ESET NOD32 ANTIVIRUS 9

Benutzerhandbuch

(für Produktversion 9.0 und höher)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista / XP

Klicken Sie hier, um die neueste Version dieses Dokuments herunterzuladen.

ENJOY SAFER TECHNOLOGY™

ESET NOD32 ANTIVIRUS

Weltweiter Support: www.eset.de/support

Versionsstand 10/6/2015

Inhalt

1. ESET NOD32 Antivirus

ESET NOD32 Antivirus ist ein neuer Ansatz für vollständig integrierte Computersicherheit. Die neueste Version des ThreatSense®-Prüfmoduls arbeitet schnell und präzise zum Schutz Ihres Computers. Auf diese Weise ist ein intelligentes System entstanden, das permanent vor Angriffen und bösartiger Software schützt, die Ihren Computer gefährden können.

ESET NOD32 Antivirus 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 Version 9 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 NOD32 Antivirus integriert und enthält dynamisch aktualisierte Supportinhalte.
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-Client-Schutz** dient der Überwachung eingehender E-Mails, die mit dem POP3(S)- oder dem IMAP(S)-Protokoll übertragen werden.
Reguläre Updates	Aktualisieren Sie Signaturdatenbank und 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 NOD32 Antivirus 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 NOD32 Antivirus arbeiten nur mit einer ordnungsgemäß aktivierten Lizenz. Wir empfehlen, die Lizenz für ESET NOD32 Antivirus einige Wochen vor dem Ablauf zu verlängern.

1.1 Neuerungen in Version 9

ESET NOD32 Antivirus Version 9 enthält die folgenden Verbesserungen:

- **Neu gestaltete Benutzeroberfläche** - Die grafische Benutzeroberfläche von ESET NOD32 Antivirus wurde komplett neu gestaltet und bietet mehr Sichtbarkeit und eine intuitivere Bedienung.Außerdem unterstützt die Benutzeroberfläche jetzt Sprachen mit Schriftbild von rechts nach links, z. B. Hebräisch und Arabisch. **Die Online-Hilfe** ist jetzt in ESET NOD32 Antivirus integriert und enthält dynamisch aktualisierte Supportinhalte.
- **Schnellere und zuverlässigere Installation** - Inklusive automatischer Anfangsprüfung 20 Minuten nach Installation und Neustart.

Weitere Details zu den neuen Funktionen in ESET NOD32 Antivirus finden Sie im folgenden ESET Knowledgebase-Artikel:
Neuheiten in ESET Smart Security 9 und ESET NOD32 Antivirus 9?

1.2 Systemanforderungen

Für einen reibungslosen Betrieb von ESET NOD32 Antivirus sollten die folgenden Hardware- und Softwareanforderungen erfüllt sein:

Unterstützte Prozessoren: Intel® oder AMD x86-x64
Betriebssysteme: Microsoft® Windows® 10/8.1/8/7/Vista/XP SP3 32-Bit/XP SP2 64-Bit/Home Server 2003 SP2 32-Bit/ Home Server 2011 64-Bit

1.3 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 Signaturdatenbank 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 NOD32 Antivirus 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 NOD32 Antivirus erforderliche Dateien werden automatisch heruntergeladen.

- Offline-Installation - Diese Art der Installation wird beim Installieren von einer CD/DVD verwendet. Die hierbei verwendete *.msi*-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 NOD32 Antivirus 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.

Nach dem Sie die **Endbenutzer-Softwarelizenzvereinbarung** akzeptiert haben, können Sie **ESET LiveGrid®** 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 Signaturdatenbank hinzugefügt werden.

Standardmäßig ist die Option **Ja, ich möchte an ESET LiveGrid® teilnehmen (empfohlen)** ausgewählt und die Funktion somit aktiviert.

Im nächsten Schritt der Installation wird die Prüfung auf eventuell unerwünschte Anwendungen konfiguriert. Bei eventuell unerwünschten Anwendungen handelt es sich um 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.

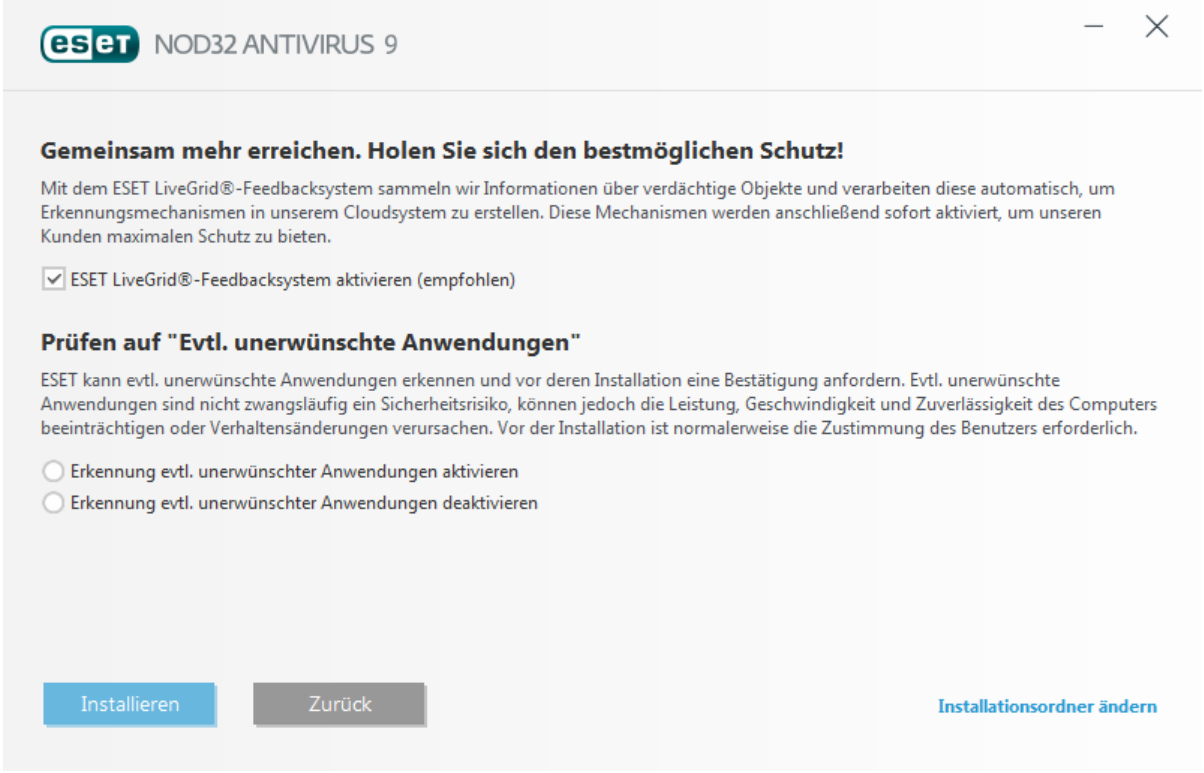
2.2 Offline-Installation

Nachdem Sie das Offline-Installationspaket (.msi) gestartet haben, führt der Installationsassistent Sie durch die Einstellungen.

Das Programm überprüft zunächst, ob eine neuere Version von ESET NOD32 Antivirus verfügbar ist. Wenn eine neuere Version erkannt wird, werden Sie im ersten Schritt der Installation darauf hingewiesen. Wenn Sie nun die Option **Neue Version herunterladen und installieren** wählen, wird die neue Version heruntergeladen und die Installation fortgesetzt. Dieses Kontrollkästchen ist nur sichtbar, wenn eine neuere Version als diejenige, die Sie gerade installieren, verfügbar ist.

Im nächsten Schritt wird die Endbenutzer-Lizenzvereinbarung angezeigt. Lesen Sie sich diese Vereinbarung sorgfältig durch. Wenn Sie damit einverstanden sind, klicken Sie auf **Ich stimme zu**. Nachdem Sie die Vereinbarung angenommen haben, wird die Installation fortgesetzt.

Weitere Anweisungen zu den Installationsschritten, zu **ThreatSense** und zu **Prüfen auf evtl. unerwünschte Anwendungen** finden Sie im Abschnitt zum Live-Installer.



2.2.1 Erweiterte Einstellungen

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

C:\Programme\ESET\ESET NOD32 Antivirus

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

Klicken Sie auf **Weiter**, um die Einstellungen für Internetverbindung festzulegen. Wenn Sie einen Proxyserver verwenden, muss dieser richtig eingestellt sein, damit die Signaturdatenbank aktualisiert werden kann. Wenn Sie sich nicht sicher sind, ob Sie zur Verbindung mit dem Internet einen Proxyserver verwenden, wählen Sie **Einstellungen aus Internet Explorer übernehmen (empfohlen)** und klicken Sie auf **Weiter**. Wenn Sie keinen Proxyserver verwenden, wählen Sie die Option **Keinen Proxyserver verwenden**.

Um die Einstellungen für Ihren Proxyserver zu konfigurieren, wählen Sie **Ich nutze einen Proxyserver** und klicken Sie auf **Weiter**. Geben Sie unter **Adresse** die IP-Adresse oder URL des Proxyservers ein. Im Feld **Port** können Sie den Port angeben, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128). Falls für den Proxyserver Zugangsdaten zur Authentifizierung erforderlich sind, geben Sie einen gültigen **Benutzernamen** und das **Passwort** ein. Die Einstellungen für den Proxyserver können auch aus dem Internet Explorer kopiert werden, falls gewünscht. Klicken Sie dazu auf **Übernehmen**, und bestätigen Sie die Auswahl.

Wenn Sie „Benutzerdefinierte Installation“ wählen, können Sie festlegen, wie Ihr System mit automatischen Programm-Updates verfahren soll. Klicken Sie auf **Ändern...**, um zu den erweiterten Einstellungen zu gelangen.

Wenn Sie nicht möchten, dass Programmkomponenten aktualisiert werden, wählen Sie **Niemals ausführen**. Wenn Sie die Option **Benutzer fragen** auswählen, wird vor dem Herunterladen von Programmkomponenten ein Bestätigungsfenster angezeigt. Um Programmkomponenten automatisch zu aktualisieren, wählen Sie **Immer ausführen**.

HINWEIS: Nach der Aktualisierung von Programmkomponenten muss der Computer üblicherweise neu gestartet werden. Wir empfehlen die Einstellung **Computer bei Bedarf ohne Benachrichtigung neu starten**.

Im nächsten Installationsfenster haben Sie die Möglichkeit, die Einstellungen des Programms mit einem Passwort zu schützen. Wählen Sie die Option **Einstellungen mit Passwort schützen** und geben Sie ein Passwort in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein. Dieses Passwort ist anschließend erforderlich, um die Einstellungen von ESET NOD32 Antivirus zu ändern bzw. auf die Einstellungen zuzugreifen. Wenn beide Passwortfelder übereinstimmen, fahren Sie mit **Weiter** fort.

Befolgen Sie zum Abschließen der weiteren Installationsschritte (**ThreatSense** und **Prüfen auf „Eventuell unerwünschte Anwendungen“**) die Anweisungen im Abschnitt zum Live-Installer.

Um die Erstprüfung nach der Installation zu deaktivieren, die Ihren Compuer normalerweise nach Abschluss der Installation auf Schadsoftware prüft, deaktivieren Sie das Kontrollkästchen neben **Scan nach der Installation aktivieren**. Klicken Sie im Fenster **Bereit zur Installation** 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 ESET NOD32 Antivirus vor dem Kauf testen möchten, wählen Sie **Kostenlose Probelizenz** aus. Geben Sie Ihre E-Mail-Adresse und Ihr Land ein, um ESET NOD32 Antivirus 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.

Wählen Sie **Später aktivieren**, wenn Sie das Produkt zunächst testen und nicht sofort aktivieren möchten, oder wenn Sie das Produkt zu einem späteren Zeitpunkt aktivieren möchten.

Sie können Ihre Installation von ESET NOD32 Antivirus auch direkt aus dem Programm aktivieren. Klicken Sie mit der rechten Maustaste auf das ESET NOD32 Antivirus-Symbol in der Taskleiste, und wählen Sie **Produkt aktivieren** im Programmmenü aus.

2.5 Eingabe eines Lizenzschlüssels

Damit alle Funktionen optimal genutzt werden können, sollte das Programm automatisch aktualisiert werden. Dies ist nur möglich, wenn der korrekte **Lizenzschlüssel** unter **Einstellungen für Updates** eingegeben wurde.

Falls Sie Ihren Lizenzschlüssel Passwort bei der Installation nicht eingegeben haben, können Sie dies nun nachholen. Klicken Sie im Hauptprogrammfenster auf **Hilfe und Support** und dann auf **Produktaktivierung**. Geben Sie im Fenster zur Produktaktivierung die Lizenzdaten ein, die Sie für Ihr ESET Security-Produkt erhalten haben.

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

- Eine eindeutige Zeichenfolge im Format XXXX-XXXX-XXXX-XXXX-XXXX zur Identifizierung des Lizenzinhabers und der 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 Upgrade auf eine aktuellere Version

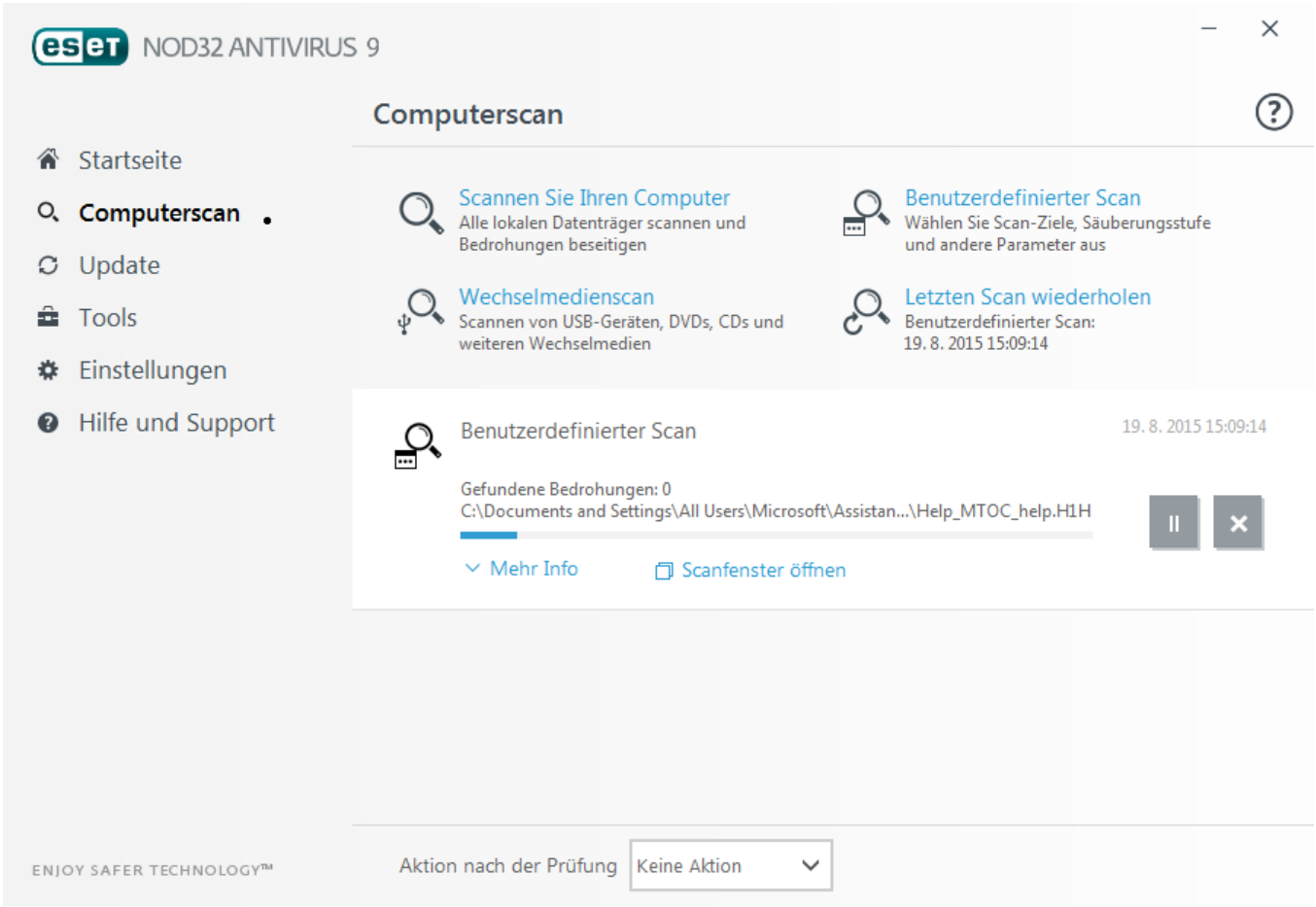
Neuere Versionen von ESET NOD32 Antivirus werden veröffentlicht, um Verbesserungen oder Patches durchzuführen, die ein automatisches Update der Programmmodule nicht leisten kann. Es gibt verschiedene Möglichkeiten, ein Upgrade auf eine aktuellere Version durchzuführen:

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)

2.7 Erstprüfung nach Installation

Nach der Installation von ESET NOD32 Antivirus wird der Computer 20 Minuten nach der Installation oder nach einem Neustart auf Schadsoftware geprüft.

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



3. Erste Schritte

Dieses Kapitel enthält eine einführende Übersicht über ESET NOD32 Antivirus und die Grundeinstellungen des Programms.

3.1 Das Haupt-Programmfenster

Das Hauptprogrammfenster von ESET NOD32 Antivirus 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 NOD32 Antivirus.

Computerscan - Konfigurieren und starten Sie einen Scan Ihres Computers oder erstellen Sie einen benutzerdefinierten Scan.

Update - Dieser Bereich zeigt Informationen zu Updates der Signaturdatenbank an.

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

Einstellungen - Mit dieser Option können Sie das Maß an Sicherheit für Ihren Computer, Ihre Internetverbindung.

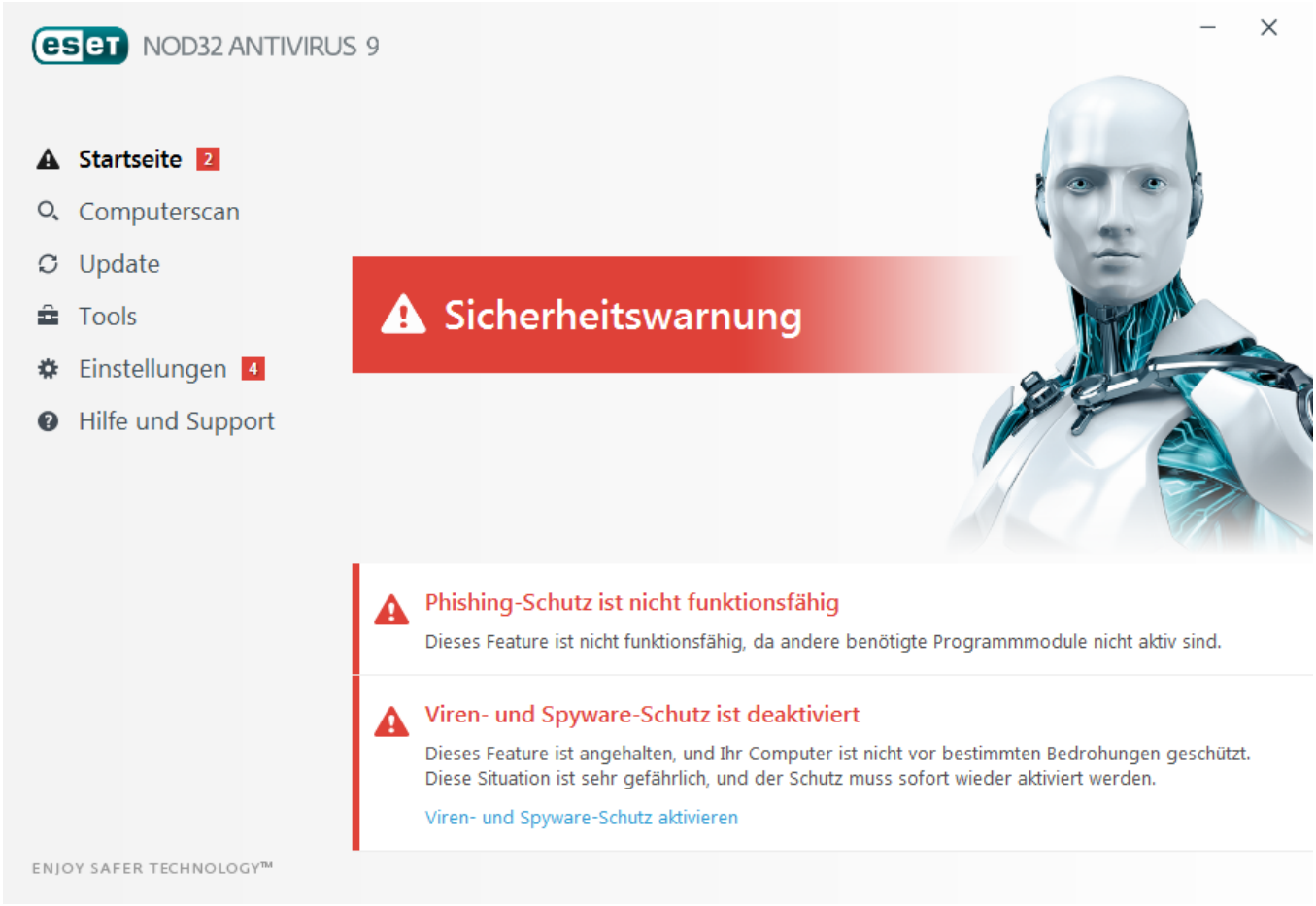
Hilfe und Support - Dieser Bereich bietet Zugriff auf die Hilfedateien, die ESET-Knowledgebase, die ESET-Website Links für die Übermittlung von Supportanfragen.

Die **Startseite** enthält Informationen über die aktuelle Schutzstufe Ihres Computers. Im Statusfenster werden die am häufigsten verwendeten Funktionen von ESET NOD32 Antivirus 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 NOD32 Antivirus entweder auf der **Startseite** unter **Produkt aktivieren** oder unter Schutzstatus über die Schaltfläche **Jetzt kaufen** aktivieren.
- **Signaturdatenbank nicht mehr aktuell** - Dieser Fehler wird angezeigt, wenn die Signaturdatenbank 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 **Alle Module des Viren- und Spyware-Schutzes 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

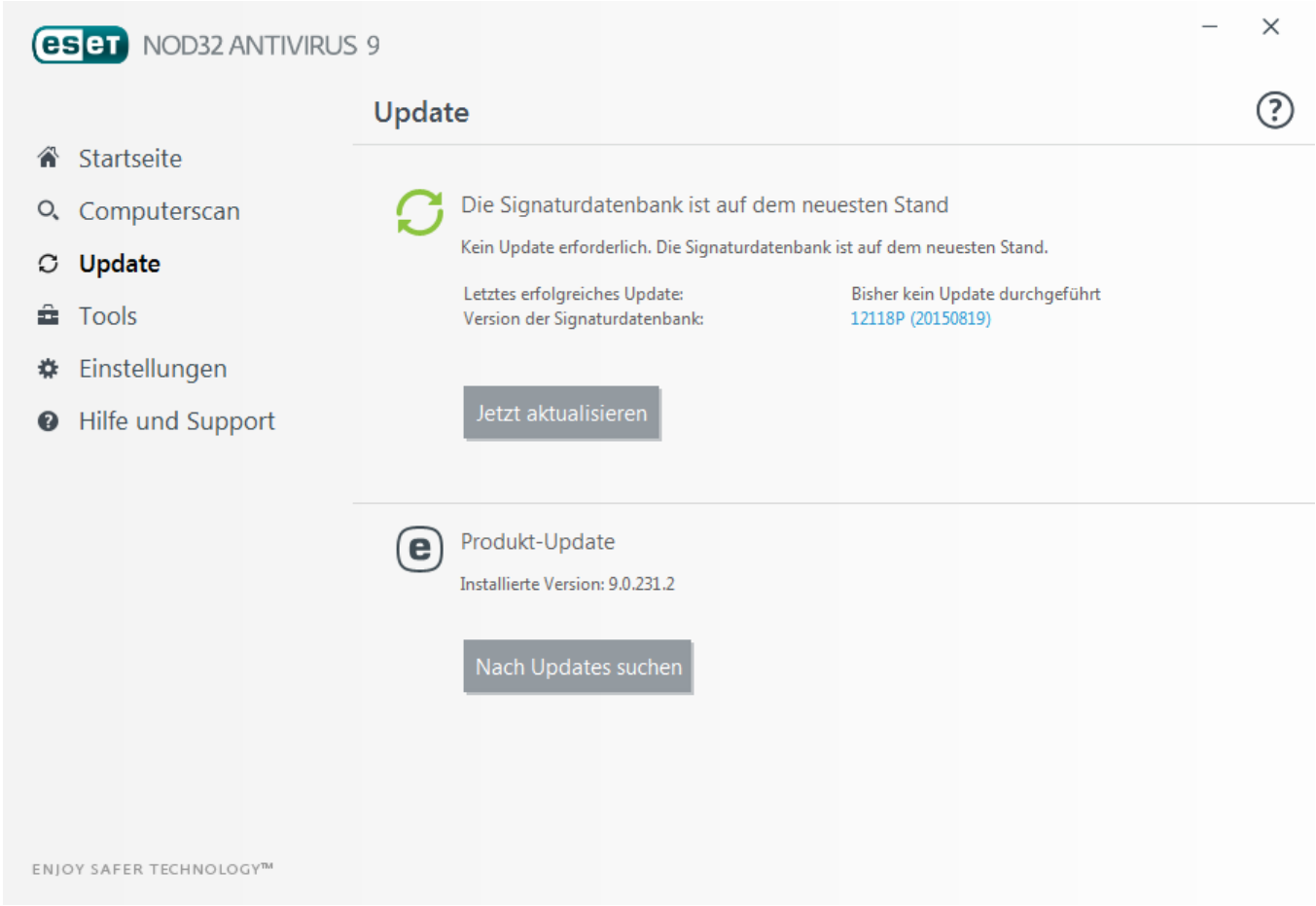
der Systemuhr angezeigt. Nach dem Ablaufen der Lizenz ist kein Programm-Update mehr möglich und das Schutzstatussymbol ist rot.

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.

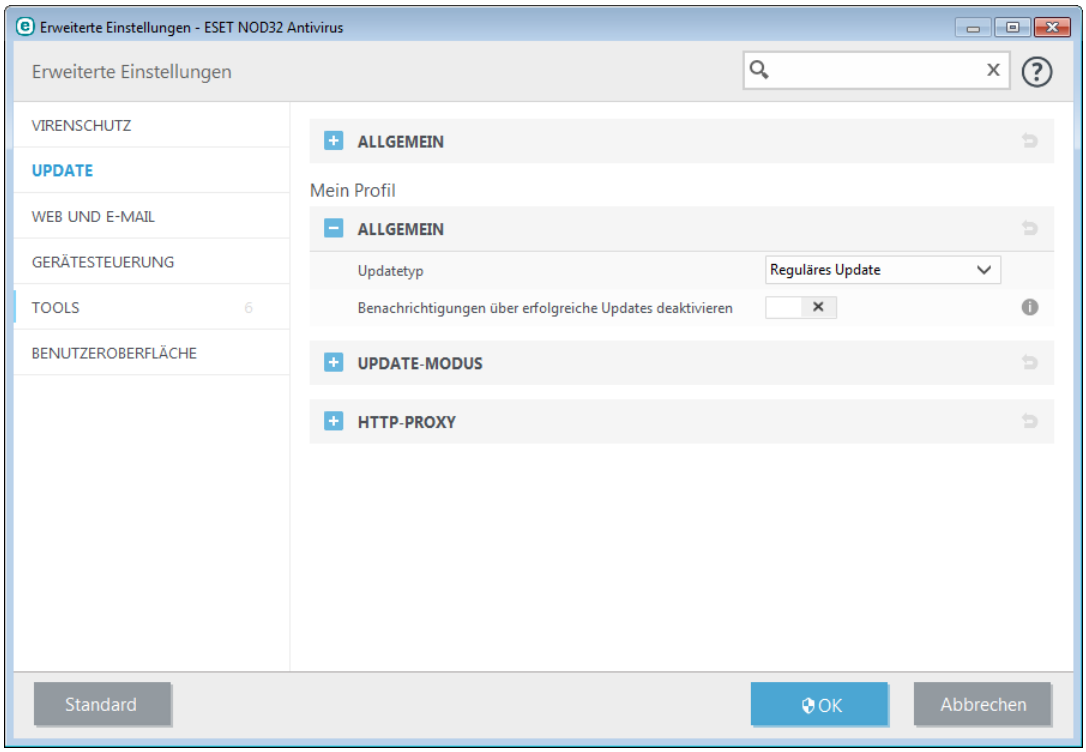
3.2 Updates

Updates der Signaturdatenbank 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 **Signaturdatenbank aktualisieren**, um nach einem Update für die Signaturdatenbank zu suchen.

Wenn die Lizenzdaten (Benutzername und Passwort) während der Aktivierung von ESET NOD32 Antivirus nicht eingegeben wurden, werden Sie nun dazu aufgefordert.

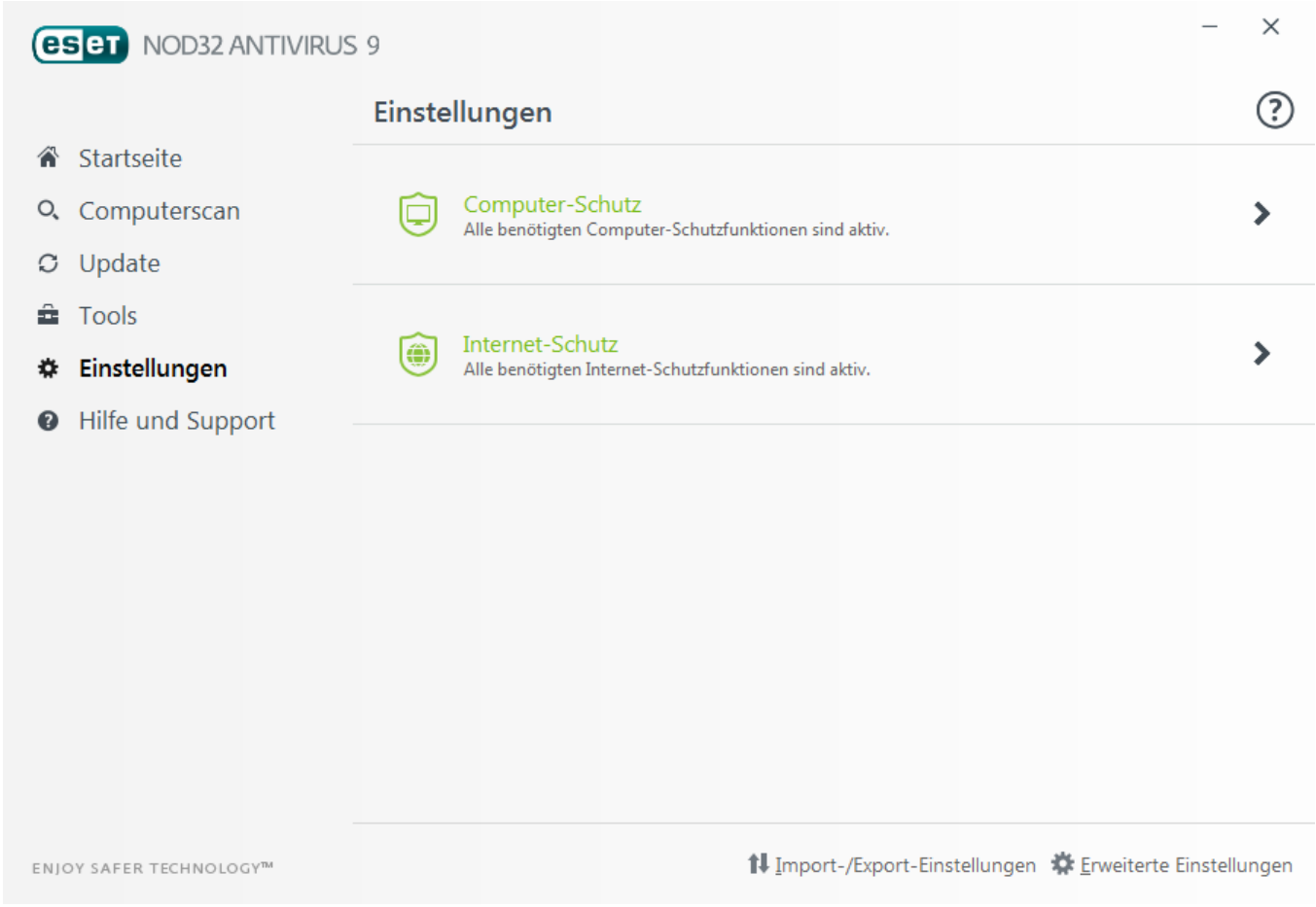


Das Fenster "Erweiterte Einstellungen" (klicken Sie im Hauptmenü auf **Einstellungen** und dann auf **Erweiterte Einstellungen** oder drücken Sie die Taste **F5**) enthält zusätzliche Update-Optionen. Um erweiterte Update-Optionen wie den Update-Modus, den Proxyserverzugriff und die LAN-Verbindungen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



4. Arbeiten mit ESET NOD32 Antivirus

ESET NOD32 Antivirus Mit den Konfigurationsoptionen können Sie Feinabstimmungen rund um den Schutz Ihres Computers vornehmen.



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

Computer-Schutz
Internet-Schutz

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.

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-Client-Schutz** - Überwacht eingehende E-Mails, die mit dem POP3- oder dem IMAP-Protokoll übertragen werden.
- **Phishing-Schutz** – Filtert Websites, für die der Verdacht besteht, dass sie Inhalte enthalten, die den Benutzer zum Einreichen vertraulicher Informationen verleiten.

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

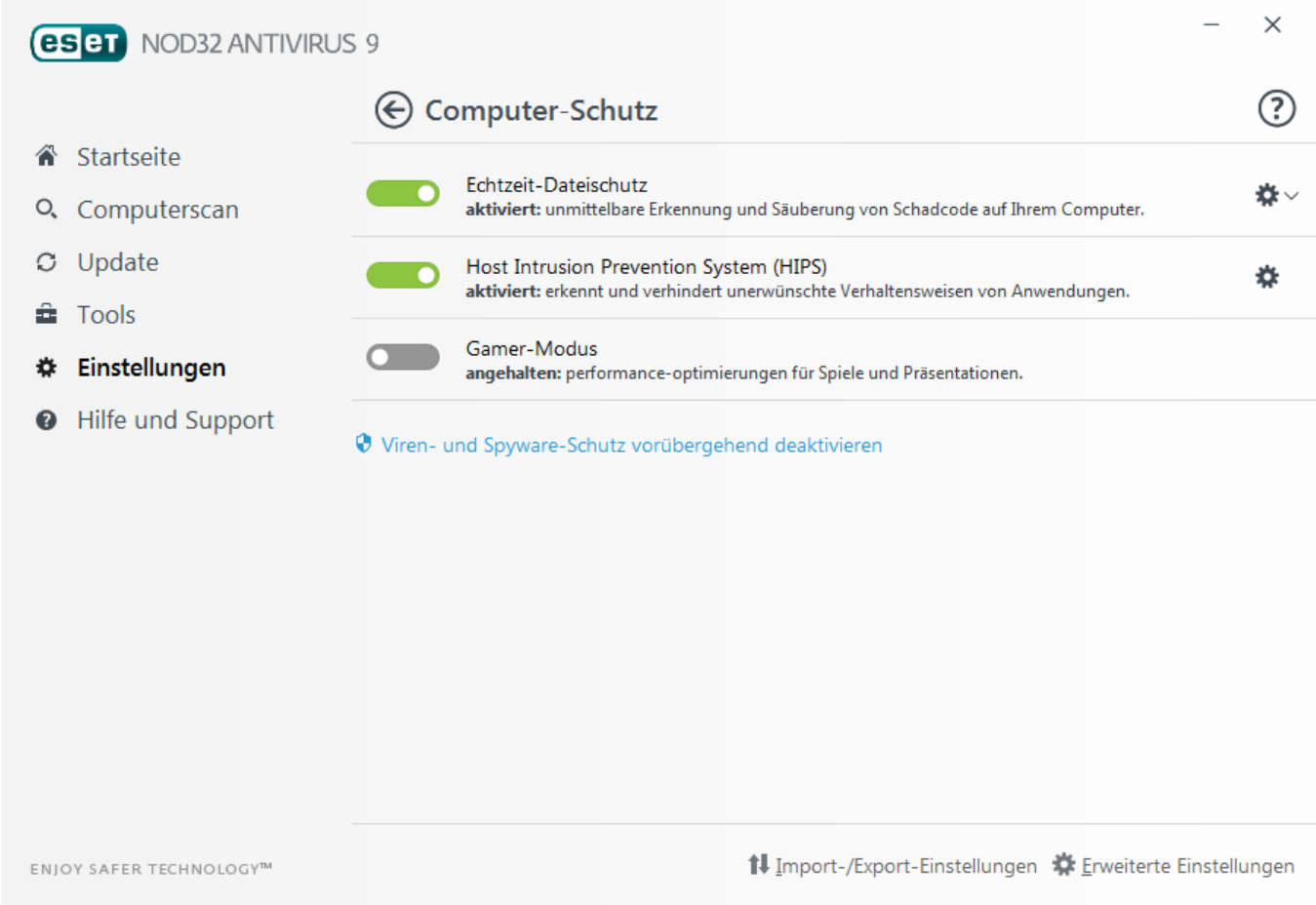
HINWEIS: Wenn Sie den Schutz auf diese Weise deaktivieren, werden alle deaktivierten Schutzmodule nach einem Computerneustart wieder aktiviert.

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.

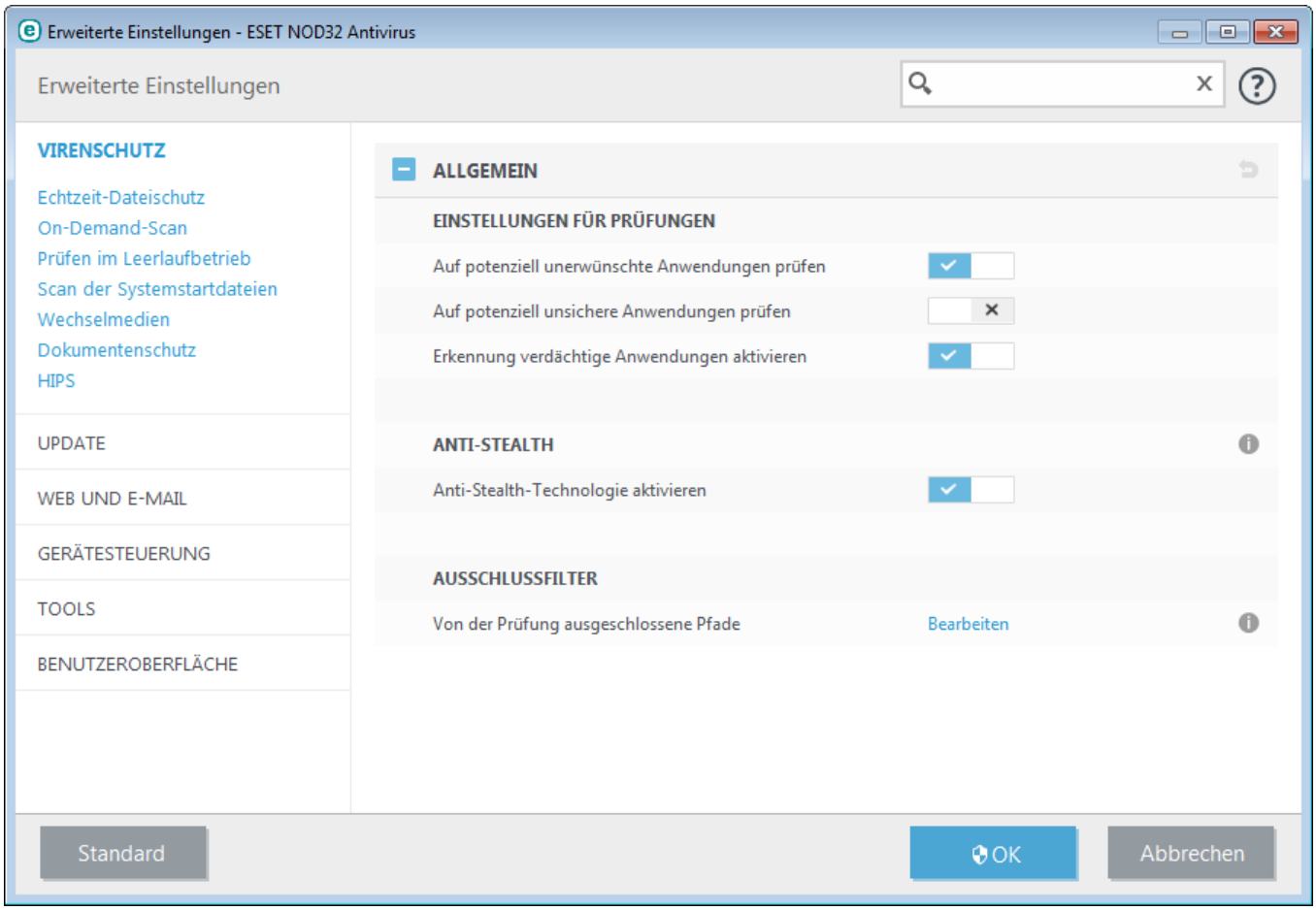
Klicken Sie auf > **Ausschlussfilter bearbeiten** neben **Echtzeit-Dateischutz**, um das Fenster für die Ausschlussfilter-Einstellungen zu öffnen. Hier können Sie Dateien und Ordner von der Prüfung ausschließen.



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 zur Bestätigung auf **OK**.

4.1.1 Virenschutz

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.

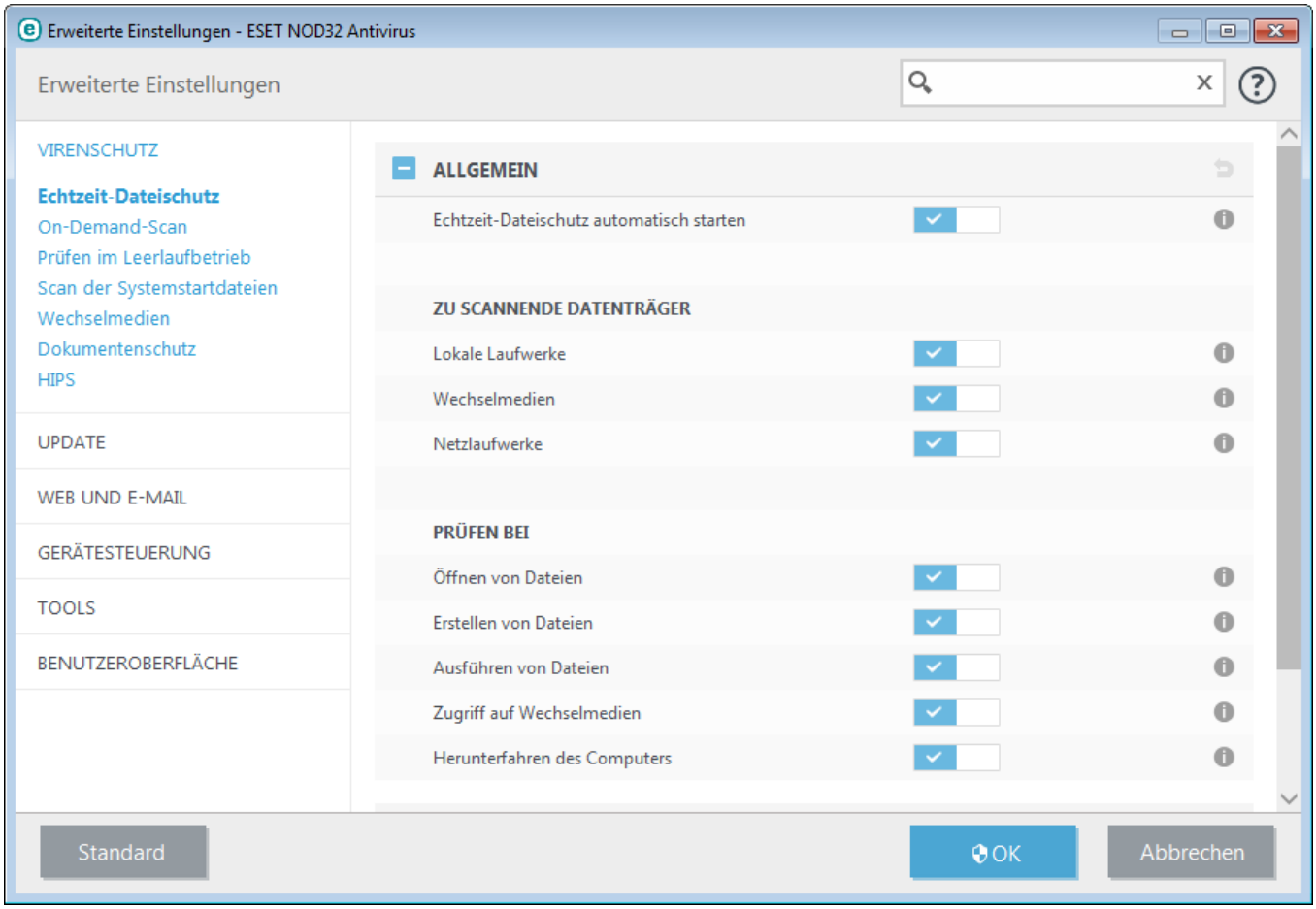
Die Anti-Stealth-Technologie ist ein fortschrittliches System zur Erkennung gefährlicher Programme wie Rootkits, die sich vor dem Betriebssystem verstecken können. Aus diesem Grund ist es nahezu unmöglich, sie mit herkömmlichen Prüfmethoden zu erkennen.

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 zum Ausschließen von Objekten von Prüfungen finden Sie unter Ausschlussfilter.

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 einem anderen Echtzeit-Scanner) kann der Echtzeit-Dateischutz deaktiviert werden. Deaktivieren Sie dazu unter **Erweiterte Einstellungen** im Bereich **Echtzeit-Dateischutz** > **Einfach** die Option **Echtzeit-Dateischutz automatisch starten**.

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.
- **Öffnen von Dateien** - Prüfen von Dateien beim Öffnen aktivieren/deaktivieren.
- **Wechselmedienzugriff** - Prüfen beim Zugriff auf Wechselmedien mit Speicherplatz aktivieren/deaktivieren.
- **Computer-Abschaltung** - Prüfen beim Herunterfahren des Computers 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 Signaturdatenbank 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 das Fenster mit den erweiterten Einstellungen mit **F5**, und navigieren Sie anschließend zu **Virenschutz** > **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 NOD32 Antivirus verwendet Advanced Heuristik zusammen mit signaturbasierten Prüfmethoden, um neue Bedrohungen zu erkennen, bevor ein Update der Signaturdatenbank 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.

Normales Säubern - 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 NOD32 Antivirus werden alle Einstellungen optimal eingerichtet, um dem Benutzer die größtmögliche Schutzstufe für das System zu bieten. Um die Standardeinstellungen wiederherzustellen, klicken Sie neben den Registerkarten im Fenster (**Erweiterte Einstellungen** > **Virenschutz** > **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.

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 automatisch starten** 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 automatisch starten** 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 Computerscan

Die manuelle Prüfung ist ein wichtiger Teil Ihrer Virenschutzlösung. Sie dient zur Prüfung von Dateien und Ordnern auf dem Computer. Aus Sicherheitsgründen ist es dringend erforderlich, dass Sie Ihren Computer nicht nur bei Infektionsverdacht prüfen, sondern diese Prüfung in die allgemeinen Sicherheitsroutinen integrieren. 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 Signaturdatenbank nicht auf dem neuesten Stand ist oder die Datei nicht als Virus erkannt wird, wenn sie auf dem Datenträger gespeichert wird.

Die hierfür vorgesehene Funktion **Computerscan** hat zwei Unterbefehle. **Scannen Sie Ihren Computer** führt eine schnelle Systemprüfung ohne spezielle Prüfparameter durch. Unter **Benutzerdefinierter Scan** 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.

Benutzerdefinierter Scan

Beim Benutzerdefinierter Scan 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 "Scannen Sie Ihren Computer" 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 **Benutzerdefinierter Scan** 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** > **Taskplaner** konfigurieren. So planen Sie eine wöchentliche Computerprüfung

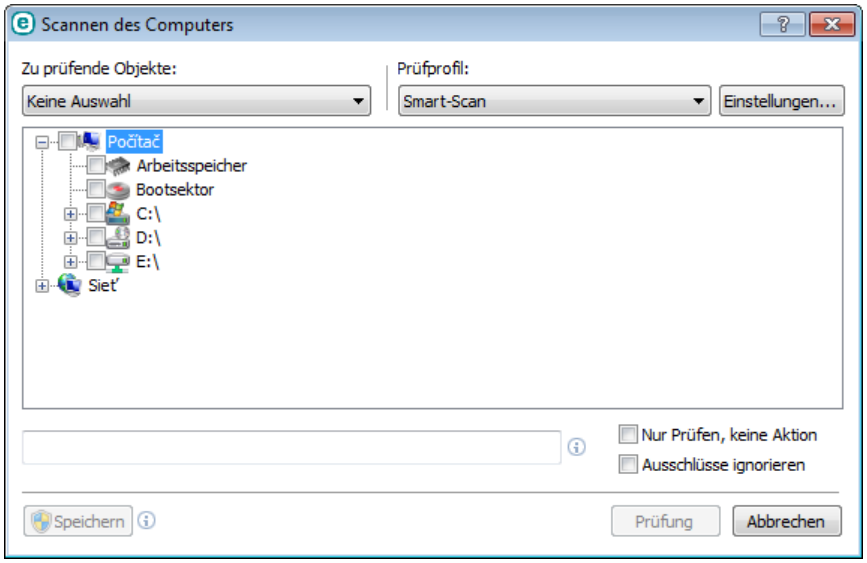
4.1.1.2.1 Benutzerdefinierter Scan

Wenn Sie nicht den gesamten Festplattenspeicher, sondern nur bestimmte Objekte prüfen möchten, klicken Sie auf **Computerscan** > **Benutzerdefinierter Scan**. Wählen Sie die zu prüfenden Objekte aus dem Dropdown-Menü **Zu prüfende Objekte** oder in der Ordnerstruktur (Baumstruktur) aus.

Im Fenster der zu prüfenden Objekte können Sie definieren, welche Objekte (Arbeitsspeicher, Laufwerke, Dateien und Ordner) auf Infiltrationen geprüft werden. Wählen Sie die zu prüfenden Objekte aus der Baumstruktur aus, in der alle auf dem Computer verfügbaren Ordner aufgelistet werden. Im Dropdown-Menü **Zu prüfende Objekte** können Sie vordefinierte Optionen für die zu prüfenden Objekte auswählen.

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

Um schnell zu einem zu prüfenden Objekt zu navigieren oder um ein gewünschtes Objekt (Ordner oder Datei(ein)) direkt hinzuzufügen, geben Sie den Pfad in das leere Textfeld unter der Ordnerliste ein. Dies ist nur möglich, wenn keine Objekte aus der Baumstruktur zur Prüfung ausgewählt wurden und im Menü **Zu prüfende Objekte** die Option **Keine Auswahl** festgelegt ist.



Infizierte Objekte werden nicht automatisch gesäubert. Durch das Durchführen einer Prüfung ohne Aktion können Sie sich einen Eindruck des aktuellen Schutzstatus verschaffen. Wenn Sie nur das System ohne zusätzliche Säuberung prüfen möchten, wählen Sie die Option **Nur prüfen, keine Aktion**. Außerdem können Sie zwischen drei Säuberungsstufen wählen. Klicken Sie dazu auf **Einstellungen** > **Säubern**. Die Informationen zur Prüfung werden in einem Log gespeichert.

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

Aus dem Dropdown-Menü **Prüfprofil** können Sie ein Profil auswählen, um ausgewählte Objekte zu prüfen. Das Standardprofil ist **Scannen Sie Ihren Computer**. Es stehen außerdem zwei weitere vordefinierte Prüfprofile zur Verfügung: **Tiefenprüfung** und **Kontextmenü-Prüfung**. Diese Prüfprofile verwenden unterschiedliche ThreatSense-Einstellungen. Klicken Sie auf **Einstellungen...**, um ein ausgewähltes Prüfprofil detailliert zu konfigurieren. Die verfügbaren Optionen sind im Abschnitt **Sonstige** unter Einstellungen für ThreatSense beschrieben.

Klicken Sie auf **Speichern**, um die an den zu prüfenden Objekten vorgenommenen Änderungen zu speichern, einschließlich der Auswahl in der Baumstruktur.

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. Wählen Sie diese Option, wenn der aktuell angemeldete Benutzer keine ausreichenden Zugriffsrechte auf die zu

prüfenden Dateien hat. Diese Schaltfläche ist nur verfügbar, wenn der aktuell angemeldete Benutzer UAC-Vorgänge als Administrator aufrufen kann.

4.1.1.2.2 Stand der Prüfung

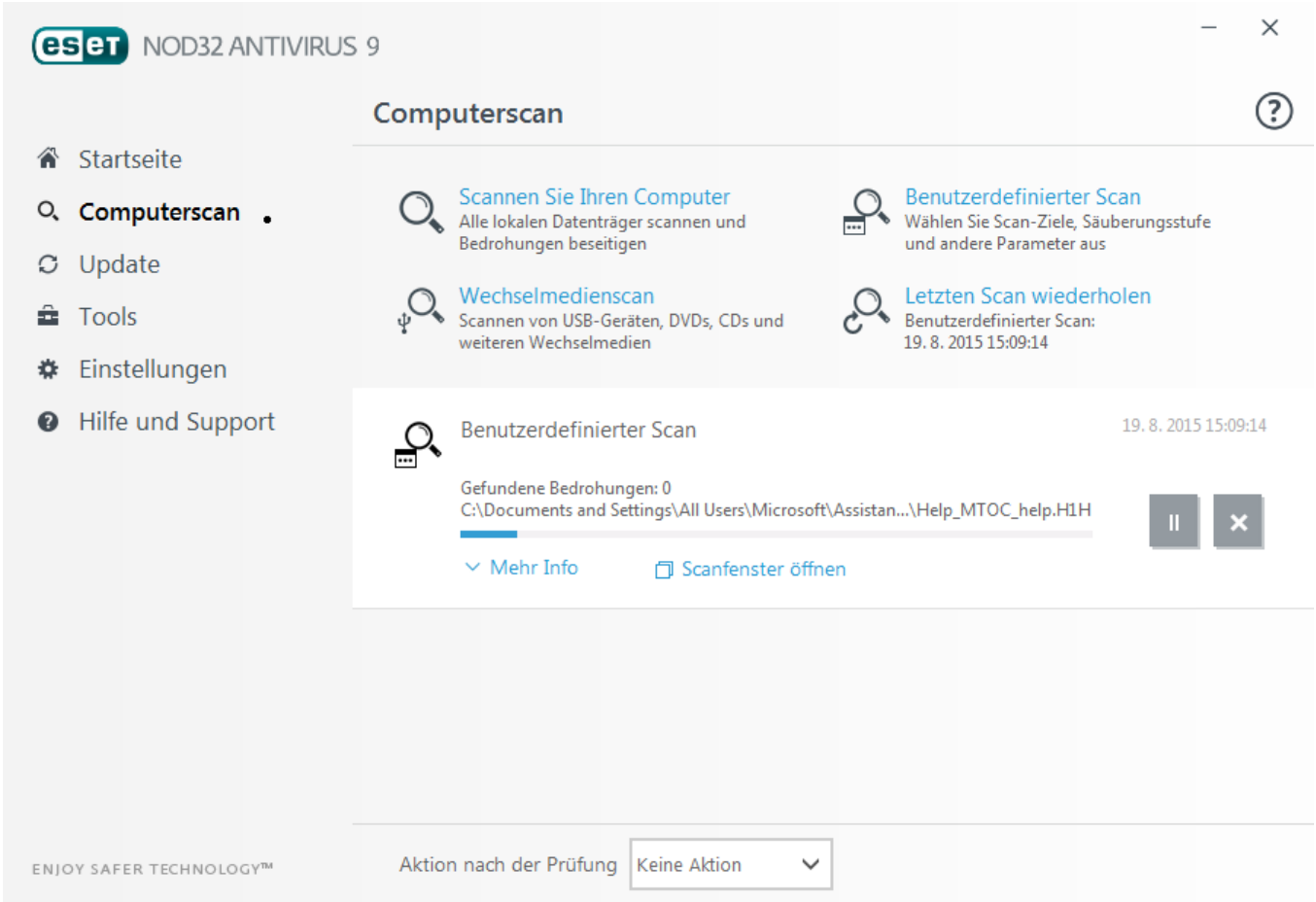
Die Fortschrittsanzeige enthält den aktuellen Stand der Prüfung sowie die Anzahl der bisher gefundenen infizierten Dateien.

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.

Scan-Fortschritt - Die Fortschrittsanzeige zeigt den Status der bereits gescannten Objekte in Bezug auf die noch zu scannenden 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 ist wählbar, 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.

TIPP:

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 **Scannen Sie Ihren Computer** oder **Benutzerdefinierter Scan** 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 Sie auf **Virenschutz** > **On-Demand-Scan** > **Einfach** > **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.

Beispiel: Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Option **Scannen Sie Ihren Computer** 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.

4.1.1.3 Scan der Systemstartdateien

Die automatische Prüfung der Systemstartdateien wird standardmäßig beim Systemstart und beim Update der Signaturdatenbank 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 **Scan 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.

4.1.1.3.1 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 - Die Priorität, mit der der Prüfbeginn ermittelt wird:

- **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.

4.1.1.4 Prüfen im Leerlaufbetrieb

Sie können die Prüfung im Leerlaufbetrieb in den **Erweiterten Einstellungen** unter **Virenschutz** > **Prüfen im Leerlaufbetrieb** > **Einfach** aktivieren. Stellen Sie den Schalter neben **Prüfung im Leerlaufbetrieb aktivieren** auf **Ein**, um diese Funktion zu aktivieren. Wenn der Computer im Leerlauf ist, wird auf allen lokalen Festplatten eine Prüfung ausgeführt. unter Auslöser für die Prüfung im Leerlaufbetrieb finden Sie eine Liste der Bedingungen, die die Prüfung im Leerlaufbetrieb auslösen.

Diese Prüfung wird nur dann ausgeführt, wenn der Computer (Notebook) an die Netzversorgung angeschlossen ist. Sie können diese Einstellung überschreiben, indem Sie die Option neben **Auch ausführen, wenn der Computer im Batteriebetrieb ausgeführt wird** in den erweiterten Einstellungen aktivieren.

Aktivieren Sie **Erstellen von Logs aktivieren** unter **Erweiterte Einstellungen** > **Tools** > **ESET LiveGrid®**, um die Ausgabe einer Computerprüfung in den Log-Dateien abzulegen (Klicken Sie im Hauptprogrammfenster auf **Tools** > **Log-Dateien** und wählen Sie **Computerscan** im Dropdown-Menü **Log** aus).

Die Prüfung im Leerlaufbetrieb erfolgt, wenn sich der Computer im folgenden Zustand befindet:

- Bildschirmschoner
- Computersperre
- Benutzerabmeldung

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

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.

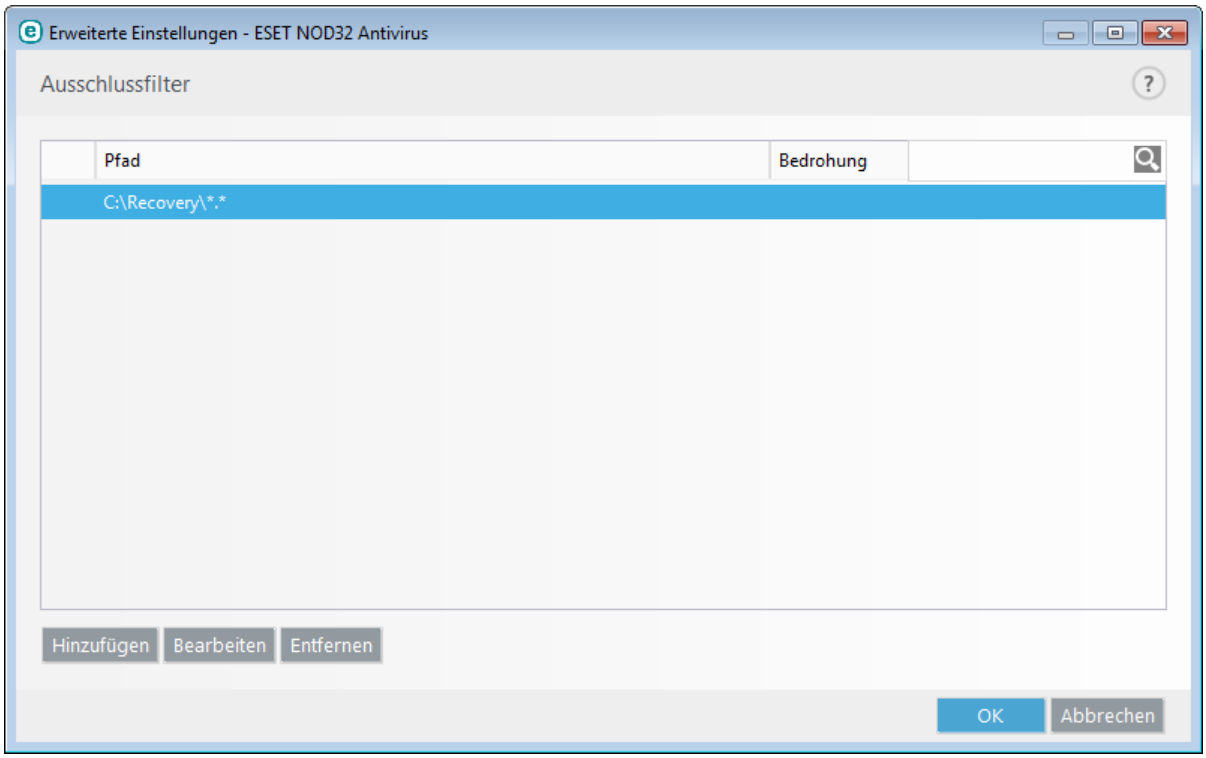
So schließen Sie ein Objekt von Prüfungen aus:

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 Zeichen (und diese variieren) 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** > **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 Erkennung ausnehmen.

Bearbeiten - Ausgewählte Einträge bearbeiten.

Entfernen - Ausgewählten Eintrag entfernen.

4.1.1.6 ThreatSense -Parameter

ThreatSense ist eine Technologie, die verschiedene Methoden zur Erkennung von Bedrohungen verwendet. 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. ThreatSense -Technologie entfernt auch erfolgreich Rootkits.

ThreatSense In den Moduleinstellungen 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,
- Scannen im Leerlaufbetrieb,
- Scannen der Systemstartdateien,
- Dokumentenschutz,
- E-Mail-Client-Schutz,
- Web-Schutz,
- Computerscan.

ThreatSense -Parameter sind für jedes Modul optimal eingerichtet. Eine Veränderung der Einstellungen kann den Systembetrieb deutlich beeinflussen. So kann zum Beispiel eine Änderung der Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der Advanced Heuristik im Modul "Echtzeit-Dateischutz" dazu führen, dass das System langsamer arbeitet (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 - Prüft 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 Archive, die ohne externe Programme dekomprimiert werden 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 Signaturdatenbank verzeichnet sind. Nachteilig ist, dass es in Einzelfällen zu Fehlalarmen kommen kann.

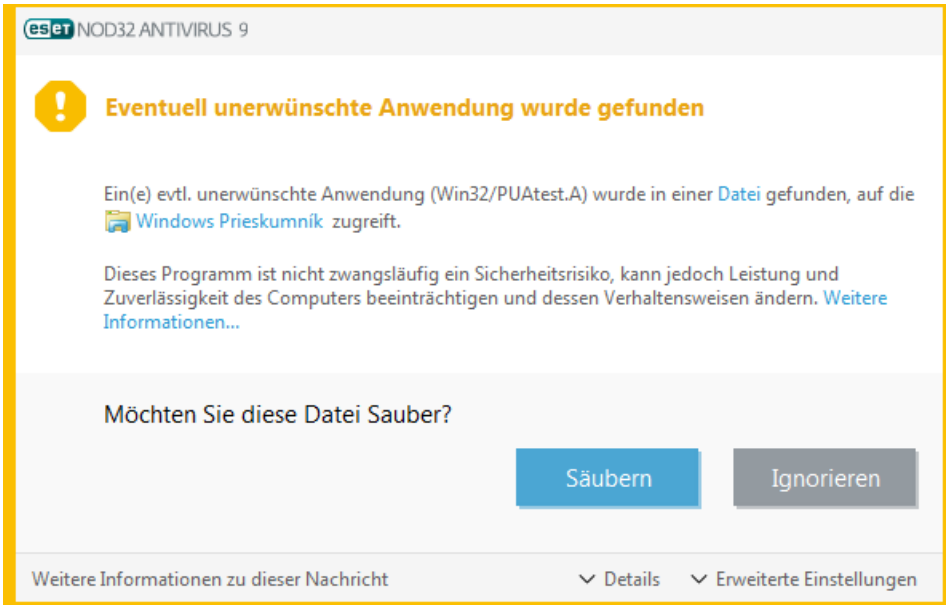
Advanced Heuristik/DNA/Smart-Signaturen - Als Advanced Heuristik werden besondere heuristische Verfahren bezeichnet, die von ESET entwickelt wurden, um eine verbesserte Erkennung von Würmern und Trojanern zu ermöglichen und Schadprogramme zu erkennen, die in höheren Programmiersprachen geschrieben wurden. 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.

Eine eventuell unerwünschte Anwendung ist ein Programm, das Adware enthält, Toolbars installiert oder andere unklare Ziele hat. In manchen Fällen kann ein Benutzer der Meinung sein, dass die Vorteile der evtl. unerwünschten Anwendung bedeutender sind als die Risiken. Aus diesem Grund weist ESET solchen Anwendungen eine niedrigere Risikoeinstufung zu als anderen Schadcodearten wie Trojanern oder Würmern.

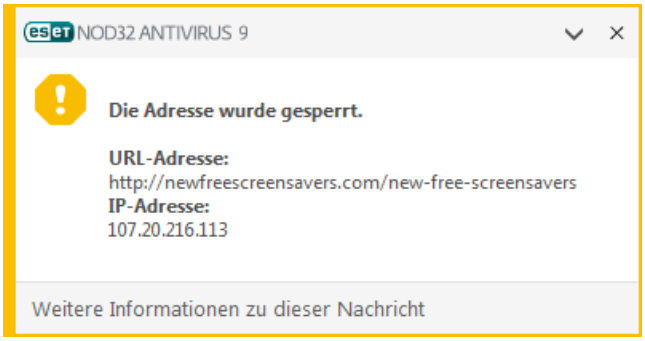
Warnung - Potenzielle Bedrohung erkannt

Wenn eine potenziell unerwünschte Anwendung erkannt wird, können Sie auswählen, welche Aktion ausgeführt werden soll:

1. **Säubern/Trennen**: Mit dieser Option wird die Aktion beendet und die potenzielle Bedrohung daran gehindert, in das System zu gelangen.
2. **Ignorieren**: Bei dieser Option kann eine potenzielle Bedrohung in Ihr System gelangen.
3. Wenn die Anwendung zukünftig ohne Unterbrechung auf dem Computer ausgeführt werden soll, klicken Sie auf **Erweiterte Optionen** und aktivieren Sie das Kontrollkästchen neben **Von der Erkennung** ausschließen.

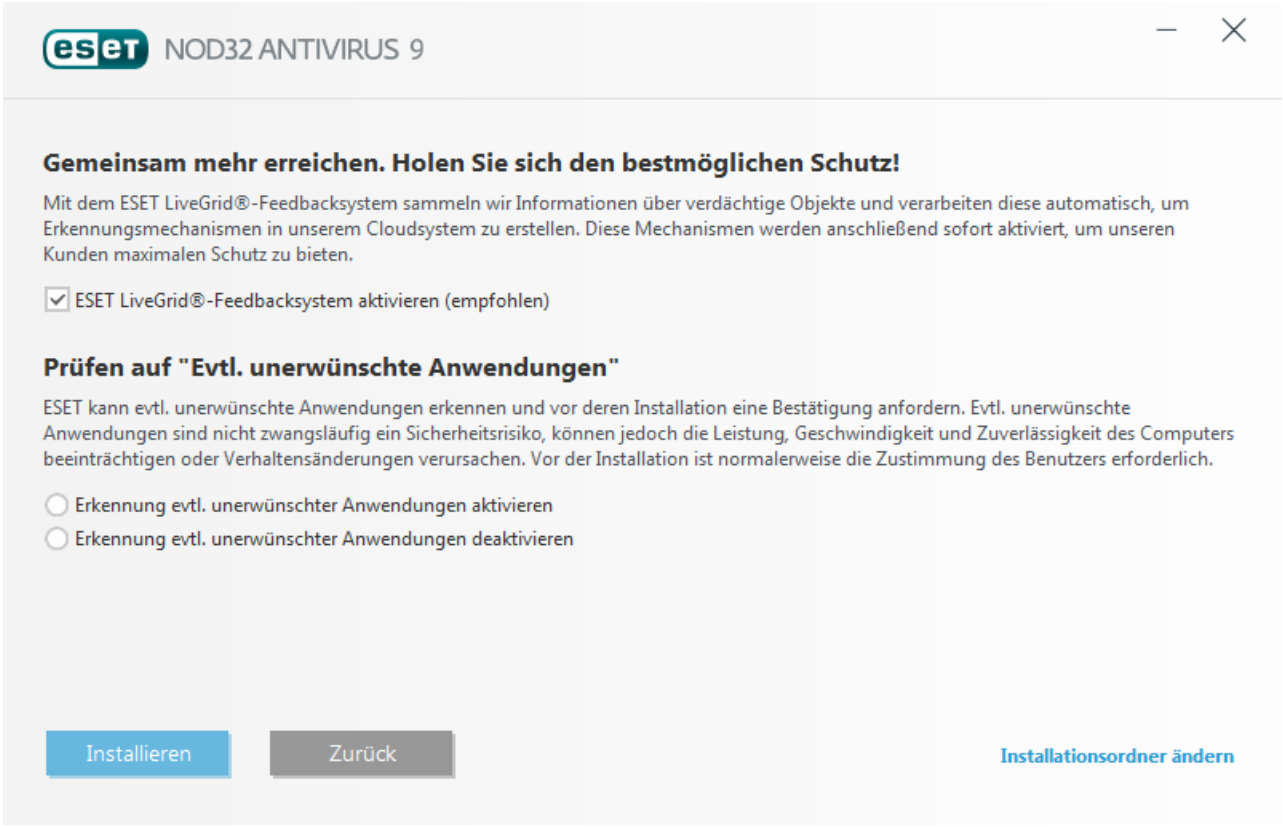


Wenn eine evtl. unerwünschte Anwendung erkannt wird und nicht gesäubert werden kann, erscheint unten rechten im Bildschirm die Benachrichtigung **Adresse wurde gesperrt**. Weitere Informationen hierzu finden Sie unter **Tools** > **Log-Dateien** > **Gefilterte Websites** im Hauptmenü.



Eventuell unerwünschte Anwendungen - Einstellungen

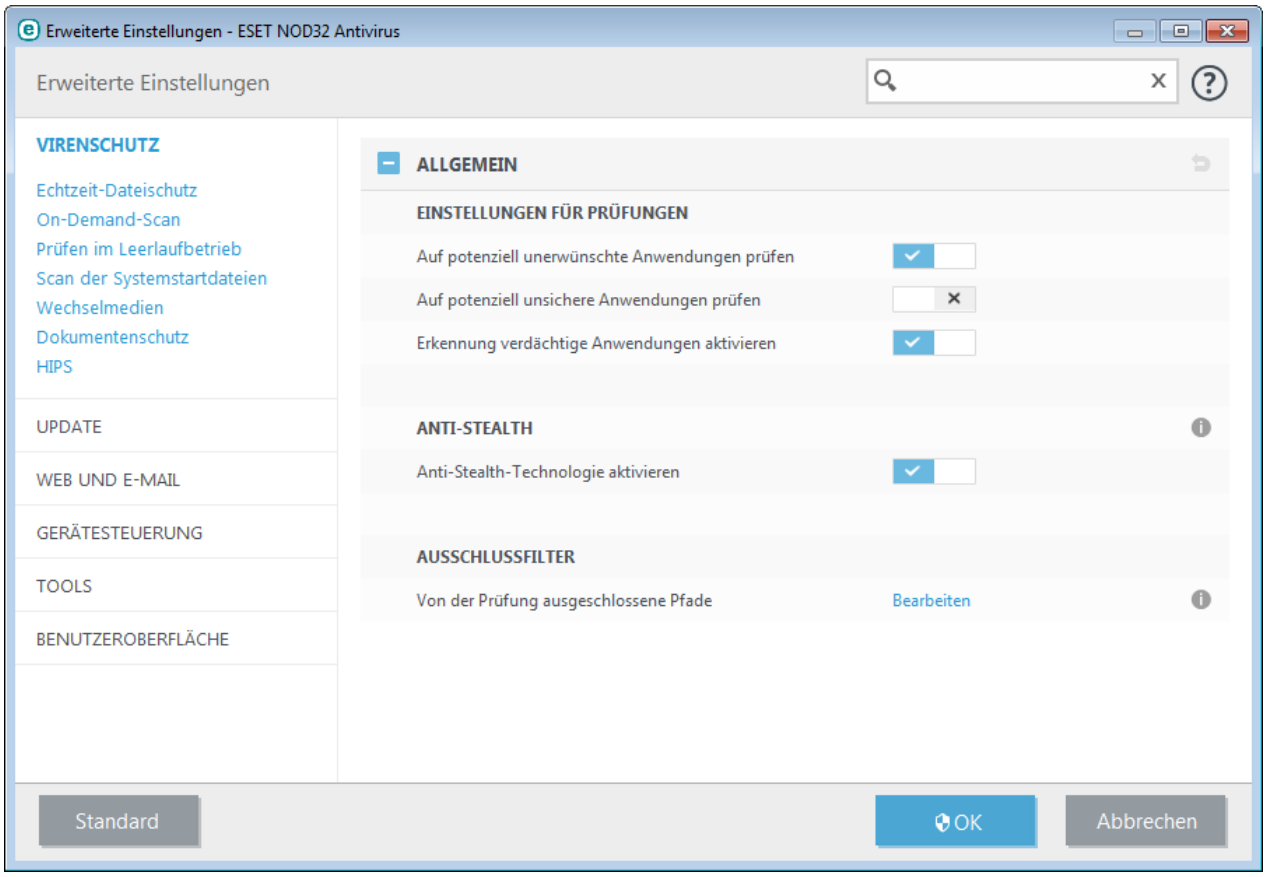
Bei der Installation des ESET-Produkts können Sie auswählen, ob Sie die Erkennung evtl. unerwünschter Anwendungen aktivieren möchten:



Eventuell unerwünschte Anwendungen können Adware oder Toolbars installieren oder andere unerwünschte oder unsichere Programmfunktionen enthalten.

Diese Einstellungen können jederzeit in den Programmeinstellungen geändert werden. Gehen Sie folgendermaßen vor, um die Erkennung evtl. unerwünschter, unsicherer oder verdächtiger Anwendungen zu deaktivieren:

1. Öffnen Sie das ESET-Produkt. Wie öffne ich mein ESET-Produkt?
2. Drücken Sie **F5**, um die **Erweiterten Einstellungen** zu öffnen.
3. Klicken Sie auf **Virenschutz** und aktivieren bzw. deaktivieren Sie die Optionen **Erkennung evtl. unerwünschter Anwendungen aktivieren**, **Auf potenziell unsichere Anwendungen prüfen** und **Auf potenziell verdächtige Anwendungen prüfen**. Klicken Sie zum Bestätigen auf **OK**.



Eventuell unerwünschte Anwendungen - Software-Wrapper

Ein Software-Wrapper ist eine besondere Art Anwendungsänderung, die von einigen Dateihost-Websites verwendet wird. Es handelt sich um ein Drittanbieter-Tool, das neben der gewünschten Anwendung zusätzliche Software wie Toolbars oder Adware installiert. Die zusätzliche Software kann auch Änderungen an der Startseite des Webbrowsers und an den Sucheinstellungen vornehmen. Außerdem setzen Dateihost-Websites den Softwarehersteller oder den Download-Empfänger oft nicht über solche Änderungen in Kenntnis und ermöglichen nicht immer eine einfach Abwahl der Änderung. Aus diesem Grund stuft ESET Software-Wrapper als eine Art evtl. unerwünschter Anwendung ein, damit der Benutzer den Download wissen annehmen oder ablehnen kann.

Eine aktualisierte Version dieser Hilfeseite finden Sie in diesem ESET-Knowledgebase-Artikel.

Potenziell unsichere Anwendungen - Potenziell unsichere Anwendungen sind zum Beispiel Programme zum Fernsteuern von Computern (Remotedesktopverbindung), zum Entschlüsseln von Passwörtern sowie Keylogger (Programme, die Tastenanschläge von Benutzern aufzeichnen). 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 - Mit dieser Option werden alle geprüften Dateien im Log eingetragen, also auch Dateien, 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 Prüfzeit 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.

In der Standardeinstellung werden alle Dateien unabhängig von ihrer Erweiterung 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 und klicken Sie anschließend 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 „*“ (Sternchen) und „?“ (Fragezeichen) verwenden. Das Sternchen ersetzt eine beliebige Zeichenfolge, das Fragezeichen ein beliebiges Symbol.

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

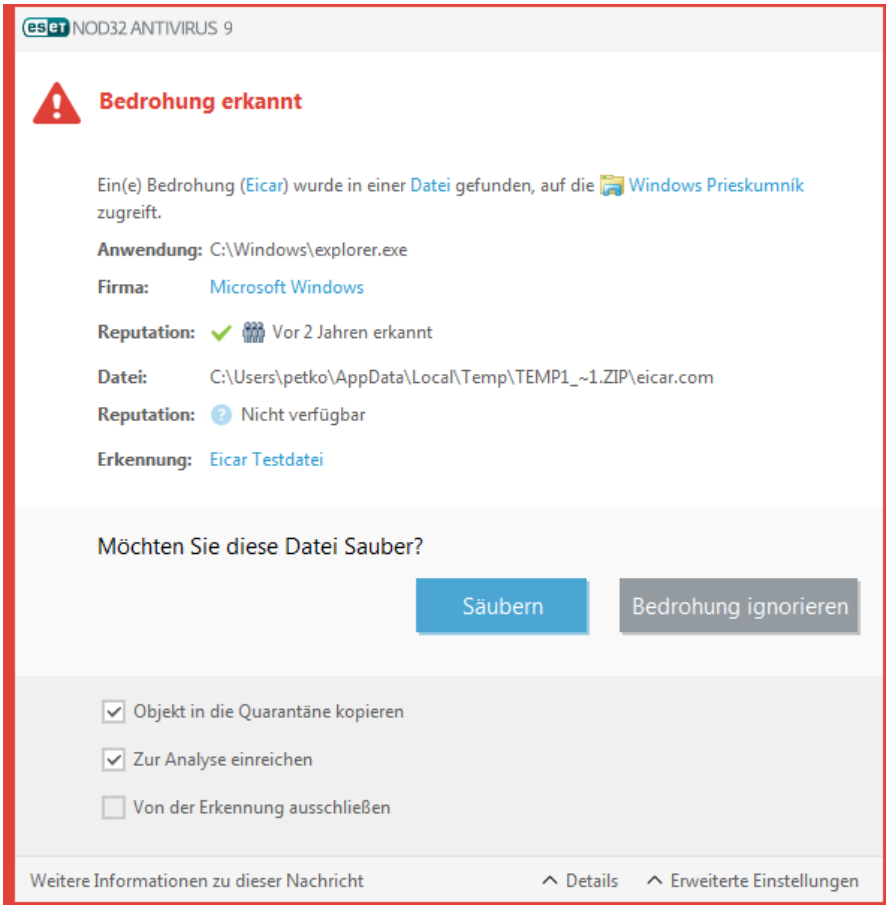
ESET NOD32 Antivirus kann Bedrohungen mit einem der folgenden Module erkennen:

- Echtzeit-Dateischutz
- Web-Schutz
- E-Mail-Client-Schutz
- On-Demand-Scan

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 NOD32 Antivirus und klicken Sie auf „Computer prüfen“
- Klicken Sie auf **Scannen Sie Ihren Computer** (weitere Informationen siehe Computerscan)
- 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 **Benutzerdefinierter Scan** 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 auf Systemen, die keiner großen Anzahl an Microsoft Office-Dokumenten ausgesetzt sind, die Leistung zu verbessern.

Die Option **Systemintegration** aktiviert das Schutzmodul. Um die Option zu ändern, klicken Sie in den **Erweiterten Einstellungen** (F5) in der Baumstruktur auf **Virenschutz** > **Dokumentenschutz**.

Die Funktion wird von Anwendungen aktiviert, die Microsoft Antivirus API verwenden (beispielsweise Microsoft Office 2000 und später oder Microsoft Internet Explorer 5.0 und später).

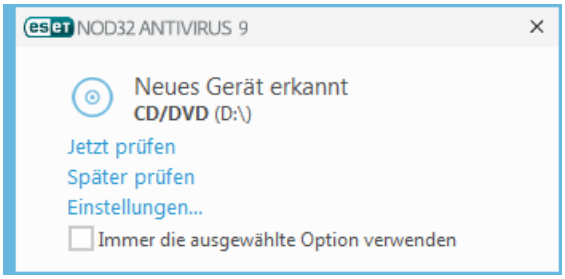
4.1.2 Wechselmedien

ESET NOD32 Antivirus 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 scannen** - Es wird keine Aktion ausgeführt und das Fenster **Neues Gerät erkannt** wird geschlossen.
- **Automatischer Gerätescan** - Eine On-Demand-Prüfung des eingelegten Wechselmediums wird durchgeführt.
- **Scanoptionen anzeigen** - Öffnet die Einstellungen für Wechselmedien.

Beim Einlegen eines Wechselmediums wird folgender Dialog angezeigt:



Jetzt scannen - Startet den Wechselmedienscan.

Später scannen - Der Wechselmedienscan 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 NOD32 Antivirus 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

ESET NOD32 Antivirus bietet Methoden zur automatischen Prüfung von Geräten (CD/DVD/USB/...). Mit diesem Modul können Sie Medien bzw. Geräte prüfen oder 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
- Alle Gerätetypen

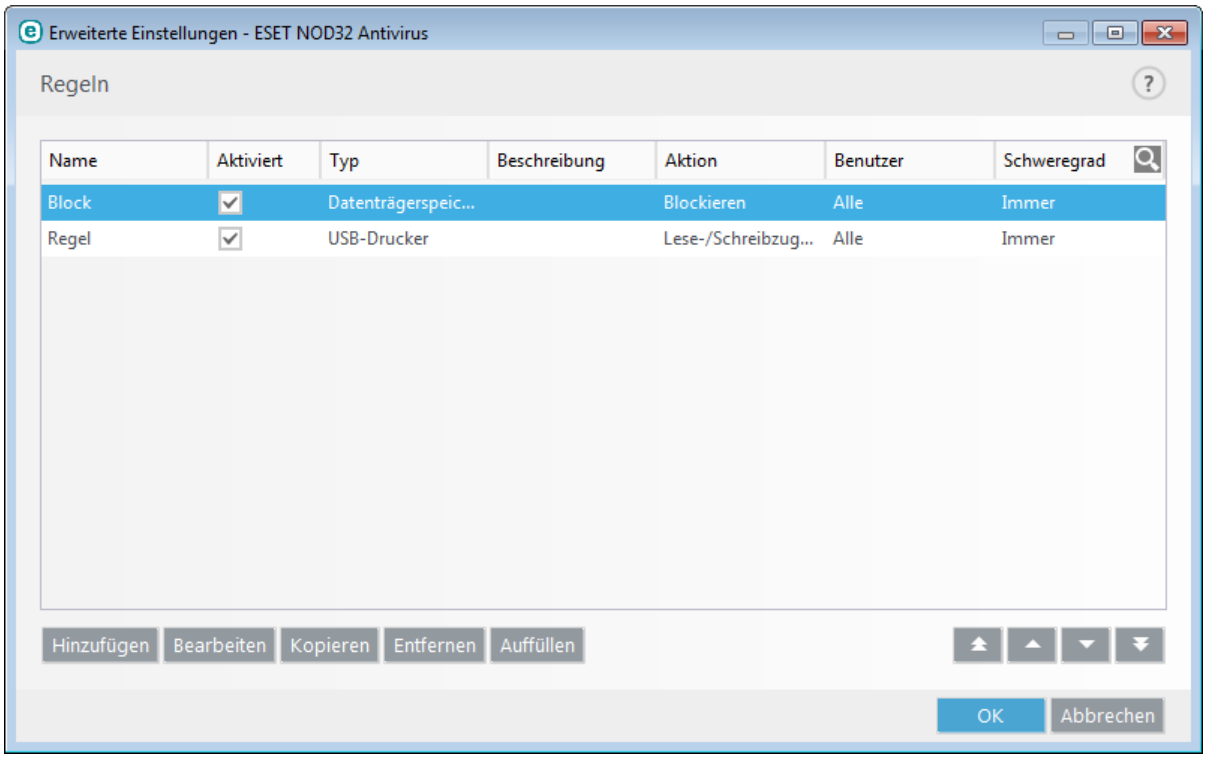
Die Einstellungen für die Medienkontrolle können unter **Erweiterte Einstellungen** (F5) > **Medienkontrolle** geändert werden.

Über das Kontrollkästchen **Systemintegration** aktivieren Sie die Funktion Medienkontrolle in ESET NOD32 Antivirus. 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.

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

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 zum Bearbeiten von Regeln auf **Hinzufügen** oder **Bearbeiten**. Klicken Sie auf **Kopieren**, um eine neue Regel mit vordefinierten Optionen 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. Über das Kontrollkästchen **Aktiviert** können Sie eine Regel deaktivieren und aktivieren. Dies ist besonders dann hilfreich, wenn Sie eine Regel nicht dauerhaft löschen möchten, um sie gegebenenfalls zu einem späteren Zeitpunkt wieder verwenden zu können.

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

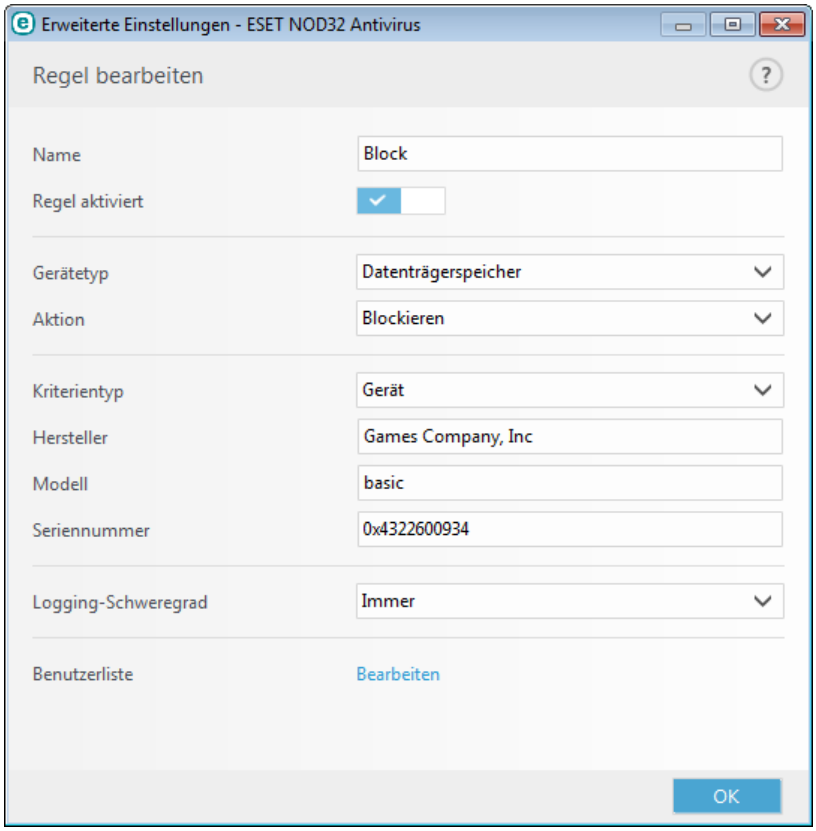
Um Log-Einträge anzuzeigen, klicken Sie im Hauptfenster von ESET NOD32 Antivirus auf **Tools** > **Log-Dateien**.

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

Klicken Sie auf die Option **Auffüllen**, um automatisch die Parameter für am Computer angeschlossene Wechselmedien zu übernehmen.

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. Click the switch next to **Rule enabled** to disable or enable this rule; this can be useful if you don't want to delete the rule permanently.

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.

TIPP: 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 NOD32 Antivirus 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.

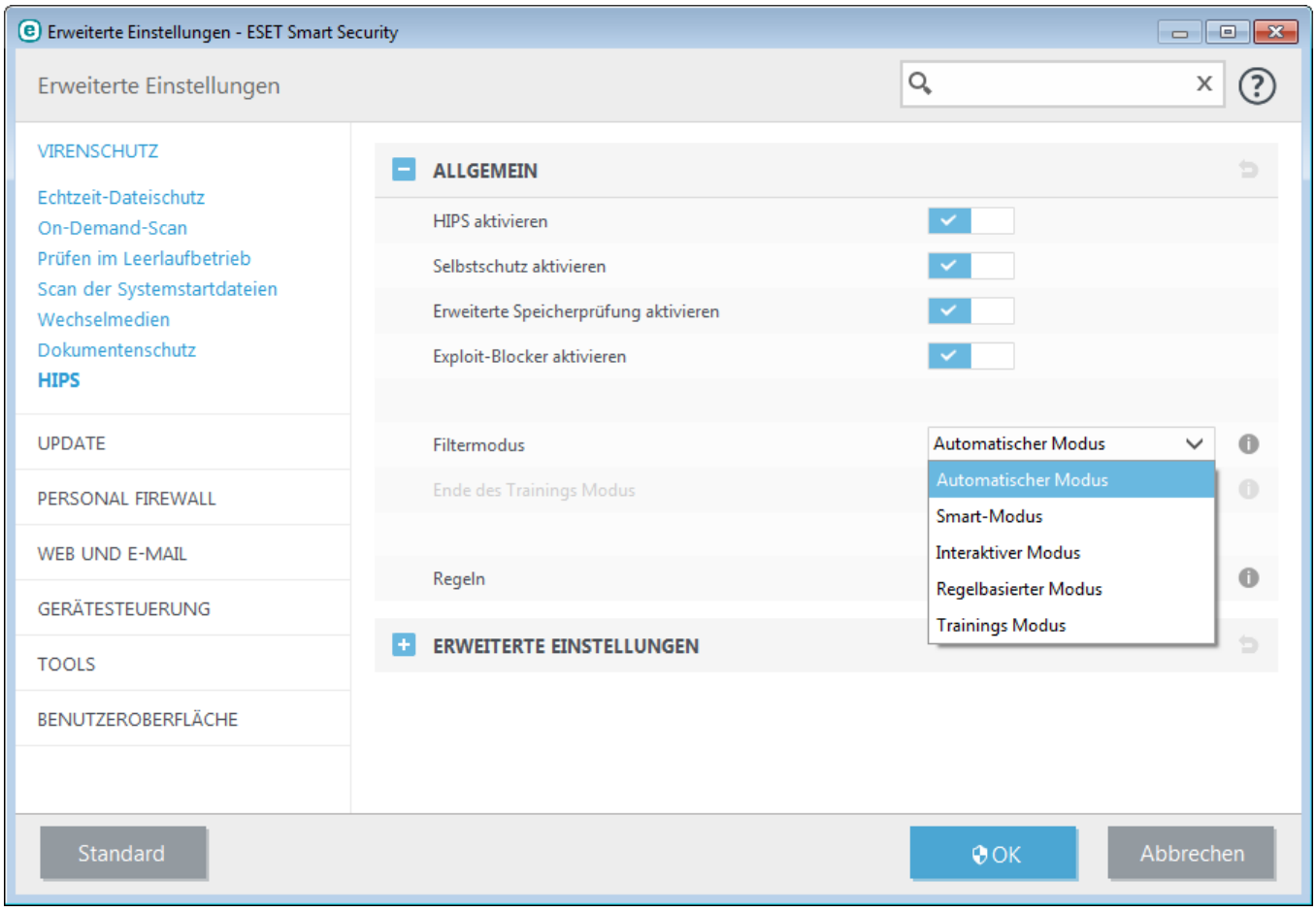
HINWEIS: Alle Geräte können über Benutzerregeln eingeschränkt werden (Bildverarbeitungsgeräte liefern beispielsweise keine Informationen über Benutzer, sondern nur über ausgeführte Aktionen).

4.1.4 Host-based Intrusion Prevention System (HIPS)

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.

Die HIPS-Einstellungen finden Sie unter **Erweiterte Einstellungen** (F5) > **Virenschutz** > **HIPS** > **Einfach**. Der HIPS-Status (aktiviert/deaktiviert) wird im Hauptprogrammfenster von ESET NOD32 Antivirus unter **Einstellungen** > **Computer-Schutz** angezeigt.



ESET NOD32 Antivirus nutzt die integrierte **Self-Defense**-Technologie, die Beschädigungen oder eine Deaktivierung Ihres Viren- und Spyware-Schutzes durch Schadsoftware verhindert. So ist Ihr System nie ungeschützt. Um HIPS oder die Self-Defense-Technologie zu deaktivieren, ist ein Neustart von Windows erforderlich.

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 dieser Art des Schutzes finden Sie in unserem 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.

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.

Smart-Modus - Der Benutzer wird nur über sehr verdächtige Ereignisse benachrichtigt.

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

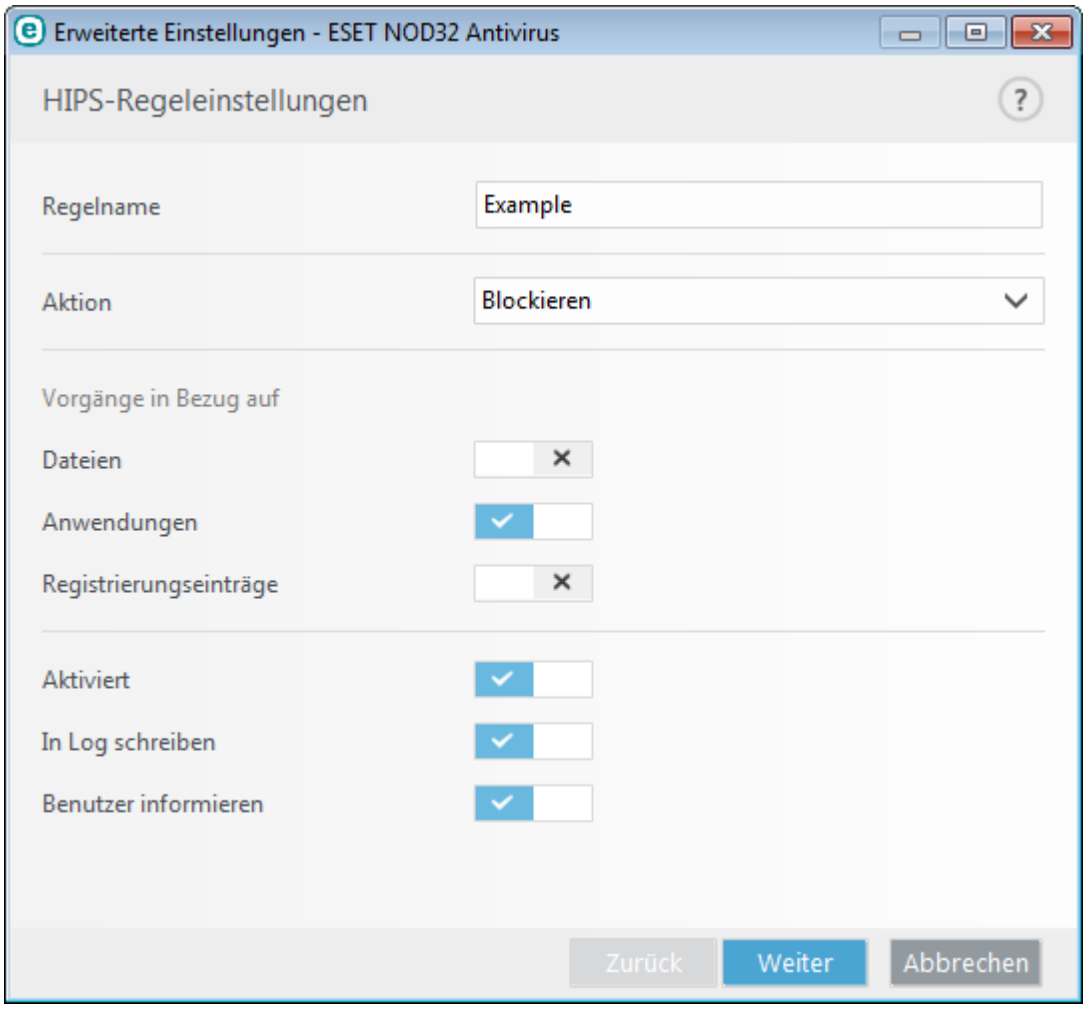
Regelbasierter Filtermodus - Vorgänge werden blockiert.

Trainingsmodus - Vorgänge werden ausgeführt, 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 Dauer für den Trainingsmodus aus. Die maximale Dauer ist 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.

HIPS überwacht Ereignisse auf Betriebssystemebene und führt Aktionen gemäß Regeln aus, die den Regeln für die Personal Firewall ähneln. Klicken Sie auf **Bearbeiten**, um das Fenster zur HIPS-Regelverwaltung zu öffnen. Hier können Sie Regeln auswählen, erstellen, bearbeiten und löschen.

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.

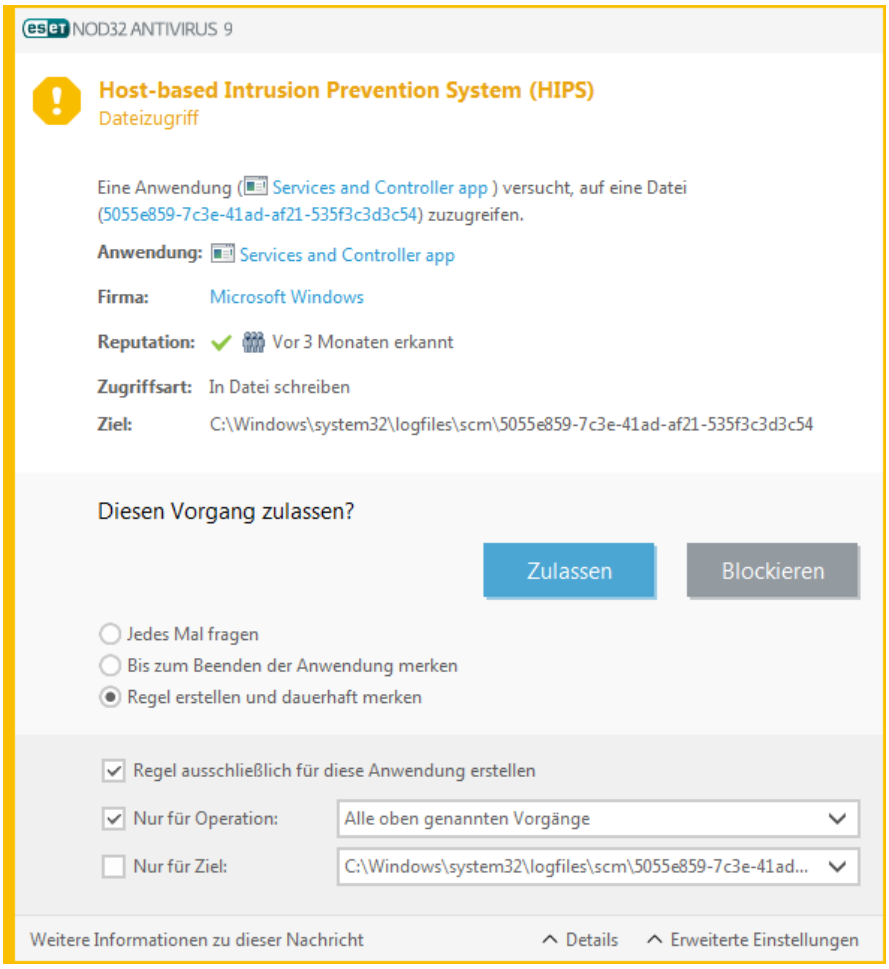
Alle blockierten Vorgänge in Log aufnehmen - Alle blockierten Vorgänge werden in den HIPS-Log geschrieben.

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.

4.1.5 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 angezeigt.

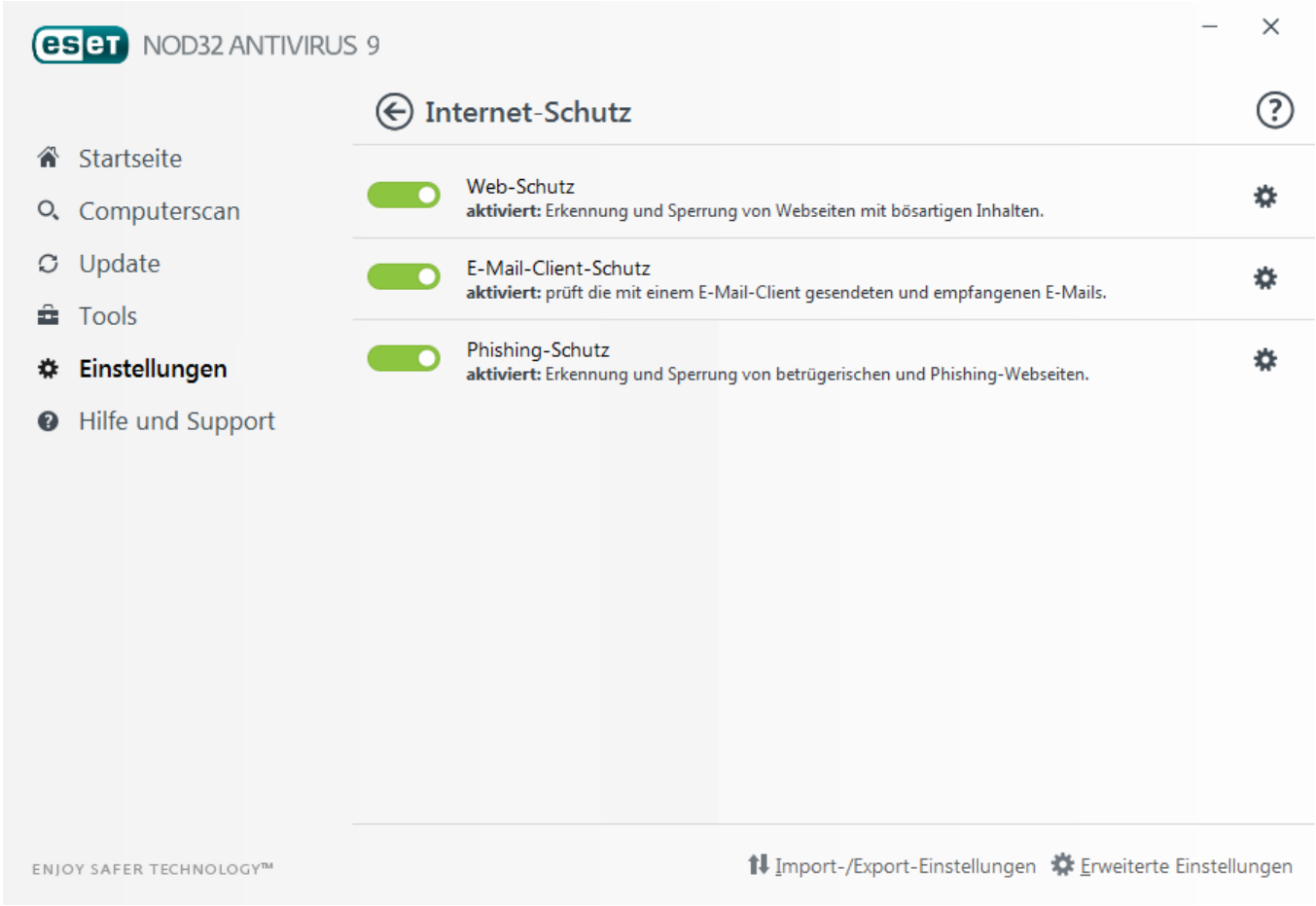
Alternativ können Sie den Gamer-Modus über die erweiterten Einstellungen (F5) aktivieren, indem Sie den Eintrag **Computer** erweitern, auf **Gamer-Modus** klicken und das Kontrollkästchen neben **Gamer-Modus aktivieren** aktivieren.

Mit der Option **Gamer-Modus automatisch aktivieren, wenn Anwendungen im Vollbildmodus ausgeführt werden** unter Erweiterte Einstellungen (F5) 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.

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- 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 NOD32 Antivirus Kontrollfunktionen für die gesamte ein- und ausgehende E-Mail-Kommunikation (POP3, MAPI, IMAP, HTTP) bereit.

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

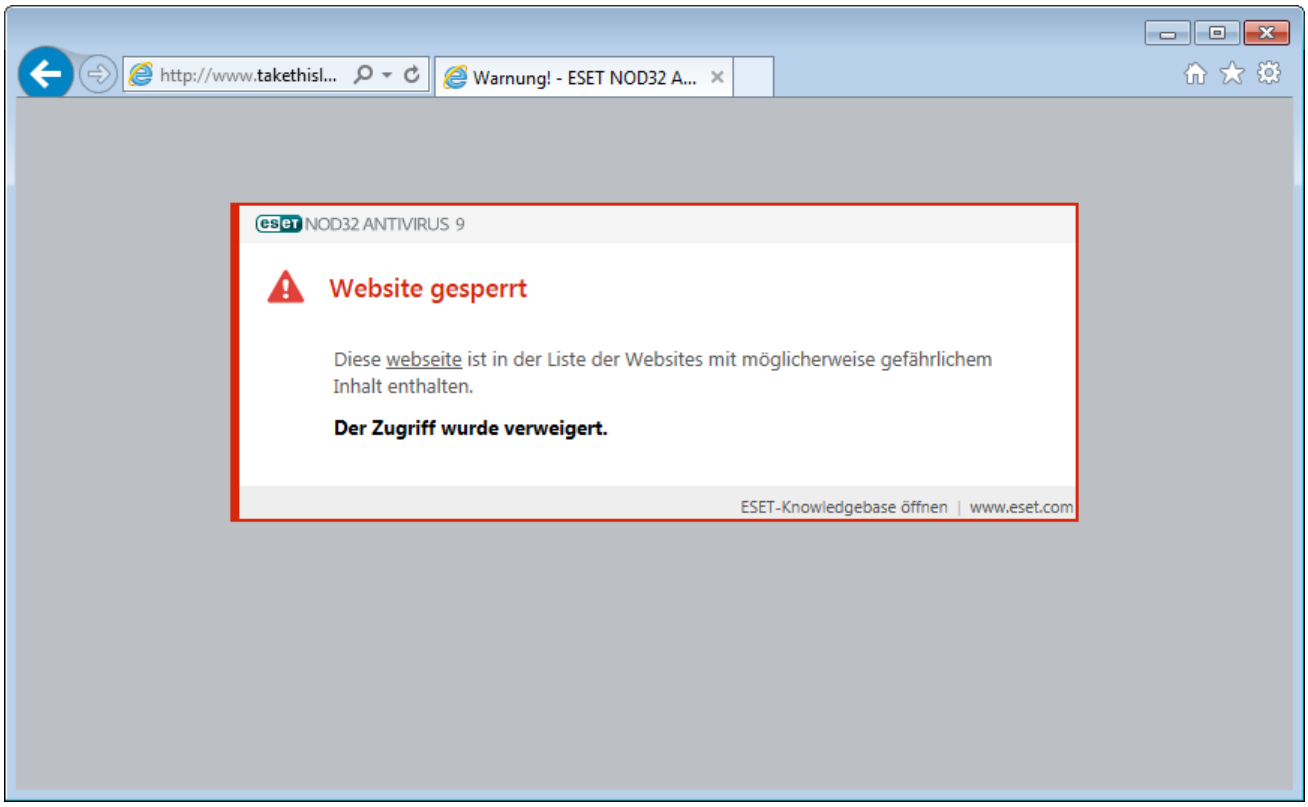
Sie können den Web-/E-Mail-/Phishing Schutz kann durch Klicken auf  vorübergehend deaktivieren.

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 bekanntermaßen 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 NOD32 Antivirus 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 möglicherweise nicht ordnungsgemäß.

HINWEIS: Es wird dringend empfohlen, diese Option aktiviert zu lassen.

4.2.1.2 Webprotokolle

ESET NOD32 Antivirus 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 NOD32 Antivirus unterstützt auch die HTTPS-Protokollprüfung. Bei der HTTPS-Kommunikation wird ein verschlüsselter Kanal für die Datenübertragung zwischen Server und Client verwendet. ESET NOD32 Antivirus 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 unter **Vom HTTPS-Protokoll verwendete Ports** definiert wurden.

Der Datenverkehr über verschlüsselte Verbindungen wird nicht geprüft. Zur Aktivierung der Prüfung verschlüsselter Verbindungen und zur Anzeige der Prüfeinstellungen 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.

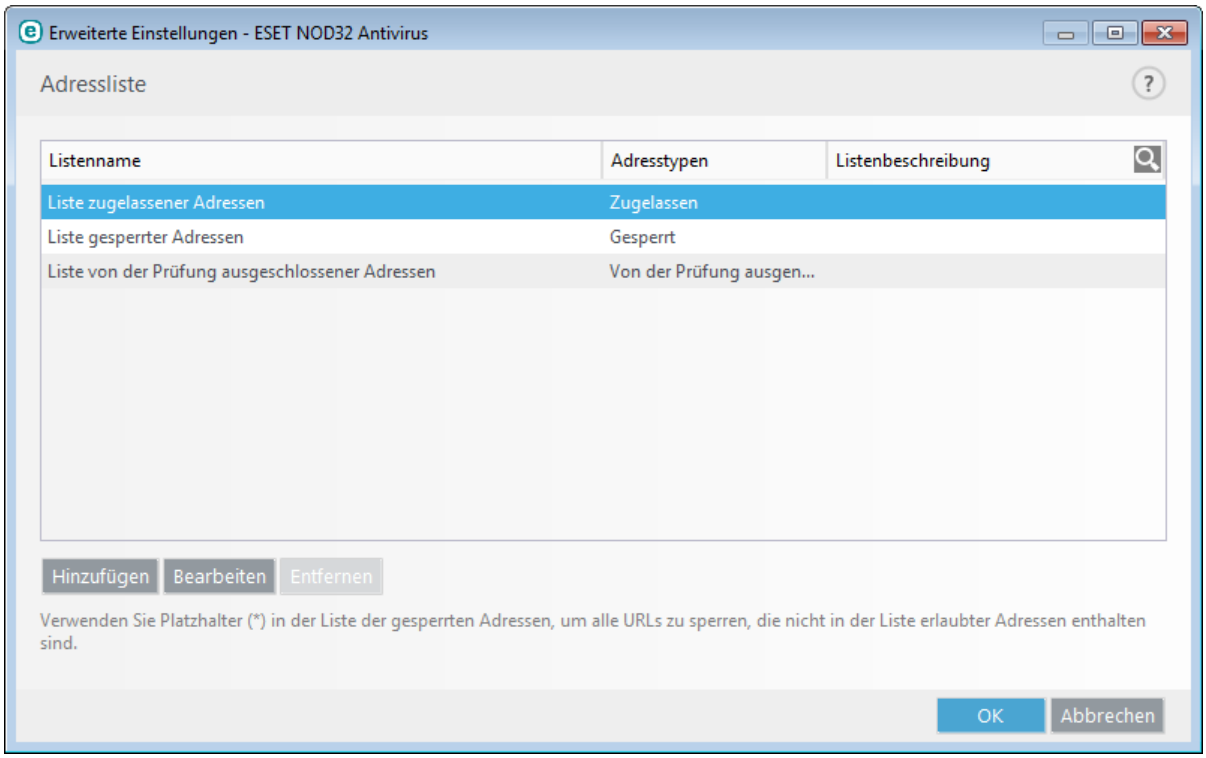
Wenn Sie eine URL-Adresse zur **Liste der von der Prüfung ausgenommenen Adressen** hinzufügen, wird diese von der Prüfung ausgenommen. Sie können auch bestimmte Adressen zulassen oder blockieren, indem Sie sie zur **Liste zugelassener Adressen** oder zur **Liste blockierter Adressen** hinzufügen.

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.

TIPP: 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.

Entfernen - Löschen einer bestehenden Liste. Es können nur Listen entfernt werden, die mit der Option **Hinzufügen** erstellt wurden; nicht Standardlisten.

4.2.2 E-Mail-Client-Schutz

4.2.2.1 E-Mail-Programme

Die Integration von ESET NOD32 Antivirus 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 NOD32 Antivirus aktiviert werden. Wenn die Integration aktiviert ist, wird die ESET NOD32 Antivirus-Symbolleiste direkt in das E-Mail-Programm integriert und ermöglicht einen effizienteren E-Mail-Schutz (bei neueren Versionen von Windows Live Mail wird die Symbolleiste nicht integriert). Die Integrationseinstellungen befinden sich unter **Einstellungen** > **Erweiterte Einstellungen** > **Web und E-Mail** > **E-Mail-Client-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-Client-Schutz (POP3, IMAP) weiterhin geschützt.

Aktivieren Sie die Option **Prüfen neuer Elemente im Posteingang deaktivieren**, falls Sie während der Arbeit mit

Ihrem E-Mail-Programm eine Systemverlangsamung bemerken (nur MS Outlook). Dies kann der Fall sein, wenn Sie E-Mails vom Kerio Outlook Connector Store abrufen.

Zu prüfende E-Mails

Eingehende E-Mails - Aktiviert/deaktiviert die Überprüfung empfangener Nachrichten.
Ausgehende E-Mails - Aktiviert/deaktiviert die Überprüfung ausgehender Nachrichten.
Gelesene E-Mails - 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.

Scan nach Signaturdatenbank-Update wiederholen - Aktiviert/deaktiviert die erneute Prüfung nach einem Signaturdatenbank-Update.

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

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 NOD32 Antivirus 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.

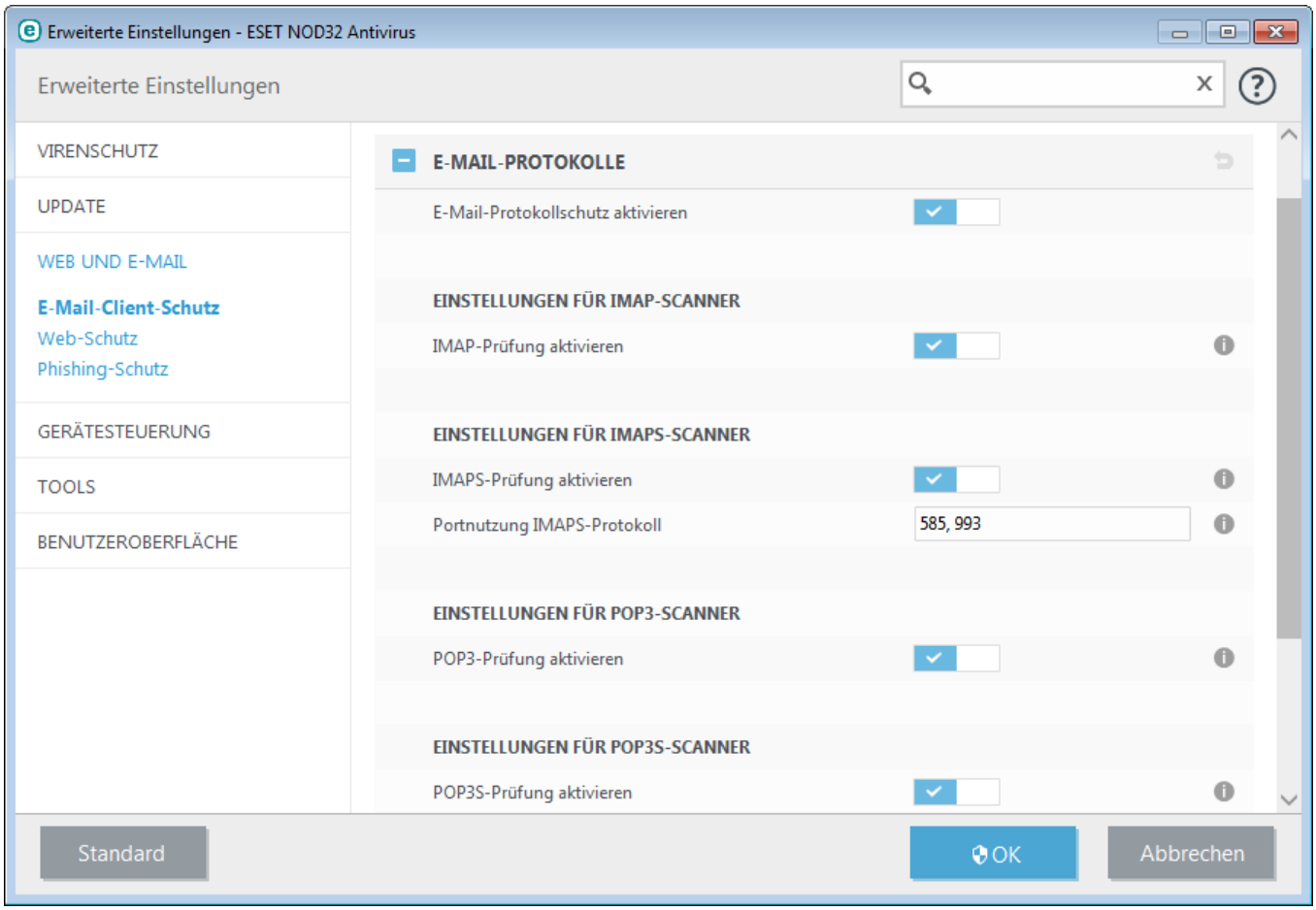
Die IMAP/IMAPS- und POP3/POP3S-Protokollprüfung kann in den erweiterten Einstellungen konfiguriert werden. Sie finden diese Einstellung unter **Web und E-Mail** > **E-Mail-Schutz** > **E-Mail-Protokolle**.

E-Mail-Protokollschutz 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 NOD32 Antivirus unterstützt außerdem die Prüfung von IMAPS- und POP3S-Protokollen, die Daten zwischen Server und Client über einen verschlüsselten Kanal übertragen. ESET NOD32 Antivirus 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.

Der Datenverkehr über verschlüsselte Verbindungen wird nicht geprüft. Zur Aktivierung der Prüfung verschlüsselter Verbindungen und zur Anzeige der Prüfeinstellungen 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. Mithilfe der Plug-In-Software für Microsoft Outlook und andere E-Mail-Programme stellt ESET NOD32 Antivirus Kontrollfunktionen für die gesamte E-Mail-Kommunikation (POP3, MAPI, IMAP, HTTP) bereit. Für die Prüfung eingehender Nachrichten verwendet das Programm alle erweiterten ThreatSense-Prüfmethoden. Die Erkennung von Schadcode findet also noch vor dem Abgleich mit der Signaturdatenbank 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-Client-Schutz** > **Warnungen und Hinweise**.

ThreatSense Parameter - Dieser Bereich enthält erweiterte Einstellungen für den Virenschutz. Hier können Sie Einstellungen für zu scannende Objekte, Erkennungsmethoden usw. festlegen. Klicken Sie, um die erweiterten Einstellungen für den Virenschutz anzeigen.

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 zu E-Mails 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 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 beim Empfänger auch die Glaubwürdigkeit von

Nachrichten. Bei der Erkennung von eingedrungener Schadsoftware stehen wertvolle Informationen zur Verfügung, um den Bedrohungsgrad durch die Nachricht oder den Absender einzuschätzen.

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 NOD32 Antivirus 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 NOD32 Antivirus aktiviert werden. Bei aktivierter Integration wird die ESET NOD32 Antivirus-Symbolleiste vom E-Mail-Programm übernommen, d. h. die Verbindungen werden kontrolliert und die E-Mail-Kommunikation wird dadurch sicherer. Die Integrationseinstellungen finden Sie unter **Einstellungen** > **Erweiterte Einstellungen...** > **Web und E-Mail** > **E-Mail-Client-Schutz** > **Integration in E-Mail-Programme**.

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-Client-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 NOD32 Antivirus 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.

Der Datenverkehr über verschlüsselte Verbindungen wird nicht geprüft. Zur Aktivierung der Prüfung verschlüsselter Verbindungen und zur Anzeige der Prüfeinstellungen 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.

Prüfen von E-Mails 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 NOD32 Antivirus unterstützt auch die Überwachung von POP3S-Protokollen. Bei dieser Kommunikationsart wird zur Datenübertragung zwischen Server und Client ein verschlüsselter Kanal verwendet. ESET NOD32 Antivirus 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).

4.2.3 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 NOD32 Antivirus 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.

Web 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.

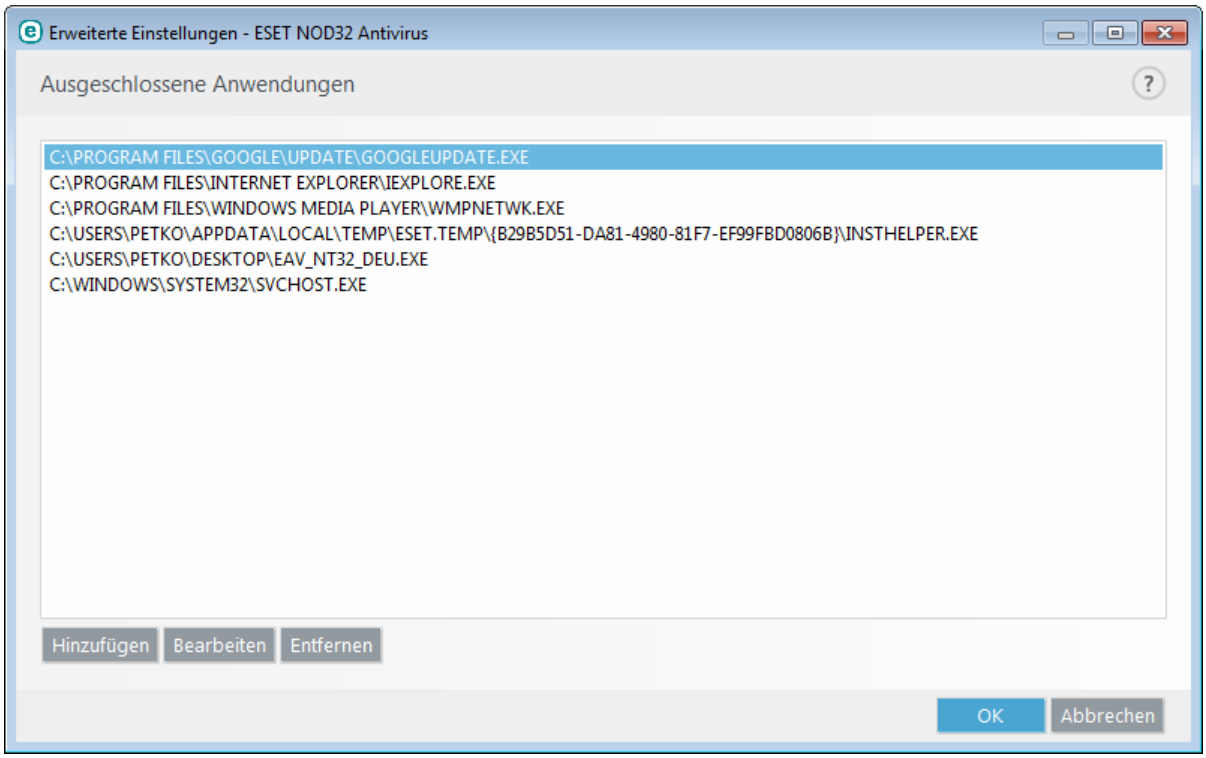
Da im Internet Sicherheitsbedrohungen allgegenwärtig sind, ist sicheres Internetsurfen besonders wichtig. Durch Sicherheitslücken in Webbrowsern und gefälschte Hyperlinks kann Schadcode unbemerkt in Ihr System eindringen. Deshalb bietet ESET NOD32 Antivirus besondere Funktionen zur Verbesserung der Sicherheit 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.

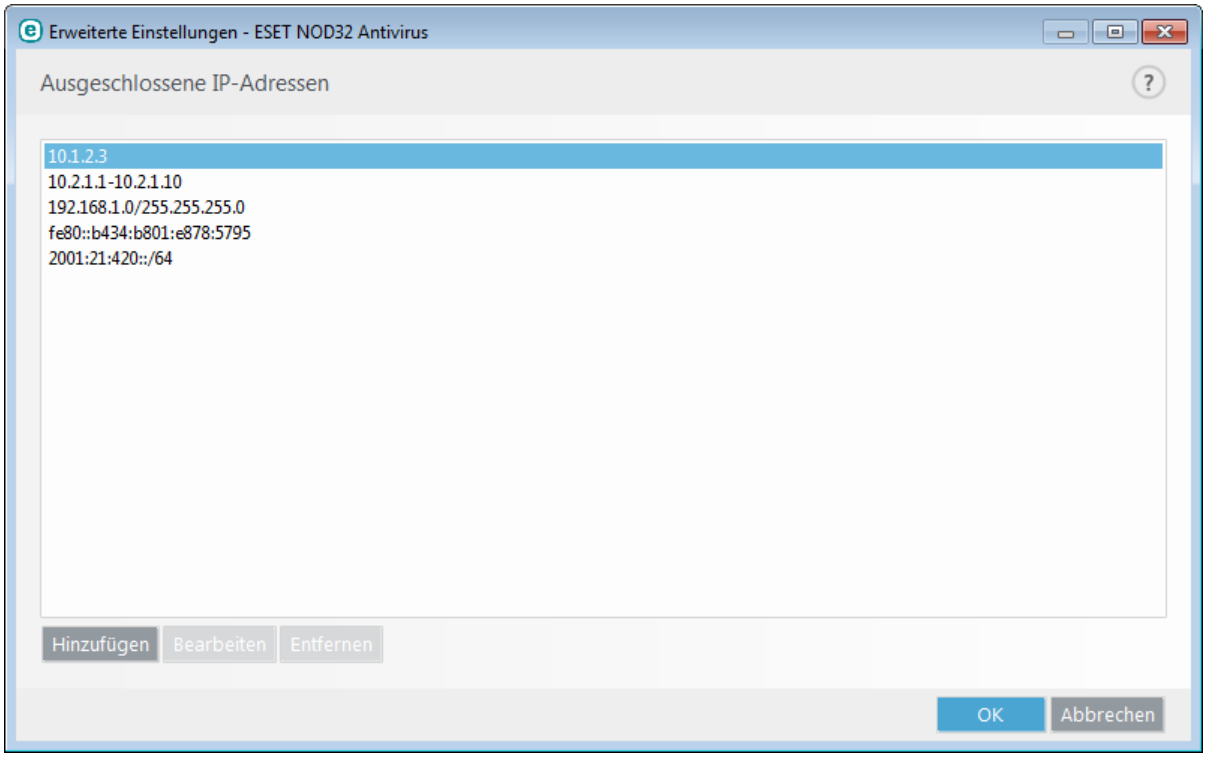


4.2.3.3 Ausgeschlossene IP-Adressen

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 NOD32 Antivirus 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, mit SSL geschützten Seite (mit unbekanntem Zertifikat) wird ein Dialogfeld mit möglichen Aktionen angezeigt. In diesem Modus können Sie eine Liste von SSL-Zertifikaten 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 NOD32 Antivirus für bestimmte Anwendungen anpassen.

Liste bekannter Zertifikate - Mit dieser Liste können Sie das Verhalten von ESET NOD32 Antivirus für bestimmte SSL-Zertifikate anpassen.

Kommunikation mit Zertifikaten für die erweiterte Überprüfung (EV-Zertifikate) ausschließen - Mit dieser Option wird die Kommunikation mit dieser Art von SSL-Zertifikat von der Prüfung ausgeschlossen. Zertifikate für die erweiterte Überprüfung stellen sicher, dass Sie wirklich die gewünschte Website sehen, und keine Fälschung (typisch für Phishing-Seiten).

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 NOD32 Antivirus 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 wurde 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.

4.2.3.4.2 Liste bekannter Zertifikate

Mit der **Liste bekannter Zertifikate** können Sie das Verhalten von ESET NOD32 Antivirus 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.

Scannen - Wählen Sie **Scannen** oder **Ignorieren** als **Scan-Aktion** 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

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-Filter betroffenen Anwendungen

Mit der **Liste der vom SSL-Filter betroffenen Anwendungen** können Sie das Verhalten von ESET NOD32 Antivirus für bestimmte Anwendungen anpassen und gewählte Aktionen speichern, wenn der **Interaktive Modus** als **Filtermodus für das SSL-Protokoll** ausgewählt ist. Sie können die Liste unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **SSL/TLS** > **Liste der vom SSL-Filter betroffenen Anwendungen** anzeigen und bearbeiten.

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

Spalten

Anwendung - Name der Anwendung.

Scan-Aktion - Wählen Sie **Scannen** oder **Ignorieren** aus, um die Kommunikation 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 - 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

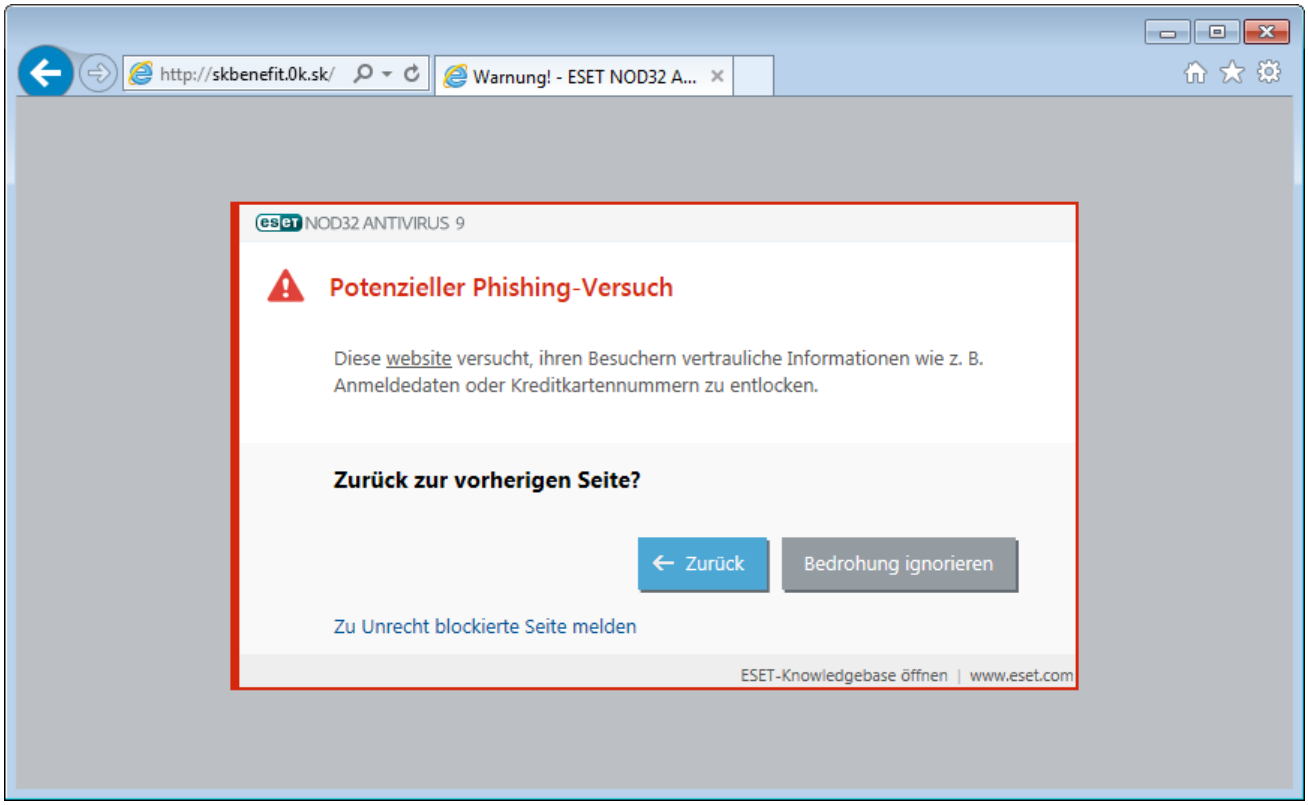
Der Begriff „Phishing“ bezeichnet eine kriminelle Vorgehensweise, die sich Techniken des Social Engineering (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Phishing wird oft eingesetzt, um Zugriff auf vertrauliche Daten zu erlangen, wie Kontonummern oder PIN-Codes. Weitere Informationen zu diesem Angriffstyp finden Sie im Glossar. ESET NOD32 Antivirus enthält einen Phishing-Schutz: Webseiten, die dafür bekannt sind, Phishing-Inhalte zu enthalten, können gesperrt werden.

Wir empfehlen, den Phishing-Schutz in ESET NOD32 Antivirus 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 NOD32 Antivirus.

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.).

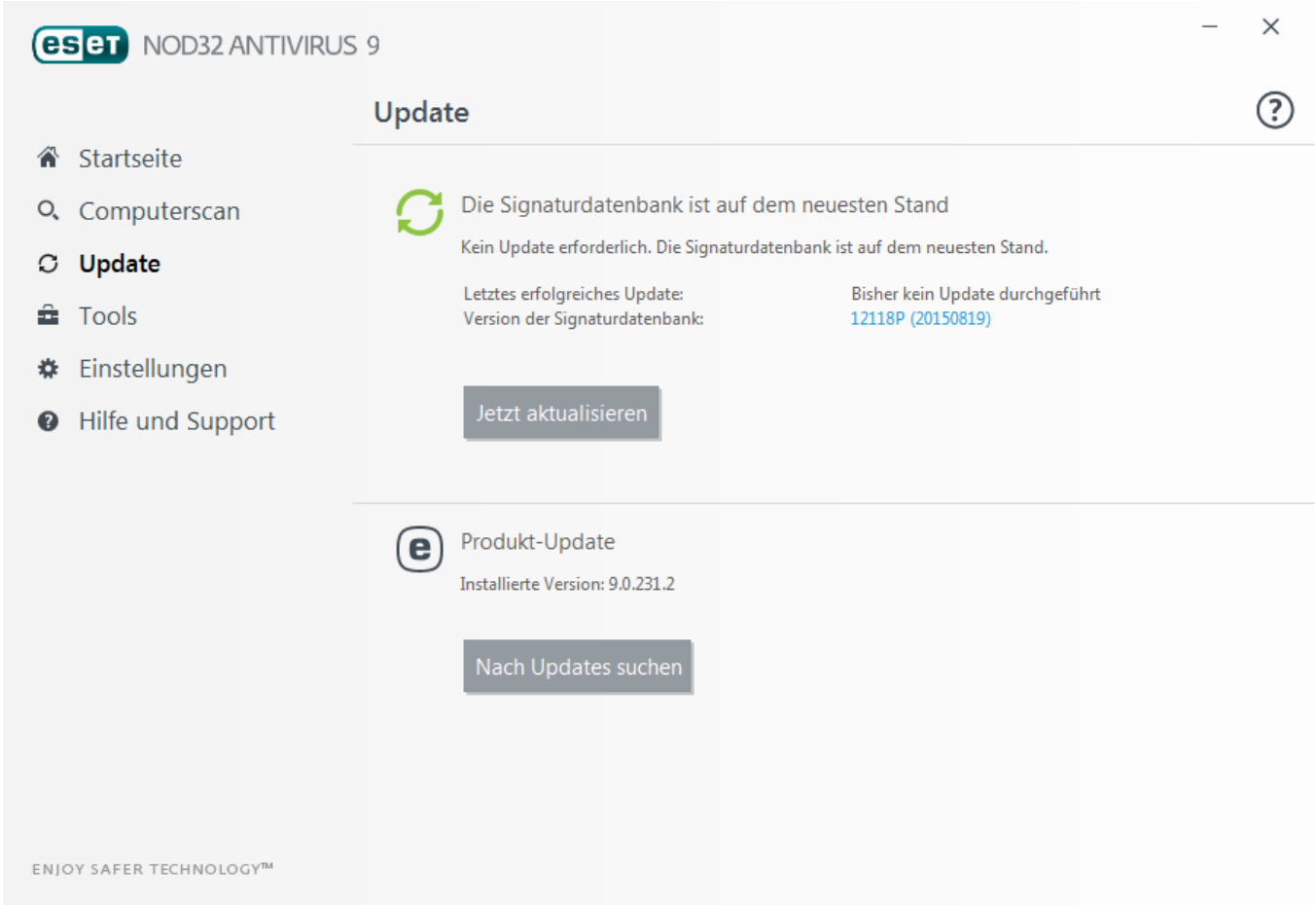
4.3 Aktualisieren des Programms

Den optimalen Schutz Ihres Computers gewährleisten Sie, indem Sie ESET NOD32 Antivirus regelmäßig aktualisieren. Die Updates halten das Programm fortlaufend auf dem neuesten Stand, indem die Signaturdatenbank und die Programmkomponenten aktualisiert werden.

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. Die Versionsnummer der Signaturdatenbank wird ebenfalls in diesem Fenster angezeigt. Diese Nummer ist ein aktiver Link zur Website von ESET, auf der alle Signaturen aufgeführt werden, die bei dem entsprechenden Update hinzugefügt wurden.

Zusätzlich zu automatischen Updates können Sie auf **Jetzt aktualisieren** klicken, um ein Update manuell auszulösen. Updates der Signaturdatenbank und Updates von Programmkomponenten sind wichtige Bestandteile 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 NOD32 Antivirus.



Letztes erfolgreiches Update - Das Datum des letzten Updates. Wenn das angezeigte Datum bereits einige Zeit zurückliegt, ist die Signaturdatenbank möglicherweise nicht auf dem neuesten Stand.

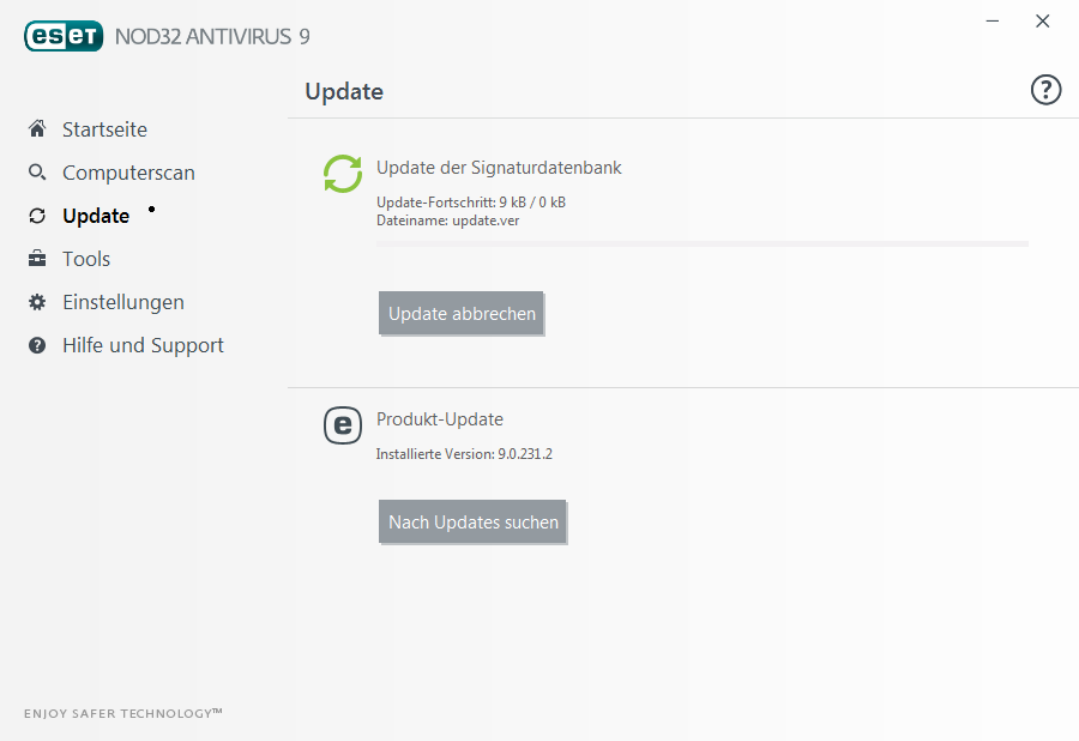
Version der Signaturdatenbank - Die Nummer der Signaturdatenbank. Diese Nummer ist gleichzeitig ein aktiver Link zur Website von ESET. Klicken Sie darauf, um eine Liste aller Signaturen anzuzeigen, die mit einem bestimmten Update hinzugefügt wurden.

Klicken Sie auf **Nach Updates suchen**, um die neueste verfügbare Version ESET NOD32 Antivirus zu ermitteln.

Update-Vorgang

Klicken Sie auf **Jetzt aktualisieren**, um den Download zu starten. Eine Fortschrittsanzeige und die verbleibende Zeit

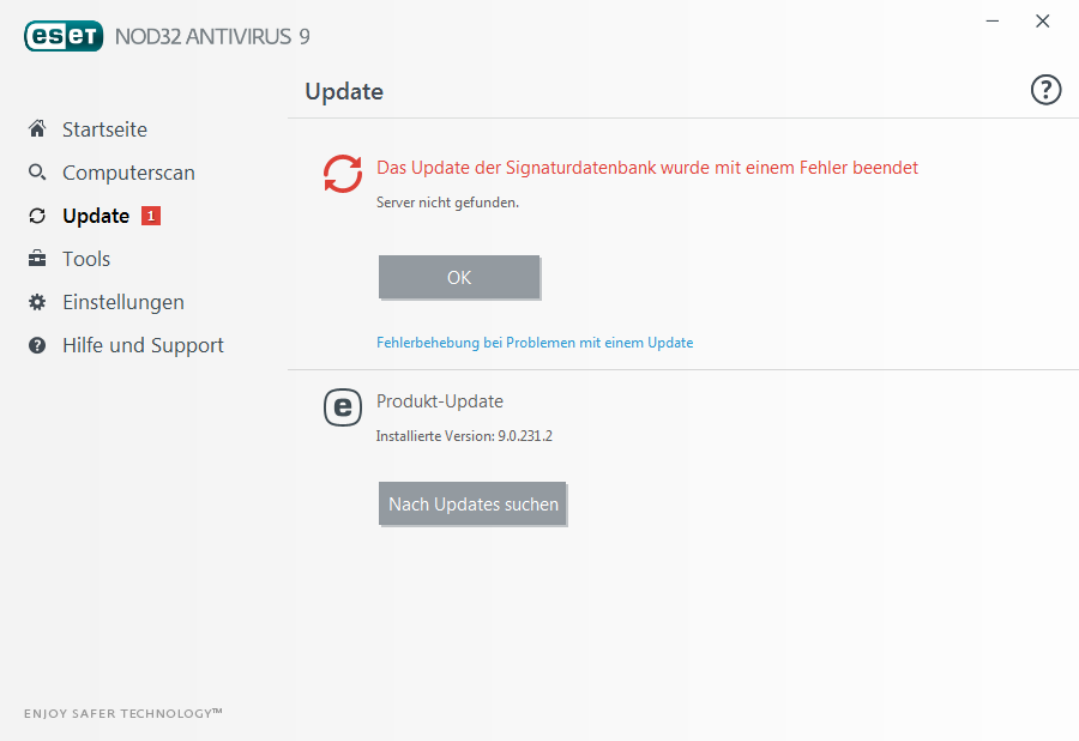
wird angezeigt. Um den Update-Vorgang abzubrechen, klicken Sie auf **Update abbrechen**.



Wichtig: Unter normalen Umständen wird im **Update**-Fenster der Hinweis **Update nicht erforderlich - die Signaturdatenbank ist auf dem neuesten Stand** angezeigt. Andernfalls ist das Programm nicht auf dem neuesten Stand und anfälliger für Infektionen. Aktualisieren Sie die Signaturdatenbank so schnell wie möglich. In allen anderen Fällen erhalten Sie eine der folgenden Fehlermeldungen:

Die eben erwähnte Meldung steht im Zusammenhang mit den folgenden beiden **Während des Updates der Signaturdatenbank sind Fehler aufgetreten**-Meldungen über nicht erfolgreiche Updates:

1. **Ungültige Lizenz** - Der Lizenzschlüssel wurde in den Update-Einstellungen falsch 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.



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

4.3.1 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.

Allgemein

Das aktuell verwendete Update-Profil wird im Dropdownmenü **Ausgewähltes Profil** angezeigt. Zum Erstellen eines neuen Profils klicken Sie neben **Profilliste** auf **Bearbeiten**. Geben Sie den **Namen des Profils** ein und klicken Sie auf **Hinzufügen**.

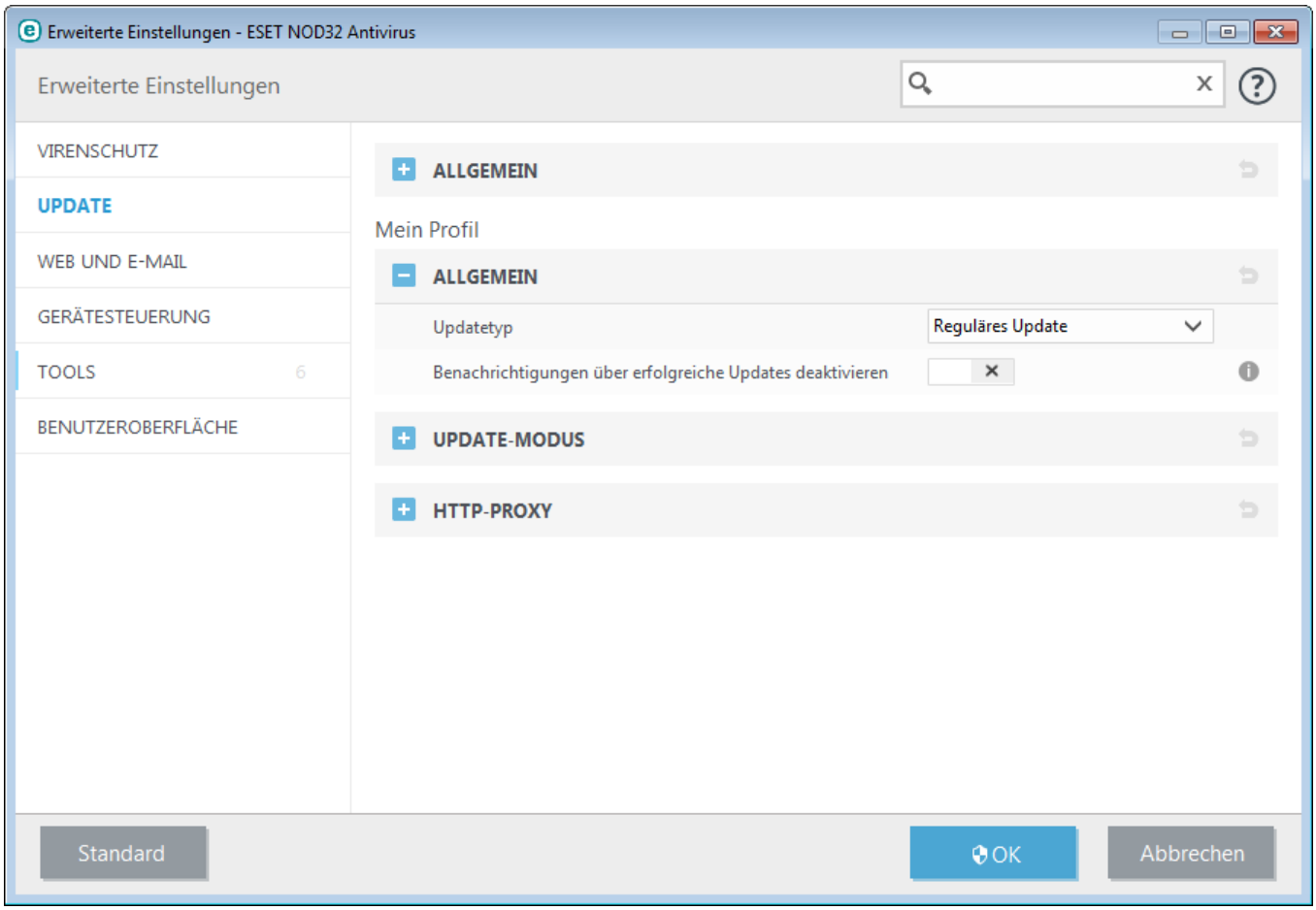
Wenn beim Download der Updates für die Signaturdatenbank Fehler auftreten, klicken Sie auf **Löschen**, um temporäre Update-Dateien und Cache zu löschen.

Rollback

Wenn Sie befürchten, dass ein neues Update der Signaturdatenbank 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 NOD32 Antivirus zeichnet Snapshots der Signaturdatenbank und der Programmmodule zur späteren Verwendung mit der *Rollback*-Funktion auf. Um Snapshots der Signaturdatenbank 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 Signaturdatenbank gespeichert werden.

Wenn Sie auf **Rollback** (**Erweiterte Einstellungen** (F5) > **Update** > **Allgemein**) klicken, müssen Sie im Dropdownmenü einen Zeitraum auswählen. Dieser Wert legt fest, wie lange die Updates der Signaturdatenbank 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).

Einfach

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.

Benachrichtigungen über erfolgreiche Updates deaktivieren - Deaktiviert die Hinweise 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 Präsentationsmodus deaktiviert ist.

4.3.1.1 Update-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.

Die Liste **Ausgewähltes Profil** zeigt das aktuelle Profil an; standardmäßig ist dies **Mein Profil**. Zum Erstellen eines neuen Profils klicken Sie auf **Profile** und dann auf **Hinzufügen**. Geben Sie anschließend den **Namen des Profils** ein. Wenn Sie ein neues Profil erstellen, können Sie die Einstellungen eines bereits bestehenden Profils kopieren, indem Sie die Option **Einstellungen kopieren von Profil** aus der Liste wählen.

4.3.1.2 Erweiterte Einstellungen für Updates

Klicken Sie zum Anzeigen der erweiterten Einstellungen für Updates auf **Einstellungen**. In den erweiterten Einstellungen finden Sie Optionen zur Konfiguration von **Update-Modus**, **HTTP-Proxy** und **LAN**.

4.3.1.2.1 Update-Modus

Auf der Registerkarte **Update-Modus** finden Sie Optionen zum Aktualisieren der Programmkomponenten. Sie können festlegen, wie das Programm reagieren soll, wenn neue Updates für Programmkomponenten verfügbar sind.

Mit Updates für Programmkomponenten können neue Funktionen in das Programm integriert oder bestehende Funktionen modifiziert werden. Nach der Installation von Updates der Programmkomponenten muss der Computer möglicherweise neu gestartet werden.

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

Wenn die Option **Vor dem Herunterladen von Updates fragen** aktiviert ist, wird eine Benachrichtigung angezeigt, wenn ein neues Update verfügbar ist.

Wenn die Größe des Updates den unter **Fragen, falls Update größer ist als (KB)** angegebenen Wert überschreitet, wird ein Hinweis angezeigt.

4.3.1.2.2 HTTP-Proxy

Sie finden die Optionen für Proxyserver-Einstellungen unter der Option **Update** in den **Erweiterten Einstellungen** (F5) unter **HTTP-Proxy**. 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

Mit dem Aktivieren der Option **In Systemsteuerung eingestellten Proxy verwenden** wird die unter „Erweiterte Einstellungen“ (**Tools** > **Proxyserver**) bereits festgelegte Proxyserver-Konfiguration übernommen.

Mit der Option **Keinen Proxyserver verwenden** legen Sie fest, dass kein Proxyserver für Updates von ESET NOD32 Antivirus genutzt wird.

Die Option **Verbindung über Proxyserver** sollten Sie wählen, wenn:

- Ein Proxyserver für Updates von ESET NOD32 Antivirus benötigt wird, bei dem es sich nicht um den in den allgemeinen Einstellungen festgelegten Proxyserver handelt (**Tools** > **Proxyserver**). In diesem Fall sind an dieser Stelle Einstellungen erforderlich: **Proxyserver**-Adresse, Kommunikations-**Port** (standardmäßig 3128) sowie **Benutzername** und **Passwort** für den Proxyserver, falls erforderlich.
- Die Proxyserver-Einstellungen nicht für das gesamte Programm festgelegt wurden, ESET NOD32 Antivirus jedoch Updates über einen Proxyserver herunterladen soll.
- Ihr Computer über einen Proxyserver mit dem Internet verbunden ist. Während der Installation werden die Einstellungen aus Internet Explorer übernommen. Falls Sie später Änderungen vornehmen (zum Beispiel wenn Sie den Internetanbieter wechseln), müssen Sie hier die HTTP-Proxy-Einstellungen prüfen und gegebenenfalls

ändern. Sonst kann keine Verbindung zu den Update-Servern hergestellt werden.

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

HINWEIS: Die Felder mit den Anmeldedaten (**Benutzername** und **Passwort**) sind nur für den Zugriff auf den Proxyserver vorgesehen. Geben Sie in diesen Feldern nur Daten ein, wenn diese für den Zugriff auf den Proxyserver erforderlich sind. Beachten Sie, dass in diese Felder nicht das Passwort und der Benutzername für ESET NOD32 Antivirus eingetragen werden. Eine Eingabe ist nur dann erforderlich, wenn Sie für die Internetverbindung über den Proxyserver ein Passwort benötigen.

4.3.1.2.3 Verbindung mit dem LAN herstellen als

Beim Aktualisieren von einem lokalen Server mit einem Windows NT-Betriebssystem ist standardmäßig eine Authentifizierung für jede Netzwerkverbindung erforderlich.

Wählen Sie im Dropdownmenü **Lokaler Benutzertyp** einen Wert aus, um ein solches Konto zu konfigurieren:

- **Systemkonto (Standard)**,
- **Aktueller Benutzer**,
- **Angegebener Benutzer**.

Wählen Sie **Systemkonto (Standard)** aus, um das Systemkonto für die Authentifizierung zu verwenden. Normalerweise findet keine Authentifizierung statt, wenn in den Haupteinstellungen für Updates keine Anmeldedaten angegeben sind.

Wenn sich das Programm mit dem Konto des aktuell angemeldeten Benutzers anmelden soll, wählen Sie **Aktueller Benutzer**. Nachteil dieser Lösung ist, dass das Programm keine Verbindung zum Update-Server herstellen kann, wenn kein Benutzer angemeldet ist.

Wählen Sie **Folgender Benutzer**, wenn das Programm ein spezielles Benutzerkonto für die Authentifizierung verwenden soll. Nutzen Sie diese Option, wenn eine Anmeldung mit dem standardmäßigen Systemkonto nicht möglich ist. Beachten Sie, dass für das ausgewählte Benutzerkonto Zugriffsrechte auf den Ordner mit den Update-Dateien definiert sein müssen. Wenn keine Zugriffsrechte definiert sind, kann das Programm keine Updates abrufen.

Warnung: Wenn entweder **Aktueller Benutzer** oder **Folgender Benutzer** aktiviert ist, kann ein Fehler beim Wechsel der Identität zum gewünschten Benutzer auftreten. Aus diesem Grund wird empfohlen, die LAN-Anmeldedaten in den Haupteinstellungen für Updates einzugeben. In diesen Update-Einstellungen geben Sie die Anmeldedaten wie folgt ein: *Domänenname**Benutzer* (bei einer Arbeitsgruppe geben Sie *Arbeitsgruppenname**Name* ein) und das Passwort. Bei Aktualisierung von der HTTP-Version des lokalen Servers ist keine Authentifizierung erforderlich.

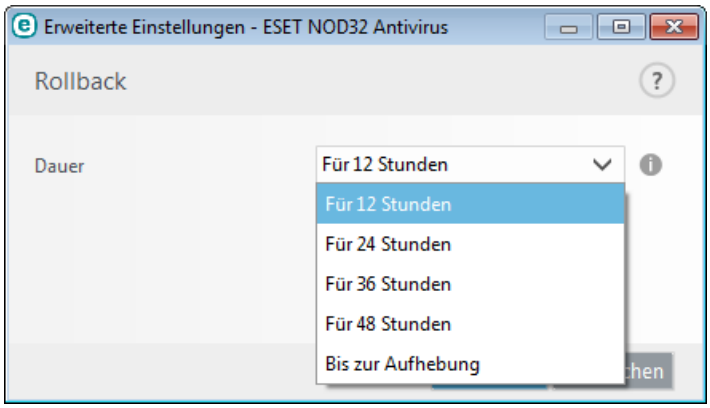
Aktivieren Sie die Option **Nach Update Verbindung zum Server trennen**, um die Serververbindung zu trennen, falls diese nach dem Abrufen von Update-Dateien aktiv bleibt.

4.3.2 Update-Rollback

Wenn Sie befürchten, dass ein neues Update der Signaturdatenbank 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.

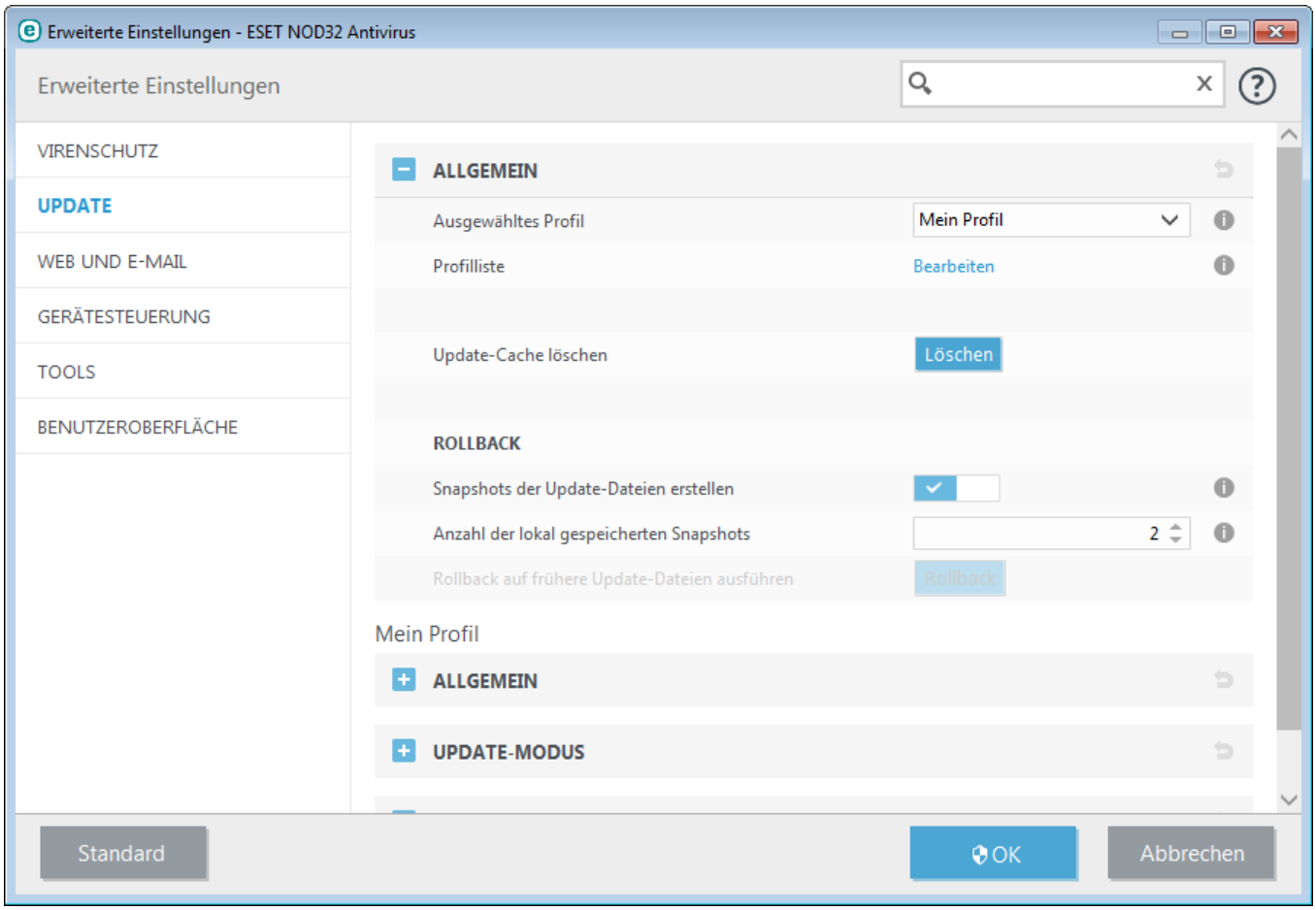
ESET NOD32 Antivirus zeichnet Snapshots der Signaturdatenbank und der Programmmodule zur späteren Verwendung mit der *Rollback*-Funktion auf. Um Snapshots der Signaturdatenbank zu erstellen, lassen Sie das Kontrollkästchen **Snapshots der Update-Dateien erstellen** aktiviert. Das Feld **Zahl der lokal gespeicherten Snapshots** legt fest, wie viele vorige Snapshots der Signaturdatenbank gespeichert werden.

Wenn Sie auf **Rollback ausführen** (**Erweiterte Einstellungen** (F5) > **Update** > **Erweitert**) klicken, müssen Sie im Dropdown-Menü **Updates unterbrechen** einen Zeitraum auswählen. Dieser Wert legt fest, wie lange die Updates der Signaturdatenbank 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 Signaturdatenbank wird auf die älteste verfügbare Version herabgestuft und als Snapshot im lokalen Dateisystem des Computers gespeichert.



Beispiel: Die aktuellste Version der Signaturdatenbank ist beispielsweise 6871. Die Versionen 6870 und 6868 sind als Snapshots der Signaturdatenbank 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 in das Feld **Zahl der lokal gespeicherten Snapshots** den Wert „2“ (zwei) eingegeben haben und auf **Rollback ausführen** klicken, wird die Version 6868 der Signaturdatenbank (und Programmmodule) wiederhergestellt. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Überprüfen Sie, ob die Version der Signaturdatenbank im Hauptprogrammfenster von ESET NOD32 Antivirus im Abschnitt Update herabgestuft wurde.

4.3.3 So erstellen Sie Update-Tasks

Mit der Option **Signaturdatenbank aktualisieren** können Updates manuell ausgeführt werden. Klicken Sie dazu im Hauptmenü auf **Update** und wählen Sie im daraufhin angezeigten Dialogfenster die entsprechende Option 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 NOD32 Antivirus folgende Tasks aktiviert:

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

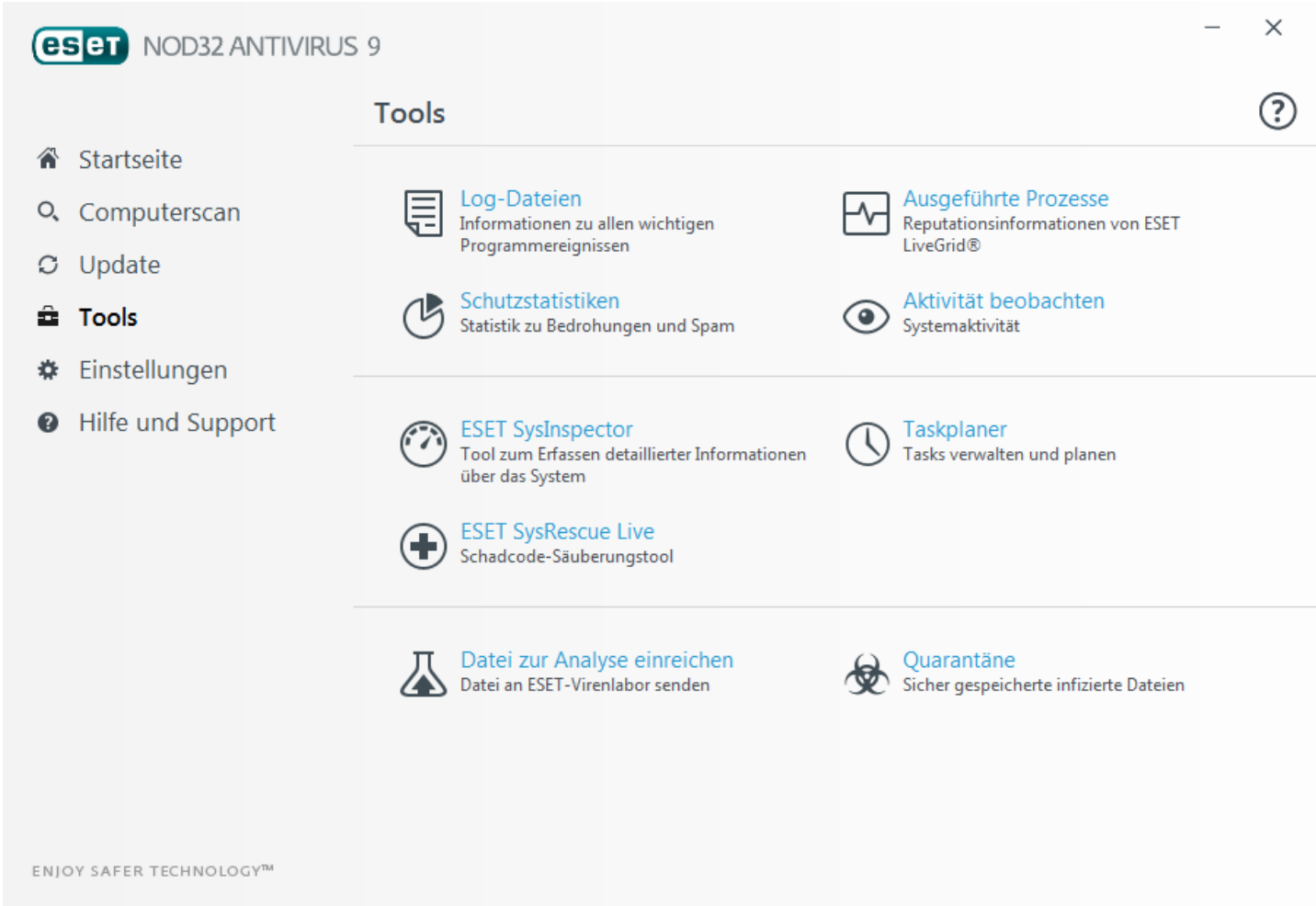
Jeder Update-Task kann bei Bedarf angepasst werden. Neben den standardmäßig ausgeführten Update-Tasks können zusätzliche Update-Tasks mit benutzerdefinierten Einstellungen erstellt werden. Weitere Informationen zum Erstellen und Konfigurieren von Update-Tasks finden Sie im Abschnitt Taskplaner.

4.4 Tools

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

4.4.1 Tools in ESET NOD32 Antivirus

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



Dieser Bereich enthält die folgenden Elemente:

 Log-Dateien

 Schutzstatistiken

 Aktivität beobachten

 Ausgeführte Prozesse (wenn ThreatSense in ESET NOD32 Antivirus aktiviert ist)

 ESET SysInspector

 ESET SysRescue Live - Leitet Sie zur ESET SysRescue Live-Seite weiter, wo Sie das Live-Abbild von ESET SysRescue oder den "Live CD/USB Creator" für Microsoft Windows-Betriebssysteme herunterladen können.

 Taskplaner

 Probe 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.

4.4.1.1 Log-Dateien

Die Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen und geben 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 NOD32 Antivirus 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** > **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 NOD32 Antivirus 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 NOD32 Antivirus 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.
- **Computerscan** - 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 erstellten Regelnamen.
- **Gefilterte Websites** - Diese Liste enthält die durch den Web-Schutz gesperrten Websites. Die Logs enthalten die Uhrzeit, die URL-Adresse, den Benutzer und die Anwendung, die eine Verbindung zur gegebenen Website erstellt hat.
- **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. Hier können Sie außerdem Details wie Gerätetyp, Seriennummer, Herstellername und Mediengröße (je nach Verfügbarkeit der Informationen) anzeigen.

In jedem Abschnitt können die angezeigten Informationen in die Zwischenablage kopiert werden. Wählen Sie dazu die gewünschten Einträge aus und drücken Sie die Tastenkombination **STRG + C**. Zur Auswahl mehrerer Einträge verwenden Sie die **Strg**- und die **Umschalttaste**.

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

Das Kontextmenü können Sie über einen Rechtsklick auf einen Eintrag 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 auf diese Option klicken, 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.

4.4.1.1.1 Log-Dateien

Die Log-Konfiguration für ESET NOD32 Antivirus 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-Modulsusw.) 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.

4.4.1.1.2 Microsoft NAP

Mit dem Netzwerkzugriffsschutz (Network Access Protection, NAP) stellt Microsoft eine Funktion zur Verfügung, die die Systemintegrität des Client bewertet und auf Grundlage dessen den Zugriff auf das Netzwerk kontrolliert. Mit NAP können Systemadministratoren für ihr Netzwerk die Richtlinien für den erforderlichen Systemzustand festlegen.

Zweck von NAP ist es, Administratoren bei der Aufrechterhaltung der Integrität der Computer im Netzwerk zu unterstützen, wodurch wiederum die gesamte Integrität des Netzwerks erhalten bleibt. Die Funktion dient nicht dazu, das Netzwerk vor schädlichen Benutzern zu schützen. Wenn ein Computer beispielsweise über alle Softwareprogramme und Einstellungen gemäß den Netzwerkzugriffsrichtlinien verfügt, gilt er als integer oder konform und erhält entsprechenden Zugriff auf das Netzwerk. NAP ist nicht in der Lage, einen befugten Benutzer mit einem konformen Computer davon abzuhalten, Schadsoftware im Netzwerk hochzuladen oder ihm auf andere Art und Weise Schaden zuzufügen.

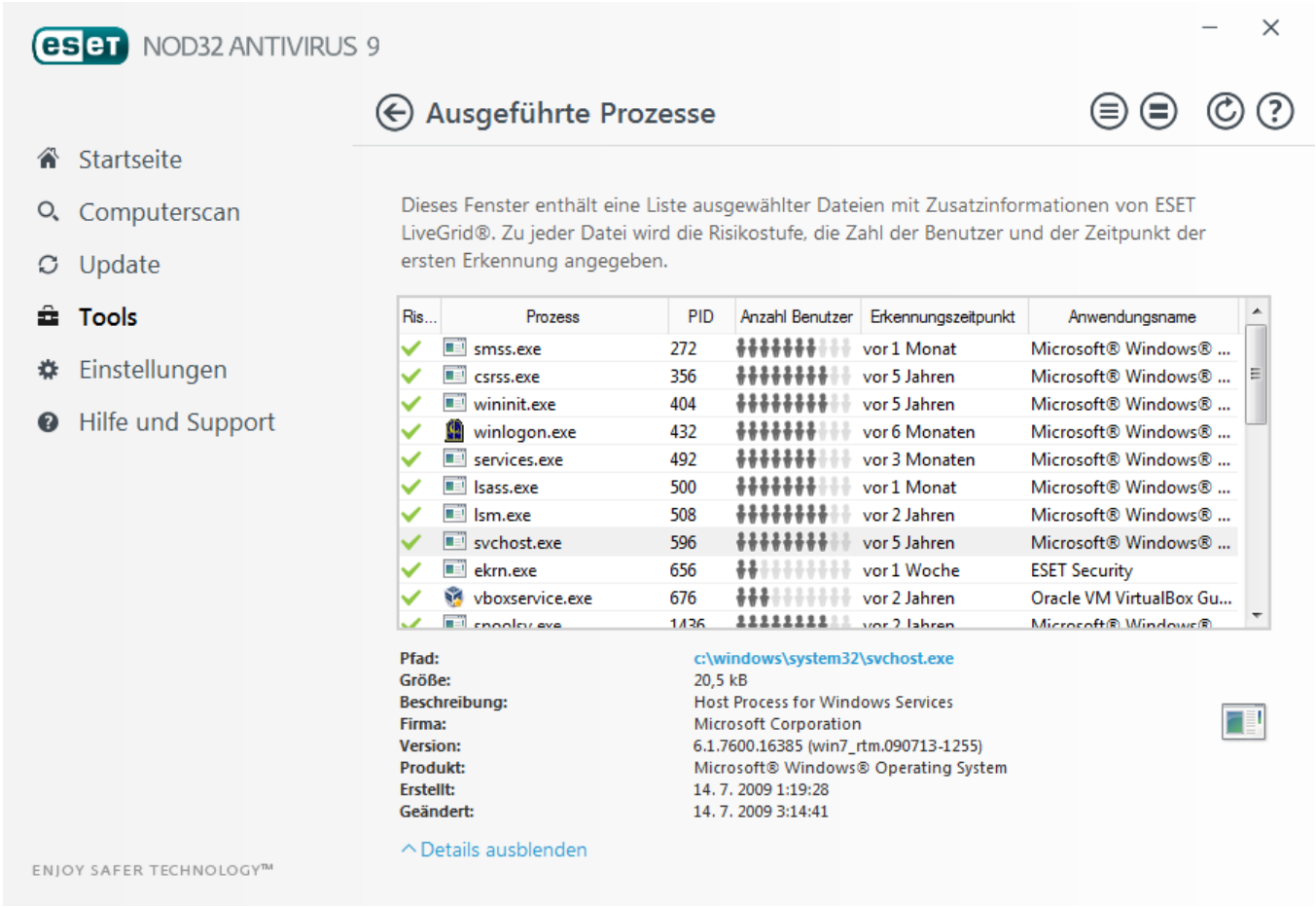
NAP ermöglicht es Administratoren, Integritätsrichtlinien für Computer im Firmennetzwerk zu erstellen und durchzusetzen. Die Richtlinien gelten sowohl für installierte Softwarekomponenten als auch für Systemeinstellungen. Die Computer (Laptops, Workstations und andere derartige Geräte) im Netzwerk werden entsprechend den konfigurierten Integritätsanforderungen geprüft.

Es gelten u. a. folgende Integritätsanforderungen:

• Eine Firewall ist aktiviert,
• Ein Virenschutzprogramm ist installiert,
• Das Virenschutzprogramm ist auf dem neuesten Stand,
• Die automatische Aktualisierung durch Windows Update ist aktiviert usw.

4.4.1.2 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 NOD32 Antivirus bietet ausführliche Informationen zu ausgeführten Prozessen, um den Benutzern den Schutz der ThreatSense-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 auf 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 NOD32 Antivirus 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. Basierend auf dieser Heuristik wird Objekten dann eine Risikostufe zugewiesen, von 1 - In Ordnung (grün) bis 9 - Risikoreich(rot).

HINWEIS: Bekannte Anwendungen, die als In Ordnung (grün) markiert sind, sind in jedem Fall sauber (Positivliste) und werden von der Prüfung ausgenommen. Dadurch wird die Geschwindigkeit der On-Demand-Prüfung bzw. des Echtzeit-Dateischutzes auf Ihrem Computer erhöht.

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: Wenn eine Anwendung als Unbekannt (orange) eingestuft wurde, muss es sich nicht zwangsläufig um Schadsoftware handeln. 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. Wenn sich herausstellt, dass die Datei Schadcode enthält, werden entsprechende Erkennungsfunktionen in zukünftigen Updates berücksichtigt.

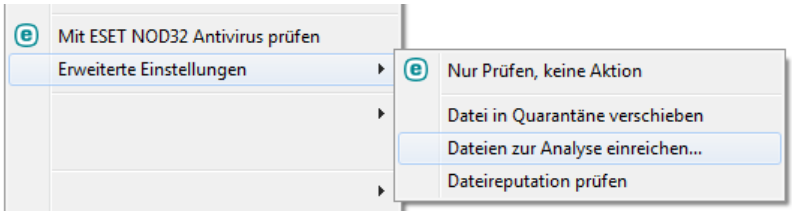
Anwendungsname - Der Name eines Programms oder Prozesses.

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

Wenn Sie unten auf eine Anwendung klicken, werden unten im Fenster die folgenden Informationen angezeigt:

- **Datei** - Speicherort einer Anwendung auf Ihrem Computer
- **Dateigröße** - Dateigröße in B (Byte).
- **Dateibeschreibung** - Dateieigenschaften auf Grundlage der Beschreibung des Betriebssystems
- **Firmenname** - Name des Herstellers oder des Anwendungsprozesses
- **Dateiversion** - Information vom Herausgeber der Anwendung
- **Produktname** - Name der Anwendung und/oder Firmenname

HINWEIS: Der Reputations-Check kann auch auf Dateien angewendet werden, die nicht als Programme/Prozesse ausgeführt werden. - Markieren Sie die Dateien, die Sie überprüfen möchten, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Erweiterte Einstellungen** > **Dateireputation mit ThreatSense überprüfen** aus.



4.4.1.3 Schutzstatistiken

Um statistische Daten zu den Schutzmodulen von ESET NOD32 Antivirus in einem Diagramm anzeigen zu lassen, klicken Sie auf **Tools** > **Schutzstatistiken**. Wählen Sie im Dropdown-Menü **Statistik** das gewünschte Schutzmodul, um das entsprechende Diagramm und die Legende zu betrachten. Wenn Sie mit dem Mauszeiger über einen bestimmten Punkt in der Legende fahren, werden im Diagramm nur die Daten für diesen Punkt angezeigt.

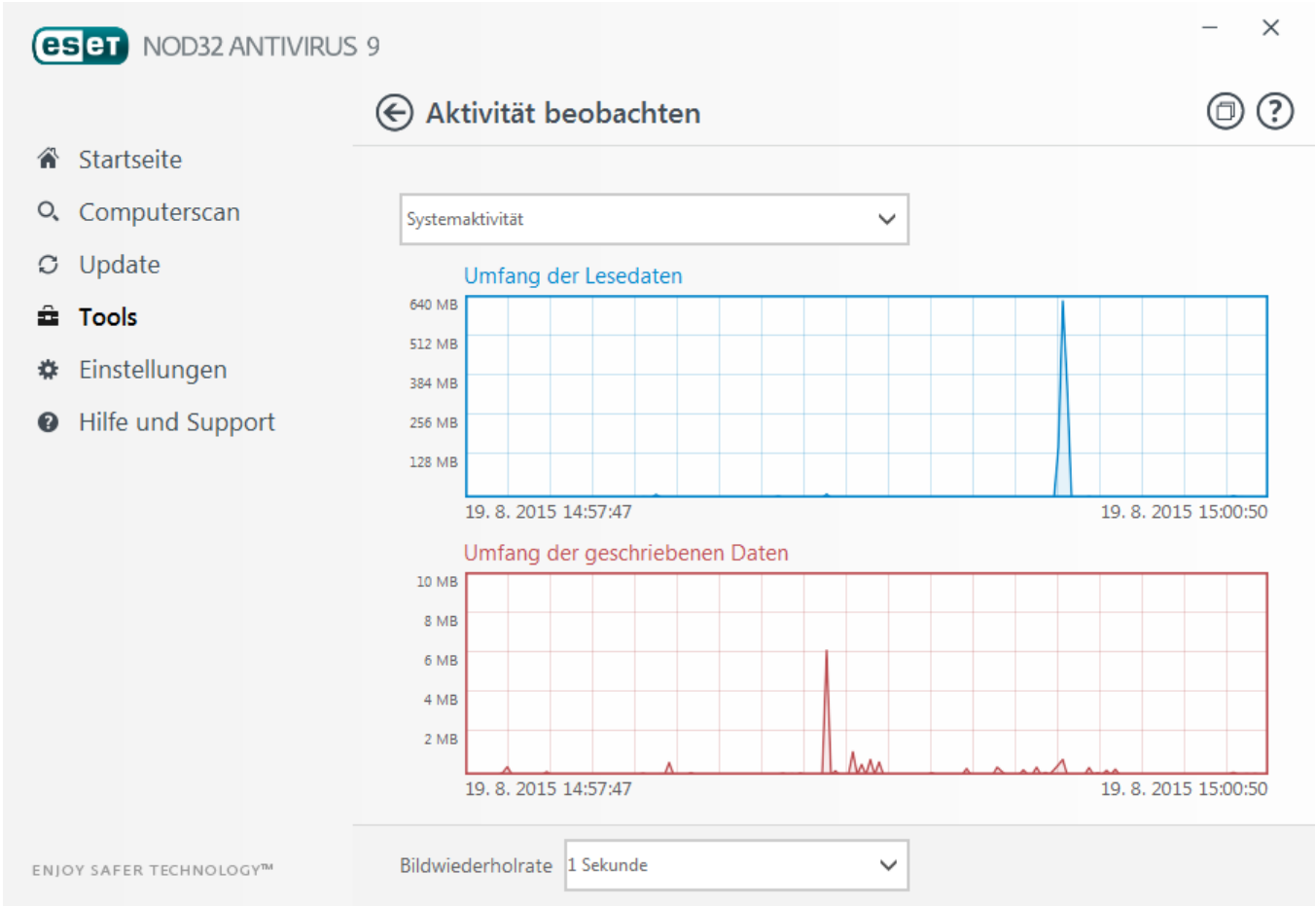
Folgende Diagramme stehen zur Auswahl:

- **Viren- und Spyware-Schutz** - Anzeige der Anzahl infizierter Objekte und gesäuberter Objekte
- **Dateischutz** - Lediglich Anzeige von Objekten, die aus dem Dateisystem gelesen oder in das Dateisystem geschrieben wurden
- **E-Mail-Client-Schutz** - Lediglich Anzeige von Objekten, die von E-Mail-Programmen gesendet oder empfangen wurden
- **Web- und Phishing-Schutz** - Lediglich Anzeige von Objekten, die von einem Webbrowser heruntergeladen wurden

Unter dem Statistik-Diagramm wird die Gesamtanzahl der geprüften Objekte, das zuletzt geprüfte Objekt und der Zeitstempel der Statistik angezeigt. Klicken Sie auf **Zurücksetzen**, um alle Statistikdaten zurückzusetzen.

4.4.1.4 Aktivität beobachten

Um die aktuelle **Systemaktivität** als Diagramm anzuzeigen, klicken Sie auf **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 zeigt die letzten 10 Minuten.
- **Schritt: 1 Minute (letzte 24 Stunden)** - Das Diagramm wird jede Minute aktualisiert. Die Zeitleiste zeigt die letzten 24 Stunden.
- **Schritt: 1 Stunde (letzter Monat)** - Das Diagramm wird jede Stunde aktualisiert. Die Zeitleiste zeigt den letzten Monat.
- **Schritt: 1 Stunde (ausgewählter Monat)** - Das Diagramm wird jede Stunde aktualisiert. Die Zeitleiste zeigt 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.

4.4.1.5 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:

- **Öffnen** - Öffnet das erstellte Log. Sie können auch mit der rechten Maustaste auf die Log-Datei klicken und im Kontextmenü **Anzeigen** auswählen.
- **Vergleichen** - Vergleich zweier vorhandener Logs
- **Erstellen** - Erstellen eines neuen Logs Warten Sie, bis ESET SysInspector die Erstellung abgeschlossen hat (Log-Status "Erstellt"), bevor Sie versuchen, auf die Log-Datei zuzugreifen.
- **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** - Vergleich zweier vorhandener Logs.
- **Erstellen...** - Erstellen eines neuen Logs. Warten Sie, bis ESET SysInspector die Erstellung abgeschlossen hat (Log-Status "Erstellt"), bevor Sie versuchen, auf die Log-Datei zuzugreifen.
- **Alle löschen** - Löschen aller Logs
- **Exportieren** - Exportieren des Logs in eine *.xml*-Datei oder eine komprimierte *.xml*-Datei

4.4.1.6 Taskplaner

Der Taskplaner verwaltet und startet Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften.

Um ihn zu öffnen, klicken Sie im Hauptprogrammfenster von ESET NOD32 Antivirus unter **Tools** auf **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: Update der Signaturdatenbank, Prüftask, Prüfung Systemstartdateien und Log-Wartung. Tasks können direkt über das Fenster „Taskplaner“ hinzugefügt oder gelöscht werden. (Klicken Sie dazu unten auf **Hinzufügen** oder **Löschen**.) 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 Signaturdatenbank)
- **Automatischer erster Scan**

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.
- **Prüfung erstellen** - Erstellt einen ESET SysInspector-Snapshot und eine genaue (Risikostufen-)Analyse Ihrer Systemkomponenten (z. B. Treiber und Anwendungen).
- **On-Demand-Scan** - Prüft die Dateien und Ordner auf Ihrem Computer.
- **Erster Scan** - Standardmäßig wird 20 Minuten nach Installation oder Neustart eine Prüfung als Task mit geringer Priorität ausgeführt.
- **Update** - Erstellt einen Update-Task. Dieser besteht aus der Aktualisierung der Signaturdatenbank und der Aktualisierung der Programmmodule.

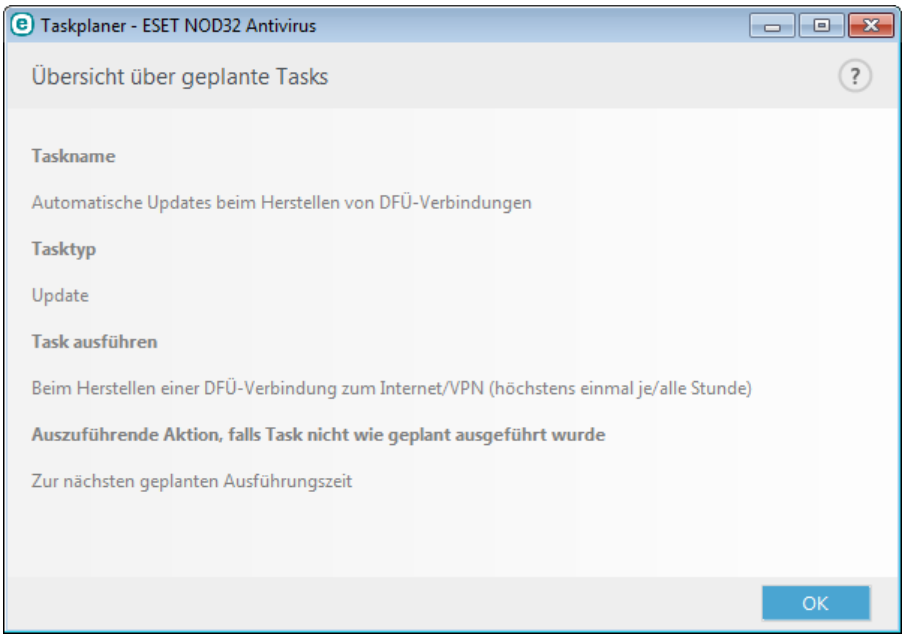
4. Aktivieren Sie den Task mit der Option **Aktivieren** (Sie können dies auch später tun, indem Sie das Kontrollkästchen in der Liste der geplanten Tasks markieren oder die Markierung daraus entfernen), klicken Sie auf **Weiter** und wählen Sie eine Zeitangabe aus:

- **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.



4.4.1.7 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 Smart Security oder bestimmte Serverprodukte. 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.

4.4.1.8 ESET LiveGrid®

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 haben die Möglichkeit, ESET LiveGrid® nicht zu aktivieren. Die Funktionalität in der Software geht nicht verloren, in einigen Fällen reagiert ESET NOD32 Antivirus jedoch möglicherweise schneller auf neue Bedrohungen als die Aktualisierung der Signaturdatenbank.
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 NOD32 Antivirus ist standardmäßig so konfiguriert, dass verdächtige Dateien zur genauen Analyse an ESET 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 Einstellungsmenü für ESET LiveGrid® bietet verschiedene Optionen zum Aktivieren/Deaktivieren von ESET LiveGrid®, mit dem verdächtige Dateien und anonyme statistische Daten an ESET übermittelt werden. Um darauf zuzugreifen, klicken Sie in der Baumstruktur der erweiterten Einstellungen auf **Tools** > **ESET LiveGrid®**.

An ESET LiveGrid® teilnehmen (empfohlen) - Das ESET LiveGrid®-Reputationssystem erhöht die Wirksamkeit der ESET-Sicherheitslösungen, indem es gescannte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht.

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.

Dateien einreichen - Verdächtige Dateien, die auf eine Bedrohung hinweisen, und/oder Dateien mit ungewöhnlichen Eigenschaften oder ungewöhnlichem Verhalten werden zur Analyse an ESET gesendet.

Wählen Sie die Option **Erstellen von Logs aktivieren** aus, um ein Ereignis-Log zu erstellen, in dem eingereichte Dateien und statistische Daten protokolliert werden. Dadurch werden Einträge im Ereignis-Log erstellt, wenn Dateien oder statistische Daten eingereicht werden.

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.

Ausschlussfilter - 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 der Ausschlussliste weitere Dateien 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.

4.4.1.8.1 Verdächtige Dateien

In der Registerkarte **Dateien** in den erweiterten Einstellungen von ESET LiveGrid® können Sie konfigurieren, wie Bedrohungen zur Analyse an ESET gesendet werden.

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 Signaturdatenbank 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.

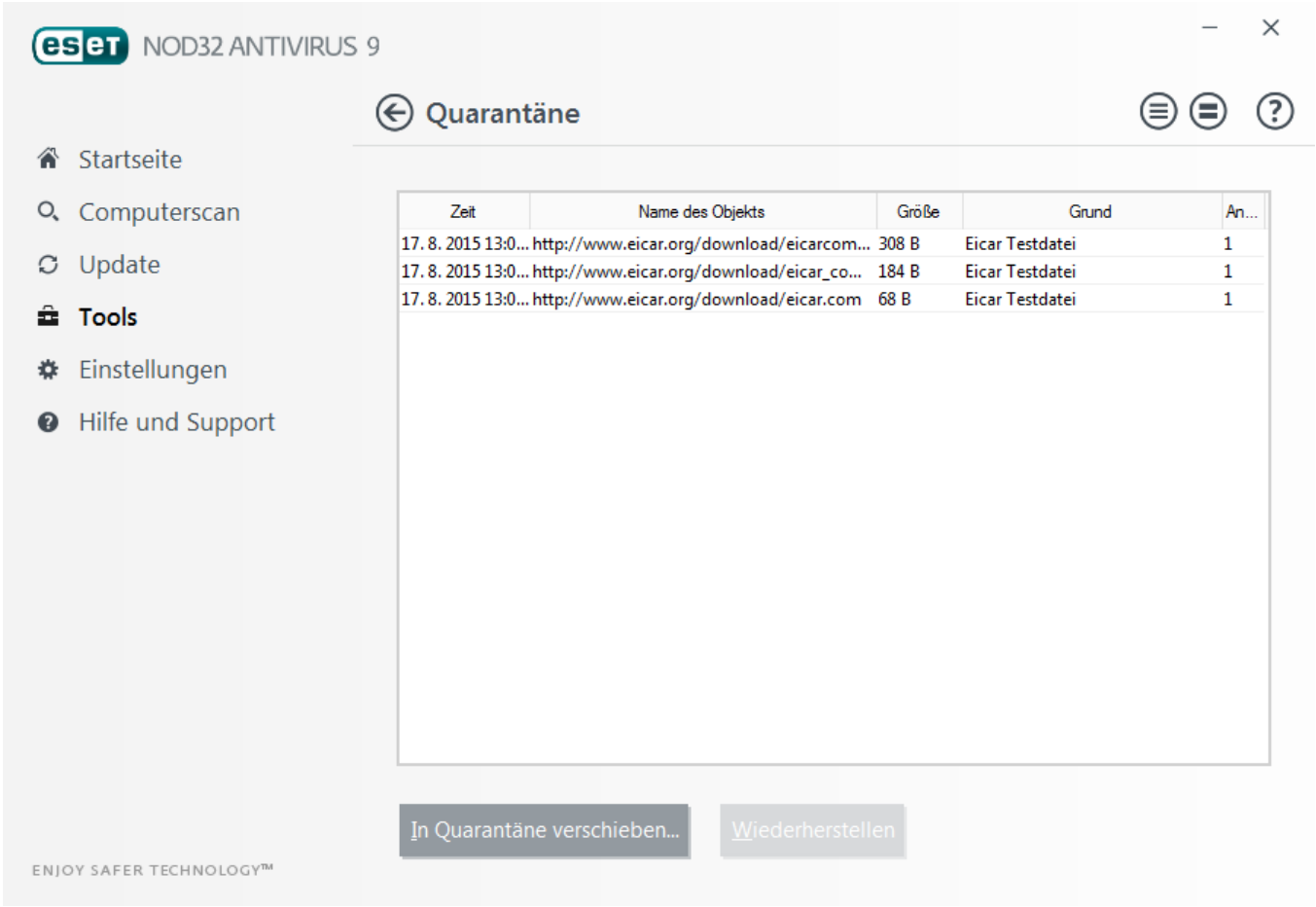
E-Mail-Adresse für Rückfragen (optional) - Sie können mit den verdächtigen Dateien eine E-Mail-Adresse für Rückfragen angeben, wenn zur Analyse weitere Informationen erforderlich sind. Beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.

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.

4.4.1.9 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 NOD32 Antivirus 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 NOD32 Antivirus 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.

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**.

4.4.1.10 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 NOD32 Antivirus 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 NOD32 Antivirus 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.

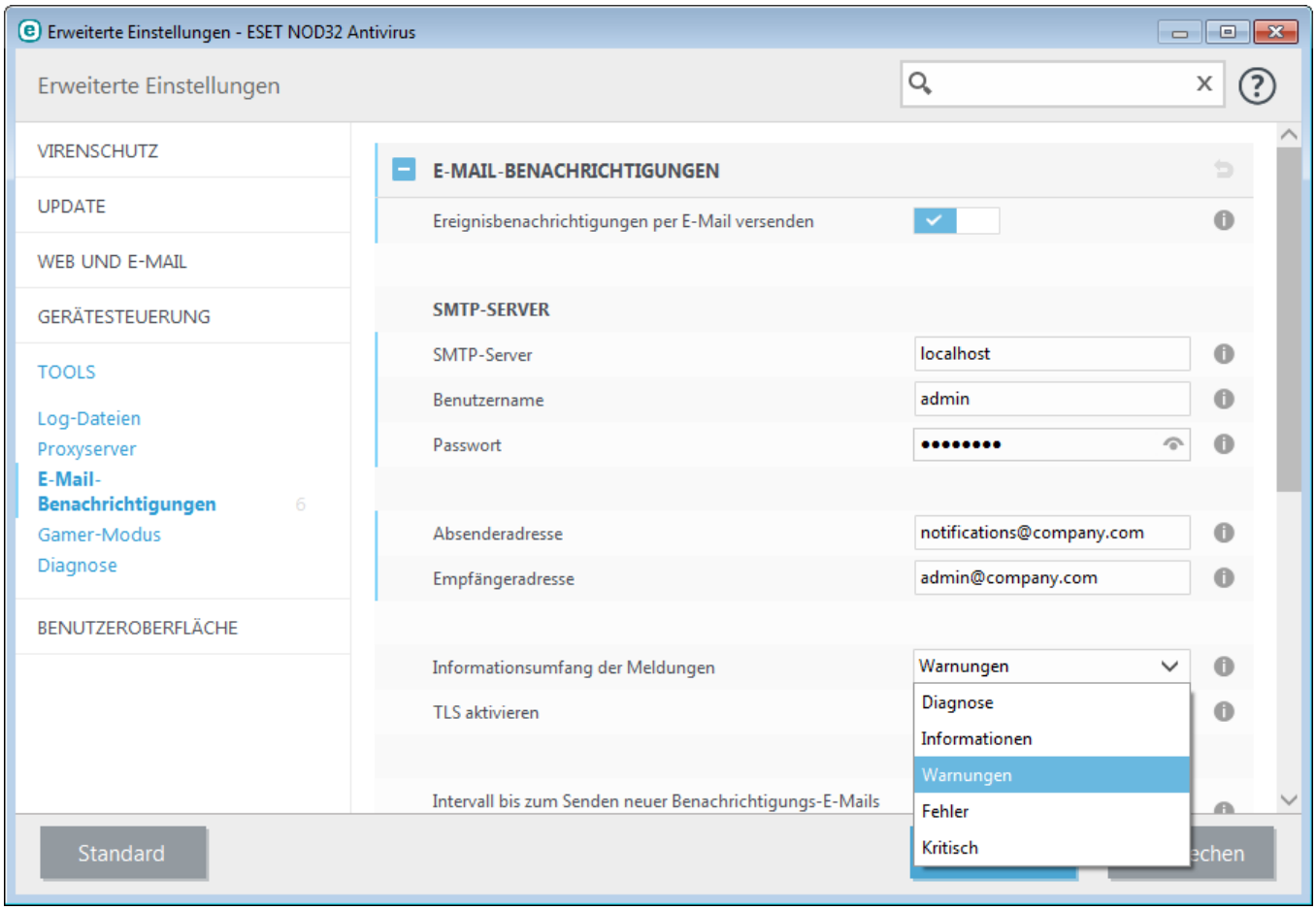
Wenn der Proxyserver eine Authentifizierung benötigt, aktivieren Sie **Proxyserver erfordert Authentifizierung** und geben einen gültigen **Benutzernamen** sowie das entsprechende **Passwort** ein. Klicken Sie auf **Erkennen**, wenn die Einstellungen des Proxyservers automatisch erkannt und ausgefüllt 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.

Sie können die Proxyserver-Einstellungen auch in den erweiterten Einstellungen für Updates ändern (**Erweiterte Einstellungen** > **Update** > **HTTP-Proxy**, 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 Signaturdatenbank oft remote beziehen. Weitere Informationen zu diesen Einstellungen finden Sie unter Erweiterte Einstellungen für Updates.

4.4.1.11 E-Mail-Benachrichtigungen

ESET NOD32 Antivirus 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 für den Versand von Benachrichtigungen (z. B. *smtp.Anbieter.com:587*, der Standardport ist 25).

HINWEIS: ESET NOD32 Antivirus unterstützt keine SMTP-Server mit TLS-Verschlüsselung.

Benutzername und **Passwort** - Falls der SMTP-Server Authentifizierung verwendet, geben Sie hier einen gültigen Benutzernamen und das Passwort ein.

Absenderadresse - Dieses Feld enthält die Adresse, die in Ereignismeldungen als Absender verzeichnet sein soll.

Empfängeradresse - Dieses Feld enthält die Adresse, die in Ereignismeldungen als Empfänger verzeichnet sein soll.

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 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.

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-ASCII 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).

4.4.1.11.1 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
- **%ErrorDescription%** - Beschreibung eines nicht durch Viruscode 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).

4.4.1.12 Probe für die Analyse auswählen

Über das Dialogfenster zum Dateiversand können Sie Dateien bei ESET zur Analyse einreichen. Sie öffnen es unter **Tools** > **Probe 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. 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.

4.4.1.13 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 NOD32 Antivirus über fehlende Updates. Folgende Richtlinien sind verfügbar:

- **Keine Updates** - Es werden keine Updates zum Download angeboten.
- **Optionale Updates** - Updates mit beliebiger Priorität werden zum Download angeboten.
- **Empfohlene Updates** - Updates mit normaler Priorität und höher werden zum Download angeboten.
- **Wichtige Updates** - Updates mit hoher Priorität und kritische Updates 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.

4.5 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.

Wenn Sie festlegen, dass bestimmte Hinweise nicht angezeigt werden sollen, werden diese in die Liste Versteckte Hinweisfenster aufgenommen. Hier können Sie den Status der Hinweise einsehen, sie detaillierter anzeigen lassen oder sie aus dem Fenster entfernen.

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.

Das Kontextmenü wird angezeigt, wenn Sie mit der rechten Maustaste auf ein Element klicken. Mit diesem Tool können ESET NOD32 Antivirus-Steuerelemente in das Kontextmenü integriert werden.

4.5.1 Elemente der Benutzeroberfläche

Über die Konfigurationsoptionen für die Benutzeroberfläche von ESET NOD32 Antivirus können Sie die Arbeitsumgebung an Ihre Anforderungen anpassen. Sie finden diese Optionen unter **Benutzeroberfläche** > **Elemente der Benutzeroberfläche** in den erweiterten Einstellungen von ESET NOD32 Antivirus.

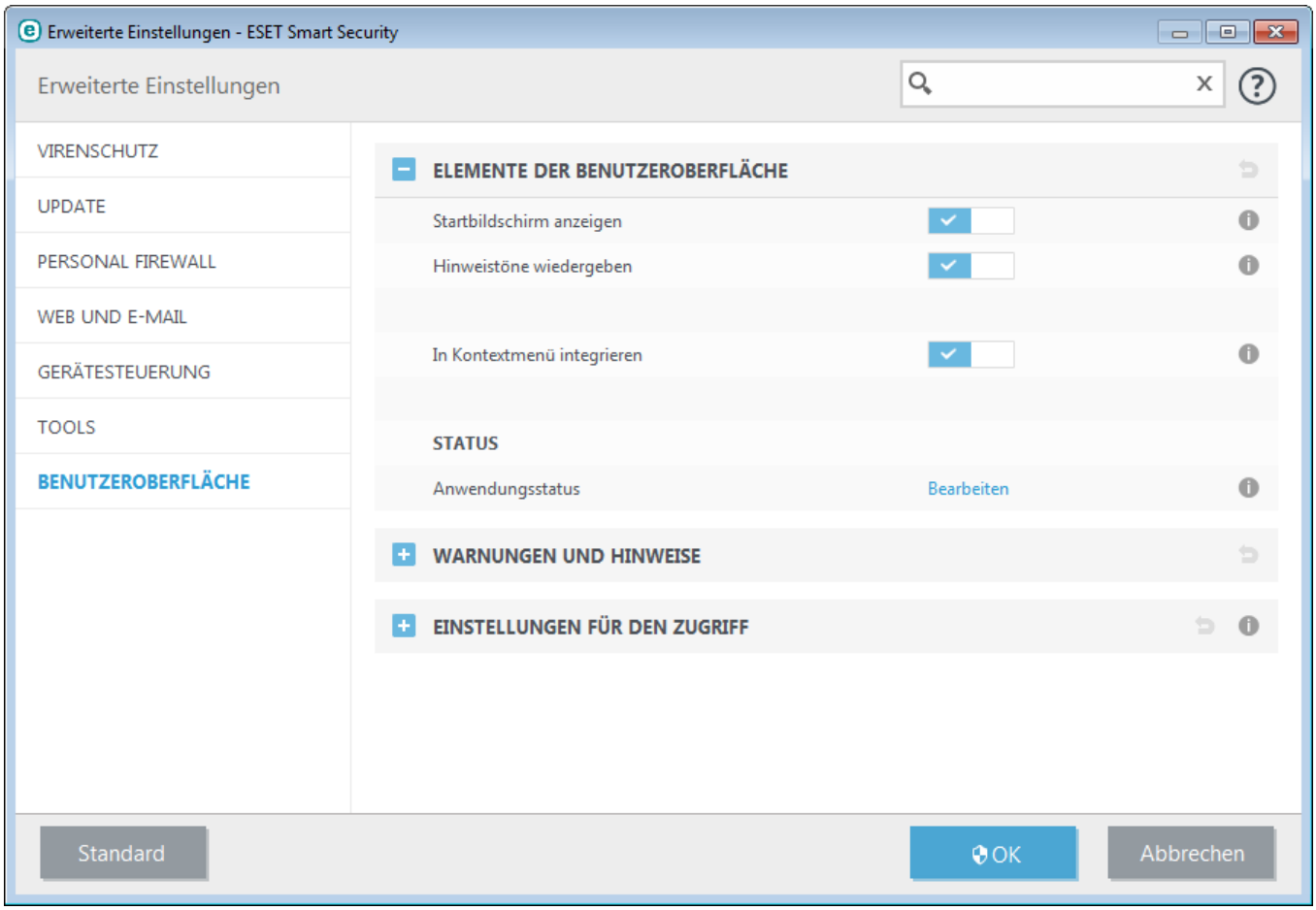
Wenn ESET NOD32 Antivirus ohne Anzeige des Startbilds gestartet werden soll, deaktivieren Sie die Option **Startbild anzeigen**.

Wenn ESET NOD32 Antivirus 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 - Die Steuerelemente von ESET NOD32 Antivirus können in das Kontextmenü integriert werden.

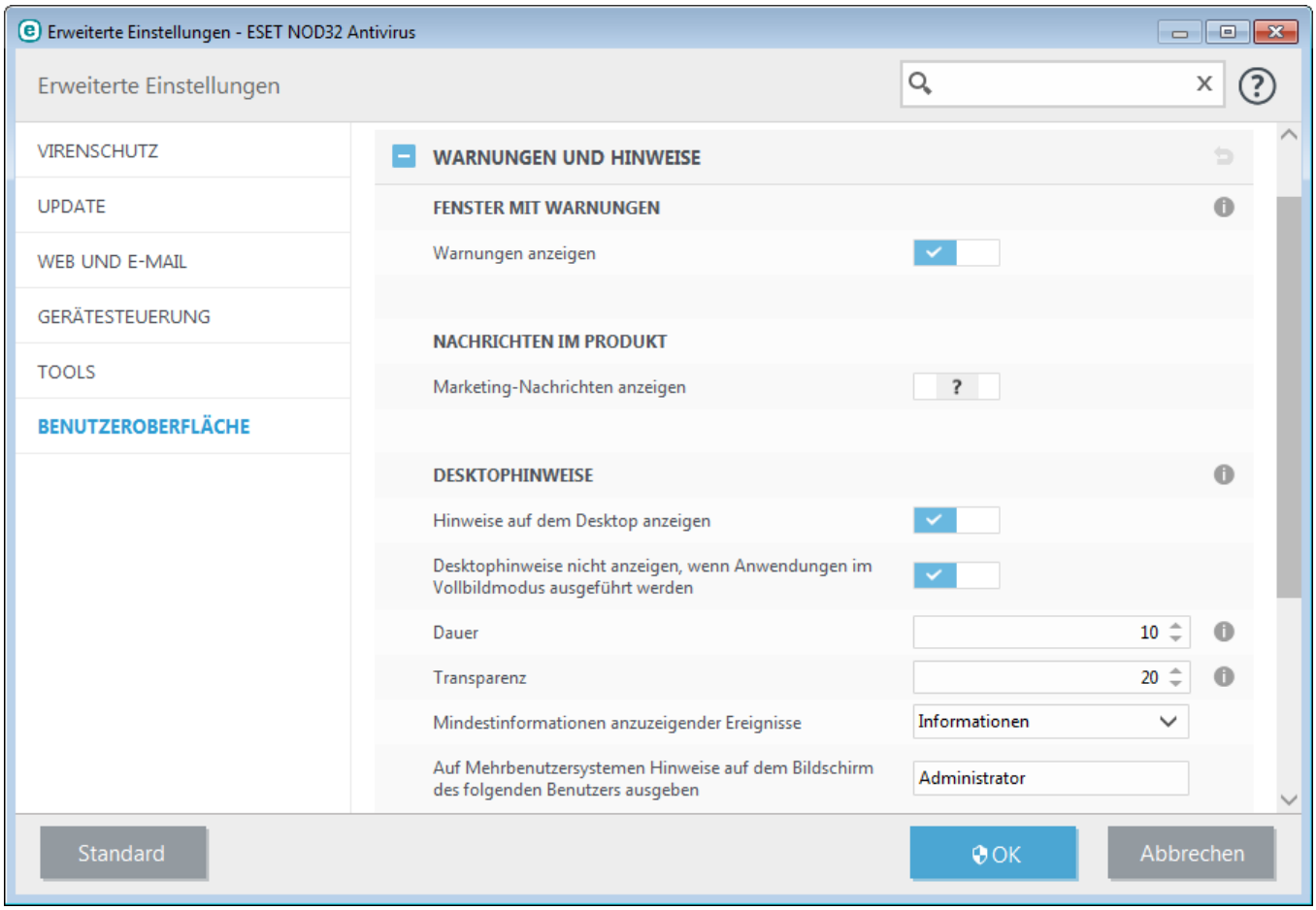
Status

Anwendungsstatus - Klicken Sie auf **Bearbeiten**, um Status, die im Hauptmenü im Bereich **Schutzstatus** angezeigt werden, zu verwalten (zu deaktivieren).


Erweiterte Einstellungen - ESET Smart Security
Erweiterte Einstellungen
VIRENSCHUTZ
UPDATE
PERSONAL FIREWALL
WEB UND E-MAIL
GERÄTESTEUERUNG
TOOLS
BENUTZEROBERFLÄCHE
ELEMENTE DER BENUTZEROBERFLÄCHE
Startbildschirm anzeigen
Hinweistöne wiedergeben
In Kontextmenü integrieren
STATUS
Anwendungsstatus
Bearbeiten
WARNUNGEN UND HINWEISE
EINSTELLUNGEN FÜR DEN ZUGRIFF
Standard
OK
Abbrechen

4.5.2 Warnungen und Hinweise

Im Bereich **Warnungen und Hinweise** unter **Benutzeroberfläche** können Sie festlegen, wie ESET NOD32 Antivirus 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. Deaktivieren Sie diese Option, wenn Sie keine Marketing-Nachrichten erhalten möchten.

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.

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,usw.) 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, die Sie zur Anzeige oder zur Nicht-Anzeige auswählen können.

4.5.2.1 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-Modulsusw.) 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.

4.5.3 Versteckte Hinweisfenster

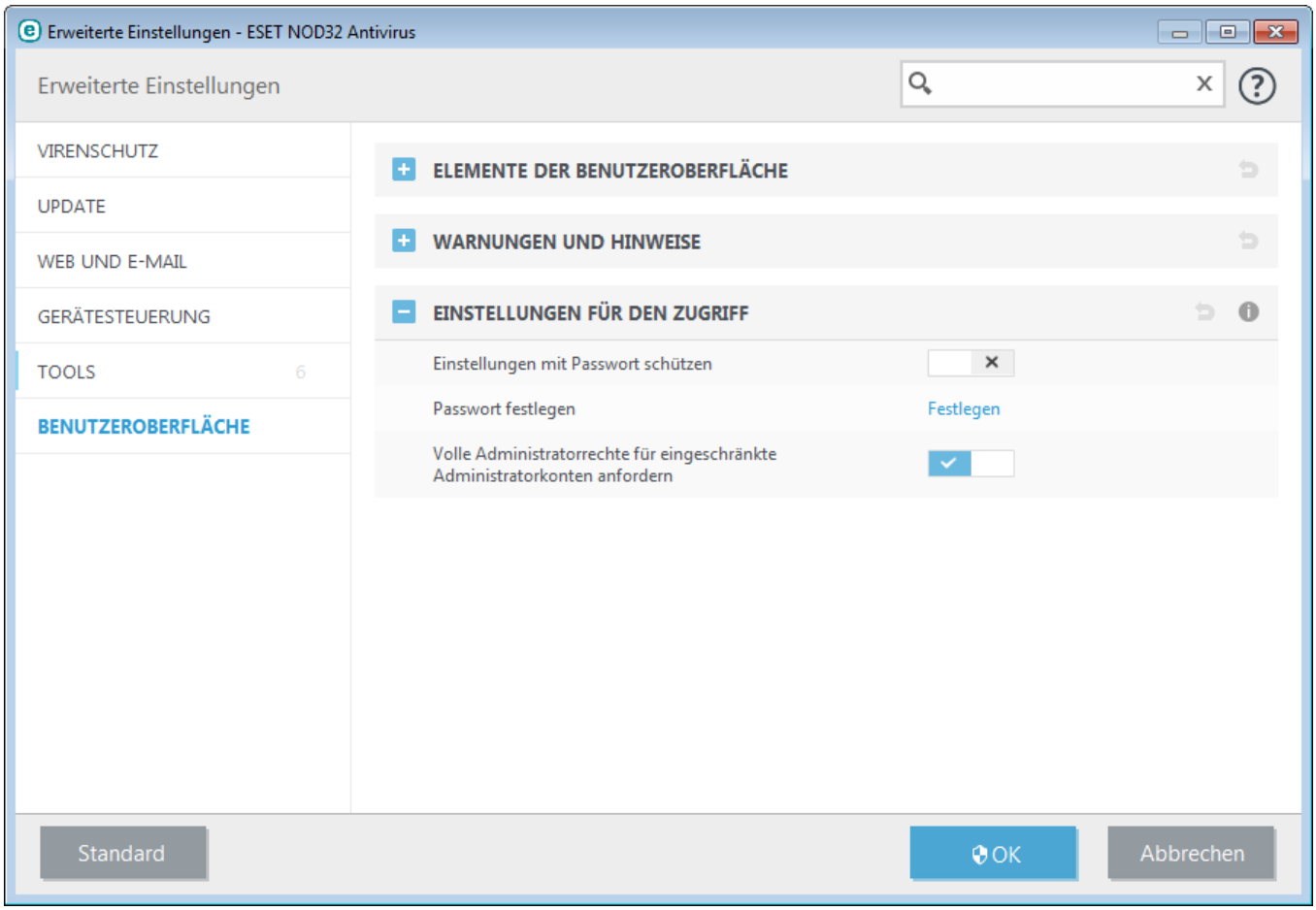
Wenn die Option **Dieses Fenster nicht mehr anzeigen** für ein Hinweisfenster (eine Warnung) aktiviert wurde, das schon einmal angezeigt wurde, wird dieses in der Liste der versteckten Hinweisfenster angezeigt. Aktionen, die nunmehr automatisch ausgeführt werden, werden in der Spalte mit dem Titel **Bestätigen** angezeigt.

Anzeigen - Zeigt eine Vorschau aller Hinweisfenster an, die derzeit nicht angezeigt werden und für die eine automatische Aktion konfiguriert wurde.

Entfernen - Entfernen von **Versteckten Hinweisfenstern** aus der Liste. Alle aus der Liste entfernten Hinweisfenster werden wieder angezeigt.

4.5.4 Einstellungen für den Zugriff

Die Einstellungen von ESET NOD32 Antivirus 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 NOD32 Antivirus 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.

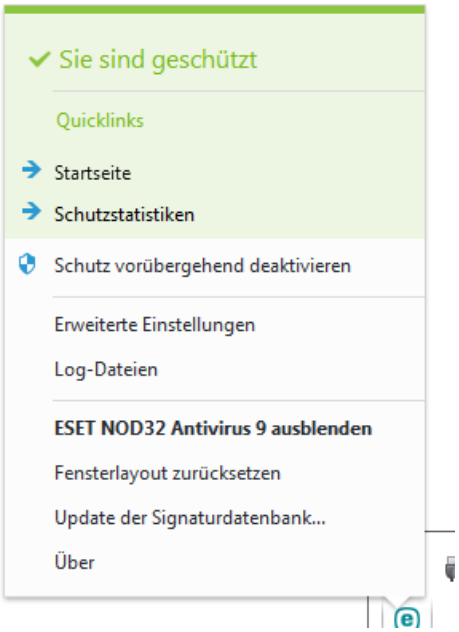
Volle Administratorrechte für eingeschränkte Administratorkonten anfordern - Aktivieren Sie dies, damit Benutzer ohne Administratorrechte zur Eingabe eines Administratorbenutzernamens und -passworts aufgefordert werden, wenn sie bestimmte Systemeinstellungen ändern möchten (ähnlich der Benutzerkontensteuerung/UAC in Windows Vista und Windows 7). Dazu gehört das Deaktivieren von Schutzmodulen. 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 NOD32 Antivirus zur Eingabe des Administratornachweises auffordert.

4.5.5 Programmmenü

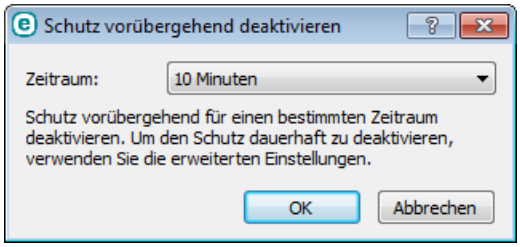
Einige der wichtigsten Einstellungsoptionen und -funktionen können durch Klicken mit der rechten Maustaste auf das Symbol im Infobereich der Taskleiste geöffnet werden.



Häufig verwendet - Zeigt die am häufigsten verwendeten Komponenten von ESET NOD32 Antivirus 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.



Erweiterte Einstellungen - Öffnet das Menü **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 NOD32 Antivirus minimieren - Blendet das ESET NOD32 Antivirus-Fenster auf dem Bildschirm aus.

Fensterlayout zurücksetzen - Stellt die standardmäßige Fenstergröße von ESET NOD32 Antivirus und deren Standardposition auf dem Bildschirm wieder her.

Produkt aktivieren... - Wählen Sie diese Option aus, wenn Sie Ihr ESET-Sicherheitsprodukt noch nicht aktiviert haben, oder um die Produktaktivierungsdaten nach einer Lizenzverlängerung erneut einzugeben.

Signaturdatenbank - Beginnt mit der Aktualisierung der Signaturdatenbank, um den Schutz vor Schadcode zu gewährleisten.

Über - Bietet Systeminformationen zur installierten Version von ESET NOD32 Antivirus und zu den installierten Programmmodulen. Hier finden Sie außerdem das Lizenzablaufdatum und Informationen zum Betriebssystem und zu den Systemressourcen.

4.5.6 Kontextmenü

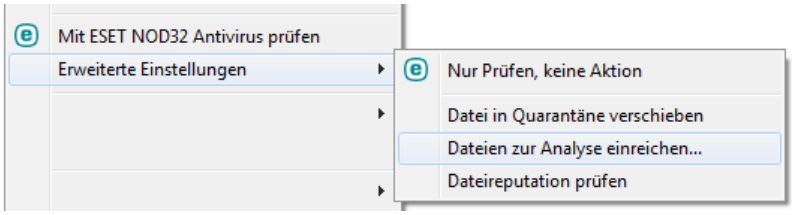
Das Kontextmenü wird angezeigt, wenn Sie mit der rechten Maustaste auf ein Element klicken. Das Menü enthält alle Optionen, die auf das Objekt angewendet werden können.

Bestimmte Steuerungselemente von ESET NOD32 Antivirus können in das Kontextmenü integriert werden. Weitere Einstellungsoptionen für diese Funktion sind unter „Erweiterte Einstellungen“ im Bereich **Benutzeroberfläche** > **Kontextmenü** verfügbar.

In Kontextmenü integrieren - ESET NOD32 Antivirus kann in das Kontextmenü integriert werden.

Folgende Optionen stehen in der Liste **Menütyp** zur Verfügung:

- **Voll (zuerst prüfen)** - Aktiviert alle Optionen für das Kontextmenü; das Hauptmenü zeigt die Option **Mit ESET NOD32 Antivirus prüfen, ohne zu säubern** als Erstes und **Scan and clean** (Prüfen und säubern) als untergeordnete Option.
- **Voll (zuerst säubern)** - Aktiviert alle Optionen für das Kontextmenü; das Hauptmenü zeigt die Option **Prüfen mit ESET NOD32 Antivirus** als Erstes und **Prüfen, ohne zu säubern** als untergeordnete Option.



- **Nur scannen** - Im Kontextmenü wird nur die Option **Mit ESET NOD32 Antivirus prüfen, ohne zu säubern** angezeigt.
- **Nur säubern** - Im Kontextmenü erscheint nur die Option **Prüfen mit ESET NOD32 Antivirus**.

5. Fortgeschrittene Benutzer

5.1 Profilmanager

An zwei Stellen von ESET NOD32 Antivirus wird der Profilmanager verwendet: in den Bereichen **On-Demand-Scan** und **Update**.

Computerscan

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 Sie auf **Virenschutz** > **On-Demand-Scan** > **Einfach** > **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.

Beispiel: Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Option **Scannen Sie Ihren Computer** 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.

Ausgewähltes Profil - Das momentan verwendete Update-Profil. Um es zu ändern, wählen Sie ein Profil aus dem Dropdown-Menü aus.

Hinzufügen - Erstellen neuer Updateprofile.

Im unteren Teil des Fensters sind die vorhandenen Profile aufgelistet.

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

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 NOD32 Antivirus 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, mit denen möglicherweise die Ursache für den Absturz der Anwendung ermittelt werden kann. 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 Protokollfilterung aktivieren - Alle Daten, die die Protokollfilterung durchlaufen, im PCAP-Format aufzeichnen. Diese Aufzeichnungen helfen Entwicklern bei der Behebung von Problemen mit der Protokollfilterung.

Die Log-Dateien befinden sich unter:
C:\ProgramData\ESET\ESET Smart 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.

5.4 Einstellungen importieren/exportieren

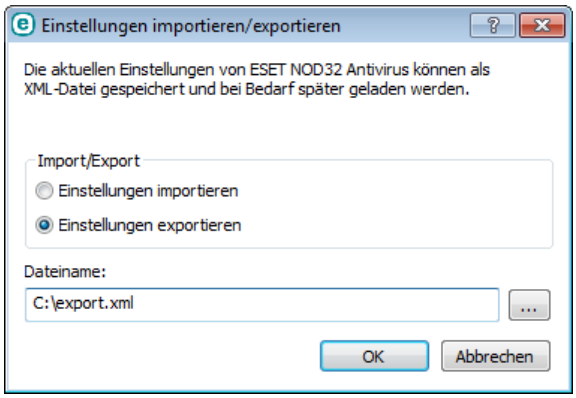
Über das Menü **Einstellungen** können Sie die XML-Datei mit Ihrer benutzerdefinierten Konfiguration von ESET NOD32 Antivirus importieren und exportieren.

Das Importieren und Exportieren der Konfigurationsdatei ist hilfreich, wenn Sie zur späteren Verwendung eine Sicherung der aktuellen Konfiguration von ESET NOD32 Antivirus 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 Erkennen des Leerlaufs

Die Erkennung des Ruhezustands kann in **Erweiterte Einstellungen** unter **Tools** > **Erkennen des Leerlaufs** konfiguriert werden. Unter diesen Einstellungen können folgende Auslöser für das Prüfen im Leerlaufbetrieb festgelegt werden:

- Aktivierung des Bildschirmschoners
- Sperren des Computers
- Abmelden eines Benutzers

Aktivieren bzw. deaktivieren Sie die Auslöser für die Prüfung im Ruhezustand über die entsprechenden Kontrollkästchen.

5.6 ESET SysInspector

5.6.1 Einführung in ESET SysInspector

ESET SysInspector ist eine Anwendung, die den Computer gründlich durchsucht und die gesammelten Daten ausführlich anzeigt. 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 Arten auf ESET SysInspector zugreifen: über die in ESET Security-Lösungen integrierte Version oder indem Sie die eigenständige Version (SysInspector.exe) kostenlos von der ESET-Website herunterladen. Die Funktionen und Steuerelemente beider Programmversionen sind identisch. Die Versionen unterscheiden sich nur in der Ausgabe der Informationen. Sowohl mit der eigenständigen als auch der integrierten Version können Snapshots des Systems in einer XML-Datei ausgegeben und auf einem Datenträger gespeichert werden. Mit der integrierten Version ist es jedoch auch möglich, die System-Snapshots direkt unter **Tools** > **ESET SysInspector** zu speichern (außer ESET Remote Administrator). Weitere Informationen finden Sie im Abschnitt ESET SysInspector als Teil von ESET NOD32 Antivirus.

Bitte gedulden Sie sich ein wenig, während ESET SysInspector Ihren Computer prüft. Je nach aktueller Hardware-Konfiguration, Betriebssystem und Anzahl der installierten Anwendungen kann die Prüfung zwischen 10 Sekunden und einigen Minuten dauern.

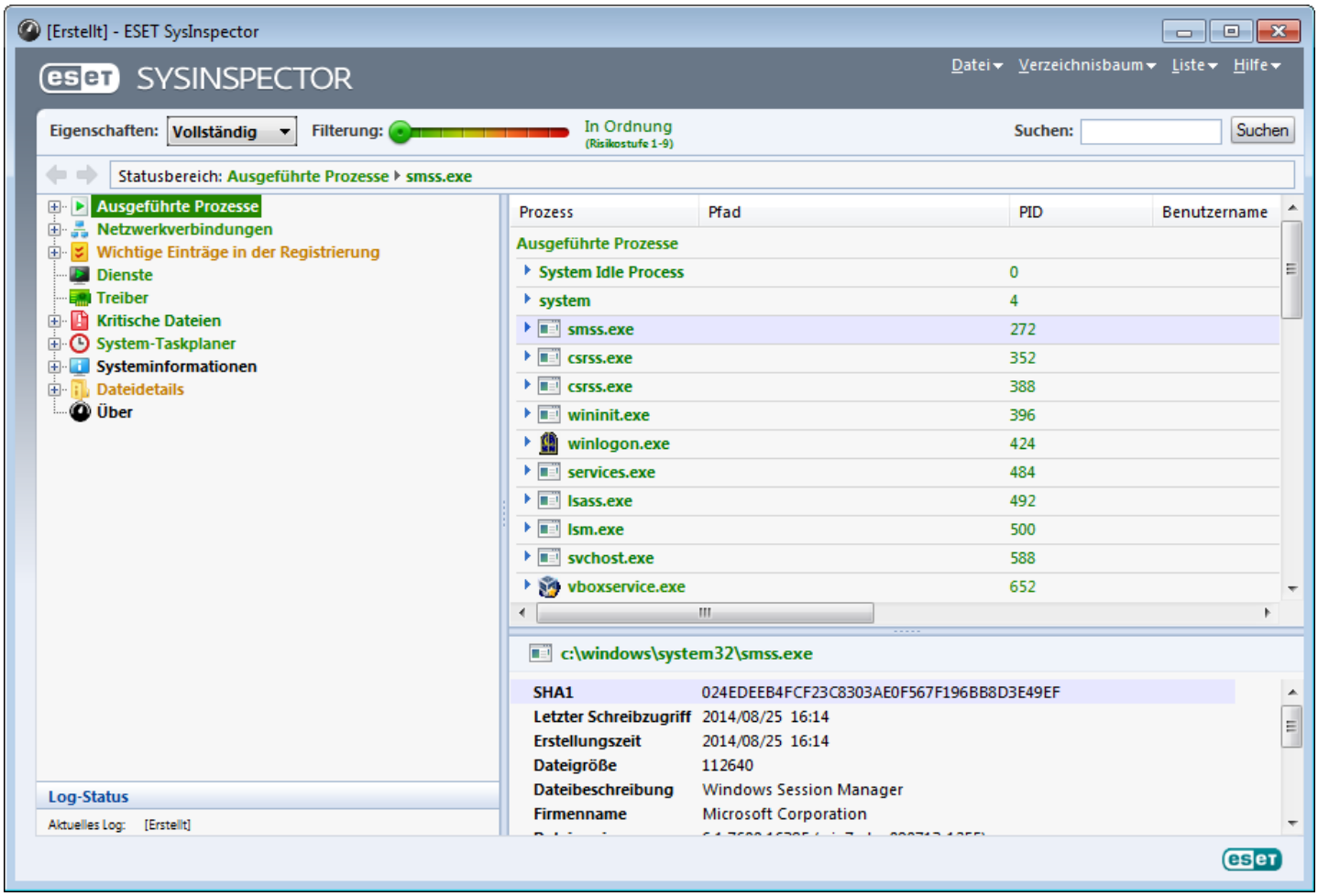
5.6.1.1 Starten von ESET SysInspector

Zum Starten von ESET SysInspector führen Sie einfach die von der ESET-Website heruntergeladene Programmdatei *SysInspector.exe* aus. Wenn bereits ein ESET Security-Produkt installiert ist, können Sie ESET SysInspector direkt aus dem Startmenü starten (**Programme** > **ESET** > **ESET NOD32 Antivirus**).

Warten Sie, während die Anwendung das System überprüft. Dies kann einige Minuten in Anspruch nehmen.

5.6.2 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. Im Bereich „Log-Status“ werden die grundlegenden Parameter eines Logs aufgeführt: Filterverwendung, Filtertyp, ob das Log Ergebnis eines Vergleichs ist usw.



5.6.2.1 Menüs und Bedienelemente

Dieser Abschnitt beschreibt die Menüs und sonstigen Bedienelemente in ESET SysInspector.

Datei

Über das Menü **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.

Verzeichnisbaum

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.

Eigenschaften

Dieses Menü beeinflusst die Informationen, die im Hauptprogrammfenster dargestellt werden und vereinfacht somit ihre Verwendung. Im Modus „Einfach“ haben Sie Zugang zu Informationen, die Hilfestellung bei gewöhnlichen Problemen im System liefern. Im Modus „Mittel“ sehen Sie weniger häufig benötigte Informationen. Im Modus „Vollständig“ zeigt ESET SysInspector alle verfügbaren Informationen an, sodass Sie auch sehr spezielle Probleme beheben können.

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. Befindet sich der Schieberegler ganz links (Risikostufe 1), werden alle Einträge 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. Steht der Schieberegler ganz rechts, zeigt das Programm nur die als schädlich bekannten Einträge an.

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.

Vergleichen

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 Suchergebnisse werden im Beschreibungsfenster angezeigt.

Zurück/Vor

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 Navigationsbereich 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.

5.6.2.2 Navigation in ESET SysInspector

In ESET SysInspector gliedern sich die unterschiedlichen Systeminformationen in eine Reihe von Hauptabschnitten, die so genannten „Knoten“. Falls zusätzliche Informationen verfügbar sind, erreichen Sie diese, indem Sie einen Knoten um seine Unterknoten erweitern. 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 Beschreibungsbereich Detailinhalte zum gerade im Navigationsbereich ausgewählten Knoten angezeigt. Diese Einträge im Beschreibungsbereich können Sie dann wiederum auswählen, um (soweit vorhanden) im Detailbereich weitere Detailinformationen dazu anzuzeigen.

Im Folgenden sind die Hauptknoten im Navigationsbereich sowie die dazugehörigen Informationen im Beschreibungs- und Detailbereich 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 und die Risikostufe der Dateien.

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. Diese Symbole stellen eine vor dem Start liegende Optimierung für derartige Prozesse dar. Sie sind für das System ungefährlich.

Netzwerkverbindungen

Wenn Sie im Navigationsbereich ein Protokoll (TCP oder UDP) auswählen, erscheint im Beschreibungsbereich 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 Beschreibungsbereich werden die mit dem jeweiligen Registrierungseintrag verbundenen Dateien angezeigt. Das Detailfenster zeigt ggf. zusätzliche Informationen an.

Dienste

Bei diesem Knoten enthält der Beschreibungsbereich eine Liste der Dateien, die als Windows-Dienste registriert sind. Das Detailfenster informiert über spezifische Details und darüber, auf welche Art ein Dienst gestartet wird.

Treiber

Dieser Knoten enthält eine Liste der im System installierten Treiber.

Kritische Dateien

Unter diesem Knoten können Sie sich im Beschreibungsbereich den Inhalt wichtiger Konfigurationsdateien von Microsoft Windows anzeigen lassen.

System-Taskplaner

Hier finden Sie eine Liste der Tasks, die vom Windows-Taskplaner zu einer bestimmten Zeit oder in einem bestimmten Intervall ausgeführt werden.

Systeminformationen

Hier finden Sie ausführliche Informationen zu Hardware und Software, den gesetzten Umgebungsvariablen, den Benutzerberechtigungen und dem System-Ereignislog.

Dateidetails

Dieser Knoten enthält eine Liste der wichtigen Systemdateien sowie der Dateien im Ordner „Programme“. Zusätzliche Informationen speziell für diese Dateien werden im Beschreibungs- und Detailfenster angezeigt.

Über

Informationen zur Version von ESET SysInspector sowie eine Liste der Programmmodule

5.6.2.2.1 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 Computerstatus erstellen
Strg+H	erstellt einen Snapshot des Computerstatus, der auch sicherheitsrelevante Informationen im Log enthalten kann

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

Ctrl+A	Vollständige Angaben zu einem Element anzeigen
Strg+C	Daten/Baumpfad des aktuellen Elements kopieren
Strg+X	Elemente ausschneiden
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

Allgemein

F1	Hilfe anzeigen
Alt+F4	Programm beenden
Alt+Umschalt+F4	Programm ohne Rückfrage beenden
Strg+I	Log-Statistik anzeigen

5.6.2.3 Vergleichsfunktion

Mit der „Vergleichen“-Funktion ist es möglich, zwei bestehende Log-Dateien miteinander zu 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. Um das Log zu speichern, klicken Sie auf **Datei** > **Log speichern**. Gespeicherte Log-Dateien können Sie später wieder öffnen, um sie einzusehen. Ein bestehendes Log öffnen Sie über **Datei** > **Log öffnen**. Im Hauptfenster von ESET SysInspector wird immer nur jeweils ein Log angezeigt.

Die Vergleichsfunktion hat den Vorteil, dass Sie sich eine aktive und eine gespeicherte Log-Datei anzeigen lassen können. Klicken Sie dazu auf **Datei** > **Logs vergleichen** und wählen dann **Datei auswählen**. Das ausgewählte Log wird nun mit dem aktiven (im Programmfenster angezeigten) Log verglichen. Das Vergleichs-Log führt lediglich Unterschiede zwischen diesen beiden Logs auf.

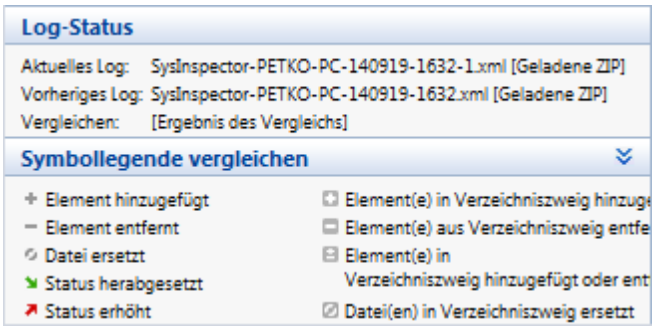
HINWEIS: Wenn Sie nach dem Vergleich zweier Logs auf **Datei** > **Log speichern** klicken und das Ergebnis als ZIP-Datei speichern, werden beide Log-Dateien gespeichert. Wenn Sie die so entstandene Datei später öffnen, werden die enthaltenen Logs automatisch verglichen.

Neben den einzelnen Einträgen sehen Sie in ESET SysInspector Symbole, 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, das die ursprünglichen Informationen über das System enthält, als vorher.xml. Nachdem Sie Änderungen am System vorgenommen haben, öffnen Sie ESET SysInspector und erstellen Sie ein neues Log. 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:

SysInspector.exe neu.xml vorher.xml

5.6.3 Kommandozeilenparameter

Mit ESET SysInspector können Sie auch von der Kommandozeile 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.

5.6.4 Dienste-Skript

Ein Dienste-Skript ist ein Hilfsmittel für Benutzer von ESET SysInspector zur einfachen Entfernung unerwünschter Objekte aus dem System.

Über ein Dienste-Skript können Sie das gesamte ESET SysInspector-Log oder ausgewählte Teile davon exportieren. Nach dem Export 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. Unqualifizierte Änderungen können das Betriebssystem beschädigen.

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 den ersten Menüpunkt im Bereich auf der linken Seite (in der Baumstruktur). Halten Sie die Umschalttaste gedrückt und wählen Sie den letzten Menüpunkt, um alle Menüpunkte 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, auf „+“. Stellen Sie sicher, dass Sie keine wichtige Betriebssystem-Dateien oder -Objekte markieren.
6. Öffnen Sie ESET SysInspector, klicken Sie auf **Datei** > **Dienste-Skript ausführen** und geben Sie den Pfad zu Ihrem Skript ein.
7. Klicken Sie auf **OK**, um das Skript auszuführen.

5.6.4.1 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 dann entweder **Alle Bereiche in das Dienste-Skript** exportieren oder **Ausgewählte Bereiche in das Dienste-Skript exportieren**.

HINWEIS: Wenn Sie gerade zwei Logs miteinander vergleichen, ist kein Export in ein Dienste-Skript möglich.

5.6.4.2 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 wird die Ausführung der ausgewählten Treiber beendet. Beachten Sie bitte, dass dies bei einigen Treibern nicht möglich ist.

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
[...]
```

5.6.4.3 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 Bestätigung Ihrer Auswahl weist unter Umständen eine weitere Warnmeldung darauf hin, dass das auszuführende Dienste-Skript nicht signiert wurde. Klicken Sie auf **Starten**, um das Skript auszuführen.

Ein Dialogfenster mit der Bestätigung über die erfolgreiche Ausführung des Skripts wird angezeigt.

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 trägt keine Signatur. 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.

5.6.5 Häufige Fragen (FAQ)

Muss ESET SysInspector mit Administratorrechten ausgeführt werden?

ESET SysInspector muss zwar nicht unbedingt 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 zu speichern, wählen Sie im Hauptprogrammfenster **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“. Falls Sie es vorziehen, können Sie Speicherort und -namen 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 ist es unter Windows Vista und Windows 7 ggf. nicht möglich, Dateien per Drag and Drop zwischen Fenstern mit unterschiedlichen Sicherheitsberechtigungen zu verschieben.

Ist eine Spezifikation für das Format der Log-Dateien verfügbar? Wie steht es um ein Software Development Kit (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 abzuschätzen. Basierend auf dieser Heuristik wird Objekten dann eine Risikostufe zugewiesen, von 1 - In Ordnung (grün) bis 9 - Risikoreich(rot). Die Farbe der Abschnitte im Navigationsbereich im linken Teil des Programmfensters richtet sich nach der höchsten Risikostufe, die ein darin enthaltenes Objekt hat.

Bedeutet eine Risikostufe von „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 ins 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. Dies ist ein normaler Vorgang für alle digital signierten Programme unter Microsoft Windows.

Was ist Anti-Stealth-Technologie?

Die Anti-Stealth-Technologie ermöglicht eine effektive Erkennung von Rootkits.

Wenn ein System von Schadcode angegriffen wird, der sich wie ein Rootkit verhält, ist der Benutzer dem Risiko von Datenverlust oder -diebstahl ausgesetzt. 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?

Beim Versuch, die digitale Signatur einer ausführbaren Datei zu ermitteln, überprüft ESET SysInspector zuerst, ob in der Datei eine eingebettete Signatur vorhanden ist. Wenn ja, wird die Datei anhand dieser Informationen überprüft. Falls die Datei keine digitale Signatur enthält, sucht ESI nach einer zugehörigen CAT-Datei (Sicherheitskatalog - *%systemroot%\system32\catroot*), die Informationen über die Datei enthält. Falls eine entsprechende CAT-Datei existiert, wird deren digitale Signatur beim Überprüfungsprozess für die ausführbare Datei übernommen.

Aus diesem Grund sind einige Dateien mit „Signatur MS“ markiert, obwohl unter „Firmenname“ ein anderer Eintrag vorhanden ist.

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.

5.6.6 ESET SysInspector als Teil von ESET NOD32 Antivirus

Um den ESET SysInspector-Bereich in ESET NOD32 Antivirus zu öffnen, klicken Sie auf **Tools** > **ESET SysInspector**. Das Verwaltungssystem im ESET SysInspector-Fenster ähnelt dem von Prüfungslogs oder geplanten Tasks. Alle Vorgänge mit Systemsnapshots - Erstellen, Anzeigen, Vergleichen, Entfernen und Exportieren - sind mit einem oder zwei Klicks zugänglich.

Das ESET SysInspector-Fenster enthält Basisinformationen zum erstellten Snapshot wie z. B. Erstellungszeitpunkt, kurzer Kommentar, Name des Benutzers, der den Snapshot erstellt hat, sowie den Status des Snapshots.

Zum Vergleichen, Erstellen oder Löschen von Snapshots verwenden Sie die entsprechenden Schaltflächen unter der Snapshot-Liste im ESET SysInspector-Fenster. Dieselben Optionen stehen auch über das Kontextmenü zur Verfügung. Um den ausgewählten Systemsnapshot anzuzeigen, klicken Sie im Kontextmenü auf **Anzeigen**. Um den ausgewählten Snapshot in eine Datei zu exportieren, klicken Sie mit der rechten Maustaste darauf und wählen **Exportieren**.

Die einzelnen Befehle sind nachstehend noch einmal ausführlicher beschrieben:

- **Vergleichen** - Hiermit können Sie zwei vorhandene Logs vergleichen. Diese Funktion eignet sich dafür, alle Unterschiede zwischen dem aktuellen und einem älteren Log zu ermitteln. Um sie zu nutzen, müssen Sie zwei Snapshots zum Vergleich auswählen.
- **Erstellen...** - Erstellen eines neuen Snapshots. Hierzu müssen Sie zunächst einen kurzen Kommentar zum Snapshot eingeben. Der Erstellungsfortschritt wird in der Spalte **Status** angezeigt. Fertige Snapshots haben den Status **Erstellt**.
- **Löschen/Alle löschen** - Entfernt Einträge aus der Liste.
- **Exportieren...** - Speichert den ausgewählten Eintrag als XML-Datei (wahlweise auch komprimiert als ZIP-Datei).

5.7 Kommandozeile

Das Virenschutz-Modul von ESET NOD32 Antivirus 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	Signaturdatenbank verwenden (Standard)
/no-pattern	Signaturdatenbank 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 findet keine automatische Säuberung statt.
- **standard** (default) - 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 z. B. 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. Glossar

6.1 Schadsoftwaretypen

Bei Schadsoftware handelt es sich um bösartige Software, die versucht, in einen Computer einzudringen und/oder auf einem Computer Schaden anzurichten.

6.1.1 Viren

Ein Computervirus ist Schadcode, der an vorhandene Dateien auf Ihrem Computer vorangestellt oder angehängt wird. Ihren Namen haben sie nicht umsonst mit den Viren aus der Biologie gemein. Schließlich verwenden sie ähnliche Techniken, um sich von einem zum anderen Computer auszubreiten. Der Begriff „Virus“ wird jedoch häufig fälschlicherweise für eine beliebige Art von Bedrohung verwendet. Heute setzt sich mehr und mehr der neue, treffendere Ausdruck „Malware“ (Schadcode; engl. bösartige Software) durch.

Computerviren greifen hauptsächlich ausführbare Dateien und Dokumente an. Und so funktioniert ein Computervirus: Beim Ausführen einer infizierten Datei wird zunächst der Schadcode aufgerufen und ausgeführt, noch bevor die ursprüngliche Anwendung ausgeführt wird. Viren können beliebige Dateien infizieren, für die der aktuelle Benutzer über Schreibberechtigungen verfügt.

Computerviren unterscheiden sich nach Art und Schweregrad der durch sie verursachten Schäden. Einige von ihnen sind aufgrund ihrer Fähigkeit, Dateien von der Festplatte gezielt zu löschen, äußerst gefährlich. Andererseits gibt es aber auch Viren, die keinen Schaden verursachen. Ihr einziger Zweck besteht darin, den Benutzer zu verärgern und die technischen Fähigkeiten ihrer Urheber unter Beweis zu stellen.

Wenn Ihr Computer mit einem Virus infiziert ist und nicht gesäubert werden kann, senden Sie die Datei zur genaueren Prüfung an das ESET-Virenlabor. In einigen Fällen können infizierte Dateien so stark geändert werden, dass eine Säuberung nicht möglich ist und die Datei durch eine saubere Kopie ersetzt werden muss.

6.1.2 Würmer

Bei einem Computerwurm handelt es sich um ein Programm, das Schadcode enthält, der Hostcomputer angreift und sich über Netzwerke verbreitet. Der grundlegende Unterschied zwischen Viren und Würmern besteht darin, dass Würmer in der Lage sind, sich selbstständig zu vermehren und zu verbreiten. Sie sind unabhängig von Hostdateien (oder Bootsektoren). Würmer verbreiten sich an die E-Mail-Adressen in Ihrer Kontaktliste oder nutzen Sicherheitslücken von Anwendungen in Netzwerken.

Daher sind Würmer wesentlich funktionsfähiger als Computerviren. Aufgrund der enormen Ausdehnung des Internets können sich Würmer innerhalb weniger Stunden und sogar Minuten über den gesamten Globus verbreiten. Da sich Würmer unabhängig und rasant vermehren können, sind sie gefährlicher als andere Arten von Schadsoftware.

Ein innerhalb eines Systems aktivierter Wurm kann eine Reihe von Unannehmlichkeiten verursachen: Er kann Dateien löschen, die Systemleistung beeinträchtigen oder Programme deaktivieren. Aufgrund ihrer Beschaffenheit können Würmer als Transportmedium für andere Arten von Schadcode fungieren.

Wurde Ihr Computer mit einem Wurm infiziert, empfiehlt es sich, alle betroffenen Dateien zu löschen, da sie höchstwahrscheinlich Schadcode enthalten.

6.1.3 Trojaner

Trojaner (trojanische Pferde) galten früher als eine Klasse von Schadprogrammen, die sich als nützliche Anwendungen tarnen, um den Benutzer zur Ausführung zu verleiten.

Da es sich hierbei um eine sehr breite Kategorie handelt, werden „Trojaner“ oft in mehrere Unterkategorien unterteilt:

- **Downloader** - Schadcode, der das Herunterladen anderer Bedrohungen aus dem Internet verursacht
- **Dropper** - Schadcode, der andere Arten von Schadcode auf gefährdete Computer verteilen kann
- **Backdoor** - Schadcode, der Remote-Angreifern die Möglichkeit gibt, auf den Computer zuzugreifen und ihn zu steuern
- **Keylogger** - Programm, das die Tastenanschläge eines Benutzers aufzeichnet und die Informationen an Angreifer sendet.
- **Dialer** - Schadcode, der Verbindungen zu teuren Einwahlnummern herstellt. Dass eine neue Verbindung erstellt wurde, ist für den Benutzer nahezu unmöglich festzustellen. Dialer sind nur eine Gefahr für Benutzer von Einwahlmodems. Diese werden allerdings nur noch selten eingesetzt.

Wenn auf Ihrem Computer eine Datei als Trojaner identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit ausschließlich Schadcode enthält.

6.1.4 Rootkits

Rootkits sind bösartige Programme, die Hackern unbegrenzten und verdeckten Zugriff auf ein System verschaffen. Nach dem Zugriff auf ein System (in der Regel unter Ausnutzung einer Sicherheitslücke) greifen Rootkits auf Funktionen des Betriebssystems zurück, um nicht von der Virenschutz-Software erkannt zu werden: Prozesse, Dateien und Windows-Registrierungsdaten werden versteckt. Aus diesem Grund ist es nahezu unmöglich, Rootkits mithilfe der üblichen Prüfmethoden zu erkennen.

Rootkits können auf zwei verschiedenen Ebenen entdeckt werden:

1. Beim Zugriff auf ein System. Die Rootkits haben das System noch nicht befallen, sind also inaktiv. Die meisten Virenschutzsysteme können Rootkits auf dieser Ebene entfernen (vorausgesetzt, dass solche Dateien auch als infizierte Dateien erkannt werden).
2. Wenn sie sich vor der üblichen Prüfung verbergen. Die Anti-Stealth-Technologie von ESET NOD32 Antivirus kann auch aktive Rootkits erkennen und entfernen.

6.1.5 Adware

Adware ist eine Abkürzung für durch Werbung (engl. Advertising) unterstützte Software. In diese Kategorie fallen Programme, die zur Anzeige von Werbung dienen. Adware-Anwendungen öffnen häufig in Internetbrowsern neue Popup-Fenster mit Werbung oder ändern die Startseite des Browsers. Adware gehört oftmals zu Freeware-Programmen, damit deren Entwickler auf diesem Weg die Entwicklungskosten ihrer (gewöhnlich nützlichen) Anwendungen decken können.

Adware selbst ist nicht gefährlich - allerdings werden die Benutzer mit Werbung belästigt. Bedenklich ist Adware, insofern sie auch dazu dienen kann, Daten zu sammeln (wie es bei Spyware der Fall ist).

Wenn Sie sich dafür entscheiden, ein Freeware-Produkt zu verwenden, sollten Sie bei der Installation besonders aufmerksam sein. Die meisten Installationsprogramme benachrichtigen Sie über die Installation eines zusätzlichen Adware-Programms. In vielen Fällen ist es möglich, diesen Teil der Installation abzubrechen und das Programm ohne Adware zu installieren.

In einigen Fällen lassen sich Programme jedoch nicht ohne die Adware installieren, oder nur mit eingeschränktem Funktionsumfang. Das bedeutet, dass Adware häufig ganz „legal“ auf das System zugreift, da sich die Benutzer damit einverstanden erklärt haben. In diesem Fall gilt: Vorsicht ist besser als Nachsicht. Wird auf Ihrem Computer ein Adware-Programm entdeckt, sollten Sie die Datei löschen, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

6.1.6 Spyware

Der Begriff „Spyware“ fasst alle Anwendungen zusammen, die vertrauliche Informationen ohne das Einverständnis/ Wissen des Benutzers versenden. Diese Programme verwenden Überwachungsfunktionen, um verschiedene statistische Daten zu versenden, z. B. eine Liste der besuchten Websites, E-Mail-Adressen aus dem Adressbuch des Benutzers oder eine Auflistung von Tastatureingaben.

Die Entwickler von Spyware geben vor, auf diesem Weg die Interessen und Bedürfnisse der Benutzer erkunden zu wollen. Ziel sei es, gezieltere Werbeangebote zu entwickeln. Das Problem dabei ist, dass nicht wirklich zwischen nützlichen und bösartigen Anwendungen unterschieden werden kann. Niemand kann sicher sein, dass die gesammelten Informationen nicht missbraucht werden. Die von Spyware gesammelten Daten enthalten möglicherweise Sicherheitscodes, PINs, Kontonummern usw. Spyware wird oft im Paket mit der kostenlosen Version eines Programms angeboten, um so Einkünfte zu erzielen oder einen Anreiz für den Erwerb der kommerziellen Version zu schaffen. Oft werden die Benutzer bei der Programminstallation darüber informiert, dass Spyware eingesetzt wird, um sie damit zu einem Upgrade auf die kommerzielle, Spyware-freie Version zu bewegen.

Beispiele für bekannte Freeware-Produkte, die zusammen mit Spyware ausgeliefert werden, sind Client-Anwendungen für P2P-Netzwerke. Programme wie Spyfalcon oder Spy Sheriff gehören zur einer besonderen Kategorie von Spyware: Getarnt als Spyware-Schutzprogramme üben sie selbst Spyware-Funktionen aus.

Wenn auf Ihrem Computer eine Datei als Spyware identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

6.1.7 Packprogramme

Ein Packprogramm ist eine selbstextrahierende, ausführbare Anwendung, mit der verschiedene Arten Malware in einem einzigen Paket gebündelt werden können.

Zu den bekanntesten Packprogrammen zählen UPX, PE_Compact, PKLite und ASPack. Die Erkennung einer bestimmten Malware unterscheidet sich je nach dem verwendeten Packprogramm. Packprogramme können außerdem ihre „Signatur“ verändern, sodass die Malware schwieriger zu erkennen und zu entfernen ist.

6.1.8 Potenziell unsichere Anwendungen

Es gibt zahlreiche seriöse Programme, die die Verwaltung miteinander vernetzter Computer vereinfachen sollen. Wenn sie aber in die falschen Hände geraten, kann mit ihnen Schaden angerichtet werden. Mit ESET NOD32 Antivirus können solche Bedrohungen erkannt werden.

Zur Kategorie der **Potenziell unsicheren Anwendungen** zählen Programme, die zwar erwünscht sind, jedoch potenziell gefährliche Funktionen bereitstellen. Dazu 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).

Sollten Sie feststellen, dass auf Ihrem Computer eine potenziell unsichere Anwendung vorhanden ist (die Sie nicht selbst installiert haben), wenden Sie sich an Ihren Netzwerkadministrator oder entfernen Sie die Anwendung.

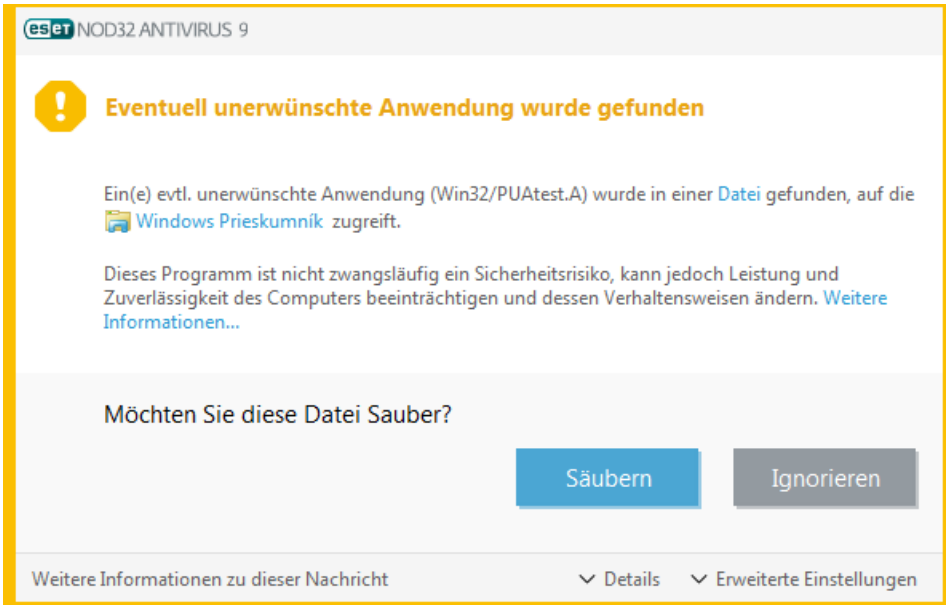
6.1.9 Eventuell unerwünschte Anwendungen

Eine eventuell unerwünschte Anwendung ist ein Programm, das Adware enthält, Toolbars installiert oder andere unklare Ziele hat. In manchen Fällen kann ein Benutzer der Meinung sein, dass die Vorteile der evtl. unerwünschten Anwendung bedeutender sind als die Risiken. Aus diesem Grund weist ESET solchen Anwendungen eine niedrigere Risikoeinstufung zu als anderen Schadcodearten wie Trojanern oder Würmern.

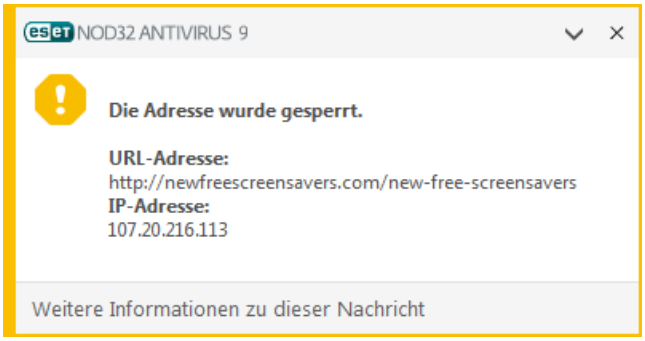
Warnung - Potenzielle Bedrohung erkannt

Wenn eine potenziell unerwünschte Anwendung erkannt wird, können Sie auswählen, welche Aktion ausgeführt werden soll:

1. **Säubern/Trennen**: Mit dieser Option wird die Aktion beendet und die potenzielle Bedrohung daran gehindert, in das System zu gelangen.
2. **Ignorieren**: Bei dieser Option kann eine potenzielle Bedrohung in Ihr System gelangen.
3. Wenn die Anwendung zukünftig ohne Unterbrechung auf dem Computer ausgeführt werden soll, klicken Sie auf **Erweiterte Optionen** und aktivieren Sie das Kontrollkästchen neben **Von der Erkennung** ausschließen.

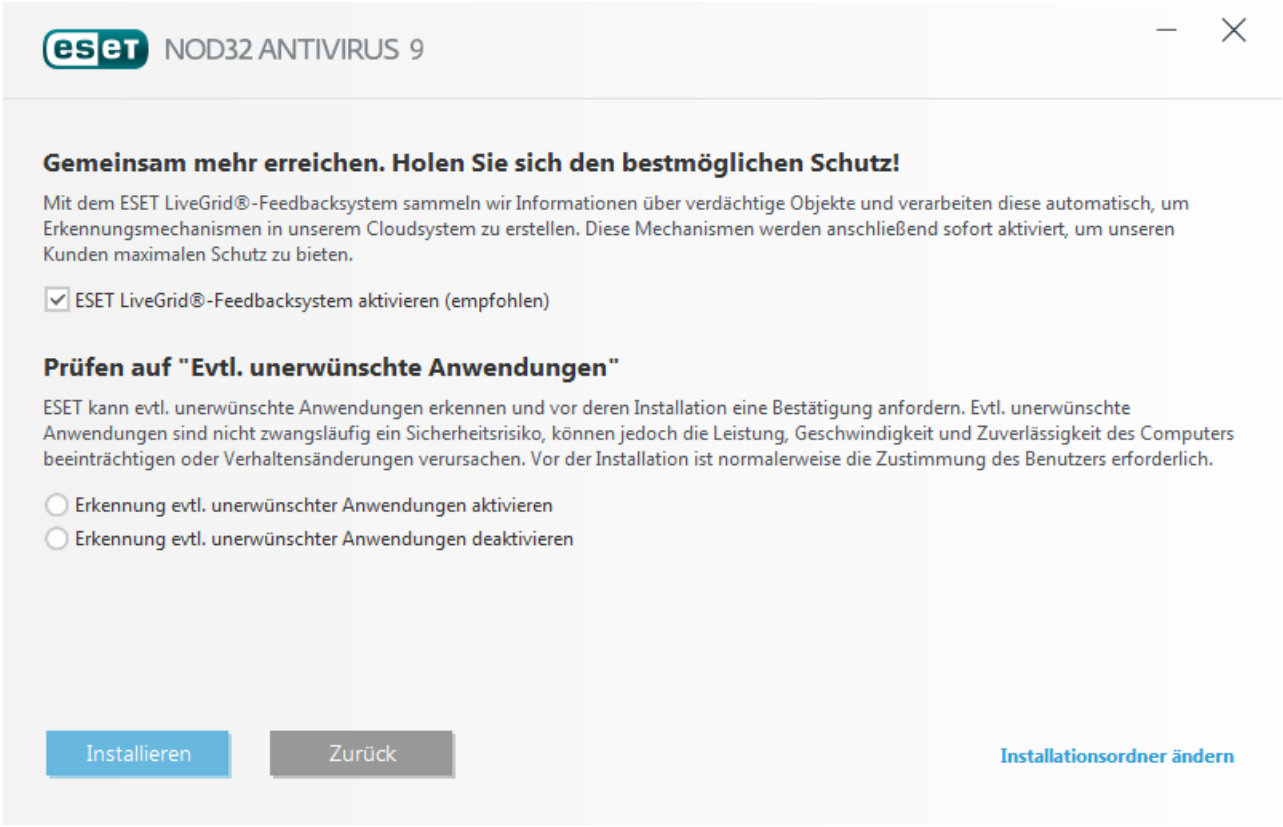


Wenn eine evtl. unerwünschte Anwendung erkannt wird und nicht gesäubert werden kann, erscheint unten rechten im Bildschirm die Benachrichtigung **Adresse wurde gesperrt**. Weitere Informationen hierzu finden Sie unter **Tools** > **Log-Dateien** > **Gefilterte Websites** im Hauptmenü.



Eventuell unerwünschte Anwendungen - Einstellungen

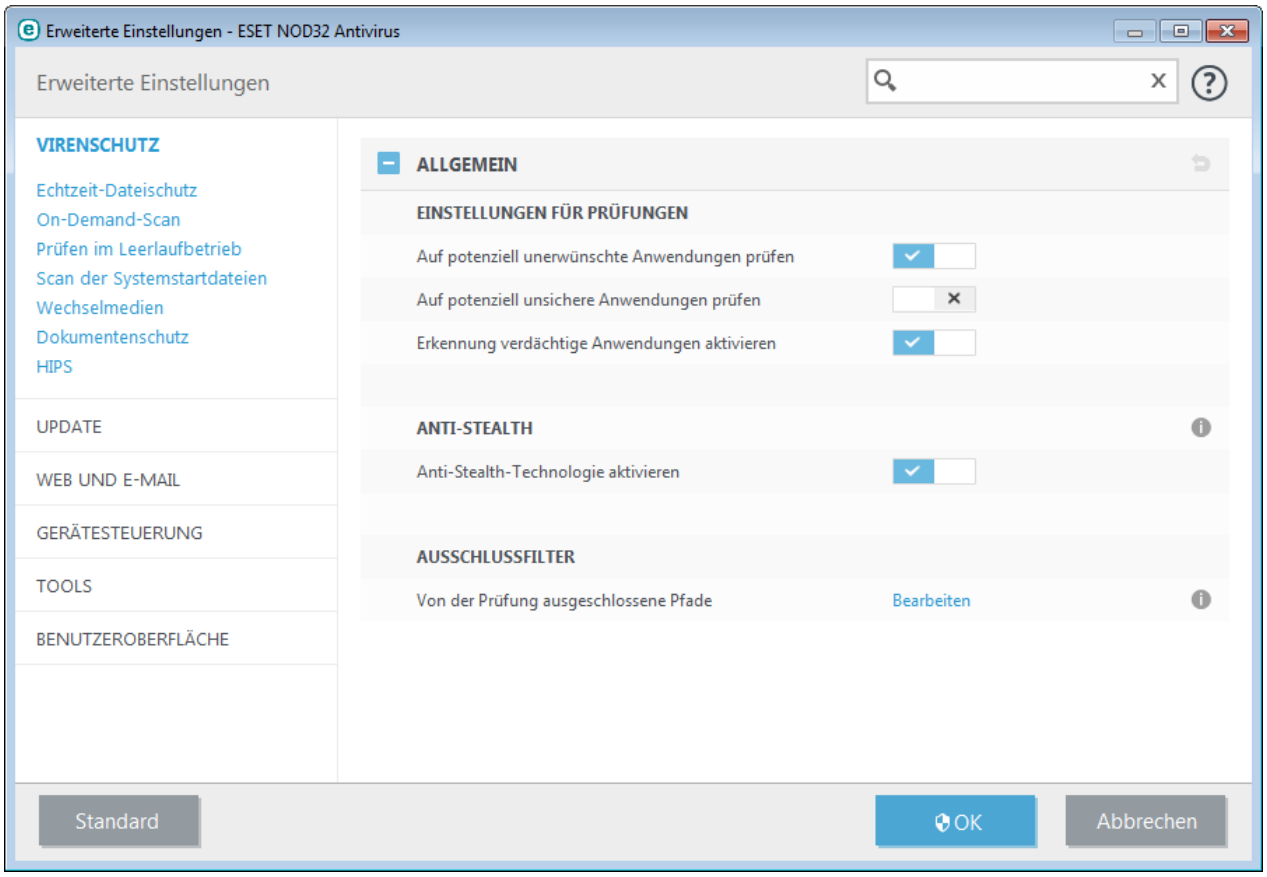
Bei der Installation des ESET-Produkts können Sie auswählen, ob Sie die Erkennung evtl. unerwünschter Anwendungen aktivieren möchten:



Eventuell unerwünschte Anwendungen können Adware oder Toolbars installieren oder andere unerwünschte oder unsichere Programmfunktionen enthalten.

Diese Einstellungen können jederzeit in den Programmeinstellungen geändert werden. Gehen Sie folgendermaßen vor, um die Erkennung evtl. unerwünschter, unsicherer oder verdächtiger Anwendungen zu deaktivieren:

1. Öffnen Sie das ESET-Produkt. Wie öffne ich mein ESET-Produkt?
2. Drücken Sie **F5**, um die **Erweiterten Einstellungen** zu öffnen.
3. Klicken Sie auf **Virenschutz** und aktivieren bzw. deaktivieren Sie die Optionen **Erkennung evtl. unerwünschter Anwendungen aktivieren**, **Auf potenziell unsichere Anwendungen prüfen** und **Auf potenziell verdächtige Anwendungen prüfen**. Klicken Sie zum Bestätigen auf **OK**.



Eventuell unerwünschte Anwendungen - Software-Wrapper

Ein Software-Wrapper ist eine besondere Art Anwendungsänderung, die von einigen Dateihost-Websites verwendet wird. Es handelt sich um ein Drittanbieter-Tool, das neben der gewünschten Anwendung zusätzliche Software wie Toolbars oder Adware installiert. Die zusätzliche Software kann auch Änderungen an der Startseite des Webbrowsers und an den Sucheinstellungen vornehmen. Außerdem setzen Dateihost-Websites den Softwarehersteller oder den Download-Empfänger oft nicht über solche Änderungen in Kenntnis und ermöglichen nicht immer eine einfach Abwahl der Änderung. Aus diesem Grund stuft ESET Software-Wrapper als eine Art evtl. unerwünschter Anwendung ein, damit der Benutzer den Download wissen annehmen oder ablehnen kann.

Eine aktualisierte Version dieser Hilfeseite finden Sie in diesem ESET-Knowledgebase-Artikel.

6.2 ESET-Technologie

6.2.1 Exploit-Blocker

Der Exploit-Blocker sichert besonders anfällige Anwendungstypen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme und MS Office-Komponenten ab. Er überwacht das Verhalten von Prozessen auf verdächtige Aktivitäten, die auf einen Exploit hinweisen könnten.

Wenn der Exploit-Blocker einen verdächtigen Prozess identifiziert, kann er ihn sofort anhalten und Daten über die Bedrohung erfassen, die dann an das ThreatSense-Cloudsystem gesendet werden. Diese Daten werden im ESET-Virenlabor analysiert und genutzt, um alle Anwender besser vor unbekannten Bedrohungen und neuesten Angriffen durch Malware, für die noch keine Erkennungssignaturen vorhanden sind, zu schützen.

6.2.2 Erweiterte Speicherprüfung

Die erweiterte Speicherprüfung bietet im Zusammenspiel mit dem Exploit-Blocker stärkeren Schutz vor Malware, die darauf ausgelegt ist, der Erkennung durch Anti-Malware-Produkte mittels Verschleierung und/oder Verschlüsselung zu entgehen. In Fällen, in denen herkömmliche Emulation oder Heuristik eine Bedrohung eventuell nicht aufspüren, kann die erweiterte Speicherprüfung verdächtiges Verhalten identifizieren und Bedrohungen erkennen, wenn sie sich im Arbeitsspeicher manifestieren. Diese Lösung kann selbst gegen stark verschleierte Malware wirkungsvoll agieren.

Anders als der Exploit-Blocker sucht die erweiterte Speicherprüfung nach ausgeführter Malware. Damit ist das Risiko verbunden, dass vor der Erkennung einer Bedrohung bereits schädliche Aktivitäten durchgeführt wurden; falls jedoch andere Erkennungsmethoden versagt haben, bietet sie eine zusätzliche Schutzebene.

6.2.3 ThreatSense

ESET LiveGrid® basiert auf dem ThreatSense.Net®-Frühwarnsystem, nutzt übermittelte Daten von ESET-Benutzern auf der ganzen Welt und sendet diese an das ESET-Virenlabor. 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. Die ESET-Schadcodeforscher gewinnen aus diesen Informationen ein präzises Bild von Eigenschaften und Umfang aktueller weltweiter Bedrohungen, wodurch wir uns auf die relevanten Ziele konzentrieren können. ESET LiveGrid® -Daten spielen eine wichtige Rolle für die Prioritäten in unserer automatisierten Datenverarbeitung.

Zudem wird ein Reputations-Check umgesetzt, der die Effizienz unserer Anti-Malware-Lösung insgesamt weiter steigern kann. Wenn eine ausführbare Datei oder ein Archiv im System eines Anwenders untersucht werden, wird als erstes das Hash-Tag mit einer Datenbank mit Positiv- und Negativeinträgen abgeglichen. Wird es auf der Positivliste gefunden, gilt die untersuchte Datei als sauber und wird bei zukünftigen Prüfungen übersprungen. Wenn es sich auf der Negativliste befindet, werden ja nach Art der Bedrohung geeignete Maßnahmen getroffen. Sollte keine Übereinstimmung gefunden werden, wird die Datei gründlich analysiert. Auf dieser Grundlage werden Dateien als Bedrohung oder keine Bedrohung kategorisiert. Dieser Ansatz wirkt sich sehr positiv auf die Prüfleistung aus.

Dieser Reputations-Check ermöglicht die effektive Erkennung von Malwareproben, selbst wenn ihre Signaturen noch nicht per Aktualisierung der Virusdatenbank auf den Computer des Anwenders übertragen wurden (was mehrmals täglich geschieht).

6.2.4 Java-Exploit-Blocker

Der Java-Exploit-Blocker ist eine Erweiterung des existierenden Exploit-Blocker-Schutzes. Er überwacht Java und sucht nach exploitverdächtigen Verhaltensweisen. Blockierte Proben können an Schadsoftware-Analysten gemeldet werden, sodass diese Signaturen zum Blockieren der Bedrohung auf anderen Ebenen erstellen können (URL-Sperren, Dateidownload usw.).

6.3 E-Mail

Die E-Mail („elektronische Post“) ist ein modernes Kommunikationsmittel mit vielen Vorteilen. Dank ihrer Flexibilität, Schnelligkeit und Direktheit spielte die E-Mail bei der Verbreitung des Internets in den frühen 1990er Jahren eine entscheidende Rolle.

Doch aufgrund der Anonymität, die E-Mails und das Internet bieten, wird diese Kommunikationsform auch häufig für illegale Aktivitäten wie das Versenden von Spam-Mails genutzt. Als „Spam“ gelten z. B. unerwünschte Werbeangebote, Hoaxes (Falschmeldungen) und E-Mails, mit denen Schadsoftware verbreitet werden soll. Die Belästigung und Gefährdung durch Spam wird zusätzlich dadurch gefördert, dass E-Mails praktisch kostenlos versendet werden können und den Verfassern von Spam-Mails verschiedenste Tools und Quellen zur Verfügung stehen, um an neue E-Mail-Adressen zu gelangen Die große Anzahl und Vielfalt, in der Spam-Mails auftreten, erschwert die Kontrolle. Je länger Sie eine E-Mail-Adresse verwenden, desto wahrscheinlicher ist es, dass diese in einer Spam-Datenbank erfasst wird. Einige Tipps zur Vorbeugung:

- Veröffentlichen Sie Ihre E-Mail-Adresse, soweit möglich, nicht im Internet
- Geben Sie Ihre E-Mail-Adresse nur an vertrauenswürdige Personen weiter
- Benutzen Sie, wenn möglich, keine üblichen Aliasnamen - bei komplizierten Aliasnamen ist die Wahrscheinlichkeit der Verfolgung niedriger
- Antworten Sie nicht auf Spam-Mails, die sich in Ihrem Posteingang befinden
- Seien Sie vorsichtig, wenn Sie Internetformulare ausfüllen - achten Sie insbesondere auf Optionen wie „Ja, ich möchte per E-Mail informiert werden“.
- Verwenden Sie separate E-Mail-Adressen - z. B. eine für Ihre Arbeit, eine für die Kommunikation mit Freunden usw.
- Ändern Sie Ihre E-Mail-Adresse von Zeit zu Zeit
- Verwenden Sie eine Spamschutz-Lösung

6.3.1 Werbung

Werbung im Internet ist eine der am schnellsten wachsenden Formen von Werbung. Die wesentlichen Vorteile für das Marketing liegen im geringen finanziellen Aufwand und dem hohen Grad von Direktheit. Davon abgesehen erreichen E-Mails die Empfänger fast ohne Zeitverzögerung. In vielen Unternehmen werden E-Mail-Marketingtools für eine effektive Kommunikation mit aktuellen und zukünftigen Kunden verwendet.

Da Sie Interesse an kommerziellen Informationen zu bestimmten Produkten haben könnten, handelt es sich dabei um rechtmäßige Werbung. Doch vielfach werden unerwünschte Massen-E-Mails mit Werbung versendet. In solchen Fällen ist die Grenze der E-Mail-Werbung überschritten, und diese E-Mails gelten als Spam.

Die Masse der unerwünschten E-Mails hat sich zu einem Problem entwickelt, ohne dass ein Nachlassen abzusehen ist. Die Verfasser unerwünschter E-Mails versuchen häufig, Spam-E-Mails wie rechtmäßige Nachrichten aussehen zu lassen.

6.3.2 Falschmeldungen (Hoaxes)

Ein Hoax ist eine Spam-Nachricht, die über das Internet verbreitet wird. Hoaxes werden im Allgemeinen per E-Mail oder über Kommunikationstools wie ICQ oder Skype versendet. Der Inhalt der Nachricht ist meist ein Scherz oder eine Falschmeldung.

Oft werden dabei Falschmeldungen zu angeblichen Computerviren verbreitet. Der Empfänger soll verunsichert werden, indem ihm mitgeteilt wird, dass sich auf seinem Computer ein „nicht identifizierbarer Virus“ befindet, der Dateien zerstört, Passwörter abruft oder andere schädliche Vorgänge verursacht.

Es kommt vor, dass ein Hoax den Empfänger auffordert, die Nachricht an seine Kontakte weiterzuleiten, wodurch er sich verbreitet. Es gibt verschiedenste Arten von Hoaxes - Mobiltelefon-Hoaxes, Hilferufe, Angebote zu Geldüberweisungen aus dem Ausland usw. Häufig ist es nicht möglich, die tatsächliche Absicht des Autors zu durchschauen.

Wenn Sie eine Nachricht lesen, in der Sie aufgefordert werden, diese an alle Ihre Kontakte weiterzuleiten, so handelt es sich möglicherweise um einen Hoax. Es gibt viele Internetseiten, auf denen Sie prüfen können, ob eine

E-Mail rechtmäßig ist oder nicht. Bevor Sie eine fragliche Nachricht weiterleiten, versuchen Sie über eine Internetsuche abzuklären, ob es sich um einen Hoax handelt.

6.3.3 Phishing

Der Begriff „Phishing“ bezeichnet eine kriminelle Vorgehensweise, die sich Techniken des Social Engineering (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Das Ziel von Phishing ist es, an vertrauliche Daten wie Kontonummern, PIN-Codes usw. heranzukommen.

Der Zugriff auf vertrauliche Informationen wird oft durch das Versenden von E-Mails erreicht, die von einer scheinbar vertrauenswürdigen Person bzw. von einem scheinbar seriösen Unternehmen (z. B. Finanzinstitution, Versicherungsunternehm) stammen. Eine solche E-Mail kann sehr echt aussehen. Grafiken und Inhalte wurden möglicherweise sogar von der Quelle entwendet, die nachgeahmt werden soll. Sie werden unter einem Vorwand (Datenprüfung, finanzielle Transaktionen usw.) aufgefordert, persönliche Daten einzugeben, wie Ihre Bankverbindung, Benutzernamen und Passwörter. Alle diese Daten, werden Sie denn übermittelt, können mühelos gestohlen oder missbraucht werden.

Banken, Versicherungen und andere rechtmäßige Unternehmen fragen nie in einer E-Mail nach Benutzername und Passwort.

6.3.4 Erkennen von Spam-Mails

Es gibt verschiedene Anzeichen, die darauf hindeuten, dass es sich bei einer bestimmten E-Mail in Ihrem Postfach um Spam handelt. Wenn eines oder mehrere der folgenden Kriterien zutreffen, handelt es sich höchstwahrscheinlich um eine Spam-Nachricht:

- Die Adresse des Absenders steht nicht in Ihrer Kontaktliste.
- Ihnen wird ein größerer Geldbetrag in Aussicht gestellt, Sie sollen jedoch zunächst eine kleinere Summe zahlen.
- Sie werden unter einem Vorwand (Datenprüfung, finanzielle Transaktionen usw.) aufgefordert, persönliche Daten einzugeben, wie Ihre Bankverbindung, Benutzernamen und Passwörter
- Die Nachricht ist in einer anderen Sprache verfasst.
- Sie werden aufgefordert, ein Produkt zu erwerben, das Sie nicht bestellt haben. Falls Sie das Produkt dennoch kaufen möchten, prüfen Sie, ob der Absender ein vertrauenswürdiger Anbieter ist (fragen Sie beim Hersteller nach).
- Einige Wörter sind falsch geschrieben, um den Spamfilter zu umgehen, z. B. „Vaigra“ statt „Viagra“ usw.

7. 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 NOD32 Antivirus
So entfernen Sie einen Virus von Ihrem PC
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 NOD32 Antivirus-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 dies?
Wie kann ich meinen Benutzernamen/Passwort in ESET Smart Security/ESET NOD32 Antivirus eingeben?
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 NOD32 Antivirus, auf der Registerkarte **Hilfe und Support**.

7.1 So aktualisieren Sie ESET NOD32 Antivirus

Die Aktualisierung von ESET NOD32 Antivirus 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.)

7.2 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 **Computerscan**.
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 **Benutzerdefinierter Scan** und wählen Sie dann die Ziele aus, die auf Viren geprüft werden sollen.

Weitere Informationen finden Sie in diesem regelmäßig aktualisierten ESET-Knowledgebase-Artikel.

7.3 So erstellen Sie eine neue Aufgabe im Taskplaner

Zum Erstellen eines Tasks unter **Tools** > **Taskplaner** klicken Sie auf **Hinzufügen** oder klicken mit der rechten Maustaste und wählen 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 (Risikostufen-)Analyse Ihrer Systemkomponenten (z. B. Treiber und Anwendungen).
- **On-Demand-Scan** - Prüft die Dateien und Ordner auf Ihrem Computer.
- **Erster Scan** - Standardmäßig wird 20 Minuten nach Installation oder Neustart eine Prüfung als Task mit geringer Priorität ausgeführt.
- **Update** - Erstellt einen Update-Task. Dieser besteht aus der Aktualisierung der Signaturdatenbank und der Aktualisierung der Programmmodule.

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.

7.4 So planen Sie eine wöchentliche Computerprüfung

Um eine regelmäßige Prüfung zu planen, öffnen Sie das Hauptprogrammfenster und klicken Sie auf **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-Scan**.
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.