgeführt werden.

4.6.3.9 ESET SysRescue

ESET SysRescue ist ein Dienstprogramm, mit dem Sie einen bootfähigen Datenträger mit einer ESET Security-Lösung erstellen können, wie z. B. ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security, ESET Smart Security Premium oder bestimmte serverorientierte Produkte. Der große Vorteil von ESET SysRescue ist, dass ESET Security damit unabhängig vom Betriebssystem auf dem jeweiligen Rechner ausgeführt werden kann, aber direkten Zugriff auf die Festplatte und das gesamte Dateisystem hat. Auf diese Weise lässt sich auch Schadsoftware entfernen, bei der dies normalerweise (bei laufendem Betriebssystem usw.) nicht möglich wäre.

4.6.3.10 Cloudbasierter Schutz

ESET LiveGrid® basiert auf dem ESET ThreatSense.Net -Frühwarnsystem und arbeitet mit von ESET-Anwendern weltweit übermittelten Daten, die es an das ESET-Virenlabor sendet. ESET LiveGrid® stellt verdächtige Proben und Metadaten „aus freier Wildbahn“ bereit und gibt uns so die Möglichkeit, unmittelbar auf die Anforderungen unserer Kunden zu reagieren und sie vor den neuesten Bedrohungen zu schützen. Weitere Informationen zu ESET LiveGrid® finden Sie in unserem Glossar.

Benutzer können sich direkt im Programmfenster oder im jeweiligen Kontextmenü anzeigen lassen, wie ausgeführte Prozesse oder Dateien eingeschätzt werden. Zudem sind über ESET LiveGrid® weitere Informationen verfügbar. Als Benutzer haben Sie zwei Möglichkeiten:

1. Sie können ESET LiveGrid® deaktiviert lassen. Die Funktionalität in der Software geht nicht verloren, in einigen Fällen reagiert ESET Internet Security jedoch möglicherweise schneller auf neue Bedrohungen als die Aktualisierung der Erkennungsroutine.
2. Sie können ESET LiveGrid® so konfigurieren, dass Informationen über neue Bedrohungen und Fundstellen von gefährlichem Code übermittelt werden. Die Informationen bleiben anonym. Diese Datei kann zur

detaillierten Analyse an ESET gesendet werden. Durch die Untersuchung dieser Bedrohungen kann ESET die Fähigkeit seiner Software zur Erkennung von Schadsoftware aktualisieren und verbessern.

ESET LiveGrid® sammelt Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden. Dazu können auch Proben oder Kopien der Datei gehören, in der eine Bedrohung aufgetreten ist, der Pfad zu dieser Datei, der Dateiname, Datum und Uhrzeit, der Prozess, über den die Bedrohung auf Ihrem Computer in Erscheinung getreten ist, und Informationen zum Betriebssystem des Computers.

ESET Internet Security ist standardmäßig so konfiguriert, dass verdächtige Dateien zur genauen Analyse beim ESET-Virenlabor eingereicht werden. Dateien mit bestimmten Erweiterungen (z. B. *.doc* oder *.xls*) sind immer von der Übermittlung ausgeschlossen. Sie können andere Dateierweiterungen hinzufügen, wenn es bestimmte Dateitypen gibt, die Sie oder Ihr Unternehmen nicht übermitteln möchten.

Das Reputationssystem von ESET LiveGrid® arbeitet mit Cloud-basierten Positiv- und Negativlisten. Um auf die Einstellungen von ESET LiveGrid® zuzugreifen, öffnen Sie durch Drücken der Taste **F5** die erweiterten Einstellungen und wählen Sie **Tools** > **ESET LiveGrid®**.

An ESET LiveGrid® teilnehmen (empfohlen) – Das ESET LiveGrid®-Reputationssystem erhöht die Wirksamkeit der ESET-Sicherheitslösungen, indem es geprüfte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht.

ESET LiveGrid®-Feedbacksystem aktivieren – Die Daten werden zur weiteren Analyse an das ESET-Virenlabor übermittelt.

Absturzberichte und Diagnosedaten senden – Daten wie Absturzberichte und Speicherabbilder von Modulen werden übermittelt.

Anonyme Statistiken senden– Zulassen, dass ESET Informationen über neu erkannte Bedrohungen erfasst, wie den Bedrohungsnamen, das Datum und die Uhrzeit der Erkennung, die Erkennungsmethode und verknüpften Metadaten oder die Produktversion und -konfiguration, einschließlich Daten zum System.

E-Mail-Adresse für Rückfragen (optional) – Sie können mit den verdächtigen Dateien eine E-Mail-Adresse für Rückfragen angeben, wenn zur Analyse weitere Informationen erforderlich sind. Beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.

Proben einreichen

Infizierte Proben einreichen – Diese Option sendet alle infizierten Proben zur Analyse und Verbesserung der zukünftigen Erkennung an ESET. Die folgenden Optionen sind verfügbar:

- Alle infizierten Proben
- Alle Proben mit Ausnahme von Dokumenten
- Nicht übermitteln

Verdächtige Proben einreichen

Ausführbare Dateien – Dateien mit den Endungen .exe, .dll, .sys.
Archive – Dateien mit den Endungen .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
Skripts – Dateien mit den Endungen .bat, .cmd, .hta, .js, .vbs, .ps1.
Sonstige – Dateien mit den Endungen .jar, .reg, .msi, .sfw, .lnk.
Mögliche Spam-E-Mails – Senden Sie mögliche Spam-Komponenten oder ganze Spam-E-Mails mit Anhang zur weiteren Analyse an ESET. Diese Option verbessert die globale Spam-Erkennung inklusive der zukünftigen Spam-Erkennung für Sie selbst.
Dokumente – Umfasst Microsoft Office-Dokumente und PDFs mit aktiven Inhalten.

Ausschlüsse – Mit dem Ausschlussfilter können Sie bestimmte Dateien/Ordner von der Übermittlung ausschließen. So kann es beispielsweise nützlich sein, Dateien mit vertraulichen Informationen wie Dokumente oder Tabellenkalkulationen auszuschließen. Hier eingetragene Dateien werden nicht an ESET übermittelt, auch wenn sie verdächtigen Code enthalten. Einige typische Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (.doc usw.). Sie können weitere Dateien zur Ausschlussliste hinzufügen.

Wenn Sie ESET LiveGrid® einige Zeit verwendet haben, kann es sein, dass auch nach dem Deaktivieren des Systems noch einige Datenpakete zum Senden vorliegen. Derartige Datenpakete werden auch nach der Deaktivierung noch

an ESET gesendet. Nachdem alle aktuellen Informationen versendet wurden, werden keine weiteren Pakete mehr erstellt.

4.6.3.10.1 Verdächtige Dateien

Wenn Sie eine verdächtige Datei finden, können Sie sie zur Analyse an unser ESET-Virenlabor einreichen. Sollte dabei schädlicher Code zu Tage treten, wird dieser beim nächsten Update der Erkennungsroutine berücksichtigt.

Ausschlussfilter - Über diese Option können Sie bestimmte Dateien oder Ordner vom Senden ausschließen. Hier eingetragene Dateien werden nicht an das ESET-Virenlabor übermittelt, auch wenn sie verdächtigen Code enthalten. Hier können Dateien eingetragen werden, die eventuell vertrauliche Informationen enthalten, wie zum Beispiel Textdokumente oder Tabellen. Einige typische Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (.doc usw.). Sie können der Ausschlussliste weitere Dateien hinzufügen.

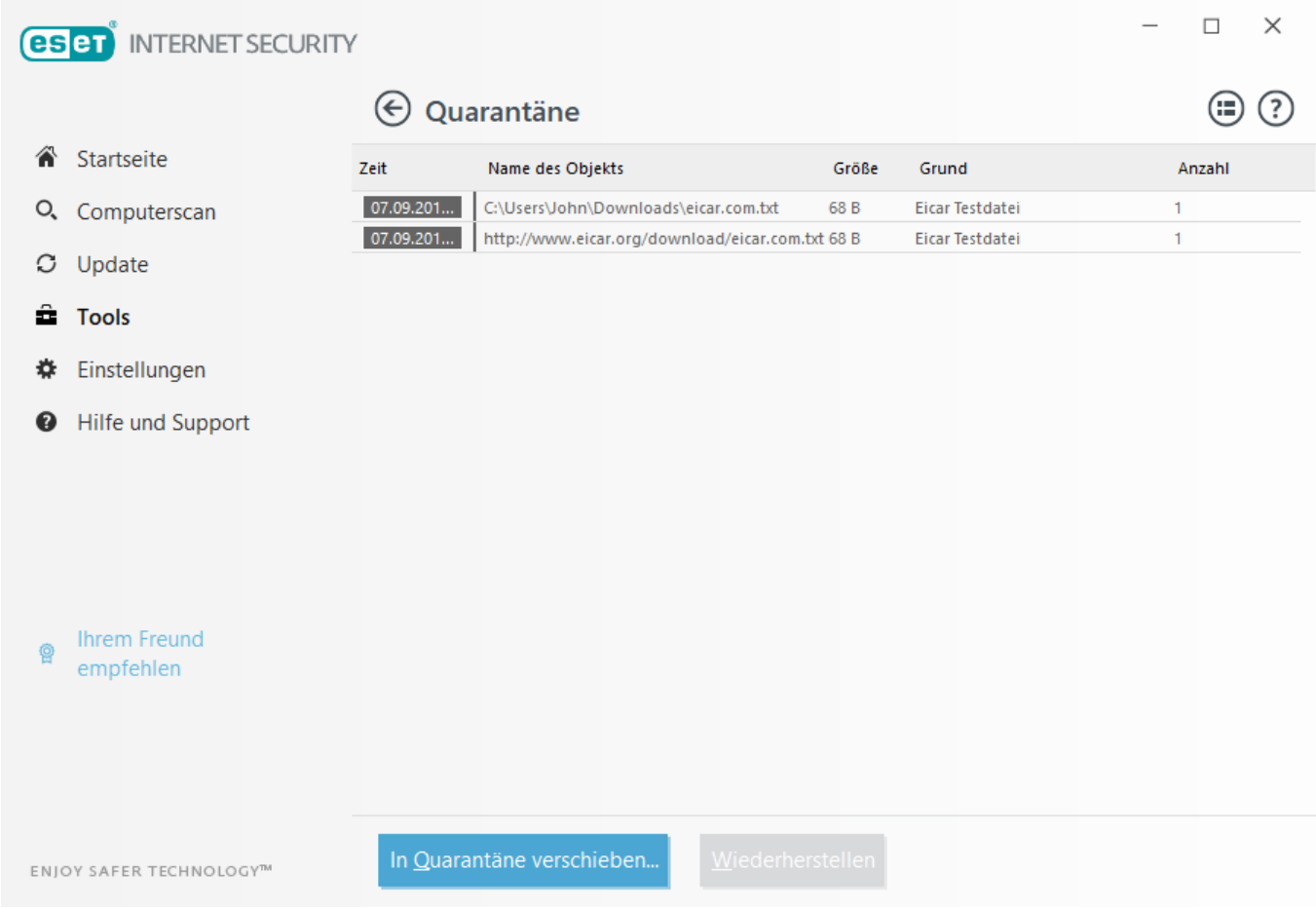
E-Mail-Adresse für Rückfragen (optional) – Sie können mit den verdächtigen Dateien eine E-Mail-Adresse für Rückfragen angeben, wenn zur Analyse weitere Informationen erforderlich sind. Beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.

Wählen Sie die Option **Erstellen von Logs aktivieren** aus, um einen Event Log zu erstellen, in dem alle Informationen über das Einreichen von Dateien und statistischen Daten protokolliert werden. Dadurch werden Einträge im Ereignis-Log erstellt, wenn Dateien oder statistische Daten eingereicht werden.

4.6.3.11 Quarantäne

Die Hauptfunktion der Quarantäne ist die sichere Verwahrung infizierter Dateien. Dateien sollten in die Quarantäne verschoben werden, wenn sie nicht gesäubert werden können, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Internet Security fälschlicherweise erkannt worden sind.

Sie können beliebige Dateien gezielt in die Quarantäne verschieben. Geschehen sollte dies bei Dateien, die sich verdächtig verhalten, bei der Virenprüfung jedoch nicht erkannt werden. Dateien aus der Quarantäne können zur Analyse an das ESET-Virenlabor eingereicht werden.



Die Dateien im Quarantäneordner können in einer Tabelle angezeigt werden, die Datum und Uhrzeit der Quarantäne, den Pfad zum ursprünglichen Speicherort der infizierten Datei, ihre Größe in Byte, einen Grund (z. B. Objekt hinzugefügt durch Benutzer) und die Anzahl der Bedrohungen (z. B. bei Archiven, in denen an mehreren Stellen Schadcode erkannt wurde) enthält.

Quarantäne für Dateien

ESET Internet Security kopiert gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Auf Wunsch können Sie beliebige verdächtige Dateien manuell in die Quarantäne verschieben, indem Sie auf **Quarantäne** klicken. In diesem Fall wird die Originaldatei nicht von ihrem ursprünglichen Speicherort entfernt. Alternativ kann auch das Kontextmenü zu diesem Zweck verwendet werden: Klicken Sie mit der rechten Maustaste in das Fenster **Quarantäne**, und wählen Sie **Quarantäne**.

Wiederherstellen aus Quarantäne

Dateien aus der Quarantäne können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Dazu verwenden Sie die Funktion **Wiederherstellen** im Kontextmenü, das angezeigt wird, wenn Sie im Fenster „Quarantäne“ mit der rechten Maustaste auf eine entsprechende Datei klicken. Wenn eine Datei als eventuell unerwünschte Anwendung markiert ist, wird die Option **Wiederherstellen und von Prüfungen ausschließen** aktiviert. Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar. Das Kontextmenü enthält außerdem die Option **Wiederherstellen nach**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

Löschen aus der Quarantäne – Klicken Sie mit der rechten Maustaste auf ein Element und wählen Sie **Aus Quarantäne löschen** aus. Alternativ können Sie das zu löschende Element auswählen und auf der Tastatur die **Entf**-Taste drücken. Sie können auch mehrere Einträge gleichzeitig auswählen und gesammelt löschen.

HINWEIS
Wenn versehentlich eine harmlose Datei in Quarantäne versetzt wurde, schließen Sie die Datei nach der Wiederherstellung von der Prüfung aus und senden Sie sie an den ESET-Support.

Einreichen einer Datei aus der Quarantäne

Wenn Sie eine verdächtige, nicht vom Programm erkannte Datei in Quarantäne versetzt haben oder wenn eine Datei fälschlich als infiziert eingestuft wurde (etwa durch die heuristische Analyse des Codes) und infolgedessen in den Quarantäneordner verschoben wurde, senden Sie die Datei zur Analyse an ESET. Um eine Datei zu senden, die in der Quarantäne gespeichert ist, klicken Sie mit der rechten Maustaste darauf und wählen im angezeigten Kontextmenü die Option **Datei zur Analyse einreichen**.

4.6.3.12 Proxyserver

In großen LAN-Netzwerken wird die Verbindung zum Internet häufig über Proxyserver vermittelt. In einer solchen Konfiguration müssen die folgenden Einstellungen definiert werden. Wenn die Einstellungen nicht vorgenommen werden, ist es möglicherweise nicht möglich, automatisch Updates über das Internet zu beziehen. Die Proxyserver-Einstellungen in ESET Internet Security sind über zwei verschiedene Bereiche der erweiterten Einstellungen verfügbar.

Die Einstellungen für den Proxyserver können zum einen in **Erweiterte Einstellungen** unter **Tools** > **Proxyserver** konfiguriert werden. So legen Sie die allgemeinen Proxyserver-Einstellungen für alle Funktionen von ESET Internet Security fest. Diese Parameter werden von allen Modulen verwendet, die eine Verbindung zum Internet benötigen.

Um die Proxyserver-Einstellungen für diese Ebene festzulegen, aktivieren Sie die Option **Proxyserver verwenden** und geben im Feld **Proxyserver** die entsprechende Adresse zusammen mit dem **Port** des Proxyservers ein.

Wenn der Proxyserver eine Authentifizierung benötigt, aktivieren Sie **Proxyserver erfordert Authentifizierung** und geben einen gültigen **Benutzernamen** sowie das entsprechende **Passwort** ein. Klicken Sie auf **Erkennen**, wenn die Einstellungen des Proxyservers automatisch erkannt und ausgefüllt werden sollen. Die in Internet Explorer festgelegten Einstellungen werden kopiert.

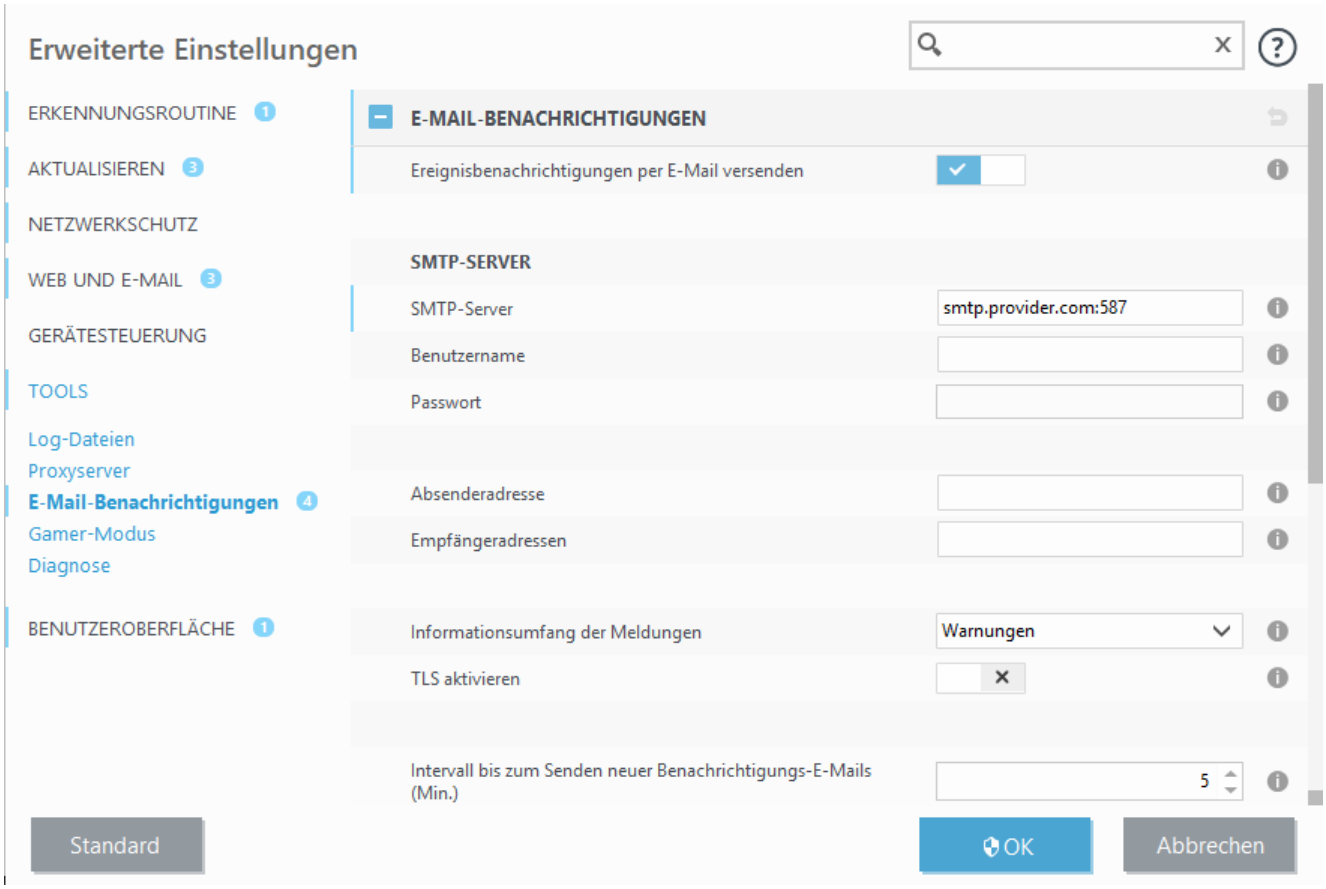
HINWEIS
Sie müssen den Benutzernamen und das Passwort manuell in den Einstellungen für den **Proxyserver** eingeben.

Direktverbindung verwenden, wenn Proxy nicht verfügbar ist – Wenn in der Produktkonfiguration die Nutzung eines HTTP-Proxys vorgesehen ist und der Proxy nicht erreichbar ist, umgeht das Produkt den Proxy und kommuniziert direkt mit ESET-Servern.

Die Proxyserver-Einstellungen können auch in den erweiterten Einstellungen für Updates festgelegt werden (**Erweiterte Einstellungen** > **Update** > **Profile** > **Update** > **Verbindungsoptionen** , Option **Verbindung über Proxyserver** im Dropdown-Menü **Proxy-Modus**). Die Einstellungen gelten dann für das entsprechende Update-Profil. Diese Methode empfiehlt sich für Laptops, da diese die Updates der Erkennungsroutine oft remote beziehen. Weitere Informationen zu diesen Einstellungen finden Sie unter Erweiterte Einstellungen für Updates.

4.6.3.13 E-Mail-Benachrichtigungen

ESET Internet Security kann automatisch Ereignismeldungen senden, wenn ein Ereignis mit dem ausgewählten Informationsumfang auftritt. Aktivieren Sie die Option **Ereignismeldungen per E-Mail versenden**, um Ereignismeldungen zu verschicken.



SMTP-Server

SMTP-Server – Der SMTP-Server, über den Benachrichtigungen verschickt werden (z. B. *smtp.Anbieter.com:587*, der Standardport ist 25).

HINWEIS
ESET Internet Security unterstützt keine SMTP-Server mit TLS-Verschlüsselung.

Benutzername und **Passwort** – Falls für den SMTP-Server Zugangsdaten zur Authentifizierung erforderlich sind, geben Sie hier einen gültigen Benutzernamen und das Passwort ein.

Absenderadresse – Geben Sie die Adresse an, die in Ereignismeldungen als Absender angezeigt werden sein soll.

Empfängeradressen – Geben Sie die Empfängeradressen an, die in Ereignismeldungen als Empfänger angezeigt werden sein sollen. Sie können mehrere Werte mit Semikolon „;“ als Trennzeichen eingeben.

Im Dropdownmenü **Informationsumfang der Meldungen** können Sie festlegen, für welchen anfänglichen Schweregrad Benachrichtigungen gesendet werden sollen.

- **Diagnose** – Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.
- **Informationen** – Informationsmeldungen, wie nicht standardmäßige Netzwerkereignisse und erfolgreiche Updates, sowie alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen** – Schwerwiegende Fehler und Warnmeldungen werden aufgezeichnet (z. B. Anti-Stealth wird nicht ordnungsgemäß ausgeführt oder bei einem Update ist ein Fehler aufgetreten).
- **Fehler** – Fehler (z. B. Dokumentschutz nicht gestartet) und schwerwiegende Fehler werden aufgezeichnet.
- **Kritische Warnungen** – Nur kritische Fehler werden aufgezeichnet, z. B. Fehler beim Starten des Virenschutz-Moduls oder ein infiziertes System.

TLS aktivieren – Hiermit werden von der TLS-Verschlüsselung unterstützte Warnungen und Hinweismeldungen versendet.

Intervall bis zum Senden neuer Benachrichtigungs-E-Mails (Min.) – Intervall in Minuten, nach dem neue Benachrichtigungen per E-Mail gesendet werden. Wenn der Wert auf „0“ festgelegt wird, werden die Benachrichtigungen sofort gesendet.

Jede Benachrichtigung in einer getrennten E-Mail senden – Wenn diese Option aktiviert ist, erhält der Empfänger für jede einzelne Benachrichtigung eine separate E-Mail. Dies kann dazu führen, dass innerhalb kurzer Zeit eine große Anzahl E-Mails empfangen werden.

Format von Meldungen

Format der Meldungen bei Ereignissen – Format der Meldungen bei auf Remotecomputern angezeigten Ereignissen.

Format der Meldungen bei Bedrohungen – Warnungen und Benachrichtigungen besitzen ein vordefiniertes Standardformat. Dieses Format sollte nicht geändert werden. Unter bestimmten Umständen (etwa, wenn Sie ein automatisiertes E-Mail-Verarbeitungssystem verwenden) ist es jedoch möglicherweise erforderlich, das Meldungsformat zu ändern.

Zeichensatz – Konvertiert eine E-Mail-Nachricht in den ANSI-Zeichensatz gemäß der Windows-Regionseinstellungen (z. B. windows-1250), Unicode (UTF-8), ASCII 7-Bit (dabei wird beispielsweise „á“ in „a“ geändert, und unbekannte Zeichen in „?“) oder Japanisch (ISO-2022-JP).

Quoted-Printable-Kodierung verwenden – Die E-Mail-Nachrichtenquelle wird in das QP-Format konvertiert, das ASCII-Zeichen verwendet und besondere regionale Zeichen in der E-Mail korrekt im 8-Bit-Format überträgt (áéíóú).

4.6.3.13.1 Format von Meldungen

Hier können Sie das Format der Ereignismeldungen festlegen, die auf Remote-Computern angezeigt werden.

Warnungen und Hinweismeldungen besitzen ein vordefiniertes Standardformat. Dieses Format sollte nicht geändert werden. Unter bestimmten Umständen (etwa, wenn Sie ein automatisiertes E-Mail-Verarbeitungssystem verwenden) ist es jedoch möglicherweise erforderlich, das Meldungsformat zu ändern.

Schlüsselwörter (durch %-Zeichen abgetrennte Zeichenfolgen) in der Meldung werden durch entsprechende Informationen ersetzt. Folgende Schlüsselwörter sind verfügbar:

- **%TimeStamp%** – Datum und Uhrzeit des Ereignisses
- **%Scanner%** – betroffenes Modul
- **%ComputerName%** – Name des Computers, auf dem die Warnmeldung aufgetreten ist
- **%ProgramName%** – Programm, das die Warnung erzeugt hat
- **%InfectedObject%** – Name der infizierten Datei, Nachricht usw.
- **%VirusName%** – Angabe des Infektionsverursachers
- **%Action%** – bei der Infiltration durchgeführte Aktion
- **%ErrorDescription%** – Beschreibung eines nicht durch einen Virus ausgelösten Ereignisses

Die Schlüsselwörter **%InfectedObject%** und **%VirusName%** werden nur in Warnmeldungen bei Bedrohungen verwendet, **%ErrorDescription%** nur in Ereignismeldungen.

Lokalen Zeichensatz verwenden – Konvertiert eine E-Mail-Nachricht anhand der Ländereinstellungen in Windows in eine ANSI-Zeichenkodierung (z. B. Windows-1250). Wenn Sie diese Option deaktiviert lassen, werden Nachrichten in 7-Bit-ACSII kodiert (dabei wird z. B. „à“ zu „a“ geändert und ein unbekanntes Symbol durch ein Fragezeichen ersetzt).

Lokale Zeichenkodierung verwenden – Die E-Mail-Nachrichtenquelle wird in das QP-Format konvertiert, das ASCII-Zeichen verwendet und besondere regionale Zeichen in der E-Mail korrekt im 8-Bit-Format überträgt (áéíóú).

4.6.3.14 Probe für die Analyse auswählen

Über das Dialogfenster zum Dateiversand können Sie Dateien bei ESET zur Analyse einreichen. Sie öffnen es unter **Tools** > > **Datei zur Analyse einreichen**. Wenn Ihnen eine Datei auf Ihrem Computer oder eine Webseite verdächtig erscheint, können Sie die Datei zur Analyse an das ESET-Virenlabor senden. Wenn sich herausstellt, dass die Datei bzw. Webseite Schadcode enthält, werden entsprechende Erkennungsfunktionen in zukünftigen Updates berücksichtigt.

Sie können Dateien auch per E-Mail einsenden. Komprimieren Sie in diesem Fall die Datei(en) mit WinRAR/WinZIP, verschlüsseln Sie das Archiv mit dem Passwort „infected“ und senden Sie es an samples@eset.com. Formulieren Sie eine aussagekräftige Betreffzeile, und notieren Sie möglichst viele ergänzende Informationen zu den eingesandten Dateien (z. B. von welcher Website Sie die Dateien heruntergeladen haben).

HINWEIS
Auf Dateien, die Sie an ESET senden, sollte mindestens eines der folgenden Kriterien zutreffen:

- Die Datei wird nicht als Bedrohung erkannt
- Die Datei wird als Bedrohung erkannt, obwohl Sie keinen Schadcode enthält

ESET wird nur dann Kontakt mit Ihnen aufnehmen, wenn zusätzliche Angaben für die Dateianalyse benötigt werden.

Wählen Sie aus dem Dropdownmenü **Grund für Einreichen der Datei** die Beschreibung aus, die am besten auf Ihre Mitteilung zutrifft:

- **Verdächtige Datei**
- **Verdächtige Website** (eine Website, die mit Schadsoftware infiziert ist)
- **Fehlalarm Datei** (als Bedrohung erkannte Datei, die jedoch nicht infiziert ist)
- **Fehlalarm Webseite**
- **Sonstige**

Datei/Webseite – Der Pfad zu der Datei oder Webseite, die eingesandt werden soll.

E-Mail-Adresse – Diese E-Mail-Adresse wird zusammen mit verdächtigen Dateien an ESET übermittelt. Möglicherweise wird ESET über diese Adresse Kontakt mit Ihnen aufnehmen, wenn zusätzliche Angaben für die Dateianalyse benötigt werden. Diese Angabe ist freiwillig. Diese Probe kann **anonym übermittelt** werden. Sie werden nur im Ausnahmefall eine Antwort von ESET erhalten, da täglich mehrere Zehntausend Dateien auf unseren Servern eingehen und wir nicht jede Meldung individuell beantworten können.

4.6.3.15 Microsoft Windows® update

Die Windows Update-Funktion ist ein wichtiger Bestandteil des Schutzes vor bösartiger Software. Aus diesem Grund ist es essenziell, dass Sie verfügbare Microsoft Windows-Updates sofort installieren. Entsprechend der von Ihnen festgelegten Richtlinien benachrichtigt Sie ESET Internet Security über fehlende Updates. Folgende Richtlinien sind verfügbar:

- **Keine Updates** - Es werden keine Updates zum Download angeboten.
- **Optionale Updates** - Updates mit niedriger Priorität und höher werden zum Download angeboten.
- **Empfohlene Updates** - Updates mit normaler Priorität und höher werden zum Download angeboten.
- **Wichtige Updates** - Updates mit hoher Priorität und höher werden zum Download angeboten.
- **Kritische Updates** - Nur kritische Updates werden zum Download angeboten.

Klicken Sie auf **OK**, um die Änderungen zu speichern. Das Fenster „System-Updates“ wird nach erfolgter Statusverifizierung durch den Update-Server angezeigt. Dementsprechend stehen die aktualisierten Systemdaten möglicherweise nicht unmittelbar nach Speicherung der Änderungen zur Verfügung.

4.6.3.16 ESET CMD

Diese Funktion aktiviert erweiterte ECMD-Befehle. Sie können Einstellungen über die Befehlszeile (ecmd.exe) importieren und exportieren. Bisher konnten Einstellungen nur über die Benutzeroberfläche importiert und exportiert werden. Die ESET Internet Security-Konfiguration kann in eine *.xml*-Datei exportiert werden.

Wenn Sie ESET CMD aktiviert haben, stehen zwei Autorisierungsmethoden zur Verfügung:

- **Keine** – keine Autorisierung. Diese Methode sollte nicht verwendet werden, da andernfalls beliebige unsignierte Konfigurationen importiert werden können, was ein Sicherheitsrisiko darstellt.
- **Passwort für die erweiterten Einstellungen** – Wenn Sie eine Konfiguration aus einer *.xml*-Datei importieren, benötigen Sie ein Passwort und müssen die Datei zunächst signieren (siehe „Signieren von *.xml*-Konfigurationsdateien“ weiter unten). Sie müssen das unter Einstellungen für den Zugriff festgelegte Passwort eingeben, um eine neue Konfiguration importieren zu können. Wenn Sie diese Einstellungen nicht festgelegt haben, das Passwort nicht übereinstimmt oder die *.xml*-Konfigurationsdatei nicht signiert ist, wird die Konfiguration nicht importiert.

Nachdem Sie ESET CMD aktiviert haben, können Sie ESET Internet Security-Konfigurationen über die Befehlszeile importieren und exportieren. Sie können diesen Vorgang manuell ausführen oder ein Skript für die Automatisierung erstellen.

WICHTIG
Sie müssen die erweiterten ecmd-Befehle entweder mit Administratorberechtigungen oder in einer Windows-Befehlszeile (cmd) mit der Option **Als Administrator ausführen** verwenden. Andernfalls erhalten Sie die Nachricht **Error executing command.**. Außerdem muss der ausgewählte Zielordner beim Exportieren vorhanden sein. Der Befehl zum Exportieren funktioniert auch, wenn die ESET CMD-Einstellung deaktiviert ist.

BEISPIEL
Befehl zum Exportieren von Einstellungen:
```
ecmd /getcfg c:\config\settings.xml
```

Befehl zum Importieren von Einstellungen:
```
ecmd /setcfg c:\config\settings.xml
```

HINWEIS
Die erweiterten ecmd-Befehle können nur lokal ausgeführt werden.

Signieren einer *.xml*-Konfigurationsdatei:

1. Laden Sie das ausführbare XmlSignTool herunter.
2. Öffnen Sie eine Windows-Eingabeaufforderung (cmd) mit der Option **Als Administrator ausführen**.
3. Navigieren Sie zum Speicherort der Datei `xmlsigntool.exe`
4. Führen Sie den Befehl zum Signieren der *.xml*-Konfigurationsdatei mit der folgenden Syntax aus:
   `xmlsigntool /version 1|2 <xml_file_path>`

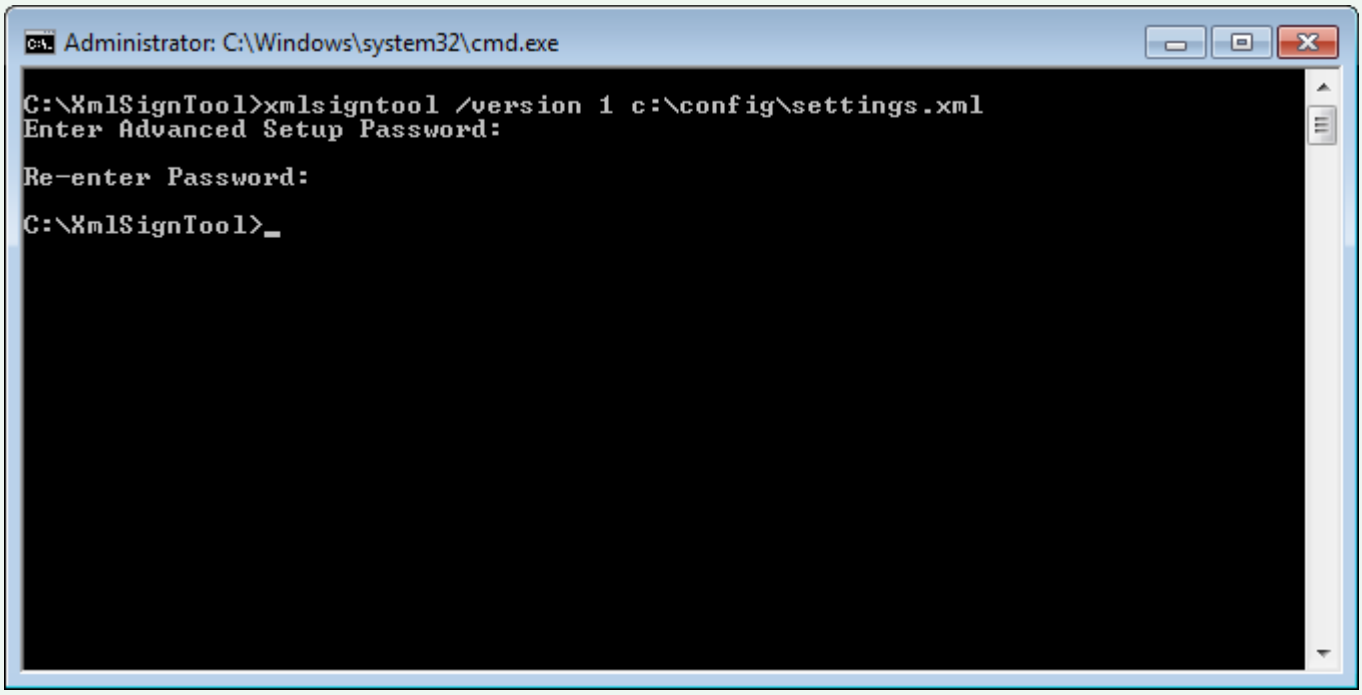
WICHTIG
Der Wert des Parameters `/version` hängt von Ihrer Version von ESET Internet Security ab. Verwenden Sie `/version 1` für Versionen von ESET Internet Security, die älter als 11.1 sind. Verwenden Sie `/version 2` für die aktuelle Version von ESET Internet Security.

5. Geben Sie das Passwort für die erweiterten Einstellungen ein und bestätigen Sie es, wenn Sie vom XmlSignTool dazu aufgefordert werden. Ihre *.xml*-Konfigurationsdatei ist jetzt signiert und kann in einer anderen Instanz von ESET Internet Security mit ESET CMD und der Passwortautorisierungsmethode importiert werden.

BEISPIEL

Befehl zum Signieren einer exportierten Konfigurationsdatei:

```
xmlsigntool /version 1 c:\config\settings.xml
```



HINWEIS

Wenn sich das Passwort für die erweiterten Einstellungen geändert hat und Sie eine Konfiguration importieren möchten, die mit dem alten Passwort signiert wurde, können Sie die *.xml*-Konfigurationsdatei mit Ihrem aktuellen Passwort erneut signieren. Auf diese Weise können Sie eine ältere Konfigurationsdatei wiederverwenden, ohne sie vor dem Importieren auf einem anderen Computer mit ESET Internet Security erneut zu exportieren.

4.7 Benutzeroberfläche

Im Abschnitt **Benutzeroberfläche** können Sie das Verhalten der grafischen Benutzeroberfläche (GUI) des Programms konfigurieren.

Mit Grafik können Sie die Darstellung und die Effekte des Programms ändern.

Konfigurieren Sie Warnungen und Hinweise, um festzulegen, wie Warnungen bei erkannten Bedrohungen und Systemhinweise angezeigt werden sollen. So können Sie diese Funktion Ihren Anforderungen anpassen.

Um Ihre Sicherheitssoftware bestmöglich zu schützen und unerlaubte Änderungen zu vermeiden, können Sie mit der Funktion Einstellungen für den Zugriff einen Passwortschutz für Ihre Einstellungen einrichten.

4.7.1 Elemente der Benutzeroberfläche

Über die Konfigurationsoptionen für die Benutzeroberfläche von ESET Internet Security können Sie die Arbeitsumgebung an Ihre Anforderungen anpassen. Sie finden diese Konfigurationsoptionen unter **Erweiterte Einstellungen** > **Benutzeroberfläche** > **Elemente der Benutzeroberfläche**.

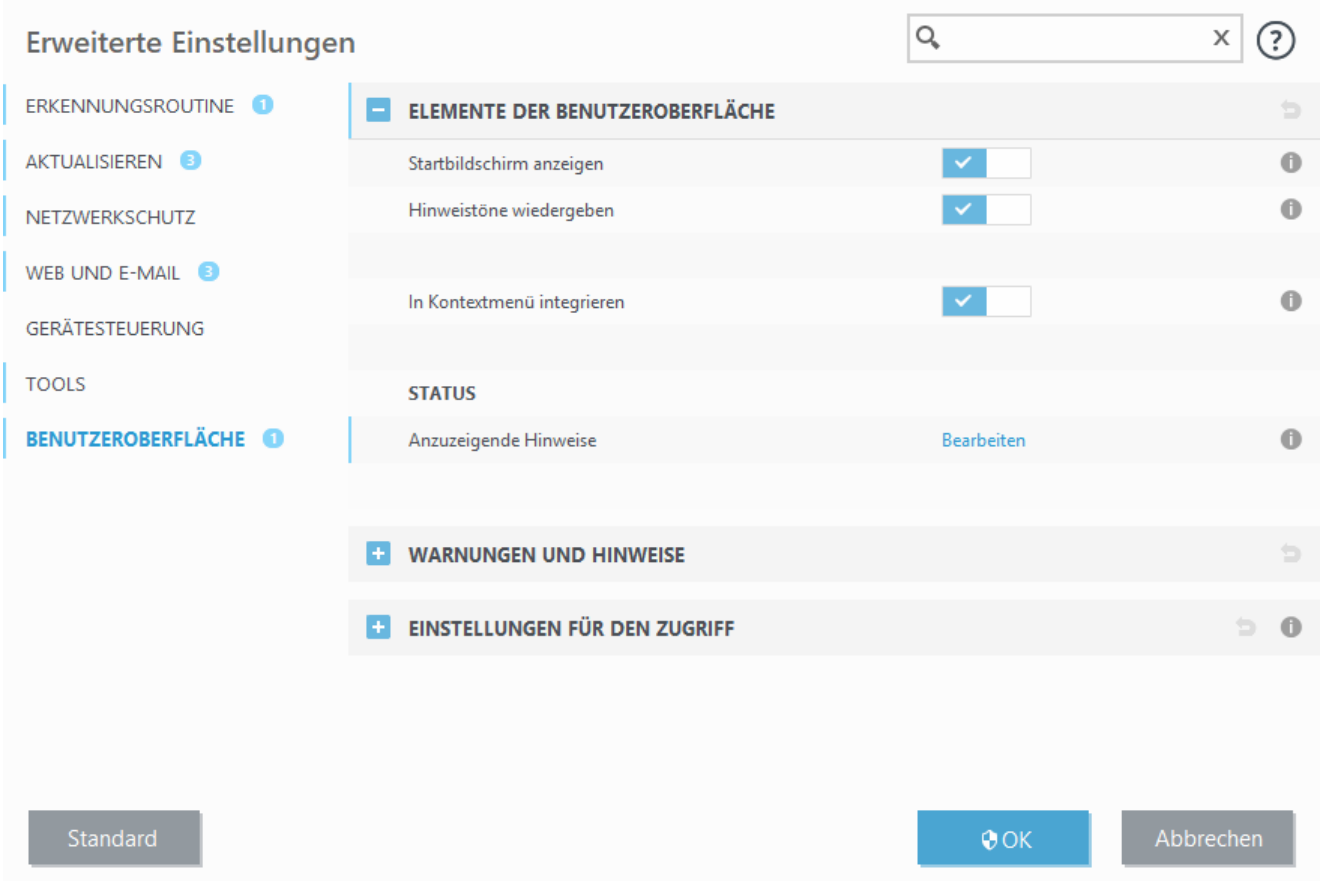
Wenn ESET Internet Security ohne Anzeige des Startbilds gestartet werden soll, deaktivieren Sie die Option **Startbild anzeigen**.

Wenn ESET Internet Security bei wichtigen Ereignissen wie z. B. der Erkennung einer Bedrohung oder nach Abschluss einer Prüfung einen Warnton ausgeben soll, aktivieren Sie die Option **Hinweistöne wiedergeben**.

In Kontextmenü integrieren - ESET Internet Security kann in das Kontextmenü integriert werden.

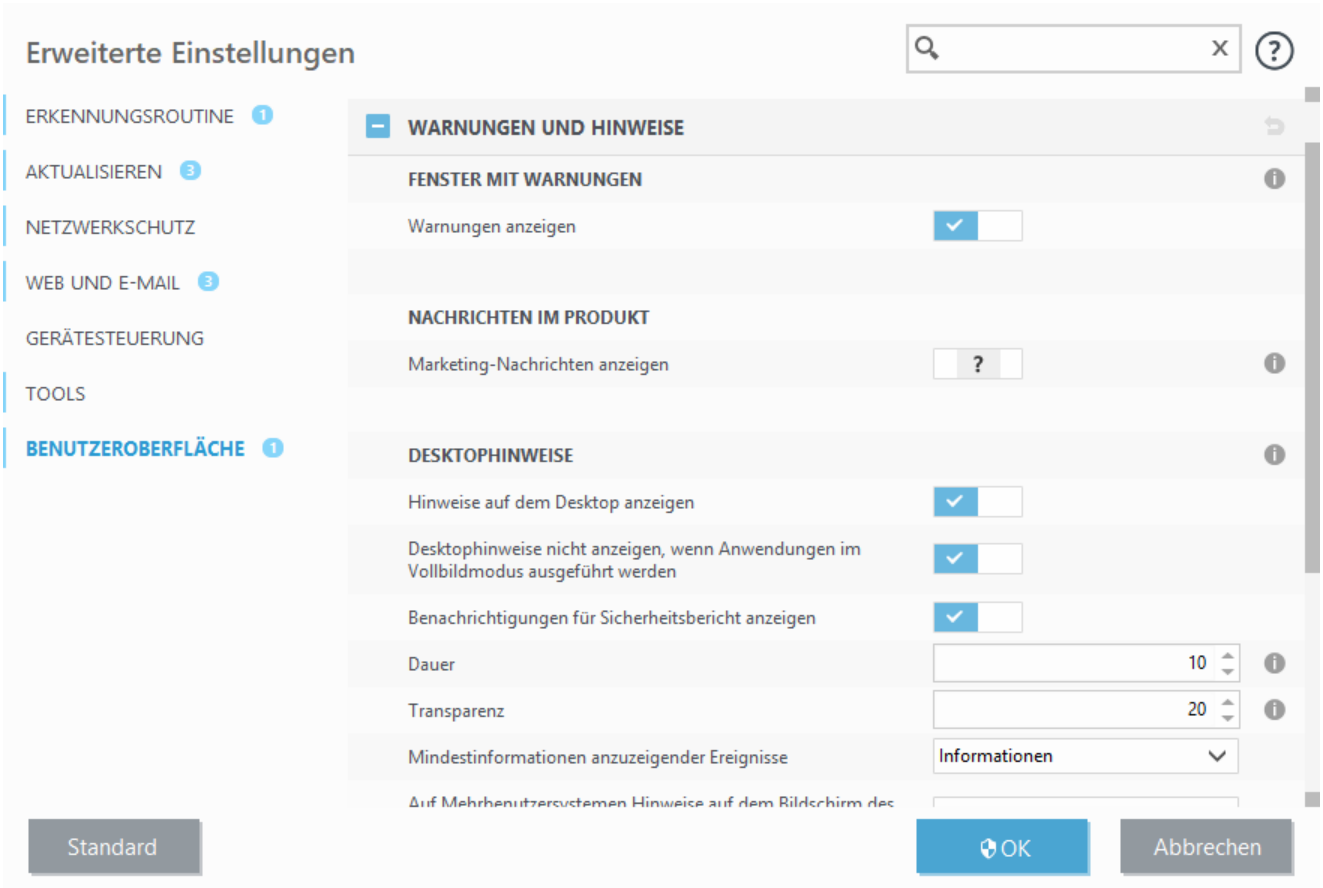
Status

Anwendungsstatus – Klicken Sie auf **Bearbeiten**, um die im ersten Bereich im Hauptmenü angezeigten Statusmeldungen zu verwalten (zu deaktivieren).



4.7.2 Warnungen und Hinweise

Im Bereich **Warnungen und Hinweise** unter **Benutzeroberfläche** können Sie festlegen, wie ESET Internet Security mit Bedrohungswarnungen und Systemmeldungen (z. B. über erfolgreiche Updates) umgehen soll. Außerdem können Sie Anzeigedauer und Transparenz von Meldungen in der Taskleiste festlegen (nur bei Systemen, die Meldungen in der Taskleiste unterstützen).



Fenster mit Warnungen

Bei Deaktivieren der Option **Warnungen anzeigen** werden keine Warnmeldungen mehr angezeigt. Diese Einstellung eignet sich nur in einigen speziellen Situationen. Für die meisten Benutzer empfiehlt es sich, die Standardeinstellung (aktiviert) beizubehalten.

Nachrichten im Produkt

Marketing-Nachrichten anzeigen – Die produktinternen Nachrichten wurden entwickelt, um Benutzer über Neuigkeiten und Ankündigungen von ESET zu informieren. Für den Versand von Marketingnachrichten ist eine Zustimmung des Benutzers erforderlich. Marketingnachrichten werden daher standardmäßig nicht verschickt (als Fragezeichen angezeigt). Aktivieren Sie diese Option, um Marketingnachrichten von ESET zu erhalten. Deaktivieren Sie die Option, wenn Sie nicht an Marketingmaterial von ESET interessiert sind.

Desktophinweise

Hinweise auf dem Desktop und Sprechblasen dienen ausschließlich zu Informationszwecken; Eingaben des Benutzers sind nicht erforderlich. Sie werden im Infobereich der Taskleiste rechts unten auf dem Bildschirm angezeigt. Zum Aktivieren von Desktophinweisen aktivieren Sie die Option **Hinweise auf dem Desktop anzeigen**.

Aktivieren Sie die Option **Desktophinweise nicht anzeigen, wenn Anwendungen im Vollbildmodus ausgeführt werden**, wenn keine nicht-interaktiven Hinweise angezeigt werden sollen. Weitere Optionen, wie Anzeigedauer und Transparenz, können unten geändert werden.

Benachrichtigungen für Sicherheitsberichte anzeigen – Hier können Sie Benachrichtigungen für Sicherheitsberichte aktivieren oder deaktivieren.

Aus der Liste **Mindestinformationen anzuzeigender Ereignisse** können Sie den niedrigsten Schweregrad der anzuzeigenden Warnungen und Benachrichtigungen wählen. Folgende Optionen stehen zur Verfügung:

- **Diagnose** – Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.
- **Informationen** - Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen** - Kritische Fehler und Warnungen werden protokolliert.
- **Fehler** – Fehler wie „Fehler beim Herunterladen der Datei“ und kritische Fehler werden aufgezeichnet.
- **Kritische Warnungen** – Nur kritische Warnungen (z. B. bei einem Fehler beim Start des Virenschutz-Moduls,integrierte Firewallusw.) werden protokolliert.

Der letzte Eintrag in diesem Bereich gibt Ihnen die Möglichkeit, die Ausgabe für Meldungen in einer Mehrbenutzerumgebung zu konfigurieren. Mit dem Feld **Auf Mehrbenutzersystemen Hinweise auf dem Bildschirm des folgenden Benutzers ausgeben** können Sie festlegen, bei welchem Benutzer Warnungen und Hinweise angezeigt werden, wenn mehrere Benutzer gleichzeitig angemeldet sind. Üblicherweise wird hier der System- oder Netzwerkadministrator gewählt. Besonders sinnvoll ist diese Option bei Terminalservern, vorausgesetzt alle Systemmeldungen werden an den Administrator gesendet.

Hinweisfenster

Wenn Popup-Fenster nach einer bestimmten Zeit automatisch geschlossen werden sollen, aktivieren Sie die Option **Fenster mit Hinweisen schließen**. Die Hinweise werden nach Ablauf der festgelegten Zeit automatisch geschlossen, sofern sie nicht bereits vom Benutzer geschlossen wurden.

Bestätigungsmeldungen – Zeigt eine Liste von Bestätigungsmeldungen an. Sie können auswählen, welche dieser Meldungen angezeigt werden sollen.

4.7.2.1 Erweiterte Einstellungen

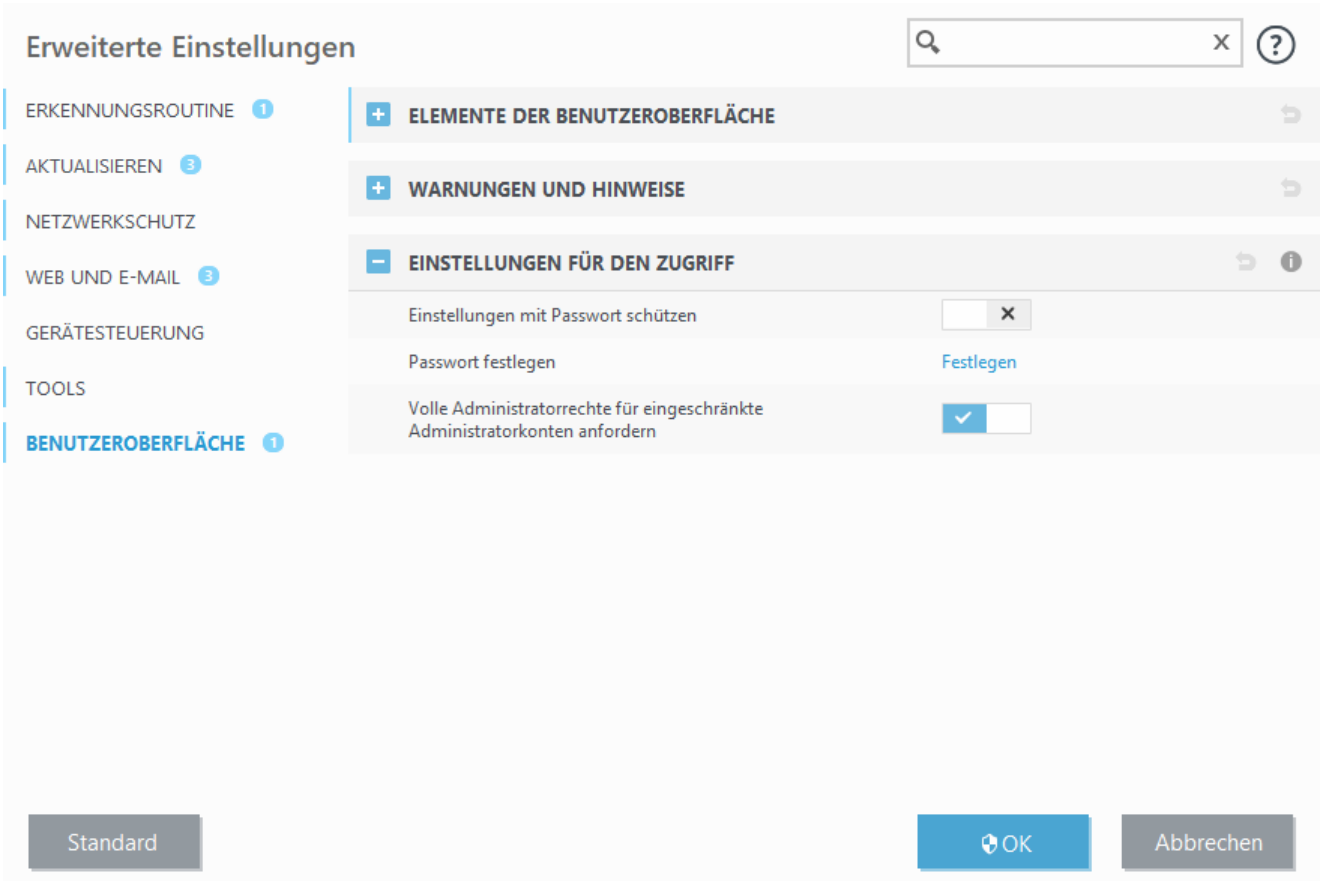
Aus der Liste **Mindestinformationen anzuzeigender Ereignisse** können Sie den niedrigsten Schweregrad der anzuzeigenden Warnungen und Hinweise wählen.

- **Diagnose** – Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.
- **Informationen** - Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen** - Kritische Fehler und Warnungen werden protokolliert.
- **Fehler** – Fehler wie *Fehler beim Herunterladen der Datei* und kritische Fehler werden aufgezeichnet.
- **Kritische Warnungen** – Nur kritische Warnungen (z. B. bei einem Fehler beim Start des Virenschutz-Moduls,, Firewallusw.) werden protokolliert.

Der letzte Eintrag in diesem Bereich gibt Ihnen die Möglichkeit, die Ausgabe für Meldungen in einer Mehrbenutzerumgebung zu konfigurieren. Mit dem Feld **Auf Mehrbenutzersystemen Hinweise auf dem Bildschirm des folgenden Benutzers ausgeben** können Sie festlegen, bei welchem Benutzer Warnungen und Hinweise angezeigt werden, wenn mehrere Benutzer gleichzeitig angemeldet sind. Üblicherweise wird hier der System- oder Netzwerkadministrator gewählt. Besonders sinnvoll ist diese Option bei Terminalservern, vorausgesetzt alle Systemmeldungen werden an den Administrator gesendet.

4.7.3 Einstellungen für den Zugriff

Die Einstellungen von ESET Internet Security sind ein wichtiger Bestandteil Ihrer Sicherheitsrichtlinien. Unbefugte Änderungen können die Stabilität und den Schutz Ihres Systems gefährden. Um unberechtigte Änderungen zu verhindern, können Sie die Einstellungen von ESET Internet Security mit einem Passwort schützen.



Einstellungen mit Passwort schützen – Legt fest, ob ein Passwortschutz angewendet wird. Durch Klicken hierauf wird das Passwortfenster geöffnet.

Klicken Sie auf **Festlegen**, um ein Passwort für den Schutz der Einstellungen festzulegen oder um es zu ändern.

HINWEIS
Wenn Sie versuchen, die geschützten erweiterten Einstellungen zu öffnen, wird ein Fenster zur Eingabe des Passworts angezeigt. Falls Sie Ihr Passwort vergessen oder verloren haben, klicken Sie unten auf **Passwort wiederherstellen** und geben Sie die E-Mail-Adresse ein, die Sie bei der Registrierung dieser Lizenz verwendet haben. Sie erhalten eine E-Mail von ESET mit dem Überprüfungscode und einer Anleitung zum Zurücksetzen Ihres Passworts. Weitere Informationen erhalten Sie hier.

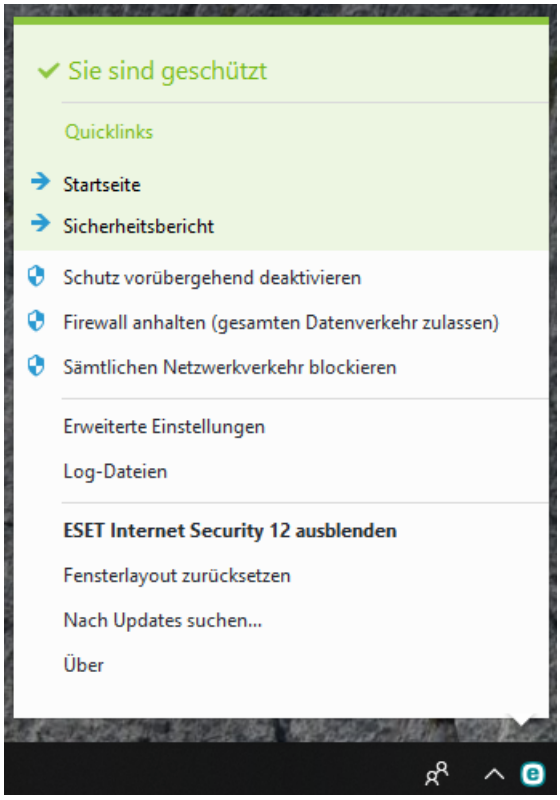
Volle Administratorrechte für eingeschränkte Administratorkonten anfordern - Wenn Sie diese Option aktivieren, werden Benutzer ohne Administratorrechte zur Eingabe eines Administratorbenutzernamens und -passworts aufgefordert, wenn sie bestimmte Systemeinstellungen ändern möchten (ähnlich der Benutzerkontensteuerung/UAC in Windows Vista und Windows 7). Dazu gehören das Deaktivieren von Schutzmodulen oder das Abschalten der Firewall. Auf Windows XP-Systemen, auf denen die Benutzerkontensteuerung (UAC) nicht ausgeführt wird, ist die Option **Administratorrechte bei Bedarf anfordern (Systeme ohne UAC-Support)** verfügbar.

Nur für Windows XP:

Administratorrechte anfordern (Systeme ohne UAC-Support) – Aktivieren Sie diese Option, damit ESET Internet Security zur Eingabe des Administratornachweises auffordert.

4.7.4 Programmmenü

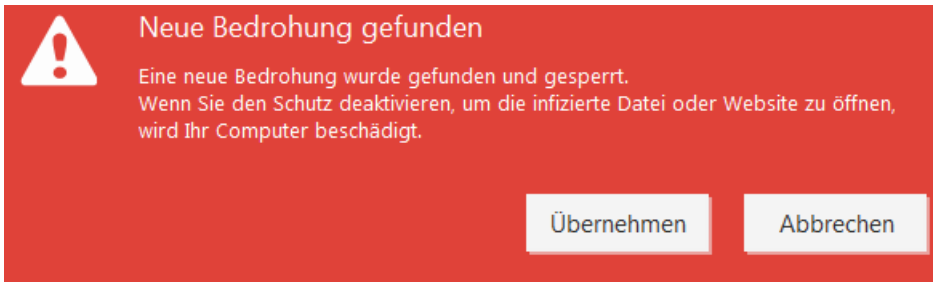
Einige der wichtigsten Einstellungsoptionen und -funktionen können durch Klicken mit der rechten Maustaste auf das Symbol im Infobereich der Taskleiste geöffnet werden.



Quicklinks - Zeigt die am häufigsten verwendeten Komponenten von ESET Internet Security an. Auf diese haben Sie direkt aus dem Programmmenü Zugriff.

Schutz vorübergehend deaktivieren - Zeigt ein Bestätigungsdialogfeld an, dass der Viren- und Spyware-Schutz deaktiviert wird, der Dateivorgänge sowie die Internet- und E-Mail-Kommunikation überwacht und Ihr System vor Angriffen schützt.

Über das Dropdown-Menü **Zeitraum** können Sie festlegen, wie lange der Viren- und Spyware-Schutz deaktiviert sein soll.



Firewall vorübergehend deaktivieren (allen Verkehr zulassen) - Schaltet die Firewall aus. Weitere Informationen finden Sie unter Netzwerk.

Sämtlichen Netzwerkverkehr blockieren – Blockiert den gesamten Netzwerkverkehr. Sie können den Netzwerkverkehr wieder aktivieren, indem Sie auf **Sämtlichen Netzwerkverkehr zulassen** klicken.

Erweiterte Einstellungen – Öffnet die Baumstruktur **Erweiterte Einstellungen**. Alternativ können die erweiterten Einstellungen auch mit der Taste F5 oder unter **Einstellungen** > **Erweiterte Einstellungen** geöffnet werden.

Log-Dateien - Log-Dateien enthalten Informationen zu wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen.

ESET Internet Security minimieren – Blendet das ESET Internet Security-Fenster auf dem Bildschirm aus.

Fensterlayout zurücksetzen - Stellt die standardmäßige Fenstergröße von ESET Internet Security und deren Standardposition auf dem Bildschirm wieder her.

Nach Updates suchen – Beginnt mit der Aktualisierung der Erkennungsroutine (bisher auch als „Signaturdatenbank“ bezeichnet), um den Schutz vor Schadcode zu gewährleisten.

Über - Zeigt Systeminformationen zur installierten Version von ESET Internet Security und zu den installierten Programmmodulen sowie das Ablaufdatum der Lizenz an. Hier finden Sie außerdem das Lizenzablaufdatum und Informationen zum Betriebssystem und zu den Systemressourcen.

5. Fortgeschrittene Benutzer

5.1 Profile

Der Profilmanager wird an zwei Stellen in ESET Internet Security verwendet: in den Bereichen **On-Demand-Prüfung** und **Update**.

Computerprüfung

Ihre bevorzugten Einstellungen können für zukünftige Prüfungen gespeichert werden. Wir empfehlen Ihnen, für jede regelmäßig durchgeführte Prüfung ein eigenes Profil zu erstellen (mit verschiedenen zu prüfenden Objekten, Prüfmethoden und anderen Parametern).

Um ein neues Profil zu erstellen, öffnen Sie die erweiterten Einstellungen (F5) und klicken auf **Erkennungsroutine** > **Schadsoftware-Prüfungen** > **On-Demand-Prüfung** > **Profilliste**. Im Fenster **Profil-Manager** finden Sie das Dropdownmenü **Ausgewähltes Profil** mit den vorhandenen Prüfprofilen und der Option zum Erstellen eines neuen Profils. Eine Beschreibung der einzelnen Prüfeinstellungen finden Sie im Abschnitt Einstellungen für ThreatSense. So können Sie ein Prüfprofil erstellen, das auf Ihre Anforderungen zugeschnitten ist.

HINWEIS
Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Option **Computerprüfung** eignet sich in gewissem Maße, aber Sie möchten keine laufzeitkomprimierten Dateien oder potenziell unsichere Anwendungen prüfen. Außerdem möchten Sie die Option **Immer versuchen, automatisch zu entfernen** anwenden. Geben Sie den Namen des neuen Profils im **Profilmanager** ein und klicken Sie auf **Hinzufügen**. Wählen Sie das neue Profil im Dropdownmenü **Ausgewähltes Profil** aus, passen Sie die restlichen Parameter nach Ihren Anforderungen an und klicken Sie auf **OK**, um das neue Profil zu speichern.

Update

Mit dem Profil-Editor unter „Einstellungen für Updates“ können Benutzer neue Update-Profile erstellen. Das Erstellen und Verwenden eigener benutzerdefinierter Profile (d. h. anderer Profile als das standardmäßige **Mein Profil**) ist nur sinnvoll, wenn Ihr Computer auf mehrere Verbindungsarten zurückgreifen muss, um eine Verbindung zu den Update-Servern herzustellen.

Nehmen wir als Beispiel einen Laptop, dessen Updates normalerweise über einen lokalen Server (einen sogenannten Mirror) im lokalen Netzwerk erfolgen, der aber seine Updates direkt von den ESET-Update-Servern bezieht, wenn keine Verbindung zum lokalen Netzwerk hergestellt werden kann (z. B. auf einer Geschäftsreise). Dieser Laptop kann zwei Profile haben: das erste Profil für die Verbindung zum lokalen Server, das zweite Profil für die Verbindung zu den ESET-Servern. Sobald diese Profile eingerichtet sind, wählen Sie **Tools** > **Taskplaner** und bearbeiten Sie die Update-Task-Einstellungen. Legen Sie eines der Profile als primäres Profil fest, das andere als sekundäres Profil.

Updateprofil - Das momentan verwendete Update-Profil. Um es zu ändern, wählen Sie ein Profil aus dem Dropdown-Menü aus.

Profilliste – Hier können Sie neue Update-Profile erstellen oder vorhanden Update-Profile entfernen.

5.2 Tastaturbefehle

Zur besseren Navigation in Ihrem ESET-Produkt stehen die folgenden Tastaturbefehle zur Verfügung:

F1	öffnet die Hilfeseiten
F5	öffnet die erweiterten Einstellungen
Pfeiltasten nach oben/unten	Navigation in der Software durch Elemente
-	reduziert den Knoten unter „Erweiterte Einstellungen“
TAB	bewegt den Cursor in einem Fenster
Esc	schließt das aktive Dialogfenster
Strg+U	Zeigt Informationen zur Lizenz an (Details für den Support)
Strg+R	Setzt Fenstergröße und Fensterposition des Produktfensters auf dem Bildschirm zurück.

5.3 Diagnose

Mit der Diagnose können Speicherabbilddateien von ESET-Prozessen erstellt werden (z. B. *ekrn*). Im Falle eines Absturzes einer Anwendung wird eine Speicherabbilddatei erstellt. Diese kann Entwicklern helfen, Fehler im Code zu finden und verschiedene Probleme von ESET Internet Security zu lösen. Klicken Sie auf das Dropdownmenü neben **Typ des Speicherabbilds** und wählen Sie eine der folgenden drei Optionen:

- Wählen Sie **Deaktivieren** (Standard), um dieses Feature zu deaktivieren.
- **Mini** – Protokolliert die kleinste Menge an Daten, die helfen könnten, die Ursache für den Absturz der Anwendung herauszufinden. Diese Art Dumpdatei kann nützlich sein, wenn beschränkter Speicherplatz verfügbar ist. Da jedoch die enthaltene Datenmenge ebenfalls begrenzt ist, könnten Fehler, die nicht direkt von dem Thread ausgelöst wurden, der zum Absturzzeitpunkt ausgeführt wurde, bei einer Dateianalyse unentdeckt bleiben.
- **Vollständig** – Zeichnet den gesamten Inhalt des Arbeitsspeichers auf, wenn die Anwendung unerwartet beendet wird. Ein vollständiges Speicherabbild kann auch Daten von Prozessen enthalten, die ausgeführt wurden, als das Speicherabbild geschrieben wurde.

Erweitertes Logging für den Netzwerk-Schutz aktivieren – Alle Daten, die die Firewall durchlaufen, im PCAP-Format aufzeichnen. Diese Aufzeichnungen helfen Entwicklern bei der Behebung von Problemen mit der Firewall.

Erweitertes Logging für Protokollfilterung aktivieren – Alle Daten, die die Protokollfilterung durchlaufen, im PCAP-Format aufzeichnen. Diese Aufzeichnungen helfen Entwicklern bei der Behebung von Problemen mit der Protokollfilterung.

Erweitertes Logging für Update-Modul aktivieren – Alle Ereignisse aufzeichnen, die während des Updates auftreten. Diese Aufzeichnungen helfen Entwicklern bei der Behebung von Problemen mit dem Update-Modul.

Erweitertes Logging für die Kindersicherung aktivieren – Alle Ereignisse aufzeichnen, die in der Kindersicherung auftreten. Diese Aufzeichnungen helfen Entwicklern bei der Behebung von Problemen mit der Kindersicherung.

Erweiterte Lizenzprotokollierung aktivieren – Sämtliche Kommunikation zwischen Produkten und Lizenzserver aufzeichnen.

Erweitertes Logging für Anti-Theft-Modul aktivieren – Alle aufgetretenen Ereignisse in Anti-Theft aufzeichnen, um Diagnose und Fehlerbehebung zu erleichtern.

Erweitertes Logging für Spamschutz-Modul aktivieren – Alle Ereignisse aufzeichnen, die bei der Spamschutz-Prüfung auftreten. Diese Aufzeichnungen helfen Entwicklern bei der Behebung von Problemen mit dem ESET Spamschutz-Modul.

Erweitertes Betriebssystem-Logging aktivieren – Zusätzliche Informationen zum Betriebssystem wie ausgeführte Prozesse, CPU-Aktivität und Laufwerksoperationen werden erfasst. Mit diesen Informationen können die

Entwickler Probleme im Zusammenhang mit dem ESET-Produkt auf Ihrem Betriebssystem verstehen und beheben (verfügbar für Windows 10).

Die Log-Dateien befinden sich unter:
C:\ProgramData\ESET\ESET Internet Security\Diagnostics unter Windows Vista und neueren Windows-Versionen und *C:\Dokumente und Einstellungen\Alle Benutzer\...* unter früheren Windows-Versionen.

Zielverzeichnis – Verzeichnis, in dem die Speicherabbilddatei während des Absturzes erstellt wird.

Diagnoseverzeichnis öffnen – Klicken Sie auf **Öffnen**, um dieses Verzeichnis in einem neuen Fenster von *Windows Explorer* zu öffnen.

Diagnoseabbild erstellen – Klicken Sie auf **Erstellen**, um ein Diagnoseabbild im **Zielverzeichnis** zu erstellen.

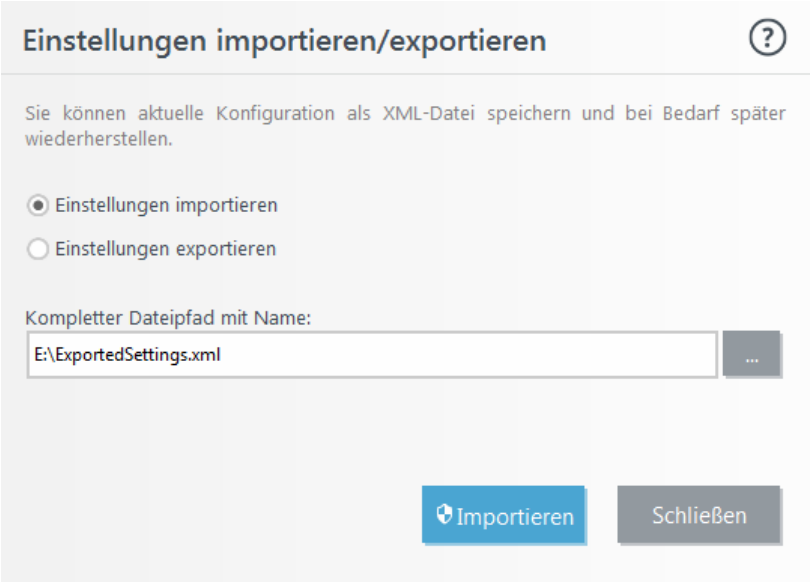
5.4 Einstellungen importieren/exportieren

Über das Menü **Einstellungen** können Sie die XML-Datei mit Ihrer benutzerdefinierten Konfiguration von ESET Internet Security importieren und exportieren.

Das Importieren und Exportieren der Konfigurationsdatei ist hilfreich, wenn Sie zur späteren Verwendung eine Sicherung der aktuellen Konfiguration von ESET Internet Security erstellen möchten. Die Exportfunktion bietet sich auch für Benutzer an, die ihre bevorzugte Konfiguration auf mehreren Systemen verwenden möchten. Um die Einstellungen zu übernehmen, wird einfach eine Datei mit der Endung *.xml* importiert.

Die Schritte zum Importieren einer Konfiguration sind sehr einfach. Klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Einstellungen importieren/exportieren**, und wählen Sie die Option **Einstellungen importieren**. Geben Sie den Namen der Konfigurationsdatei ein oder klicken Sie auf **Durchsuchen**, um die Konfigurationsdatei zu suchen, die Sie importieren möchten.

Der Export einer Konfiguration verläuft sehr ähnlich. Klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Einstellungen importieren/exportieren**. Wählen Sie **Einstellungen exportieren** und geben Sie den Namen der Konfigurationsdatei (z. B. *export.xml*) ein. Suchen Sie mithilfe des Browsers einen Speicherort auf Ihrem Computer aus, an dem Sie die Konfigurationsdatei speichern möchten.



HINWEIS
Beim Exportieren der Einstellungen kann ein Fehler auftreten, wenn Sie über unzureichende Berechtigungen für das angegebene Verzeichnis verfügen.

5.5 ESET SysInspector

5.5.1 Einführung in ESET SysInspector

ESET SysInspector ist eine Diagnoseanwendung, mit der Sie umfassende Informationen zu einem bestimmten Computer anzeigen können, etwa zu installierten Treibern und Anwendungen, Netzwerkverbindungen oder wichtigen Registrierungseinträgen. Diese Angaben helfen Ihnen bei der Problemdiagnose, wenn sich ein System nicht wie erwartet verhält - ob dies nun an einer Inkompatibilität (Software/Hardware) oder an einer Malware-Infektion liegt.

Sie können auf zwei verschiedene Arten auf ESET SysInspector zugreifen: entweder über die in ESET Security-Lösungen integrierte Version oder indem Sie eine kostenlose eigenständige Version (SysInspector.exe) von der ESET-Website herunterladen. Beide Versionen bieten die gleichen Funktionen und Bedienelemente. Der einzige Unterschied besteht in der Art und Weise, wie die Ausgaben verwaltet werden. Sowohl in der eigenständigen als auch in der integrierten Version können Sie System-Snapshots in eine *.xml*-Datei exportieren und auf einem Datenträger speichern. Mit der integrierten Version können Sie die System-Snapshots jedoch direkt über **Extras** > **ESET SysInspector** speichern (außer in ESET Remote Administrator).

Warten Sie einen Moment, während ESET SysInspector den Computer prüft. Die Dauer der Prüfung variiert je nach Hardwarekonfiguration, Betriebssystem und Anzahl der auf dem Computer installierten Anwendungen und kann zwischen 10 Sekunden und mehreren Minuten liegen.

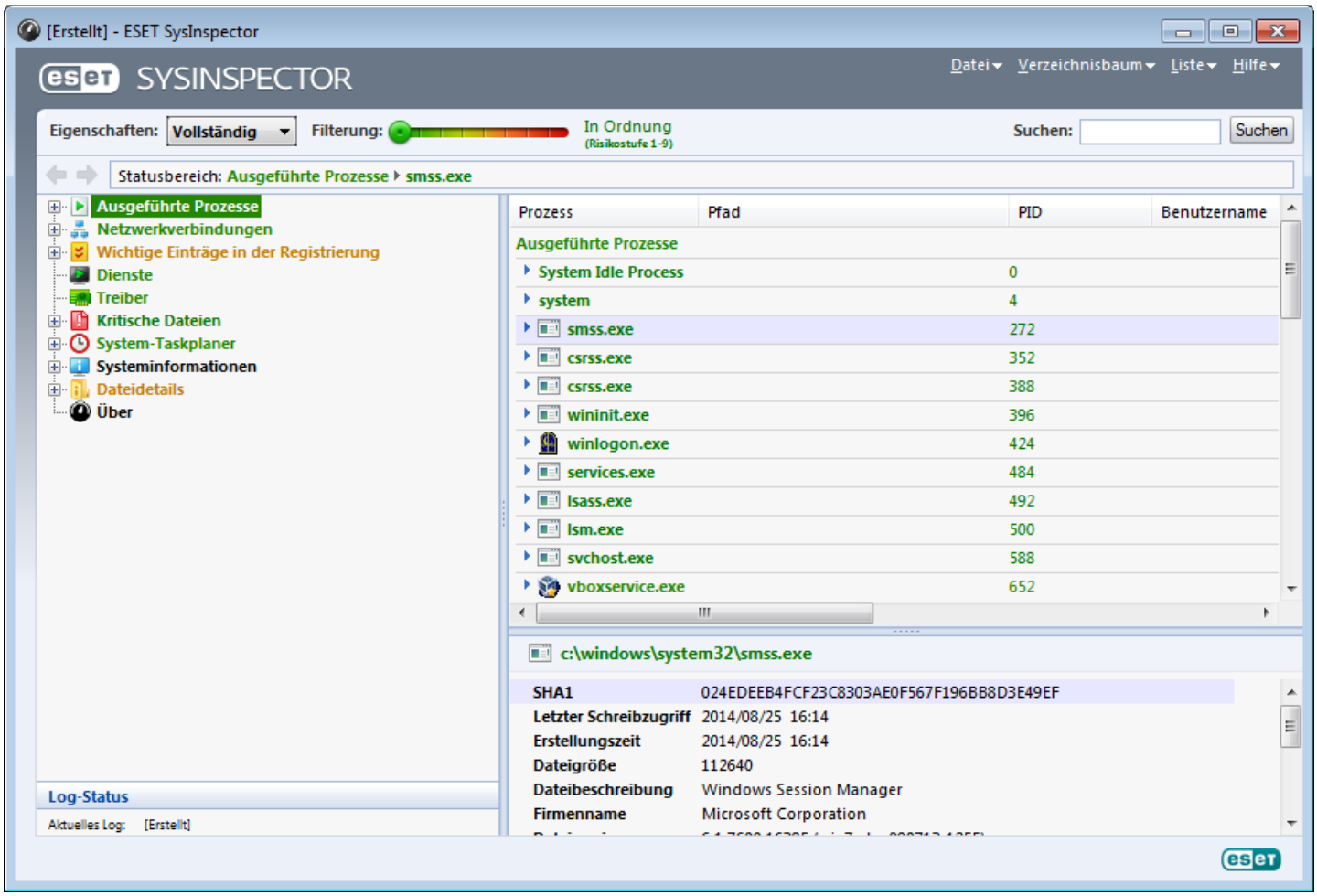
5.5.1.1 Starten von ESET SysInspector

Zum Starten von ESET SysInspector führen Sie einfach die von der ESET-Website heruntergeladene Programmdatei *SysInspector.exe* aus.

Warten Sie, während die Anwendung das System überprüft. Dies kann einige Minuten in Anspruch nehmen.

5.5.2 Benutzeroberfläche und Bedienung

Zur besseren Übersicht ist das Hauptprogrammfenster in vier größere Bereiche unterteilt: die Steuerelemente des Programms oben, das Navigationsfenster links, das Beschreibungsfenster rechts und das Detailfenster unten im Hauptfenster. Der Bereich „Log-Status“ zeigt die grundlegenden Eigenschaften eines Logs (verwendeter Filter, Filtertyp, Ergebnis eines Vergleichs, usw.).



5.5.2.1 Menüs und Bedienelemente

Dieser Abschnitt beschreibt die Menüs und sonstigen Bedienelemente in ESET SysInspector.

Datei

Durch Klicken auf **Datei** können Sie die aktuellen Systeminformationen zur späteren Untersuchung speichern oder ein zuvor gespeichertes Log wieder öffnen. Falls ein Log weitergegeben werden soll, sollten Sie es über die Funktion **Zum Senden geeignet** erstellen. Sicherheitsrelevante Daten (Name und Berechtigungen des aktuellen Benutzers, Computername, Domänenname, Umgebungsvariablen usw.) werden dann nicht in das Log aufgenommen.

HINWEIS: Gespeicherte ESET SysInspector-Logs können Sie schnell wieder öffnen, indem Sie sie auf das Hauptprogrammfenster ziehen und dort ablegen.

Baum

Hiermit können Sie alle Knoten erweitern oder schließen sowie die ausgewählten Bereiche in ein Dienste-Skript exportieren.

Liste

Dieses Menü enthält Funktionen zur einfacheren Navigation im Programm sowie eine Reihe von Zusatzfunktionen, etwa für die Online-Informationssuche.

Hilfe

Über dieses Menü finden Sie Informationen zur Anwendung und ihren Funktionen.

Detail

Dieses Menü beeinflusst die Informationen, die im Hauptprogrammfenster dargestellt werden und vereinfacht somit ihre Verwendung. Im Modus „Einfach“ werden die Informationen angezeigt, die Sie benötigen, um gängige Probleme mit dem System zu lösen. Im Modus „Mittel“ zeigt das Programm außerdem einige weniger häufig genutzte Informationen an. Im Modus „Vollständig“ zeigt ESET SysInspector alle Informationen an, die zum Beheben spezifischer Probleme erforderlich sind.

Filterung

Mit der Filterfunktion können Sie schnell verdächtige Dateien oder Registrierungseinträge auf Ihrem System finden. Durch Verschieben des Schiebereglers legen Sie fest, ab welcher Risikostufe Objekte angezeigt werden. Wenn der Schieberegler ganz links steht (Risikostufe 1), werden alle Objekte angezeigt. Steht der Schieberegler hingegen weiter rechts, werden alle Objekte unterhalb der eingestellten Risikostufe ausgeblendet, sodass Sie nur die Objekte ab einer bestimmten Risikostufe sehen. Wenn der Schieberegler ganz rechts steht, sehen Sie nur solche Objekte, die bekanntermaßen schädlich sind.

Alle Objekte der Risikostufen 6 bis 9 stellen unter Umständen ein Sicherheitsrisiko dar. Falls ESET SysInspector ein solches Objekt auf Ihrem System findet und Sie keine ESET Security-Lösung einsetzen, sollten Sie Ihr System mit ESET Online Scanner prüfen. ESET Online Scanner ist ein kostenloser Service.

HINWEIS: Um schnell herauszufinden, welche Risikostufe ein bestimmtes Objekt hat, vergleichen Sie einfach seine Farbe mit den Farben auf dem Schieberegler für die Risikostufe.

Vergleichsfunktion

Beim Vergleich zweier Log-Dateien können Sie angeben, ob alle Elemente, nur hinzugefügte Elemente, nur entfernte Elemente oder nur ersetzte Elemente angezeigt werden sollen.

Suchen

Mit der Suche können Sie ein bestimmtes Objekt schnell über seinen Namen (oder einen Teil des Namens) finden. Die Ergebnisse der Suchanfrage werden im Beschreibungsfenster angezeigt.

Zurück

Über die Schaltflächen mit den Pfeilen nach links und rechts können Sie zwischen den bisherigen Anzeigeinhalten des Beschreibungsbereichs wechseln. Anstatt auf "Vor" und "Zurück" zu klicken, können Sie auch die Leertaste bzw. Rücktaste (Backspace) verwenden.

Statusbereich

Hier sehen Sie, welcher Knoten im Navigationsfenster gerade ausgewählt ist.

Wichtig: Rot hervorgehobene Objekte sind unbekannt und werden daher als potenziell gefährlich markiert. Dies bedeutet jedoch nicht automatisch, dass Sie die Datei gefahrlos löschen können. Vergewissern Sie sich vor dem Löschen auf jeden Fall, dass die Datei tatsächlich überflüssig ist bzw. dass von ihr eine Gefahr ausgeht.

5.5.2.2 Navigation in ESET SysInspector

In ESET SysInspector gliedern sich die unterschiedlichen Systeminformationen in eine Reihe von Hauptabschnitten, die so genannten „Knoten“. Wenn zu einem Knoten weitere Details vorhanden sind, können Sie ihn erweitern (ausklappen), um seine Unterknoten anzuzeigen. Um einen Knoten zu öffnen oder zu reduzieren, doppelklicken Sie auf den Knotennamen oder klicken Sie neben dem Knotennamen auf ⊞ bzw. ⊟. Soweit vorhanden, werden im Beschreibungsfenster Detailinhalte zum gerade im Navigationsbereich ausgewählten Knoten angezeigt. Diese Einträge im Beschreibungsfenster können Sie dann wiederum auswählen, um (soweit vorhanden) im Detailfenster weitere Detailinformationen dazu anzuzeigen.

Im Folgenden sind die Hauptknoten im Navigationsfenster sowie die dazugehörigen Informationen in den Beschreibungs- und Detailfenstern beschrieben.

Ausgeführte Prozesse

Dieser Knoten enthält Informationen zu den Anwendungen und Prozessen, die zum Zeitpunkt der Log-Erstellung ausgeführt wurden. Das Beschreibungsfenster zeigt weitere Details zu jedem Prozess, etwa die verwendeten dynamischen Bibliotheken samt Speicherort, den Namen des Programmherstellers, die Risikostufe der Dateien usw.

Wenn Sie einen Eintrag im Beschreibungsfenster auswählen, erscheinen im Detailfenster weitere Informationen wie z. B. die Größe oder der Hashwert der betreffenden Datei.

HINWEIS: Ein Betriebssystem enthält verschiedene durchgängig laufende Kernelkomponenten, die grundlegende und wichtige Funktionen für andere Benutzeranwendungen bereitstellen. In bestimmten Fällen wird für solche Prozesse in ESET SysInspector ein Dateipfad angezeigt, der mit \??\ beginnt. Dies bedeutet, dass die Security-Software vor dem Start für diese Prozesse optimiert wird; sie stellen kein Risiko für die Systemsicherheit dar.

Netzwerkverbindungen

Wenn Sie im Navigationsbereich ein Protokoll (TCP oder UDP) auswählen, erscheint im Beschreibungsfenster eine Liste der Prozesse und Anwendungen, die über das betreffende Protokoll im Netzwerk kommunizieren, samt der jeweiligen Remoteadresse. Außerdem können Sie hier die IP-Adressen der DNS-Server überprüfen.

Wenn Sie einen Eintrag im Beschreibungsfenster auswählen, erscheinen im Detailfenster weitere Informationen wie z. B. die Größe oder der Hashwert der betreffenden Datei.

Wichtige Einträge in der Registrierung

Hier finden Sie eine Liste ausgewählter Registrierungseinträge, die oft im Zusammenhang mit Systemproblemen stehen. Dies betrifft beispielsweise die Registrierungseinträge für Autostart-Programme, Browser-Hilfsobjekte (BHO) usw.

Im Beschreibungsfenster werden die mit dem jeweiligen Registrierungseintrag verbundenen Dateien angezeigt. Im Detailfenster finden Sie dazu weitere Informationen.

Dienste

Bei diesem Knoten enthält das Beschreibungsfenster eine Liste der Dateien, die als Windows-Dienste registriert sind. Im Detailfenster sind die Ausführungsart des Dienstes sowie weitere Informationen zur Datei angegeben.

Treiber

Liste der im System installierten Treiber

Kritische Dateien

Unter diesem Knoten können Sie sich im Beschreibungsfenster den Inhalt wichtiger Konfigurationsdateien von Microsoft Windows anzeigen lassen.

System-Tasks im Taskplaner

Enthält eine Liste der Tasks, die vom Windows-Taskplaner zu einer bestimmten Zeit/mit einem bestimmten Intervall ausgelöst werden.

Systeminformationen

Hier finden Sie ausführliche Informationen zu Hardware und Software, den gesetzten Umgebungsvariablen, den Benutzerberechtigungen und Systemereignis-Logs.

Dateidetails

Dieser Knoten enthält eine Liste der wichtigen Systemdateien sowie der Dateien im Ordner „Programme“. Im Beschreibungs- und Detailfenster finden Sie weitere Informationen zu den einzelnen Dateien.

Über

Enthält Informationen zur Version von ESET SysInspector und eine Liste der Programmmodule.

5.5.2.2.1 Tastaturbefehle

Für die Arbeit mit ESET SysInspector stehen Ihnen die folgenden Tastaturbefehle zur Verfügung:

Datei

Strg+O	vorhandenes Log öffnen
Strg+S	erstelltes Log speichern

Erstellen

Strg+G	Standard-Snapshot des Computers erstellen
Strg+H	Standard-Snapshot des Computers erstellen und sicherheitsrelevante Informationen im Log aufzeichnen

Filterung

1, O	Risikostufe „In Ordnung“ - Objekte mit Risikostufe 1-9 anzeigen
2	Risikostufe „In Ordnung“ - Objekte mit Risikostufe 2-9 anzeigen
3	Risikostufe „In Ordnung“ - Objekte mit Risikostufe 3-9 anzeigen
4, U	Risikostufe „Unbekannt“ - Objekte mit Risikostufe 4-9 anzeigen
5	Risikostufe „Unbekannt“ - Objekte mit Risikostufe 5-9 anzeigen
6	Risikostufe „Unbekannt“ - Objekte mit Risikostufe 6-9 anzeigen
7, B	Risikostufe „Risikoreich“ - Objekte mit Risikostufe 7-9 anzeigen
8	Risikostufe „Risikoreich“ - Objekte mit Risikostufe 8-9 anzeigen
9	Risikostufe „Risikoreich“ - Objekte mit Risikostufe 9 anzeigen
-	Risikostufe vermindern
+	Risikostufe erhöhen
Strg+9	Filtermodus: Objekte ab der jeweiligen Risikostufe anzeigen
Strg+0	Filtermodus: nur Objekte mit der jeweiligen Risikostufe anzeigen

Anzeigen

Strg+5	Anzeige nach Hersteller - alle Hersteller
Strg+6	Anzeige nach Hersteller - nur Microsoft
Strg+7	Anzeige nach Hersteller - alle anderen Hersteller
Strg+3	Einstellung „Eigenschaften“ auf „Vollständig“ setzen
Strg+2	Einstellung „Eigenschaften“ auf „Mittel“ setzen
Strg+1	Einstellung „Eigenschaften“ auf „Einfach“ setzen
Rücktaste	einen Schritt zurück
Leertaste	einen Schritt weiter
Strg+W	Knoten erweitern (ausklappen)

Strg+Q	Knoten verkleinern (einklappen)

Diverse Befehle

Strg+T	zur ursprünglichen Position eines in den Suchergebnissen ausgewählten Elements springen
Strg+P	grundlegende Angaben zu einem Element anzeigen
Strg+A	vollständige Angaben zu einem Element anzeigen
Strg+C	Baumpfad des aktuellen Elements kopieren
Strg+X	Elemente kopieren
Strg+B	im Internet nach Informationen zur ausgewählten Datei suchen
Strg+L	Speicherordner der ausgewählten Datei öffnen
Strg+R	betreffenden Eintrag im Registrierungseditor öffnen
Strg+Z	Dateipfad kopieren (wenn sich das Element auf eine Datei bezieht)
Strg+F	zum Suchfeld wechseln
Strg+D	Suchergebnisse schließen
Strg+E	Dienste-Skript ausführen

Vergleich

Strg+Alt+O	ursprüngliches Log/Vergleichs-Log öffnen
Strg+Alt+R	Vergleich schließen
Strg+Alt+1	alle Elemente anzeigen
Strg+Alt+2	nur hinzugefügte Elemente anzeigen (Elemente, die nur im aktuellen Log vorhanden sind)
Strg+Alt+3	nur gelöschte Elemente anzeigen (Elemente, die nur im ursprünglichen Log vorhanden sind)
Strg+Alt+4	nur ersetzte Elemente (inkl. Dateien) anzeigen
Strg+Alt+5	nur Unterschiede zwischen den Logs anzeigen
Strg+Alt+C	Vergleich anzeigen
Strg+Alt+N	aktuelles Log anzeigen
Strg+Alt+P	ursprüngliches Log öffnen

Sonstige

F1	Hilfe anzeigen
Alt+F4	Programm beenden
Alt+Umschalt +F4	Programm ohne Rückfrage beenden
Strg+I	Log-Statistik anzeigen

5.5.2.3 Vergleichsfunktion

Mit der Funktion „Vergleichen“ können Sie zwei vorhandene Logs vergleichen. Als Ergebnis werden die Unterschiede zurückgegeben, also die Einträge, die nicht in beiden Logs enthalten sind. Diese Funktion ist geeignet, um Änderungen am System zu erkennen, und hilft so, Schadprogramme zu entdecken.

Nach dem Start erzeugt die Anwendung ein neues Log, das in einem neuen Fenster angezeigt wird. Klicken Sie auf **Datei** > **Log speichern**, um ein Log als Datei zu speichern. Gespeicherte Log-Dateien können Sie später wieder öffnen, um sie einzusehen. Klicken Sie auf **Datei** > **Log öffnen**, um ein vorhandenes Log zu öffnen. Im Hauptfenster von ESET SysInspector wird immer nur jeweils ein Log angezeigt.

Mit der Vergleichsfunktion können Sie das momentan aktive Log und ein in einer Datei gespeichertes Log vergleichen. Klicken Sie auf **Datei** > **Logs vergleichen** und dann auf **Datei auswählen**, um Logs zu vergleichen. Das ausgewählte Log wird nun mit dem aktiven (im Programmfenster angezeigten) Log verglichen. Das Vergleichs-Log zeigt nur die Unterschiede zwischen den beiden Logs an.

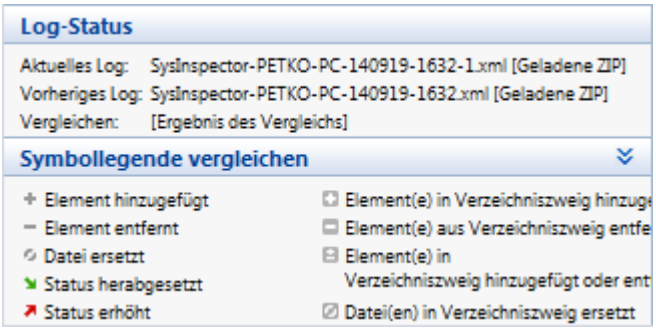
HINWEIS: Wenn Sie nach dem Vergleich zweier Logs auf **Datei** > **Log speichern** klicken und das Ergebnis als ZIP-Datei speichern, werden beide Log-Dateien gespeichert. Wenn Sie die so entstandene Datei später öffnen, werden die enthaltenen Logs automatisch verglichen.

Neben den einzelnen Einträgen zeigt ESET SysInspector Symbole an, die angeben, um was für eine Art von Unterschied es sich handelt.

Die einzelnen Symbole haben die folgende Bedeutung:

- + neuer Wert, nicht im vorherigen Log enthalten
- betreffender Zweig der Baumstruktur enthält neue Werte
- – gelöschter Wert, nur im vorherigen Log enthalten
- betreffender Zweig der Baumstruktur enthält gelöschte Werte
- Wert/Datei wurde geändert
- betreffender Zweig der Baumstruktur enthält geänderte Werte/Dateien
- Risiko ist gesunken (war im vorherigen Log höher)
- Risiko ist gestiegen (war im vorherigen Log niedriger)

Die Bedeutung aller Symbole sowie die Namen der verglichenen Logs werden auch in der Legende links unten im Programmfenster angezeigt.



Sie können jedes Vergleichs-Log in einer Datei speichern und später wieder öffnen.

Beispiel

Erstellen und speichern Sie ein Log mit einem ersten Stand der Systeminformationen in einer Datei namens „alt.xml“. Nehmen Sie einige Änderungen am System vor und öffnen Sie dann ESET SysInspector, um ein neues Log zu erstellen. Speichern Sie dieses unter dem Namen *neu.xml*.

Um die Unterschiede zwischen diesen beiden Logs zu sehen, klicken Sie auf **Datei** > **Logs vergleichen**. Das Programm erstellt so ein Vergleichs-Log, das die Unterschiede zwischen den beiden Logs zeigt.

Dasselbe Ergebnis erzielen Sie bei einem Aufruf über die Befehlszeile mit den folgenden Parametern:

SysIsnpector.exe neu.xml alt.xml

5.5.3 Befehlszeilenparameter

Mit ESET SysInspector können Sie auch von der Befehlszeile aus Berichte erzeugen. Hierzu stehen die folgenden Parameter zur Verfügung:

/gen	Log direkt über die Kommandozeile erstellen, ohne die Benutzeroberfläche zu starten
/privacy	Log ohne vertrauliche Daten erstellen
/zip	Log in komprimiertem Zip-Archiv speichern
/silent	Fortschrittsanzeige unterdrücken, wenn Log von der Kommandozeile aus erstellt wird
/blank	ESET-SysInspector starten, ohne Log zu erstellen/laden

Beispiele

Verwendung:
`Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]`

Spezielles Log direkt im Browser öffnen: *SysInspector.exe .\clientlog.xml*
Log über die Kommandozeile erstellen: *SysInspector.exe /gen=.\mynewlog.xml*
Log ohne vertrauliche Informationen direkt in einer komprimierten Datei erstellen: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Zwei Log-Dateien vergleichen und Unterschiede durchsuchen: *SysInspector.exe new.xml old.xml*

HINWEIS: Datei- und Ordnernamen mit Leerzeichen sollten in Hochkommata gesetzt werden.

5.5.4 Dienste-Skript

Mit dem Dienste-Skript können Benutzer von ESET SysInspector unerwünschte Objekte auf einfache Weise aus dem System entfernen.

Über ein Dienste-Skript können Sie das gesamte ESET SysInspector -Log oder ausgewählte Teile davon exportieren. Nach dem Exportieren können Sie unerwünschte Objekte zum Löschen markieren. Anschließend können Sie das so bearbeitete Log ausführen, um die markierten Objekte zu löschen.

Dienste-Skripte sind für erfahrene Benutzer gedacht, die sich gut mit der Diagnose und Behebung von Systemproblemen auskennen. Ungeeignete Änderungen können Probleme im Betriebssystem verursachen.

Beispiel

Wenn Sie vermuten, dass Ihr Computer mit einem Virus infiziert ist, den Ihr Virenschutzprogramm nicht erkennt, gehen Sie wie folgt vor:

1. Führen Sie ESET SysInspector aus, um einen neuen System-Snapshot zu erstellen.
2. Wählen Sie das erste Objekt im Navigationsbereich auf der linken Seite aus, halten Sie die Umschalttaste gedrückt und klicken Sie auf das letzte Objekt im Navigationsbereich, um den gesamten Inhalt zu markieren.
3. Klicken Sie mit der rechten Maustaste auf die ausgewählten Objekte und wählen Sie **Ausgewählte Bereiche in das Entfernen-Skript exportieren** aus.
4. Die ausgewählten Objekte werden in ein neues Log exportiert.
5. Sie kommen nun zum wichtigsten Schritt des gesamten Vorgangs: Öffnen Sie das neue Log und ändern Sie das Zeichen „-“ vor allen Objekten, die gelöscht werden sollen, in „+“. Achten Sie darauf, keine wichtigen Systemdateien/-objekte zu markieren
6. Öffnen Sie ESET SysInspector, klicken Sie auf **Datei** > **Dienste-Skript ausführen** und geben Sie den Pfad zum Skript ein.
7. Klicken Sie auf **OK**, um das Skript auszuführen.

5.5.4.1 Erstellen eines Dienste-Skripts

Um ein Skript zu erstellen, klicken Sie im ESET SysInspector -Hauptfenster mit der rechten Maustaste auf ein beliebiges Element im Navigationsbereich auf der linken Seite des Fensters. Wählen Sie im Kontextmenü entweder **Alle Bereiche in das Dienste-Skript exportieren** oder **Ausgewählte Bereiche in das Dienste-Skript exportieren** aus.

HINWEIS: Wenn Sie gerade zwei Logs miteinander vergleichen, ist kein Export in ein Dienste-Skript möglich.

5.5.4.2 Aufbau des Dienste-Skripts

In der ersten Zeile des Skriptheaders finden Sie Angaben zur Engine-Version (ev), zur Version der Benutzeroberfläche (gv) sowie zur Log-Version (lv). Über diese Angaben können Sie mögliche Änderungen an der XML-Datei verfolgen, über die das Skript erzeugt wird, und dadurch Inkonsistenzen bei der Ausführung vermeiden. An diesem Teil des Skripts sollten keine Änderungen vorgenommen werden.

Der Rest der Datei gliedert sich in mehrere Abschnitte, deren Einträge Sie bearbeiten können, um festzulegen, welche davon bei der Ausführung verarbeitet werden sollen. Um einen Eintrag für die Verarbeitung zu markieren, ersetzen Sie das davor stehende Zeichen „-“ durch ein „+“. Die einzelnen Skriptabschnitte sind jeweils durch eine Leerzeile voneinander getrennt. Jeder Abschnitt hat eine Nummer und eine Überschrift.

01) Running processes (Ausgeführte Prozesse)

Dieser Abschnitt enthält eine Liste mit allen Prozessen, die auf dem System ausgeführt werden. Für jeden Prozess ist der UNC-Pfad gefolgt vom CRC16-Hashwert in Sternchen (*) aufgeführt.

Beispiel:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In diesem Beispiel wurde der Prozess „module32.exe“ ausgewählt, indem er mit dem Zeichen „+“ markiert wurde. Beim Ausführen des Skripts wird dieser Prozess beendet.

02) Loaded modules (Geladene Module)

Dieser Abschnitt enthält eine Liste der momentan verwendeten Systemmodule.

Beispiel:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In diesem Beispiel wurde das Modul „khbekhb.dll“ mit einem „+“ markiert. Beim Ausführen des Skripts werden alle Prozesse, die dieses Modul verwenden, ermittelt und anschließend beendet.

03) TCP connections (TCP-Verbindungen)

Dieser Abschnitt enthält Informationen zu den aktiven TCP-Verbindungen.

Beispiel:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445
(microsoft-ds), owner: System
[...]
```

Beim Ausführen des Skripts wird der Eigentümer des Sockets der markierten TCP-Verbindungen ermittelt. Anschließend wird der Socket beendet, wodurch Systemressourcen wieder frei werden.

04) UDP endpoints (UDP-Endpunkte)

Dieser Abschnitt enthält Informationen zu den aktiven UDP-Endpunkten.

Beispiel:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Beim Ausführen des Skripts wird der Eigentümer des Sockets der markierten UDP-Verbindungen ermittelt. Anschließend wird der Socket beendet.

05) DNS server entries (DNS-Servereinträge)

Dieser Abschnitt enthält Angaben zur aktuellen DNS-Serverkonfiguration.

Beispiel:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Beim Ausführen des Skripts werden die markierten DNS-Servereinträge entfernt.

06) Important registry entries (Wichtige Registrierungseinträge)

Dieser Abschnitt enthält Informationen zu wichtigen Registrierungseinträgen.

Beispiel:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:
\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Beim Ausführen des Skripts werden die markierten Einträge gelöscht, auf eine Länge von 0 Byte abgeschnitten oder auf die Standardwerte zurückgesetzt. Was davon im Einzelfall geschieht, hängt von der Art des Eintrags und dem Wert des Schlüssels ab.

07) Services (Dienste)

Dieser Abschnitt enthält eine Liste der auf dem System registrierten Dienste.

Beispiel:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe,
state: Running, startup: Automatic
- Name: Application Experience Service, exe path: c:
\windows\system32\aelupsvc.dll, state: Running, startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:
\windows\system32\alg.exe, state: Stopped, startup: Manual
[...]
```

Beim Ausführen des Skripts werden die markierten Dienste samt davon abhängiger Dienste beendet und deinstalliert.

08) Drivers (Treiber)

Dieser Abschnitt enthält eine Liste der installierten Treiber.

Beispiel:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys,
state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:
\windows\system32\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Beim Ausführen des Skripts werden die ausgewählten Treiber gestoppt. Beachten Sie, dass bestimmte Treiber ein Beenden nicht zulassen.

09) Critical files (Kritische Dateien)

Dieser Abschnitt enthält Angaben zu Dateien, die für eine korrekte Funktion des Betriebssystems wesentlich sind.

Beispiel:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Die ausgewählten Objekte werden entweder gelöscht oder auf ihren ursprünglichen Wert zurückgesetzt.

10) Geplante Tasks

Dieser Abschnitt enthält Informationen zu geplanten Tasks.

Beispiel:

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:
\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.5.4.3 Ausführen von Dienste-Skripten

Markieren Sie die gewünschten Elemente, speichern und schließen Sie das Skript. Führen Sie das fertige Skript dann direkt aus dem ESET SysInspector -Hauptfenster aus, indem Sie im Menü „Datei“ auf **Dienste-Skript ausführen** klicken. Beim Öffnen eines Skripts wird die folgende Bestätigungsabfrage angezeigt: **Möchten Sie das Dienste-Skript "%Scriptname%" wirklich ausführen?** Nachdem Sie diese Abfrage bestätigt haben, erscheint unter Umständen eine weitere Warnmeldung, dass das auszuführende Dienste-Skript nicht signiert wurde. Klicken Sie auf **Ausführen**, um das Skript auszuführen.

Ein Dialogfenster wird angezeigt, das die Ausführung des Skripts bestätigt.

Wenn das Skript nur teilweise verarbeitet werden konnte, wird ein Dialogfenster mit der folgenden Meldung angezeigt: **Das Dienste-Skript wurde teilweise ausgeführt. Möchten Sie den Fehlerbericht anzeigen?** Wählen Sie **Ja**, um einen ausführlichen Fehlerbericht mit Informationen zu den nicht ausgeführten Aktionen anzuzeigen.

Wenn das Skript nicht erkannt wurde, wird ein Dialogfenster mit der folgenden Meldung angezeigt: **Das ausgewählte Dienste-Skript ist nicht signiert. Wenn Sie unbekannte Skripts und Skripte ohne Signatur ausführen, können die Daten Ihres Computers beschädigt werden. Möchten Sie das Skript und die Aktionen wirklich**

ausführen? Eine solche Meldung kann durch Inkonsistenzen im Skript verursacht werden (beschädigter Header, beschädigte Abschnittsüberschrift, fehlende Leerzeile zwischen Bereichen usw.). Sie können dann entweder die Skriptdatei öffnen und die Fehler beheben oder ein neues Dienste-Skript erstellen.

5.5.5 Häufige Fragen (FAQ)

Muss ESET SysInspector mit Administratorrechten ausgeführt werden?

ESET SysInspector muss zwar nicht mit Administratorrechten ausgeführt werden, einige Informationen können jedoch nur über ein Administratorkonto erfasst werden. Bei einer Ausführung unter einer niedrigeren Berechtigungsstufe (Standardbenutzer, eingeschränkter Benutzer) werden daher weniger Informationen zur Systemumgebung erfasst.

Erstellt ESET SysInspector eine Log-Datei?

ESET SysInspector kann eine Log-Datei mit der Konfiguration Ihres Computers erstellen. Um diese Logs zu speichern, klicken Sie im Hauptprogrammfenster auf **Datei** > **Log speichern**. Die Logs werden im XML-Format gespeichert. Standardmäßig erfolgt dies im Verzeichnis *%USERPROFILE%\Eigene Dateien* und unter einem Namen nach dem Muster „SysInspector-%COMPUTERNAME%-JJMMTT-HHMM.XML“. Sie können den Speicherort und den Namen der Log-Datei vor dem Speichern ändern.

Wie zeige ich eine ESET SysInspector-Log-Datei an?

Um eine von ESET SysInspector erstellte Log-Datei anzuzeigen, führen Sie das Programm aus und klicken Sie im Hauptprogrammfenster auf **Datei** > **Log öffnen**. Sie können Log-Dateien auch auf ESET SysInspector ziehen und dort ablegen. Wenn Sie häufig Log-Dateien aus ESET SysInspector anzeigen müssen, empfiehlt es sich, auf dem Desktop eine Verknüpfung zur Datei „SYSINSPECTOR.EXE“ anzulegen. So können Sie Log-Dateien einfach auf dieses Symbol ziehen, um sie zu öffnen. Aus Sicherheitsgründen lässt Windows Vista/Windows 7 unter Umständen kein Drag & Drop zwischen Fenstern mit unterschiedlichen Berechtigungsstufen zu.

Ist das Format der Log-Datei dokumentiert? Gibt es ein SDK?

Da sich das Programm noch in der Entwicklung befindet, gibt es momentan weder eine Dokumentation für das Dateiformat noch ein SDK. Je nach Kundennachfrage wird sich dies nach der offiziellen Veröffentlichung des Programms eventuell ändern.

Wie bewertet ESET SysInspector das Risiko, das von einem bestimmten Objekt ausgeht?

Um Objekten wie Dateien, Prozessen, Registrierungsschlüsseln usw. eine Risikostufe zuzuordnen, verwendet ESET SysInspector in der Regel einen Satz heuristischer Regeln, mit denen die Merkmale des Objekts untersucht werden, um anschließend nach entsprechender Gewichtung das Potenzial für schädliche Aktivitäten abschätzen. Auf der Grundlage dieser Heuristik wird den Objekten so eine Risikostufe von 1 - In Ordnung (grün) bis 9 - Risikoreich (rot) zugeordnet. Die Farbe der Abschnitte im Navigationsbereich im linken Teil des Programmfensters richtet sich nach der höchsten Risikostufe, die ein darin enthaltenes Objekt hat.

Bedeutet die Risikostufe „6 - Unbekannt (rot)“, dass ein Objekt gefährlich ist?

Die Einschätzung von ESET SysInspector legt nicht endgültig fest, ob eine Gefahr von einem Objekt ausgeht. Diese Entscheidung muss ein Sicherheitsexperte treffen. ESET SysInspector kann hierbei helfen, indem es dem Experten schnell zeigt, welche Objekte eventuell gründlicher untersucht werden müssen.

Warum stellt ESET SysInspector beim Start eine Verbindung zum Internet her?

Wie viele Anwendungen ist auch ESET SysInspector mit einem digitalen Zertifikat signiert, mit dem überprüft werden kann, dass die Software tatsächlich von ESET stammt und nicht verändert wurde. Hierzu baut das Betriebssystem eine Verbindung zu einer Zertifizierungsstelle auf, um die Identität des Softwareherstellers zu überprüfen. Es handelt sich dabei um einen normalen Vorgang, den alle digital signierten Programme unter Microsoft Windows ausführen.

Was ist Anti-Stealth-Technologie?

Die Anti-Stealth-Technologie ermöglicht eine effektive Erkennung von Rootkits.

Bei einem Angriff durch Schadcode, der das Verhalten eines Rootkits imitiert, besteht die Gefahr des Datenverlusts oder Datendiebstahls. Ohne spezielle Tools ist es quasi unmöglich, solche Rootkits zu erkennen.

Warum ist bei Dateien manchmal Microsoft als Unterzeichner angegeben, wenn gleichzeitig aber ein anderer Firmenname angezeigt wird?

Zum Ermitteln der digitalen Signatur eines ausführbaren Programms prüft ESET SysInspector zunächst, ob in der Datei eine digitale Signatur eingebettet ist. Wenn eine digitale Signatur gefunden wird, wird die Datei mit diesen Informationen validiert. Wird keine digitale Signatur gefunden, sucht ESI nach einer entsprechenden CAT-Datei (Sicherheitskatalog - *%systemroot%\system32\catroot*), die Informationen zur verarbeiteten ausführbaren Datei enthält. Ist diese Suche erfolgreich, wird die digitale Signatur dieser CAT-Datei zur Überprüfung der Programmdatei verwendet.

In einem solchen Fall kann es dann dazu kommen, dass Microsoft als Unterzeichner angegeben ist, die Angabe „Firmenname“ jedoch davon abweicht.

Beispiel:

Windows 2000 enthält die Anwendung „HyperTerminal“ in *C:\Programme\Windows NT*. Die Haupt-Programmdatei dieser Anwendung ist nicht digital signiert. ESET SysInspector weist jedoch Microsoft als Unterzeichner aus. Dies liegt daran, dass in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* ein Verweis auf *C:\Programme\Windows NT\hypertrm.exe* (die Haupt-Programmdatei von HyperTerminal) vorhanden ist und *sp4.cat* wiederum durch Microsoft digital signiert wurde.

5.6 Kommandozeile

Das Virenschutz-Modul von ESET Internet Security kann über die Kommandozeile gestartet werden, entweder manuell (mit dem Befehl „ecls“) oder über eine Batch-Datei („.bat“). Syntax zum Starten der Prüfung aus der Kommandozeile:

```
ecls [OPTIONEN..] DATEIEN..
```

Folgende Parameter und Switches stehen zur Verfügung, um die manuelle Prüfung über die Kommandozeile auszuführen:

Methoden

/base-dir=ORDNER	Module laden aus ORDNER
/quar-dir=ORDNER	Quarantäne-ORDNER
/exclude=MASKE	Dateien, die mit der MASKE übereinstimmen, von Prüfungen ausschließen
/subdir	Unterordner scannen (Standard)
/no-subdir	Unterordner nicht scannen
/max-subdir-level=STUFE	Maximale Suchtiefe von Unterordnern bei Scans
/symlink	Symbolischen Links folgen (Standardeinstellung)
/no-symlink	Symbolischen Links nicht folgen
/ads	ADS prüfen (Standard)
/no-ads	ADS nicht scannen
/log-file=DATEI	Ausgabe in DATEI protokollieren
/log-rewrite	Ausgabedatei überschreiben (Standardeinstellung: Anhängen)
/log-console	Ausgabe in Konsole protokollieren (Standard)
/no-log-console	Ausgabe nicht in Konsole protokollieren
/log-all	Saubere Dateien auch in Log aufnehmen
/no-log-all	Saubere Dateien nicht in Log aufnehmen (Standardeinstellung)
/aind	Aktivitätsanzeige anzeigen
/auto	Alle lokalen Laufwerke scannen und automatisch säubern

Einstellungen für Prüfungen

/files	Dateien scannen (Standard)
/no-files	Dateien nicht scannen
/memory	Speicher scannen
/boots	Bootsektoren scannen
/no-boots	Bootsektoren nicht scannen (Standard)
/arch	Archive scannen (empfohlen)
/no-arch	Archive nicht scannen
/max-obj-size=GRÖSSE	Nur Dateien scannen, die kleiner als GRÖSSE Megabyte sind (Standard: 0 = unbegrenzt)
/max-arch-level=TIEFE	Maximale Verschachtelungstiefe von Archiven bei Scans
/scan-timeout=LIMIT	Archive maximal MAXIMALE PRÜFDAUER Sekunden scannen
/max-arch-size=GRÖSSE	Nur Dateien in Archiven scannen, die kleiner als SIZE sind (Standard: 0 = unbegrenzt)
/max-sfx-size=GRÖSSE	Nur Dateien in selbstentpackenden Archiven scannen, die kleiner als GRÖSSE Megabyte sind (Standard: 0 = unbegrenzt)
/mail	E-Mails scannen (Standard)
/no-mail	E-Mails nicht scannen
/mailbox	Postfächer scannen (Standard)
/no-mailbox	Postfächer nicht scannen
/sfx	Selbstentpackende Archive scannen (Standard)
/no-sfx	Selbstentpackende Archive nicht scannen
/rtp	Laufzeitkomprimierte Dateien scannen (Standard)
/no-rtp	Laufzeitkomprimierte Dateien nicht scannen
/unsafe	nach potenziell unsicheren Anwendungen scannen

/no-unsafe	nicht nach potenziell unsicheren Anwendungen scannen (Standard)
/unwanted	nach evtl. unerwünschten Anwendungen scannen
/no-unwanted	nicht nach evtl. unerwünschte Anwendungen scannen (Standard)
/suspicious	nach verdächtigen Anwendungen scannen (Standard)
/no-suspicious	nicht nach verdächtigen Anwendungen scannen
/pattern	Erkennungsroutine verwenden (Standard)
/no-pattern	Erkennungsroutine nicht verwenden
/heur	Heuristik aktivieren (Standard)
/no-heur	Heuristik deaktivieren
/adv-heur	Advanced Heuristik aktivieren (Standard)
/no-adv-heur	Advanced Heuristik deaktivieren
/ext=ERWEITERUNGEN	Nur Dateien mit vorgegebenen ERWEITERUNGEN scannen (Trennzeichen Doppelpunkt)
/ext-exclude=ERWEITERUNGEN	ERWEITERUNGEN (Trennzeichen Doppelpunkt) nicht prüfen
/clean-mode=MODUS	Säuberungs-MODUS für infizierte Objekte verwenden Folgende Optionen stehen zur Verfügung: • **none** – Es wird keine automatische Säuberung ausgeführt. • **standard** (Standardeinstellung) – „ecls.exe“ versucht, infizierte Dateien automatisch zu säubern oder zu löschen. • **strict** – „ecls.exe“ versucht, infizierte Dateien ohne Benutzereingriff automatisch zu säubern oder zu löschen (Sie werden nicht aufgefordert, das Löschen von Dateien zu bestätigen). • **rigorous** – „ecls.exe“ löscht Dateien ohne vorherigen Säuberungsversuch unabhängig von der Art der Datei. • **delete** – „ecls.exe“ löscht Dateien ohne vorherigen Säuberungsversuch, lässt dabei jedoch wichtige Dateien wie Windows-Systemdateien aus.
/quarantine	Infizierte Dateien in die Quarantäne kopieren (ergänzt die beim Säubern ausgeführte Aktion)
/no-quarantine	Infizierte Dateien nicht in die Quarantäne kopieren

Allgemeine Optionen

/help	Hilfe anzeigen und beenden
/version	Versionsinformationen anzeigen und beenden
/preserve-time	Datum für „Geändert am“ beibehalten

Exitcodes

0	Keine Bedrohungen gefunden
1	Bedrohungen gefunden und entfernt
10	Einige Dateien konnten nicht geprüft werden (evtl. Bedrohungen)
50	Bedrohung gefunden
100	Fehler

HINWEIS
Exitcodes größer 100 bedeuten, dass die Datei nicht geprüft wurde und daher infiziert sein kann.

6. Häufig gestellte Fragen

In diesem Kapitel werden einige der häufigsten Fragen und Probleme behandelt. Klicken Sie auf die jeweilige Themenüberschrift, um Hilfestellung bei der Lösung Ihres Problems zu erhalten:

- So aktualisieren Sie ESET Internet Security
- So entfernen Sie einen Virus von Ihrem PC
- So lassen Sie Datenverkehr für eine bestimmte Anwendung zu
- So aktivieren Sie die Kindersicherung für ein Konto
- So erstellen Sie eine neue Aufgabe im Taskplaner

So planen Sie regelmäßige Prüfungen (im 24-Stunden-Takt)

Wenn Ihr Problem nicht in der oben aufgeführten Liste der Hilfeseiten aufgeführt ist, suchen Sie es auf den ESET Internet Security-Hilfeseiten.

Wenn Sie die Lösung für Ihr Problem bzw. die Antwort auf Ihre Frage nicht auf den Hilfeseiten finden können, steht Ihnen auch unsere regelmäßig aktualisierte Online-ESET-Wissensdatenbank zur Verfügung. Es folgt eine Liste der beliebtesten Artikel in unserer Wissensdatenbank zur Lösung häufiger Probleme:

- Bei der Installation meines ESET-Produkts ist ein Aktivierungsfehler aufgetreten. Was bedeutet das?
- Mein ESET Windows Home-Produkt mit Benutzernamen, Passwort oder Lizenzschlüssel aktivieren
- ESET Home-Produkt deinstallieren oder erneut installieren
- Ich wurde benachrichtigt, dass meine ESET-Installation vorzeitig abgebrochen wurde
- Was muss ich tun, nachdem ich meine Lizenz erneuert habe? (Benutzer der Home-Version)
- Was geschieht, wenn sich meine E-Mail-Adresse ändert?

Wie starte ich Windows im abgesicherten Modus bzw. abgesicherter Modus mit Netzwerk?

Bei Bedarf können Sie sich mit Ihren Fragen und Problemen auch direkt an unseren Support wenden. Das Kontaktformular finden Sie direkt in ESET Internet Security, auf der Registerkarte **Hilfe und Support**.

6.1 So aktualisieren Sie ESET Internet Security

Die Aktualisierung von ESET Internet Security kann manuell oder automatisch erfolgen. Klicken Sie im Bereich **Update** auf **Jetzt aktualisieren**, um eine Aktualisierung zu starten.

Bei der Standardinstallation wird stündlich ein automatisches Update ausgeführt. Wenn Sie diesen Zeitabstand ändern möchten, navigieren Sie zu **Tools** > **Taskplaner**. (Weitere Informationen zum Taskplaner finden Sie hier.)

6.2 So entfernen Sie einen Virus von Ihrem PC

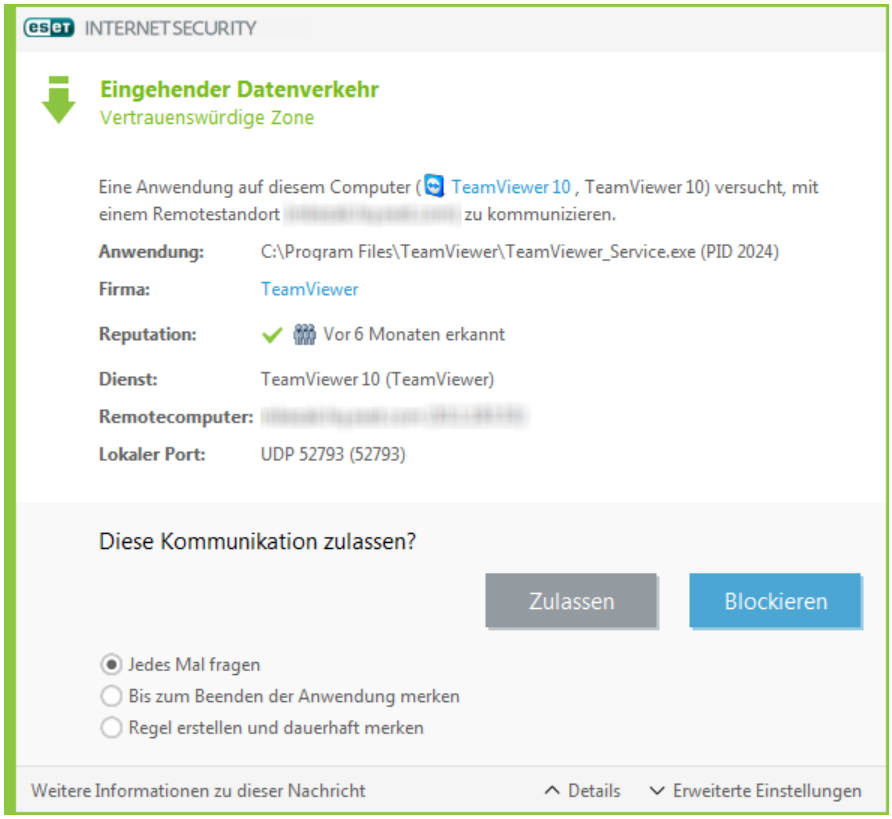
Wenn Ihr Computer die Symptome einer Infektion mit Schadsoftware aufweist (Computer arbeitet langsamer als gewöhnlich, hängt sich oft auf usw.), sollten Sie folgendermaßen vorgehen:

1. Klicken Sie im Hauptfenster auf **Computerprüfung**.
2. Klicken Sie auf **Scannen Sie Ihren Computer**, um die Systemprüfung zu starten.
3. Nachdem die Prüfung abgeschlossen ist, überprüfen Sie die Anzahl der geprüften, infizierten und wiederhergestellten Dateien im Log.
4. Wenn Sie nur einen Teil Ihrer Festplatte prüfen möchten, klicken Sie auf **Benutzerdefinierte Prüfung** und wählen Sie dann die Ziele aus, die auf Viren geprüft werden sollen.

Weitere Informationen finden Sie in diesem regelmäßig aktualisierten ESET-Knowledgebase-Artikel.

6.3 So lassen Sie Datenverkehr für eine bestimmte Anwendung zu

Wenn im interaktiven Filtermodus eine neue Verbindung erkannt wird, für die keine Regel definiert ist, wird der Benutzer aufgefordert, diese zuzulassen oder zu blockieren. Wenn ESET Internet Security jedes Mal dieselbe Aktion ausführen soll, wenn die Anwendung versucht, eine Verbindung herzustellen, aktivieren Sie das Kontrollkästchen **Auswahl dauerhaft anwenden (Regel erstellen)**.



Sie können neue Regeln für die Firewall erstellen, die auf Anwendungen angewendet werden, bevor sie von ESET Internet Security erkannt werden. Öffnen Sie hierzu die Einstellungen für die Firewall unter **Netzwerk** > **Firewall** > **Regeln und Zonen** > **Einstellungen**. Die Registerkarte **Regeln** unter **Einstellungen für Zonen und Regeln** wird nur angezeigt, wenn der Filtermodus der Firewall auf den interaktiven Modus eingestellt ist.

Geben Sie auf der Registerkarte **Allgemein** den Namen, die Richtung und das Übertragungsprotokoll für die Regel ein. Im angezeigten Fenster können Sie festlegen, welche Aktion stattfinden soll, wenn die Regel zugewiesen wird.

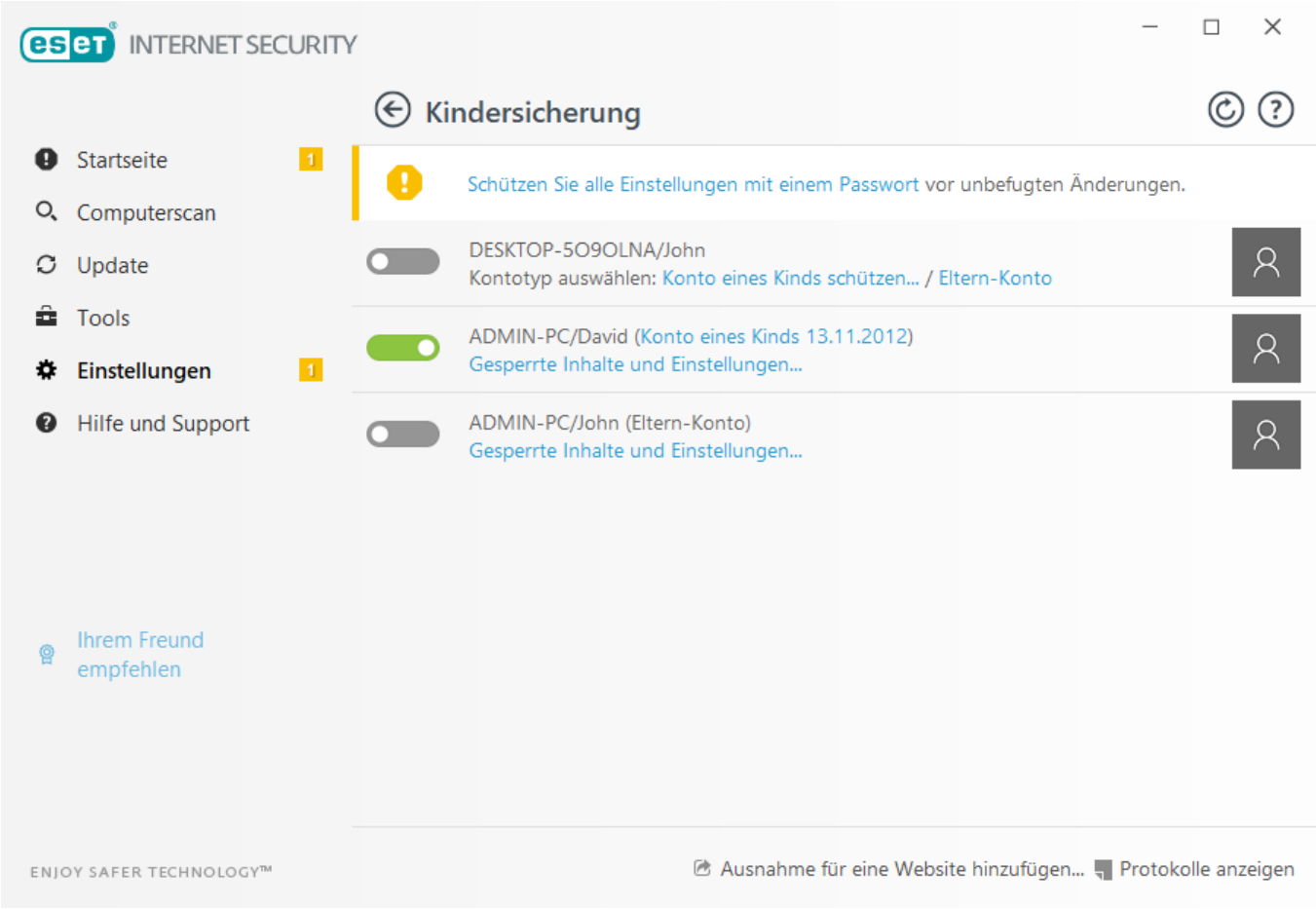
Geben Sie auf der Registerkarte **Lokal** den Pfad der ausführbaren Programmdatei und den lokalen Port ein. Klicken Sie auf die Registerkarte **Remote (Gegenstelle)** und geben Sie die Remoteadresse und den Port ein (falls zutreffend). Die neu erstellte Regel wird zugewiesen, sobald die Anwendung erneut versucht, eine Verbindung herzustellen.

6.4 So aktivieren Sie die Kindersicherung für ein Konto

Befolgen Sie die nachstehenden Schritte, um die Kindersicherung für ein bestimmtes Benutzerkonto zu aktivieren:

1. Standardmäßig ist die Kindersicherung in ESET Internet Security deaktiviert. Zur Aktivierung der Kindersicherung stehen zwei Methoden zur Verfügung:
   - Klicken Sie auf unter **Einstellungen** > **Sicherheits-Tools** > **Kindersicherung** im Hauptprogrammfenster, und ändern Sie den Status der Kindersicherung zu Aktiviert.
   - Drücken Sie F5, um die **Erweiterten Einstellungen** zu öffnen. Navigieren Sie anschließend zu **Web und E-Mail** > **Kindersicherung**, und aktivieren Sie das Kontrollkästchen neben **Systemintegration**.
2. Klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Sicherheits-Tools** > **Kindersicherung**. Auch wenn neben dem Eintrag **Kindersicherung** bereits **Aktiviert** angezeigt wird, müssen Sie die Kindersicherung für das

gewünschte Konto konfigurieren, indem Sie auf **Konto eines Kinds schützen** bzw. auf **Eltern-Konto** klicken. Geben Sie im nächsten Fenster ein Geburtsdatum ein, um die Zugriffsebene und empfohlene, altersangemessene Webseiten zu bestimmen. Die Kindersicherung wird nun für das angegebene Benutzerkonto aktiviert. Klicken Sie unter dem Kontonamen auf **Gesperrte Inhalte und Einstellungen...**, um auf der Registerkarte Kategorien festzulegen, welche Kategorien Sie blockieren bzw. zulassen möchten. Um Webseiten ohne Kategorie zu blockieren bzw. zuzulassen, klicken Sie auf die Registerkarte Ausnahmen.



6.5 So erstellen Sie eine neue Aufgabe im Taskplaner

Um einen neuen Task zu erstellen, klicken Sie unter **Tools** > **Weitere Tools** > **Taskplaner** auf **Hinzufügen**, oder klicken Sie mit der rechten Maustaste und wählen Sie im Kontextmenü die Option **Hinzufügen** aus. Es gibt fünf Arten von Tasks:

- **Start externer Anwendung** – Planen der Ausführung einer externen Anwendung.
- **Log-Wartung** – Log-Dateien enthalten auch unbenutzte leere Einträge von gelöschten Datensätzen. Dieser Task optimiert regelmäßig die Einträge in Log-Dateien.
- **Prüfung Systemstartdateien** - Prüft Dateien, die während des Systemstarts oder der Anmeldung ausgeführt werden.
- **Snapshot des Computerstatus erstellen** - Erstellt einen ESET SysInspector-Snapshot und eine genaue Risikoanalyse Ihrer Systemkomponenten (z. B. Treiber und Anwendungen).
- **On-Demand-Prüfung** - Prüft die Dateien und Ordner auf Ihrem Computer.
- **Update** – Erstellt einen Update-Task zur Aktualisierung der Module.

Da **Update**-Tasks zu den meistverwendeten Tasks gehören, wird im Folgenden das Hinzufügen eines neuen Update-Tasks beschrieben:

Wählen Sie in der Liste **Geplanter Task** den Task **Update**. Geben Sie den Namen des Tasks in das Feld **Taskname** ein und klicken Sie auf **Weiter**. Wählen Sie das gewünschte Ausführungsintervall. Folgende Optionen stehen zur Verfügung: **Einmalig**, **Wiederholt**, **Täglich**, **Wöchentlich** und **Bei Ereignis.** Wählen Sie **Task im Akkubetrieb überspringen** aus, um die Systembelastung für einen Laptop während des Akkubetriebs möglichst gering zu halten. Der angegebene Task wird zum angegeben Zeitpunkt in den Feldern **Taskausführung** ausgeführt. Im nächsten Schritt können Sie eine Aktion festlegen für den Fall, dass der Task zur geplanten Zeit nicht ausgeführt oder abgeschlossen werden kann. Folgende Optionen stehen zur Verfügung:

- **Zur nächsten geplanten Ausführungszeit**
- **Baldmöglichst**
- **Sofort ausführen, wenn Intervall seit letzter Ausführung überschritten** (das Intervall kann über das Feld **Zeit seit letzter Ausführung (Stunden)** festgelegt werden)

Anschließend wird ein Fenster mit einer vollständigen Zusammenfassung des aktuellen Tasks angezeigt. Klicken Sie auf **Fertig stellen**, wenn Sie Ihre Änderungen abgeschlossen haben.

Es wird ein Dialogfenster angezeigt, in dem Sie die Profile für den Task auswählen können. Hier können Sie das primäre und das alternative Profil festlegen. Das alternative Profil wird verwendet, wenn der Task mit dem primären Profil nicht abgeschlossen werden kann. Bestätigen Sie Ihre Auswahl mit **Fertig stellen**. Der neue Task wird zur Liste der aktuellen Tasks hinzugefügt.

6.6 So planen Sie eine wöchentliche Computerprüfung

Um einen regelmäßigen Task zu planen, öffnen Sie das Hauptprogrammfenster und klicken Sie auf **Tools** > **Weitere Tools** > **Taskplaner**. Hier finden Sie einen kurzen Überblick zum Planen eines Tasks, mit dem alle 24 Stunden eine Prüfung der lokalen Laufwerke durchgeführt wird. Weitere Informationen finden Sie in unserem Knowledgebase-Artikel.

So planen Sie eine regelmäßige Prüfung:

1. Klicken Sie im Hauptfenster des Taskplaners auf **Hinzufügen**.
2. Wählen Sie im Dropdown-Menü die Option **On-Demand-Prüfung**.
3. Geben Sie einen Namen für den Task an, und wählen Sie **Wöchentlich** unter Ausführungsintervall aus.
4. Wählen Sie Tag und Uhrzeit für die Ausführung aus.
5. Wählen Sie **Ausführung zum nächstmöglichen Zeitpunkt** aus, um den Task später auszuführen, falls die geplante Ausführung aus irgendeinem Grund nicht stattfindet (z. B. weil der Computer ausgeschaltet ist).
6. Überprüfen Sie die Zusammenfassung zum geplanten Task, und klicken Sie auf **Fertig stellen**.
7. Wählen Sie im Dropdown-Menü **Zu prüfende Objekte** die Option **Lokale Laufwerke** aus.
8. Klicken Sie auf **Fertig stellen**, um den Task zu übernehmen.

6.7 So entsperren Sie die erweiterten Einstellungen

Wenn Sie versuchen, die geschützten erweiterten Einstellungen zu öffnen, wird ein Fenster zur Eingabe des Passworts angezeigt. Falls Sie Ihr Passwort vergessen oder verloren haben, klicken Sie unten auf **Passwort wiederherstellen** und geben Sie die E-Mail-Adresse ein, die Sie bei der Registrierung dieser Lizenz verwendet haben. ESET schickt Ihnen eine E-Mail mit dem Überprüfungscode. Geben Sie den Überprüfungscode ein, geben Sie Ihr neues Passwort ein und bestätigen Sie es anschließend. Der Überprüfungscode ist sieben Tage lang gültig.

Sie können Ihr **Passwort auch über Ihr my.eset.com-Konto wiederherstellen**. Verwenden Sie diese Option, wenn die Lizenz mit Ihrem ESET License Manager verknüpft ist.

Falls Sie Ihre E-Mail-Adresse vergessen haben, klicken Sie auf **Ich kenne meine E-Mail-Adresse nicht**. Daraufhin werden Sie zur ESET-Webseite weitergeleitet, auf der Sie unsere Supportabteilung kontaktieren können.

Code für den Support generieren – Diese Option generiert einen Code für den Support. Kopieren Sie den Code und klicken Sie auf **Ich habe einen Überprüfungscode**. Geben Sie den Überprüfungscode ein, geben Sie Ihr neues Passwort ein und bestätigen Sie es anschließend. Der Überprüfungscode ist sieben Tage lang gültig.

Weitere Informationen finden Sie in diesem Artikel in der ESET-Knowledgebase.