Kaspersky Total Security

Benutzerhandbuch

PROGRAMMVERSION: 15.0 MAINTENANCE RELEASE 1

Sehr geehrter Benutzer!

Vielen Dank, dass Sie unser Produkt ausgewählt haben. Wir hoffen, dass diese Dokumentation Ihnen hilft und die meisten Fragen damit beantwortet werden können.

Achtung! Die Rechte für dieses Dokument liegen bei Kaspersky Lab ZAO (im Weiteren auch "Kaspersky Lab") und sind durch das Urheberrecht der Russischen Föderation und durch internationale Verträge geschützt. Bei illegalem Vervielfältigen und Weiterverbreiten des Dokuments oder einzelner Teile daraus kann der Beschuldigte nach geltendem Recht zivilrechtlich, verwaltungsrechtlich und strafrechtlich zur Verantwortung gezogen werden.

Das Vervielfältigen, Weiterverbreiten und Übersetzen der Unterlagen ist nur nach vorheriger schriftlicher Genehmigung von Kaspersky Lab zulässig.

Das Dokument und dazu gehörende Grafiken dürfen nur zu informativen, nicht gewerblichen oder persönlichen Zwecken gebraucht werden.

Kaspersky Lab behält sich das Recht vor, dieses Dokument ohne vorherige Benachrichtigung zu ändern. Die neueste Version finden Sie auf der Seite von Kaspersky Lab unter der Adresse http://www.kaspersky.de/docs.

Für den Inhalt, die Qualität, Aktualität und Richtigkeit der im Dokument verwendeten Unterlagen, deren Rechte anderen Rechteinhabern gehören, sowie für den möglichen Schaden durch die Nutzung dieser Unterlagen, lehnt Kaspersky Lab ZAO die Haftung ab.

Redaktionsdatum: 29.04.2015

© 2015 Kaspersky Lab ZAO. Alle Rechte vorbehalten.

http://www.kaspersky.com/de
http://support.kaspersky.com/de/

INHALT

ÜBER DIESES HANDBUCH

Dieses Dokument ist das Benutzerhandbuch für Kaspersky Total Security.

Um Kaspersky Total Security zu bedienen, sollte sich der Benutzer mit der Benutzeroberfläche und den Grundfunktionen des verwendeten Betriebssystems auskennen und mit E-Mail und Internet umgehen können.

Das Handbuch dient folgenden Zwecken:

- Hilfe bei der Installation, Aktivierung und Verwendung von Kaspersky Total Security.
- Schnelle Beantwortung von Fragen, die sich auf die Arbeit von Kaspersky Total Security beziehen.
- Hinweise auf zusätzliche Informationsquellen zum Programm und auf Möglichkeiten des technischen Supports.

IN DIESEM ABSCHNITT

IN DIESEM DOKUMENT

Dieses Dokument enthält folgende Abschnitte.

Informationsquellen zum Programm (auf S. 12)

Dieser Abschnitt beschreibt Informationsquellen zum Programm und verweist auf Webseiten, die zur Diskussion über das Programm dienen.

Kaspersky Total Security (auf S. 14)

Dieser Abschnitt beschreibt die Programm-Features und bietet kurze Informationen zu den Programmfunktionen und -komponenten. Hier werden der Lieferumfang und die Services beschrieben, die den registrierten Programmnutzern zur Verfügung stehen. Dieser Abschnitt informiert über die Hard- und Softwarevoraussetzungen, die ein Computer erfüllen muss, damit das Programm installiert werden kann.

Programm installieren und deinstallieren (auf S. 20)

Dieser Abschnitt bietet schrittweise Anleitungen zur Installation und Deinstallation des Programms.

Lizenzverwaltung des Programms (auf S. 29)

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmaktivierung zusammenhängen. Hier werden Lizenzvertrag, Methoden zur Programmaktivierung und Verlängerung der Lizenzgültigkeit erläutert.

Mit den Benachrichtigungen des Programms arbeiten (auf S. 34)

Dieser Abschnitt informiert über die Arbeit mit den Benachrichtigungen des Programms.

Mit unbekannten Programmen arbeiten (auf S. 71)

Dieser Abschnitt enthält Informationen über die Verhinderung von unberechtigten Programmaktionen auf dem Computer.

Modus für vertrauenswürdige Programme (s. S. 77)

Dieser Abschnitt enthält Informationen über den Modus für vertrauenswürdige Programme.

Datenvernichtung (auf S. 80)

Dieser Abschnitt informiert darüber, wie mithilfe von Kaspersky Total Security Daten so gelöscht werden, damit sie von Angreifern nicht wiederhergestellt werden können.

Löschen von nicht benötigten Daten (auf S. 82)

Dieser Abschnitt informiert darüber, wie temporäre und nicht benötigte Daten gelöscht werden können.

Backup (auf S. 84)

Dieser Abschnitt informiert darüber, wie mithilfe von Kaspersky Total Security Daten gesichert werden.

Daten in Datentresoren speichern (auf S. 89)

Dieser Abschnitt informiert darüber, wie Dateien und Ordner auf Ihrem Computer mithilfe von Datentresoren geschützt werden.

Zugriff auf die Verwaltung von Kaspersky Total Security mit einem Kennwort schützen (auf S. 91)

Dieser Abschnitt beschreibt, wie die Programmeinstellungen mithilfe eines Kennworts geschützt werden können.

Computerschutz anhalten und fortsetzen (auf S. 92)

Dieser Abschnitt enthält Schritt-für-Schritt-Anweisungen zur Aktivierung und Deaktivierung des Programms.

Standardeinstellungen für das Programm wiederherstellen (auf S. 93)

Dieser Abschnitt beschreibt, wie die Standardeinstellungen für das Programm wiederhergestellt werden können.

Bericht über das Programm anzeigen (auf S. 95)

Dieser Abschnitt beschreibt, wie Berichte über das Programm angezeigt werden können.

Programmeinstellungen auf einem anderen Computer übernehmen (auf S. 96)

Dieser Abschnitt enthält Informationen über den Export von Programmeinstellungen und deren Anwendung auf einem anderen Computer.

Teilnahme an Kaspersky Security Network (auf S. 97)

Dieser Abschnitt enthält Informationen über das Kaspersky Security Network und über die Möglichkeiten zur Teilnahme am KSN-Programm.

Steuerung des Programms über die Befehlszeile (auf S. 99)

Dieser Abschnitt informiert darüber, wie das Programm mithilfe der Befehlszeile gesteuert werden kann.

Kontaktaufnahme mit dem Technischen Support (auf S. 100)

Dieser Abschnitt beschreibt die Kontaktaufnahme mit dem Technischen Support.

Einschränkungen und Warnungen (auf S. 107)

Dieser Abschnitt informiert über Einschränkungen, die für die Programmfunktionen als nicht kritisch gelten.

Glossar (auf S. 110)

Dieser Abschnitt enthält eine Liste und Definitionen von Begriffen, die in diesem Dokument vorkommen.

Kaspersky Lab ZAO" (auf S. 116)

Dieser Abschnitt enthält Informationen über ZAO Kaspersky Lab.

Informationen über den Code von Drittherstellern (auf S. 117)

Dieser Abschnitt enthält Informationen über den Code von Drittherstellern, der im Programm verwendet wird.

Markeninformationen (auf S. 118)

In diesem Abschnitt werden die Marken von Drittanbietern (Rechteinhabern) genannt.

Sachregister

Dieser Abschnitt ermöglicht das schnelle Auffinden bestimmter Angaben in diesem Dokument.

FORMATIERUNG MIT BESONDERER BEDEUTUNG

Das Dokument enthält Textelemente (Warnungen, Tipps, Beispiele), die besondere Beachtung verdienen.

Zur Hervorhebung solcher Elemente werden spezielle Formatierungen verwendet. Ihre Bedeutung wird mit Beispielen in folgender Tabelle erläutert.

Tabelle 1. Formatierung mit besonderer Bedeutung

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Beachten Sie, dass ...	Warnungen sind rot hervorgehoben und eingerahmt. Warnungen informieren darüber, dass unerwünschte Aktionen möglich sind, die zu Datenverlust oder Störungen der Hardware oder des Betriebssystems führen können.
Es wird empfohlen ...	Hinweise sind eingerahmt. Hinweise können nützliche Tipps, Empfehlungen und spezielle Einstellungswerte enthalten oder sich auf wichtige Sonderfälle bei der Arbeit mit dem Programm beziehen.
Beispiel: ...	Beispiele befinden sich in gelb unterlegten Blöcken und sind mit "Beispiel" überschrieben.

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Das *Update* ist ... Das Ereignis *Die Datenbanken sind veraltet* tritt ein.	Folgende Textelemente sind kursiv geschrieben. • neue Begriffe • Namen von Statusvarianten und Programmereignissen
Drücken Sie die Taste **ENTER**. Drücken Sie die Tastenkombination **ALT+F4**.	Bezeichnungen von Tasten sind fett und in Großbuchstaben geschrieben. Tastenbezeichnungen, die durch ein Pluszeichen verbunden sind, bedeuten eine Tastenkombination. Die genannten Tasten müssen gleichzeitig gedrückt werden.
Klicken Sie auf **AKTIVIEREN**.	Die Namen von Elementen der Programmoberfläche sind fett geschrieben (z. B. Eingabefelder, Menüpunkte, Schaltflächen).
➡ *Gehen Sie folgendermaßen vor, um den Aufgabenzeitplan anzupassen:*	Der erste Satz einer Anleitung ist kursiv geschrieben und wird durch einen Pfeil markiert.
Geben Sie in der Befehlszeile den Text `help` ein. Es erscheint folgende Meldung: `Geben Sie das Datum im Format TT:MM:JJ an.`	Folgende Textarten werden durch eine spezielle Schriftart hervorgehoben: • Text einer Befehlszeile • Text von Nachrichten, die das Programm auf dem Bildschirm anzeigt. • Daten, die vom Benutzer eingegeben werden müssen.
<Benutzername>	Variable stehen in eckigen Klammern. Eine Variable muss durch einen entsprechenden Wert ersetzt werden. Dabei fallen die eckigen Klammern weg.

INFORMATIONSQUELLEN ZUM PROGRAMM

Dieser Abschnitt beschreibt Informationsquellen zum Programm und verweist auf Webseiten, die zur Diskussion über das Programm dienen.

Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage eine passende Quelle wählen.

IN DIESEM ABSCHNITT

INFORMATIONSQUELLEN ZUR SELBSTSTÄNDIGEN RECHERCHE

Sie können folgende Quellen verwenden, um nach Informationen zum Programm zu suchen:

- Seite auf der Webseite von Kaspersky Lab
- Seite auf der Webseite des Technischen Supports (Wissensdatenbank)
- Elektronisches Hilfesystem
- Dokumentation

Wenn Sie keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky Lab (s. Abschnitt "Technischer Support am Telefon" auf S. 100).

Um die Informationsquellen auf der Kaspersky-Lab-Webseite zu nutzen, ist eine Internetverbindung erforderlich.

Seite auf der Webseite von Kaspersky Lab

Die Kaspersky-Lab-Webseite bietet für jedes Programm eine spezielle Seite.

Auf der Seite (http://www.kaspersky.com/de/total-security-multi-device) finden Sie Informationen über das Programm sowie über seine Funktionen und Besonderheiten.

Auf dieser Seite befindet sich ein Link zum Online-Shop. Dort können Sie ein Programm kaufen oder die Nutzungsrechte für das Programm verlängern.

Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

Die Wissensdatenbank auf der Webseite des Technischen Supports (http://support.kaspersky.com/de/desktop) enthält Tipps zur Arbeit mit Kaspersky-Lab-Programmen. Die Wissensdatenbank bietet Hilfeartikel, die nach Themen angeordnet sind.

Auf der Seite des Programms finden Sie in der Wissensdatenbank (http://support.kaspersky.com/de/kts) nützliche Informationen, Tipps und Antworten auf häufige Fragen. Dabei werden Fragen wie Kauf, Installation und Verwendung des Programms behandelt.

Neben Fragen zu Kaspersky Total Security können die Artikel auch andere Kaspersky-Lab-Programme betreffen und Neuigkeiten über den Technischen Support enthalten.

Elektronisches Hilfesystem

Das elektronische Hilfesystem des Programms umfasst verschiedene Hilfedateien.

Die Kontexthilfe bietet Informationen über die einzelnen Programmfenster: Liste und Beschreibung der Einstellungen und Liste der entsprechenden Aufgaben.

Die vollständige Hilfe bietet ausführliche Informationen über die Verwaltung des Schutzes, die Programmeinstellungen und die zentralen Aufgaben des Benutzers.

Dokumentation

Das Benutzerhandbuch des Programms enthält Informationen zur Installation, Aktivierung und Konfiguration des Programms sowie zur Arbeit mit dem Programm. Das Handbuch bietet eine Beschreibung der Programmoberfläche und Lösungswege für typische Aufgaben, die sich dem Anwender bei der Arbeit mit dem Programm stellen.

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM FORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum diskutieren (http://forum.kaspersky.com/index.php?showforum=26).

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben und neue Themen zur Diskussion stellen.

KASPERSKY TOTAL SECURITY

Dieser Abschnitt beschreibt die Programm-Features und bietet kurze Informationen zu den Programmfunktionen und -komponenten. Hier werden der Lieferumfang und die Services beschrieben, die den registrierten Programmnutzern zur Verfügung stehen. Dieser Abschnitt informiert über die Hard- und Softwarevoraussetzungen, die ein Computer erfüllen muss, damit das Programm installiert werden kann.

IN DIESEM ABSCHNITT

NEUERUNGEN

Kaspersky Total Security verfügt über folgende Neuerungen:

- Die neuesten Versionen der gängigen Webbrowser werden unterstützt: Die Schutzkomponenten (z. B. Virtuelle Tastatur) unterstützen jetzt Mozilla™ Firefox™ 32.x, 33.x, 34.x, Google Chrome™ 37.x, 38.x.
- Der Browser Google Chrome für 64-Bit-Betriebssysteme wird unterstützt.
- Die Leistungsfähigkeit des Programms wurde erhöht und der Verbrauch von Computerressourcen wurde optimiert.
- Das Programm startet wesentlich schneller.
- Der Vorgang für das Upgrade der Programmversion wurde verbessert.
- Die Funktion der Komponente Aktivitätsmonitor wurde verbessert: Sie schützt jetzt auch vor Verschlüsselungsprogrammen. Wenn ein Chiffrierprogramm versucht, eine Datei zu verschlüsseln, erstellt Kaspersky Total Security automatisch eine Backup-Kopie der Datei, bevor das schädliche Chiffrierprogramm die Datei verschlüsselt. Die Backup-Kopien werden im Systemordner für temporäre Dateien abgelegt. Wenn das Chiffrierprogramm eine Datei verschlüsselt hat, stellt Kaspersky Total Security die Datei automatisch aus der Backup-Kopie wiederher. Die Funktionalität besitzt Einschränkungen (s. Abschnitt "Einschränkungen und Warnungen" auf S. 107).
- Die Komponente Sicherer Zahlungsverkehr wurde optimiert: Im Ereignisprotokoll werden jetzt Ereignisse protokolliert, die mit einer Schwächung des Schutzes bei der Arbeit des Sicheren Browsers zusammenhängen. Eine Untersuchung der Zertifikate von Webressourcen im Dienst Certificate Reputation 2.0 wurde hinzugefügt.

LIEFERUMFANG

Sie können das Programm folgendermaßen kaufen:

- In einer Box. Verkauf über unsere Vertriebspartner.
- Über den Online-Shop. Verkauf über den Online-Shop von Kaspersky Lab (z. B. http://www.kaspersky.com/de) oder über unsere Vertriebspartner.

Wenn Sie das Programm in einer CD-Box erworben haben, umfasst der Lieferumfang folgende Elemente:

- Versiegelter Umschlag mit Installations-CD, auf der die Programmdateien und die Dateien der Programmdokumentation gespeichert sind.
- Kurzes Benutzerhandbuch, das einen Aktivierungscode für das Programm enthält;
- Lizenzvertrag, der die Nutzungsbedingungen für das Programm festlegt.

Der Lieferumfang kann sich je nach Region, in der das Programm vertrieben wird, unterscheiden.

Wenn Sie Kaspersky Total Security in einem Online-Shop kaufen, kopieren Sie das Programm von der Seite des Online-Shops. Nach Eingang des Rechnungsbetrags erhalten Sie per E-Mail die zur Programmaktivierung erforderlichen Informationen einschließlich eines Aktivierungscodes.

HAUPTFUNKTIONEN DES PROGRAMMS

Kaspersky Total Security bietet Ihrem Computer einen komplexen Schutz vor bekannten und neuen Bedrohungen, Netzwerkangriffen und Betrugsversuchen und Spam. In Kaspersky Total Security sind unterschiedliche Funktionen und Schutzkomponenten für die einzelnen Aufgaben des umfassenden Schutzes verantwortlich.

Computersicherheit

Die *Schutzkomponenten* schützen Ihrem Computer vor bekannten und neuen Bedrohungen, Netzwerkangriffen, Betrugsversuchen und Spam. Jeder Bedrohungstyp wird von einer speziellen Schutzkomponente verarbeitet (s. Beschreibung der Komponenten weiter unten in diesem Abschnitt). Die Komponenten können unabhängig voneinander aktiviert und deaktiviert werden und lassen sich anpassen.

Zusätzlich zum Echtzeitschutz, den die Schutzkomponenten realisieren, wird empfohlen, Ihren Computer regelmäßig auf Viren und andere Schadprogramme zu *untersuchen*. Das ist erforderlich, um die Möglichkeit der Ausbreitung schädlicher Programme auszuschließen, die nicht von den Schutzkomponenten erkannt wurden, weil beispielsweise eine zu niedrige Schutzstufe eingestellt war.

Um Kaspersky Total Security auf dem neuesten Stand zu halten, ist ein *Update* der Datenbanken und Programm-Module erforderlich, die vom Programm verwendet werden.

Für spezifische Aufgaben, die nur gelegentlich anfallen, dienen *zusätzliche Tools und Assistenten*. Dazu zählt beispielsweise das Löschen von Aktivitätsspuren des Benutzers im Betriebssystem.

Der Echtzeitschutz Ihres Computers wird durch folgende Schutzkomponenten gewährleistet:

Im Folgenden werden die Schutzkomponenten von Kaspersky Total Security in dem Modus beschrieben, der von Kaspersky Lab empfohlen wird (d. h. mit den standardmäßigen Programmeinstellungen).

Datei-Anti-Virus

Datei-Anti-Virus schützt das Dateisystem des Computers vor einer Infektion. Die Komponente wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die auf Ihrem Computer und auf allen angeschlossenen Laufwerken geöffnet, gespeichert und gestartet werden. Kaspersky Total Security fängt jeden Zugriff auf eine Datei ab und untersucht die Datei auf bekannte Viren und andere Schadsoftware. Eine Datei wird nur dann zur Arbeit freigegeben, wenn die Datei virenfrei ist oder erfolgreich vom Programm desinfiziert wurde. Wenn die Desinfektion einer Datei nicht möglich ist, wird sie gelöscht. Dabei wird eine Kopie der Datei in die Quarantäne verschoben. Wenn anstelle einer gelöschten Datei eine infizierte Datei mit gleichem Namen gespeichert wird, wird nur eine Kopie der letzten Datei in der Quarantäne gespeichert. Es wird keine Kopie der vorherigen Datei mit diesem Namen gespeichert.

Mail-Anti-Virus

Mail-Anti-Virus untersucht ein- und ausgehende E-Mails auf Ihrem Computer. Eine E-Mail wird nur dann dem Empfänger zugestellt, wenn sie keine gefährlichen Objekte enthält.

Web-Anti-Virus

Web-Anti-Virus fängt die Ausführung von Skripts, die sich auf Webseiten befinden, ab und blockiert sie, falls Sie gefährlich sind. Web-Anti-Virus kontrolliert auch den Web-Datenverkehr und blockiert den gesamten Zugriff auf bekannte gefährliche Webseiten.

IM-Anti-Virus

IM-Anti-Virus sorgt für die Sicherheit bei Instant-Messengern. Die Komponente schützt die Informationen, die über Instant-Messenger-Protokolle auf Ihren Computer gelangen. IM-Anti-Virus gewährleistet Sicherheit bei der Arbeit mit vielen Programmen, die dem Sofortaustausch von Nachrichten dienen.

Programmkontrolle

Die Programmkontrolle registriert die Aktionen, die von Programmen im Betriebssystem ausgeführt werden können, und reguliert die Aktivität von Programmen. Dabei ist maßgebend, welcher Gruppe diese Programme von der Komponente zugeordnet wurden. Für jede Gruppe von Programmen ist eine Auswahl von Regeln vorgegeben. Diese Regeln steuern den Zugriff von Programmen auf unterschiedliche Ressourcen des Betriebssystems.

Firewall

Die Firewall bietet Ihnen Sicherheit in lokalen Netzwerken und im Internet. Diese Komponente filtert die gesamte Netzwerkaktivität. Dazu dienen zwei Arten von Regeln: *Regeln für Programme* und *Paketregeln*.

Netzwerkmonitor

Der Netzwerkmonitor dient dazu, in Echtzeit Informationen über die Netzwerkaktivität anzuzeigen.

Aktivitätsmonitor

Die Komponente Aktivitätsmonitor kann Aktionen von Schadsoftware im Betriebssystem rückgängig machen.

Schutz vor Netzwerkangriffen

Der Schutz wird vor Netzwerkangriffen beim Hochfahren des Betriebssystems gestartet und überwacht den eingehenden Datenverkehr auf für Netzwerkangriffe charakteristische Aktivität. Wenn ein Angriffsversuch auf den Computer erkannt wird, blockiert Kaspersky Total Security jede Art von Netzwerkaktivität des angreifenden Computers im Hinblick auf Ihren Computer.

Anti-Spam

Anti-Spam wird in Ihr Mailprogramm integriert und untersucht alle eingehenden E-Mail auf Spam. Alle E-Mails, die Spam enthalten, werden durch eine spezielle Kopfzeile markiert. Sie können festlegen, wie Anti-Spam mit Nachrichten verfahren soll, die Spam enthalten (beispielsweise: automatisch löschen oder in einen speziellen Ordner verschieben).

Anti-Phishing

Anti-Phishing erlaubt die Untersuchung von Webadressen auf ihre Zugehörigkeit zur Liste für Phishing-Webadressen. Diese Komponente wird in Web-Anti-Virus, Anti-Spam und IM-Anti-Virus integriert.

Anti-Banner

Anti-Banner blockiert Werbebanner, die sich auf Webseiten und Programmoberflächen befinden.

Sicherer Zahlungsverkehr

Der Sichere Zahlungsverkehr schützt vertrauliche Daten bei der Verwendung von Online-Banking und Zahlungssystemen, und verhindert den Diebstahl von Zahlungsmitteln bei Online-Zahlungsvorgängen.

Sichere Dateneingabe

Der Schutz für die Dateneingabe über eine Hardwaretastatur schützt persönliche Informationen, die auf Webseiten eingegeben werden, vor Keyloggern. Die Virtuelle Tastatur verhindert das Abfangen von Daten, die über eine Hardwaretastatur eingegeben werden, und schützt davor, dass persönliche Daten durch das Anlegen von Bildschirmkopien (Screenshots) abgefangen werden.

Modus für vertrauenswürdige Programme

Der Modus für vertrauenswürdige Programme schützt den Computer vor möglicherweise gefährlichen Programmen. Im Modus für vertrauenswürdige Programme wird der Start nur für jene Programme erlaubt, die von Kaspersky Total Security als vertrauenswürdig eingestuft werden (beispielsweise aufgrund von KSN-Informationen über das Programm oder aufgrund einer vertrauenswürdigen digitalen Signatur).

Kindersicherung

Die Funktionen der Kindersicherung schützen Kinder und Jugendliche bei der Arbeit am Computer und im Internet.

Die Kindersicherung erlaubt es, den Zugriff auf Internetressourcen und Programme für unterschiedliche Computerbenutzer altersabhängig flexibel einzuschränken. Außerdem erlaubt die Kindersicherung, Berichte mit einer Statistik über die Aktionen der kontrollierten Benutzer anzuzeigen.

Sichern und Wiederherstellen

Die Funktionalität zur Datensicherung dient dazu, vor einem Datenverlust aufgrund von Hardware-Funktionsstörungen zu schützen. Kaspersky Total Security kann eine zeitplangesteuerte Datensicherung auf Wechselmedien, Netzwerkspeichern oder Online-Speichern ausführen. Sie können bestimmte Dateikategorien sichern und die Anzahl der Versionen festlegen, die von einer einzelnen Datei aufbewahrt werden sollen.

Virtuelle Datentresore

Virtuelle Datentresore dienen zum Schutz Ihrer sensiblen Daten vor unbefugtem Zugriff. Um einen Datentresor zu öffnen und die darin gespeicherten Daten anzusehen, muss das Kennwort eingegeben werden.

Fernverwaltung des Computerschutzes

Wenn Kaspersky Total Security auf dem Computer installiert ist und Sie ein Benutzerkonto für das Portal My Kaspersky besitzen, können Sie den Schutz Ihres Computers fernverwalten.

SERVICE FÜR BENUTZER

Wenn Sie eine Lizenz für die Nutzung des Programms kaufen, können Sie während der Gültigkeitsdauer der Lizenz folgende Leistungen in Anspruch nehmen:

- Update der Datenbanken und Nutzung neuer Programmversionen
- Beratung bei Fragen zur Installation, Konfiguration und Nutzung des Programms per Telefon und E-Mail;
- Benachrichtigung über das Erscheinen neuer Kaspersky-Lab-Programme sowie über das Auftauchen neuer Viren und drohende Virenepidemien. Wenn Sie diesen Service nutzen möchten, abonnieren Sie auf der Webseite des Technischen Supports den Newsletter von Kaspersky Lab.

Die Beratung erstreckt sich nicht auf Fragen über die Funktionsweise von Betriebssystemen, der Software von Drittherstellern und sonstiger Technologien.

HARD- UND SOFTWAREVORAUSSETZUNGEN

Generelle Anforderungen:

- 480 MB freier Platz auf der Festplatte
- CD / DVD-ROM-Laufwerk (für die Installation von einer Installations-CD)
- Internetverbindung (für die Aktivierung des Programms und für das Update der Datenbanken und Programm-Module)
- Internet Explorer 8.0 oder höher
- Microsoft® Windows Installer 3.0 oder höher
- Microsoft .NET Framework 4 oder höher
- Der Schutz vor unberechtigtem Zugriff auf die Webcam ist nur für kompatible Webcam-Modelle http://support.kaspersky.com/de/10978 verfügbar.

Anforderungen für die Betriebssysteme Microsoft Windows XP Home Edition (Service Pack 3 oder höher), Microsoft Windows XP Professional (Service Pack 3 oder höher), Microsoft Windows XP Professional x64 Edition (Service Pack 2 oder höher):

- Prozessor 1 GHz oder höher
- 512 MB freier Arbeitsspeicher.

Anforderungen für die Betriebssysteme Microsoft Windows Vista® Home Basic (Service Pack 1 oder höher), Microsoft Windows Vista Home Premium (Service Pack 1 oder höher), Microsoft Windows Vista Business (Service Pack 1 oder höher), Microsoft Windows Vista Enterprise (Service Pack 1 oder höher), Microsoft Windows Vista Ultimate (Service Pack 1 oder höher), Microsoft Windows 7 Starter (Service Pack 1 oder höher), Microsoft Windows 7 Home Basic (Service Pack 1 oder höher), Microsoft Windows 7 Home Premium (Service Pack 1 oder höher), Microsoft Windows 7 Professional (Service Pack 1 oder höher), Microsoft Windows 7 Ultimate (Service Pack 1 oder höher), Microsoft Windows 8, Microsoft Windows 8 Pro, Microsoft Windows 8 Enterprise, Microsoft Windows 8.1 (Windows 8.1 Update), Microsoft Windows 8.1 Pro (Windows 8.1 Update), Microsoft Windows 8.1 Enterprise (Windows 8.1 Update), Microsoft Windows 10:

- Prozessor 1 GHz oder höher
- 1 GB freier Arbeitsspeicher (für 32-Bit-Betriebssysteme), 2 GB freier Arbeitsspeicher (für 64-Bit-Betriebssysteme)

Anforderungen für Tablet-PCs:

- Microsoft Tablet PC
- Prozessor Intel Celeron® 1.66 GHz oder höher
- 1000 MB freier Arbeitsspeicher

Anforderungen für Netbooks:

- Prozessor Intel Atom™ 1600 MHz oder höher
- 1024 MB freier Arbeitsspeicher
- Display 10.1 Zoll mit einer Auflösung von 1024x600
- Grafik-Chipsatz Intel GMA 950

PROGRAMM INSTALLIEREN UND DEINSTALLIEREN

Dieser Abschnitt bietet schrittweise Anleitungen zur Installation und Deinstallation des Programms.

IN DIESEM ABSCHNITT

STANDARD-INSTALLATIONSMETHODE

Kaspersky Total Security wird auf dem Computer interaktiv mit einem Installations-Assistenten installiert.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Der Assistent kann auf einer beliebigen Etappe abgebrochen werden. Dazu muss das Assistentenfenster geschlossen werden.

Wenn das Programm für den Schutz von mehr als einem Computer eingesetzt wird (die maximal zulässige Anzahl der Computer wird durch die Bedingungen des Lizenzvertrags bestimmt), verläuft die Installation auf allen Computern identisch.

- *Um Kaspersky Total Security auf Ihrem Computer zu installieren,*

  starten Sie auf der Installations-CD die Datei des Installationspakets (Datei mit der Endung exe).

Sie können auch ein Installationspaket, das Sie über das Internet erhalten haben, für die Installation von Kaspersky Total Security verwenden. Dabei zeigt der Installationsassistent für bestimmte Sprachversionen einige zusätzliche Installationsschritte an.

Zusammen mit dem Programm werden auch Plug-ins für Webbrowser installiert. Diese Plug-ins dienen der sicheren Nutzung des Internets.

IN DIESEM ABSCHNITT

SCHRITT 1. NACH NEUER PROGRAMMVERSION SUCHEN

Vor Beginn der Installation prüft der Assistent, ob eine neuere Version von Kaspersky Total Security auf den Update-Servern von Kaspersky Lab vorhanden ist.

Wenn der Installationsassistent auf den Kaspersky-Lab-Update-Servern keine neuere Programmversion findet, wird die Installation der vorliegenden Version gestartet.

Wenn der Assistent eine neuere Version von Kaspersky Total Security auf den Kaspersky-Lab-Update-Servern findet, schlägt er Ihnen vor, diese herunterzuladen und zu installieren. Es wird empfohlen, die neue Programmversion zu installieren, da neue Versionen den Schutz Ihres Computers optimieren. Wenn Sie die Installation der neuen Version ablehnen, wird die Installation der vorliegenden Programmversion gestartet. Wenn Sie der Installation der neuen Version zustimmen, kopiert der Installationsassistent die Dateien des Installationspakets auf Ihren Computer und startet die Installation der neuen Version. Eine Beschreibung zum weiteren Vorgehen bei der Installation einer neuen Programmversion finden Sie in der entsprechenden Dokumentation.

SCHRITT 2. BEGINN DER PROGRAMMINSTALLATION

Bei diesem Schritt schlägt Ihnen das Setup vor, das Programm zu installieren.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Installieren**.

Abhängig vom Installationstyp und der Sprachversion kann Ihnen der Installationsassistent bei diesem Schritt vorschlagen, den Lizenzvertrag zu lesen, der zwischen Ihnen und Kaspersky Lab abgeschlossen wird, und am Programm Kaspersky Security Network teilzunehmen.

SCHRITT 3. LIZENZVEREINBARUNG ANZEIGEN

Dieser Schritt des Installationsassistenten wird für bestimmte Sprachversionen angezeigt, wenn Kaspersky Total Security mit einem Installationspaket installiert wird, das aus dem Internet heruntergeladen wurde.

Bei diesem Schritt schlägt Ihnen der Installationsassistent vor, den Lizenzvertrag zu lesen, der zwischen Ihnen und Kaspersky Lab abgeschlossen wird.

Lesen Sie sich die Lizenzvereinbarung sorgfältig durch und klicken Sie auf die Schaltfläche **Akzeptieren**, wenn Sie mit allen Punkten einverstanden sind. Die Installation des Programms auf Ihrem Computer wird fortgesetzt.

Wenn die Bedingungen des Lizenzvertrags nicht akzeptiert werden, wird die Programminstallation abgebrochen.

SCHRITT 4. VEREINBARUNG ZUM KASPERSKY SECURITY NETWORK

Bei diesem Schritt schlägt Ihnen der Installationsassistent vor, am Programm Kaspersky Security Network teilzunehmen. Eine Beteiligung an diesem Programm sieht vor, dass Informationen über auf Ihrem Computer erkannte neue Bedrohungen, über gestartete Programme und über geladene signierte Programme sowie Informationen zum Betriebssystem an Kaspersky Lab geschickt werden. Dabei werden keine persönlichen Daten gesammelt, verarbeitet oder gespeichert.

Lesen Sie sich die Vereinbarung zum Kaspersky Security Network gründlich durch. Wenn Sie mit allen Punkten der Erklärung einverstanden sind, klicken Sie im Assistentenfenster auf **Akzeptieren**.

Wenn Sie nicht am Programm Kaspersky Security Network teilnehmen möchten, klicken Sie auf **Ablehnen**.

Nachdem Sie die Teilnahme an Kaspersky Security Network akzeptiert oder abgelehnt haben, wird die Programminstallation fortgesetzt.

SCHRITT 5. INSTALLATION

Für bestimmte Versionen von Kaspersky Total Security, die mit einem Abonnement vertrieben werden, muss vor der Installation ein Kennwort eingegeben werden. Das Kennwort erhalten Sie vom Dienstleister.

Nach der Kennworteingabe beginnt die Installation.

Die Installation des Programms nimmt einige Zeit in Anspruch. Warten Sie die Fertigstellung ab.

Der Assistent geht nach Abschluss der Installation automatisch zum nächsten Schritt.

Kaspersky Total Security führt bei der Installation eine Reihe von Untersuchungen aus. Im Rahmen dieser Untersuchungen können folgende Probleme erkannt werden:

- *Abweichung des Betriebssystems von den Softwareanforderungen*. Der Assistent überprüft bei der Installation, ob folgende Bedingungen erfüllt werden:

  - Übereinstimmung des Betriebssystems und der Service Packs mit den Softwareanforderungen
  - Vorhandensein von erforderlichen Programmen
  - Vorhandensein des für die Installation erforderlichen freien Platzes auf dem Laufwerk

  Wenn eine der aufgezählten Bedingung nicht erfüllt wird, erscheint eine entsprechende Meldung auf dem Bildschirm.

- *Vorhandensein von inkompatiblen Programmen auf dem Computer*. Werden inkompatible Programme gefunden, so wird eine entsprechende Liste auf dem Bildschirm angezeigt und Sie werden aufgefordert, die Programme zu entfernen. Programme, die nicht automatisch von Kaspersky Total Security entfernt werden können, müssen manuell deinstalliert werden. Bei der Deinstallation inkompatibler Programme wird das Betriebssystem neu gestartet. Anschließend wird die Installation von Kaspersky Total Security automatisch fortgesetzt.

- *Vorhandensein von Schadprogrammen auf dem Computer*. Wenn auf dem Computer schädliche Programme gefunden werden, die eine Installation von Antiviren-Programmen verhindern, schlägt der Installationsassistent vor, das *Kaspersky Virus Removal Tool* herunterzuladen, um die Infektion zu beseitigen.

  Wenn Sie der Installation des Tools zustimmen, lädt der Installationsassistent es von den Kaspersky-Lab-Servern herunter und startet anschließend automatisch die Installation des Tools. Wenn der Assistent das Tool nicht herunterladen kann, schlägt er Ihnen vor, es über einen Link manuell herunterzuladen. Dazu wird ein Link angegeben.

SCHRITT 6. INSTALLATION ABSCHLIEßEN

Bei diesem Schritt informiert der Assistent über den Abschluss der Programminstallation. Um Kaspersky Total Security sofort zu starten, vergewissern Sie sich, dass das Kontrollkästchen **Kaspersky Total Security starten** aktiviert ist, und klicken Sie auf **Beenden**.

Wenn Sie das Kontrollkästchen **Kaspersky Total Security starten** deaktiviert haben, bevor der Assistent beendet wurde, muss das Programm künftig manuell gestartet werden.

In einigen Fällen kann ein Neustart des Betriebssystems erforderlich sein, um die Installation abzuschließen.

SCHRITT 7. PROGRAMM AKTIVIEREN

Bei diesem Schritt schlägt Ihnen das Setup vor, das Programm zu aktivieren.

Durch die *Aktivierung* wird eine Vollversion des Programms für den entsprechenden Zeitraum aktiviert.

Wenn Sie eine Lizenz für die Nutzung von Kaspersky Total Security gekauft und das Programm über einen Online-Shop heruntergeladen haben, kann die Programmaktivierung automatisch im Rahmen der Installation ausgeführt werden.

Für die Aktivierung von Kaspersky Total Security bestehen folgende Möglichkeiten:

- **Programm aktivieren**. Wählen Sie diese Option und geben Sie den Aktivierungscode ein, wenn Sie eine Lizenz für die Programmnutzung erworben haben.

  Wenn Sie einen Aktivierungscode für Kaspersky Internet Security oder Kaspersky Anti-Virus angeben, startet nach der Aktivierung die Migration zu Kaspersky Internet Security oder Kaspersky Anti-Virus.

- **Testversion des Programms aktivieren**. Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion des Programms installieren möchten, bevor Sie über den Kauf einer Lizenz entscheiden. Sie können das Programm für eine kurze Testdauer mit vollem Funktionsumfang nutzen. Nachdem die Lizenz abgelaufen ist, kann keine weitere Testversion des Programms aktiviert werden.

Um das Programm zu aktivieren, ist eine Internetverbindung erforderlich.

Bei der Programmaktivierung kann eine Registrierung im Portal My Kaspersky erforderlich sein.

SCHRITT 8. ANMELDUNG DES BENUTZERS

Dieser Schritt ist nicht in allen Versionen von Kaspersky Total Security verfügbar.

Registrierten Benutzern stehen folgende Leistungen zur Verfügung: Senden von Anfragen an den Technischen Support und an das Virenlabor über das Portal My Kaspersky; bequeme Verwaltung von Aktivierungscodes; aktuelle Informationen über neue Programme und Sonderangebote von Kaspersky Lab.

Wenn Sie mit der Anmeldung einverstanden sind, füllen Sie die entsprechenden Felder aus und klicken Sie dann auf **Weiter**, um Ihre Anmeldung an Kaspersky Lab abzuschicken.

In bestimmten Fällen ist eine Anmeldung des Benutzers erforderlich, um das Programm nutzen zu können.

SCHRITT 9. AKTIVIERUNG ABSCHLIEßEN

Der Assistent informiert Sie darüber, dass die Aktivierung von Kaspersky Total Security erfolgreich abgeschlossen wurde. Außerdem werden in diesem Fenster Informationen über die aktuelle Lizenz angezeigt: Gültigkeitsdauer der Lizenz sowie Anzahl der Computer, für die die Lizenz gültig ist.

Bei einem Abonnement werden anstelle des Ablaufdatums der Lizenz Informationen zum Abo-Status angezeigt.

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

UPGRADE EINER FRÜHEREN PROGRAMMVERSION

Kaspersky Total Security über Kaspersky PURE installieren

Wenn auf Ihrem Computer bereits Kaspersky PURE installiert ist, können Sie das Programm auf Kaspersky Total Security upgraden. Wenn eine aktuelle Lizenz für die Nutzung von Kaspersky PURE vorliegt, müssen Sie das Programm nicht aktivieren: Der Installationsassistent erhält automatisch die Lizenzinformationen und übernimmt diese bei der Installation von Kaspersky Total Security.

Installation von Kaspersky Total Security über Kaspersky Internet Security

Wenn Sie Kaspersky Total Security auf einem Computer installieren, auf dem Kaspersky Internet Security bereits mit einer aktuellen Lizenz installiert ist, bietet Ihnen der Aktivierungs-Assistent folgende Aktionen zur Auswahl an:

- Kaspersky Internet Security mit der aktuellen Lizenz weiterverwenden. In diesem Fall startet der Migrations-Assistent und installiert Kaspersky Internet Security auf Ihrem Computer. Sie können Kaspersky Internet Security so lang nutzen, wie die Lizenz für Kaspersky Internet Security gültig ist.

- Installation der neuen Version von Kaspersky Total Security fortsetzen. In diesem Fall wird das Programm nach dem Referenzszenario installiert und aktiviert.

Kaspersky Total Security wird auf dem Computer interaktiv mit einem Installations-Assistenten installiert.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Der Assistent kann auf einer beliebigen Etappe abgebrochen werden. Dazu muss das Assistentenfenster geschlossen werden.

Wenn das Programm für den Schutz von mehr als einem Computer eingesetzt wird (die maximal zulässige Anzahl der Computer wird durch die Bedingungen des Lizenzvertrags bestimmt), verläuft die Installation auf allen Computern identisch.

Um Kaspersky Total Security auf Ihrem Computer zu installieren,

starten Sie auf der Installations-CD die Datei des Installationspakets (Datei mit der Endung exe).

Sie können auch ein Installationspaket, das Sie über das Internet erhalten haben, für die Installation von Kaspersky Total Security verwenden. Dabei zeigt der Installationsassistent für bestimmte Sprachversionen einige zusätzliche Installationsschritte an.

Zusammen mit dem Programm werden auch Plug-ins für Webbrowser installiert. Diese Plug-ins dienen der sicheren Nutzung des Internets.

Das Programm-Upgrade besitzt Einschränkungen (s. Abschnitt "Einschränkungen und Warnungen" auf S. 107).

IN DIESEM ABSCHNITT

SCHRITT 1. NACH NEUER PROGRAMMVERSION SUCHEN

Vor Beginn der Installation prüft der Assistent, ob eine neuere Version von Kaspersky Total Security auf den Update-Servern von Kaspersky Lab vorhanden ist.

Wenn der Installationsassistent auf den Kaspersky-Lab-Update-Servern keine neuere Programmversion findet, wird die Installation der vorliegenden Version gestartet.

Wenn der Assistent eine neuere Version von Kaspersky Total Security auf den Kaspersky-Lab-Update-Servern findet, schlägt er Ihnen vor, diese herunterzuladen und zu installieren. Es wird empfohlen, die neue Programmversion zu installieren, da neue Versionen den Schutz Ihres Computers optimieren. Wenn Sie die Installation der neuen Version ablehnen, wird die Installation der vorliegenden Programmversion gestartet. Wenn Sie der Installation der neuen Version zustimmen, kopiert der Installationsassistent die Dateien des Installationspakets auf Ihren Computer und startet die Installation der neuen Version. Eine Beschreibung zum weiteren Vorgehen bei der Installation einer neuen Programmversion finden Sie in der entsprechenden Dokumentation.

SCHRITT 2. BEGINN DER PROGRAMMINSTALLATION

Bei diesem Schritt schlägt Ihnen das Setup vor, das Programm zu installieren.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Installieren**.

Abhängig vom Installationstyp und der Sprachversion kann Ihnen der Installationsassistent bei diesem Schritt vorschlagen, den Lizenzvertrag zu lesen, der zwischen Ihnen und Kaspersky Lab abgeschlossen wird, und am Programm Kaspersky Security Network teilzunehmen.

SCHRITT 3. LIZENZVEREINBARUNG ANZEIGEN

Dieser Schritt des Installationsassistenten wird für bestimmte Sprachversionen angezeigt, wenn Kaspersky Total Security mit einem Installationspaket installiert wird, das aus dem Internet heruntergeladen wurde.

Bei diesem Schritt schlägt Ihnen der Installationsassistent vor, den Lizenzvertrag zu lesen, der zwischen Ihnen und Kaspersky Lab abgeschlossen wird.

Lesen Sie sich die Lizenzvereinbarung sorgfältig durch und klicken Sie auf die Schaltfläche **Akzeptieren**, wenn Sie mit allen Punkten einverstanden sind. Die Installation des Programms auf Ihrem Computer wird fortgesetzt.

Wenn die Bedingungen des Lizenzvertrags nicht akzeptiert werden, wird die Programminstallation abgebrochen.

SCHRITT 4. VEREINBARUNG ZUM KASPERSKY SECURITY NETWORK

Bei diesem Schritt schlägt Ihnen der Installationsassistent vor, am Programm Kaspersky Security Network teilzunehmen. Eine Beteiligung an diesem Programm sieht vor, dass Informationen über auf Ihrem Computer erkannte neue Bedrohungen, über gestartete Programme und über geladene signierte Programme sowie Informationen zum Betriebssystem an Kaspersky Lab geschickt werden. Dabei werden keine persönlichen Daten gesammelt, verarbeitet oder gespeichert.

Lesen Sie sich die Vereinbarung zum Kaspersky Security Network gründlich durch. Wenn Sie mit allen Punkten der Erklärung einverstanden sind, klicken Sie im Assistentenfenster auf **Akzeptieren**.

Wenn Sie nicht am Programm Kaspersky Security Network teilnehmen möchten, klicken Sie auf **Ablehnen**.

Nachdem Sie die Teilnahme an Kaspersky Security Network akzeptiert oder abgelehnt haben, wird die Programminstallation fortgesetzt.

SCHRITT 5. INSTALLATION

Für bestimmte Versionen von Kaspersky Total Security, die mit einem Abonnement vertrieben werden, muss vor der Installation ein Kennwort eingegeben werden. Das Kennwort erhalten Sie vom Dienstleister.

Nach der Kennworteingabe beginnt die Installation.

Die Installation des Programms nimmt einige Zeit in Anspruch. Warten Sie die Fertigstellung ab.

Der Assistent geht nach Abschluss der Installation automatisch zum nächsten Schritt.

Kaspersky Total Security führt bei der Installation eine Reihe von Untersuchungen aus. Im Rahmen dieser Untersuchungen können folgende Probleme erkannt werden:

- *Abweichung des Betriebssystems von den Softwareanforderungen*. Der Assistent überprüft bei der Installation, ob folgende Bedingungen erfüllt werden:
  - Übereinstimmung des Betriebssystems und der Service Packs mit den Softwareanforderungen
  - Vorhandensein von erforderlichen Programmen
  - Vorhandensein des für die Installation erforderlichen freien Platzes auf dem Laufwerk

  Wenn eine der aufgezählten Bedingung nicht erfüllt wird, erscheint eine entsprechende Meldung auf dem Bildschirm.
- *Vorhandensein von inkompatiblen Programmen auf dem Computer*. Werden inkompatible Programme gefunden, so wird eine entsprechende Liste auf dem Bildschirm angezeigt und Sie werden aufgefordert, die Programme zu entfernen. Programme, die nicht automatisch von Kaspersky Total Security entfernt werden können, müssen manuell deinstalliert werden. Bei der Deinstallation inkompatibler Programme wird das Betriebssystem neu gestartet. Anschließend wird die Installation von Kaspersky Total Security automatisch fortgesetzt.
- *Vorhandensein von Schadprogrammen auf dem Computer*. Wenn auf dem Computer schädliche Programme gefunden werden, die eine Installation von Antiviren-Programmen verhindern, schlägt der Installationsassistent vor, das *Kaspersky Virus Removal Tool* herunterzuladen, um die Infektion zu beseitigen.

  Wenn Sie der Installation des Tools zustimmen, lädt der Installationsassistent es von den Kaspersky-Lab-Servern herunter und startet anschließend automatisch die Installation des Tools. Wenn der Assistent das Tool nicht herunterladen kann, schlägt er Ihnen vor, es über einen Link manuell herunterzuladen. Dazu wird ein Link angegeben.

SCHRITT 6. INSTALLATION ABSCHLIEßEN

Dieses Fenster des Assistenten informiert über den Abschluss der Programminstallation.

Zum Abschluss der Installation muss das Betriebssystem neu gestartet werden.

Wenn das Kontrollkästchen **Kaspersky Total Security starten** aktiviert ist, wird das Programm nach einem Neustart des Computers automatisch gestartet.

Wenn Sie das Kontrollkästchen **Kaspersky Total Security starten** deaktiviert haben, bevor der Assistent abgeschlossen wurde, muss das Programm manuell gestartet werden.

PROGRAMM DEINSTALLIEREN

Wenn Kaspersky Total Security deinstalliert wird, sind der Computer und Ihre persönlichen Daten nicht mehr geschützt!

Kaspersky Total Security wird mit dem Installationsassistenten entfernt.

Um den Assistenten zu starten,

wählen Sie im Menü **Start** den Punkt **Alle Programme** → **Kaspersky Total Security** → **Kaspersky Total Security entfernen**.

IN DIESEM ABSCHNITT

SCHRITT 1. KENNWORT FÜR DIE PROGRAMMDEINSTALLATION EINGEBEN

Um Kaspersky Total Security zu entfernen, ist das Kennwort für den Zugriff auf die Programmeinstellungen erforderlich. Eine Deinstallation ist nur mit dem Kennwort möglich.

Dieser Schritt erfolgt nur, wenn ein Kennwort für die Programmdeinstallation festgelegt ist.

SCHRITT 2. DATEN ZUR ERNEUTEN VERWENDUNG SPEICHERN

Bei diesem Schritt können Sie festlegen, welche vom Programm verwendeten Daten Sie speichern möchten, um sie später bei einer Neuinstallation des Programms wiederzuverwenden (beispielsweise bei der Installation einer neueren Version).

Das Programm schlägt standardmäßig vor, die Informationen zur Lizenz zu speichern.

Um die Daten zur späteren Wiederverwendung zu speichern, aktivieren Sie die entsprechenden Kontrollkästchen:

- **Lizenzinformationen** – Daten, die es erlauben, das zu installierende Programm später nicht zu aktivieren, sondern es unter der vorherigen Lizenz zu verwenden, vorausgesetzt, die Lizenz ist zum Zeitpunkt der Installation noch gültig.

- **Quarantäne-Dateien** – Dateien, die vom Programm untersucht und in die Quarantäne verschoben wurden.

  Wenn Kaspersky Total Security vom Computer entfernt wird, besteht kein Zugriff mehr auf die Quarantäne-Dateien. Kaspersky Total Security muss installiert werden, um mit diesen Dateien zu arbeiten.

- **Programmeinstellungen** – Werte für Programmeinstellungen, die im Verlauf der Programmkonfiguration festgelegt wurden.

  Kaspersky Lab garantiert nicht, dass die Einstellungen der vorhergehenden Programmversion unterstützt werden. Es wird empfohlen, die Richtigkeit der Einstellungen zu überprüfen, nachdem eine neue Programmversion installiert wurde.

  Außerdem können Sie die Schutzeinstellungen über die Befehlszeile exportieren. Dazu dient folgender Befehl:

  ```
  avp.com EXPORT <Dateiname>
  ```

- **iChecker-Daten** – Dateien mit Informationen zu den Objekten, die bereits mithilfe der iChecker-Technologie auf Viren untersucht wurden.
- **Anti-Spam-Datenbanken** – Datenbanken, die Muster von Spam-Mails enthalten, die das Programm erhalten und gespeichert hat.
- **Virtuelle Datentresore** – Dateien, die Sie in Virtuelle Datentresore gespeichert haben.

SCHRITT 3. PROGRAMMDEINSTALLATION BESTÄTIGEN

Da durch eine Programmdeinstallation der Schutz Ihres Computers und Ihrer persönlichen Daten gefährdet werden kann, muss das Löschen des Programms bestätigt werden. Klicken Sie dazu auf die Schaltfläche **Löschen**.

SCHRITT 4. PROGRAMM DEINSTALLIEREN DEINSTALLATION ABSCHLIEßEN

Bei diesem Schritt löscht der Assistent das Programm von Ihrem Computer. Warten Sie, bis der Deinstallationsvorgang abgeschlossen wird.

Nach der Deinstallation von Kaspersky Total Security, können Sie auf der Kaspersky-Lab-Webseite angeben, warum Sie das Programm entfernt haben. Klicken Sie dazu auf **Formular ausfüllen**, um die Webseite von Kaspersky Lab zu öffnen.

Im Verlauf der Deinstallation ist ein Neustart des Systems erforderlich. Wenn Sie einen sofortigen Neustart ablehnen, wird der Abschluss der Deinstallation aufgeschoben, bis das Betriebssystem neu gestartet oder der Computer heruntergefahren und erneut hochgefahren wird.

LIZENZVERWALTUNG DES PROGRAMMS

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmaktivierung zusammenhängen. Hier werden Lizenzvertrag, Methoden zur Programmaktivierung und Verlängerung der Lizenzgültigkeit erläutert.

IN DIESEM ABSCHNITT

ÜBER DEN LIZENZVERTRAG

Der Lizenzvertrag ist ein rechtsgültiger Vertrag zwischen Ihnen und Kaspersky Lab ZAO. Er bestimmt die Nutzungsbedingungen für das Programm.

Lesen Sie den Lizenzvertrag sorgfältig, bevor Sie beginnen, mit dem Programm zu arbeiten.

Wenn Sie bei der Programminstallation dem Text des Lizenzvertrags zustimmen, gelten die Bedingungen des Lizenzvertrags als akzeptiert. Falls Sie dem Lizenzvertrag nicht zustimmen, müssen Sie die Programminstallation abbrechen oder das Programm nicht verwenden.

ÜBER DIE LIZENZ

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für ein Programm, das Ihnen auf Basis eines Lizenzvertrags überlassen wird. Der Lizenz ist ein individueller Aktivierungscode für Ihr Exemplar von Kaspersky Total Security zugeordnet.

Die Lizenz berechtigt zur Nutzung folgender Leistungen:

- Verwendung des Programms auf einem oder mehreren Geräten.

  Die Anzahl der Geräte, auf denen Sie das Programm nutzen dürfen, wird durch den Lizenzvertrag festgelegt.

- Kontaktaufnahme mit dem Technischen Support von Kaspersky Lab

- Nutzung von sonstigen Leistungen, die Ihnen von Kaspersky Lab oder den Vertriebspartnern für die Gültigkeitsdauer der Lizenz angeboten werden (s. Abschnitt "Service für Benutzer" auf S. 17).

Um das Programm zu nutzen, müssen Sie eine Lizenz für die Programmnutzung kaufen.

Eine Lizenz besitzt eine beschränkte Gültigkeitsdauer. Nach Ablauf der Lizenz funktioniert das Programm weiterhin, allerdings in einem Modus mit eingeschränktem Funktionsumfang (dann sind beispielsweise das Update und der Dienst Kaspersky Security Network nicht mehr verfügbar). Sie können weiterhin alle Programmkomponenten verwenden und eine Untersuchung auf Viren und andere bedrohliche Programme ausführen, allerdings nur mit den Datenbanken, die beim Ablauf der Lizenz installiert waren. Die Lizenz muss verlängert werden, um Kaspersky Total Security mit allen Funktionen weiter zu nutzen.

Es wird empfohlen, eine Lizenz rechtzeitig vor dem Ablaufdatum zu verlängern. Nur so lässt sich ein optimaler Schutz vor allen Computerbedrohungen gewährleisten

Bevor Sie eine Lizenz kaufen, können Sie Kaspersky Total Security kostenlos mit einer Testversion kennen lernen. Eine Testversion von Kaspersky Total Security funktioniert nur für einen kurzen Testzeitraum. Nach dem Ablauf des Testzeitraums stellt Kaspersky Total Security seine Funktionen ein. Um das Programm weiter zu nutzen, muss eine Lizenz gekauft werden.

ÜBER DEN AKTIVIERUNGSCODE

Einen *Aktivierungscode* erhalten Sie beim Kauf einer Lizenz für die Nutzung von Kaspersky Total Security. Dieser Code ist für die Programmaktivierung erforderlich.

Ein Aktivierungscode besteht aus einer unikalen Folge von zwanzig Ziffern und lateinischen Buchstaben im Format XXXXX-XXXXX-XXXXX-XXXXX.

Abhängig davon, auf welche Weise das Programm gekauft wird, bestehen folgende Varianten für die Lieferung des Aktivierungscodes:

- Wenn Sie Kaspersky Total Security in einer CD-Box gekauft haben, ist der Aktivierungscode in der Dokumentation oder auf der Verpackung angegeben, in der sich die Installations-CD befindet.

- Wenn Sie Kaspersky Total Security in einem Online-Shop gekauft haben, erhalten Sie den Aktivierungscode per E-Mail an die Adresse, die Sie bei der Bestellung angegeben haben.

Die Laufzeit einer Lizenz wird ab dem Datum der Programmaktivierung gerechnet. Wenn Sie eine Lizenz gekauft haben, mit der Kaspersky Total Security auf mehreren Geräten genutzt werden kann, so beginnt die Laufzeit der Lizenz, wenn der Aktivierungscode zum ersten Mal verwendet wird.

Wenn ein Aktivierungscode nach der Programmaktivierung verloren geht oder versehentlich gelöscht wurde, nehmen Sie Kontakt mit dem Technischen Support von Kaspersky Lab http://support.kaspersky.com/de auf, um den Code wiederherzustellen.

ÜBER DAS ABONNEMENT

Für die Nutzung des Programms mit einem Abonnement für Kaspersky Total Security gelten bestimmte Bedingungen (Ablaufdatum, Anzahl der geschützten Geräte). Ein Abonnement für Kaspersky Total Security kann bei einem Dienstleister erworben werden (z. B. bei einem Internet-Provider). Sie können ein Abonnement anhalten oder fortsetzen, automatisch verlängern lassen und kündigen. Ein Abonnement kann über Ihren Kaspersky Account auf der Webseite des Dienstleisters verwaltet werden.

Ein Dienstleister kann zwei Arten von Abonnements für die Nutzung von Kaspersky Total Security anbieten: Update-Abonnement und Update- und Schutz-Abonnement.

Ein Abonnement kann beschränkt (z. B. auf ein Jahr) oder unbeschränkt sein (ohne Ablaufdatum). Um Kaspersky Total Security weiter zu nutzen, nachdem ein beschränktes Abonnement abgelaufen ist, müssen Sie das Abo selbstständig verlängern. Ein unbeschränktes Abonnement wird automatisch verlängert, falls der vereinbarte Betrag rechtzeitig an den Dienstleister überwiesen wird.

Für ein beschränktes Abonnement wird Ihnen beim Ablauf eine Nachfrist zur Abo-Verlängerung eingeräumt, während der die Funktionsfähigkeit des Programms erhalten bleibt.

Wenn ein Abonnement innerhalb der Nachfrist nicht verlängert wird, aktualisiert Kaspersky Total Security die Programm-Datenbanken nicht mehr (für ein Update-Abonnement), stellt die Interaktion mit dem Dienst Kaspersky Security Network und den Computerschutz ein und startet keine Untersuchungsaufgaben mehr (für ein Update- und Schutz-Abonnement).

Um Kaspersky Total Security mit einem Abonnement zu nutzen, müssen Sie den Aktivierungscode eingeben, den Sie vom Dienstleister erhalten haben. In bestimmten Fällen kann der Aktivierungscode automatisch heruntergeladen und übernommen werden. Wenn Sie das Programm mit einem Abonnement verwenden, können Sie keinen anderen Aktivierungscode einsetzen, um die Lizenz zu verlängern. Dies ist erst nach Ablauf des Abonnements möglich.

Wenn Sie Kaspersky Total Security mit einer aktuellen Lizenz nutzen und ein Abonnement registrieren, wird Kaspersky Total Security nach der Abo-Registrierung im Abonnement genutzt. Der Aktivierungscode, mit dem das Programm davor aktiviert wurde, kann auf einem anderen Computer verwendet werden.

Um ein Abonnement zu kündigen, wenden Sie sich an den Dienstleister, bei dem Sie Kaspersky Total Security erworben haben.

Die Optionen für die Abonnementsverwaltung können je nach Dienstleister unterschiedlich sein. Nicht alle Anbieter gewähren eine Nachfrist für die Abo-Verlängerung.

ÜBER DIE ZURVERFÜGUNGSTELLUNG VON DATEN

Wenn Sie die Lizenzvereinbarung akzeptieren, stimmen Sie damit auch zu, dass automatisch folgende Informationen an Kaspersky Lab übertragen werden, um dadurch den Schutz für das Betriebssystem zu optimieren:

- Informationen über die Kontrollsummen verarbeiteter Dateien (MD5, sha256)
- Informationen für die Ermittlung der Reputation von Webadressen
- Statistik für die Verwendung von Programmbenachrichtigungen
- Statistische Daten für den Spam-Schutz
- Daten zur Aktivierung und zur eingesetzten Version von Kaspersky Total Security
- Informationen zur Lizenzverwaltung der installierten Version von Kaspersky Total Security
- Informationen über die Typen von gefundenen Bedrohungen
- Informationen über die verwendeten digitalen Zertifikate und Informationen, die zur Authentizitätsprüfung von Zertifikaten erforderlich sind.
- Daten über die Verwendung des Programms und über die Lizenz. Diese Daten werden benötigt, um die Anzeige von vertrauenswürdigen Seiteninhalten anzupassen.

Wenn der Computer mit dem Modul TPM (Trusted Platform Module) ausgerüstet ist, stimmen Sie außerdem zu, dass folgende Daten an Kaspersky Lab übermittelt werden: TPM-Bericht über die Auslastung des Betriebssystems des Computers und Informationen, die zur Authentifizierung des Berichts erforderlich sind. Sie stimmen zu, dass automatisch Informationen über den Fehlercode, über das verwendete Programmpaket und über den Computer an Kaspersky Lab übermittelt werden, falls bei der Installation von Kaspersky Total Security Fehler auftreten.

Wenn Sie am Programm Kaspersky Security Network (s. Abschnitt "Teilnahme an Kaspersky Security Network (KSN)" auf S. 97) teilnehmen, stimmen Sie zu, dass automatisch folgende Informationen an Kaspersky Lab übermittelt werden, die bei der Nutzung von Kaspersky Total Security auf dem Computer gesammelt wurden:

- Informationen über die installierte Hard- und Software
- Informationen über den Status des Antiviren-Schutzes auf dem Computer, Informationen über alle möglicherweise infizierten Objekte und über Entscheidungen, die im Hinblick auf diese Objekte erfolgt sind.
- Informationen über geladene und gestartete Programme
- Informationen über Fehler und über die Verwendung der Benutzeroberfläche von Kaspersky Total Security

- Informationen zum Programm wie beispielsweise Programmversion, Informationen über die Dateien von geladenen Programm-Modulen, Version der verwendeten Programm-Datenbanken
- Statistik über Updates und über Verbindungen mit den Kaspersky-Lab-Servern
- Informationen über die vom Computer verwendete drahtlose Verbindung
- Statistik für die tatsächliche Zeitdauer, die die Programmkomponenten für die Objektuntersuchung aufgewendet haben.
- Dateien, die von Angreifern benutzt werden können, um den Computer zu beschädigen. Dazu zählen auch Bestandteile solcher Dateien, auf die durch schädliche Links verwiesen wird.

Informationen, die an Kaspersky Lab übertragen werden sollen, bleiben ab der Erstellung für höchstens 30 Tage auf Ihrem Computer gespeichert. Sie werden in einem sicheren internen Speicher abgelegt. Der Höchstwert für die gespeicherten Informationen beträgt 30 MB.

Sie stimmen außerdem zu, dass für eine zusätzliche Untersuchung Dateien (oder Dateiteile) an Kaspersky Lab übertragen werden, die von Angreifern zur Beschädigung des Computers oder der Daten verwendet werden können.

Kaspersky Lab gewährleistet den gesetzlich vorgeschriebenen Schutz der übermittelten Daten. Kaspersky Lab verwendet diese Informationen nur in Form einer allgemeinen Statistik. Die Daten der allgemeinen Statistik werden automatisch aus den gesammelten Quellinformationen ermittelt und enthalten keinerlei persönliche oder sonstige vertrauliche Informationen. Die gesammelten Quellinformationen werden in verschlüsselter Form gespeichert und regelmäßig gelöscht (2 Mal jährlich). Die Daten der allgemeinen Statistik werden unbegrenzt gespeichert.

LIZENZ KAUFEN

Wenn Sie Kaspersky Total Security installiert und noch keine Lizenz gekauft haben, können Sie nach der Programminstallation eine Lizenz erwerben. Beim Kauf einer Lizenz erhalten Sie einen Aktivierungscode, mit dem Sie das Programm aktivieren müssen (s. Abschnitt "Programm aktivieren" auf S. 32).

Gehen Sie folgendermaßen vor, um eine Lizenz zu erwerben:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Hauptfensters auf den Link **Lizenz**, um das Fenster **Lizenzverwaltung** zu öffnen.
3. Klicken Sie im folgenden Fenster auf **Aktivierungscode kaufen**.

Die Webseite des Online-Shops von Kaspersky Lab oder eines Partnerunternehmens wird geöffnet, auf der Sie eine Lizenz erwerben können.

PROGRAMM AKTIVIEREN

Zur Nutzung der Programmfunktionen und der mit dem Programm verbundenen Zusatzleistungen muss das Programm aktiviert werden.

Wenn Sie das Programm nicht bei der Installation aktiviert haben, können Sie dies später nachholen. Falls eine Programmaktivierung notwendig ist, werden Sie von Kaspersky Total Security durch entsprechende Meldungen im Infobereich der Taskleiste daran erinnert.

Gehen Sie folgendermaßen vor, um Kaspersky Total Security zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Aktivierungscode eingeben**, um das Fenster **Aktivierung** zu öffnen.

3. Geben Sie im Fenster **Aktivierung** den Aktivierungscode in das Eingabefeld ein und klicken Sie auf die Schaltfläche **Aktivieren**.

   Die Anfrage zum Aktivieren der Anwendung wird durchgeführt.

4. Geben Sie die Registrierungsdaten des Benutzers ein.

   Abhängig von den Nutzungsbedingungen fordert das Programm möglicherweise zur Authentifizierung im Portal My Kaspersky auf. Wenn Sie kein registrierter Benutzer sind, füllen Sie die Felder des Registrierungsformulars aus, um auf zusätzliche Möglichkeiten zugreifen zu können.

   Registrierte Benutzer können folgende Aktionen ausführen:

   - Anfragen an den Technischen Support und an das Virenlabor senden.
   - Aktivierungscodes verwalten
   - Empfang von Informationen über neue Programme und Sonderangebote von Kaspersky Lab

   Dieser Schritt ist nicht in allen Versionen von Kaspersky Total Security verfügbar.

5. Klicken Sie im Fenster **Aktivierung** auf die Schaltfläche **Beenden**, um den Aktivierungsvorgang abzuschließen.

LIZENZ VERLÄNGERN

Sie können eine Lizenz vor dem Ablaufdatum verlängern. Dazu können Sie vor Ablauf der Lizenz einen Reserve-Aktivierungscode angeben. Wenn die Lizenz abläuft, wird das Programm Kaspersky Total Security automatisch mit dem Reserve-Aktivierungscode aktiviert.

Um einen Reserve-Aktivierungscode für die automatische Lizenzverlängerung anzugeben, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Hauptfensters auf den Link **Lizenz**, um das Fenster **Lizenzverwaltung** zu öffnen.
3. Klicken Sie im folgenden Fenster unter **Reserve-Aktivierungscode** auf **Aktivierungscode eingeben**.
4. Tragen Sie den Aktivierungscode in die entsprechenden Felder ein und klicken Sie auf **Hinzufügen**.

   Kaspersky Total Security schickt die Daten zur Überprüfung an den Kaspersky-Lab-Aktivierungsserver.

5. Klicken Sie auf **Beenden**.

Der Reserve-Aktivierungscode wird im Fenster **Lizenzverwaltung** angezeigt.

Nach Ablauf der Lizenz wird das Programm automatisch mithilfe des Reserve-Aktivierungscodes aktiviert. Sie können das Programm auch selbstständig mithilfe des Reserve-Aktivierungscodes aktivieren, indem Sie auf die Schaltfläche **Jetzt aktivieren** klicken. Die Schaltfläche ist verfügbar, wenn das Programm nicht automatisch aktiviert wurde. Vor dem Ablauf der Lizenz ist die Schaltfläche nicht verfügbar.

Falls Sie als Reserve-Aktivierungscode einen Aktivierungscode angegeben haben, der bereits auf diesen oder einem anderen Computer verwendet wurde, wird bei der Lizenzverlängerung das Datum angenommen, an dem das Programm zum ersten Mal mit diesem Aktivierungscode aktiviert wurde.

MIT DEN BENACHRICHTIGUNGEN DES PROGRAMMS ARBEITEN

Meldungen, die das Programm im Infobereich der Taskleiste anzeigt, informieren über Ereignisse bei der Arbeit des Programms und erfordern Ihre Aufmerksamkeit. In Abhängigkeit von der Priorität eines Ereignisses sind folgende Arten von Meldungen möglich:

- *Kritische Meldungen* informieren über Ereignisse, die vorrangige Priorität für die Computersicherheit besitzen (beispielsweise Fund eines schädlichen Objekts oder einer gefährlichen Aktivität im Betriebssystem). Die Fenster für kritische Meldungen und Pop-up-Fenster sind rot.

- *Wichtige Meldungen* informieren über Ereignisse, die für die Computersicherheit potenziell wichtig sind (beispielsweise Fund eines möglicherweise infizierten Objekts oder einer verdächtigen Aktivität im Betriebssystem). Die Fenster für wichtige Meldungen und Pop-up-Fenster sind gelb.

- *Informative Meldungen* informieren über Ereignisse, die keine vorrangige Sicherheitsrelevanz besitzen. Die Fenster für informative Meldungen und Pop-up-Fenster sind grün.

Wenn eine Benachrichtigung auf dem Bildschirm erscheint, muss eine der vorgegebenen Varianten ausgewählt werden. Als optimal gilt die standardmäßig von Kaspersky Lab empfohlene Variante. Eine Benachrichtigung kann bei einem Neustart des Computers, beim Schließen von Kaspersky Total Security oder im Connected Standby in Windows 8 automatisch geschlossen werden. Wenn eine Benachrichtigung automatisch geschlossen wird, führt Kaspersky Total Security die standardmäßig empfohlene Aktion aus.

Wenn das Programm Kaspersky Total Security beim Kauf Ihres Computers vorinstalliert war (OEM-Lieferung), zeigt das Programm innerhalb der ersten Stunde keine Meldungen an. Das Programm verarbeitet gefundene Objekte mit den empfohlenen Aktionen. Die Verarbeitungsergebnisse werden protokolliert.

SCHUTZSTATUS DES COMPUTERS ANALYSIEREN UND SICHERHEITSPROBLEME BEHEBEN

Probleme im Schutz des Computers werden durch einen Indikator signalisiert, der sich oben im Programmhauptfenster befindet. Grün bedeutet, dass der Computer sicher ist. Gelb weist auf Probleme im Schutz hin. Rot warnt vor einer ernsthaften Bedrohung für die Computersicherheit. Probleme und Sicherheitsrisiken sollten umgehend behoben werden.

Durch Klick auf den Indikator im Programmhauptfenster können Sie das Fenster **Mitteilungszentrale** öffnen (s. Abb. unten). Es enthält ausführliche Angaben zum Schutzstatus des Computers und bietet Optionen zum Beheben von Problemen und Bedrohungen.

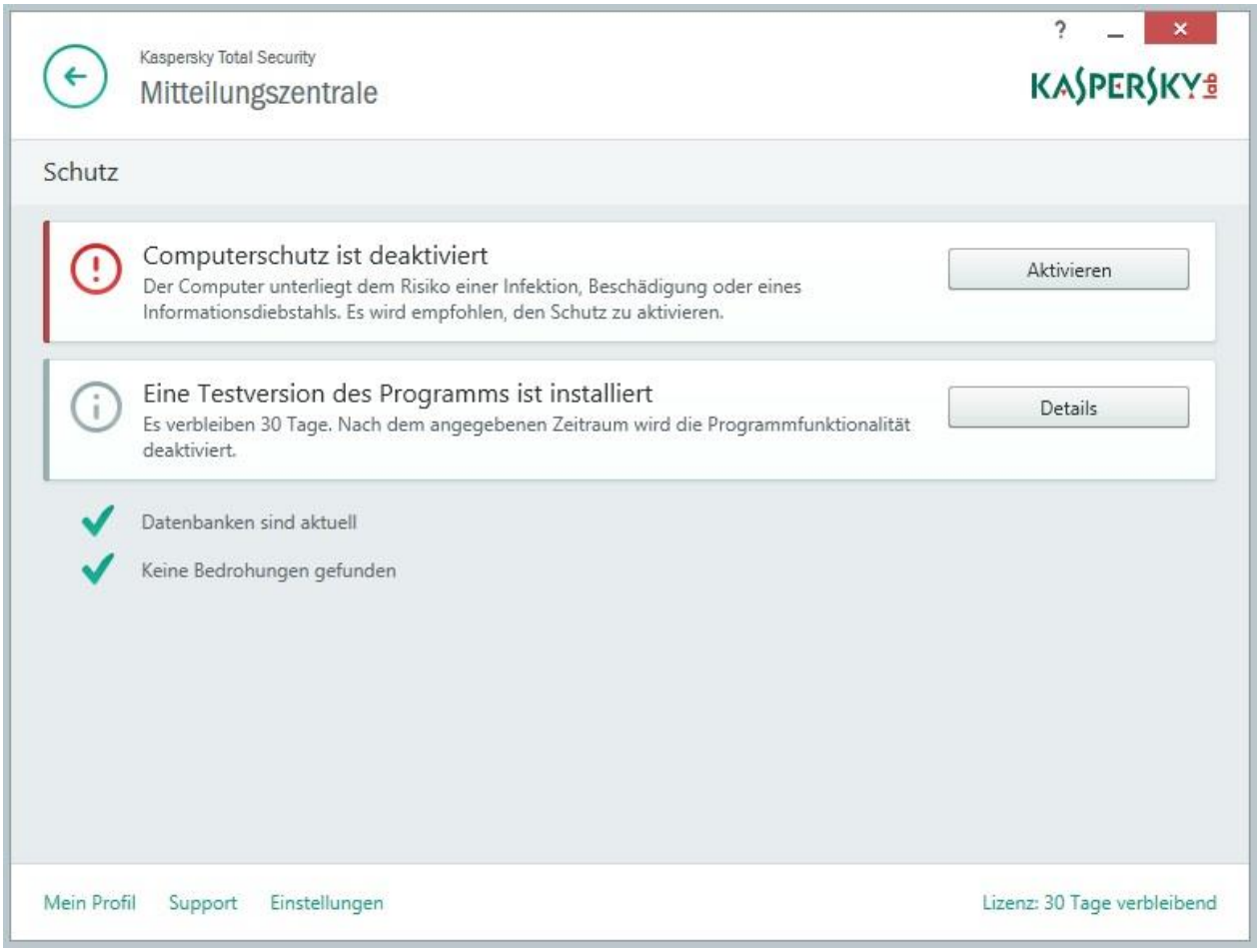

Abbildung 1. Fenster Mitteilungszentrale

Die Probleme, die im Schutz vorliegen, sind nach Kategorien angeordnet. Für jedes Problem werden Aktionen genannt, die Sie zur Problemlösung ausführen können.

UPDATE DER DATENBANKEN UND PROGRAMM-MODULE

Kaspersky Total Security überprüft in der Grundeinstellung automatisch, ob auf den Kaspersky-Lab-Updateservern neue Updates vorhanden sind. Wenn auf dem Server neue Updates vorhanden sind, lädt Kaspersky Total Security die Updates im Hintergrundmodus herunter und installiert sie. Sie können das Update von Kaspersky Total Security jederzeit manuell aus dem Programmhauptfenster oder aus dem Kontextmenü des Programmsymbols im Infobereich der Windows-Taskleiste starten.

Um Updates von den Kaspersky-Lab-Update-Servern herunterzuladen, ist eine Internetverbindung erforderlich.

Beim Einsatz von Microsoft Windows 8 werden keine Updates heruntergeladen, wenn eine mobile Hochgeschwindigkeits-Internetverbindung verwendet wird und der Datenverkehr für diesen Verbindungstyp im Programm beschränkt ist. Um Updates herunterzuladen, muss die Beschränkung im Unterabschnitt **Netzwerk** des Programmkonfigurationsfensters manuell deaktiviert werden.

- *Um das Update aus dem Kontextmenü des Programmsymbols im Infobereich der Taskleiste zu starten,*

  wählen Sie im Kontextmenü des Programmsymbols den Punkt **Update** aus.

- *Um das Update aus dem Programmhauptfenster zu starten, gehen Sie wie folgt vor:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Update**.

     Dieses Fenster enthält den Abschnitt **Update**.

  2. Klicken Sie im Abschnitt **Update** auf **Aktualisieren**.

UNTERSUCHUNG DES COMPUTERS

Dieser Abschnitt informiert darüber, wie der Computer auf Viren und andere bedrohliche Programme untersucht wird.

IN DIESEM ABSCHNITT

VOLLSTÄNDIGE UNTERSUCHUNG

Bei einer vollständigen Untersuchung scannt Kaspersky Total Security standardmäßig folgende Objekte:

- Systemspeicher
- Objekte, die beim Hochfahren des Betriebssystems geladen werden.
- Sicherungsspeicher
- Festplatten und Wechseldatenträger

Es wird empfohlen, den Computer sofort nach der Installation von Kaspersky Total Security vollständig zu untersuchen.

Um die vollständige Untersuchung zu starten, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.
3. Gehen Sie im Fenster **Untersuchung** zum Abschnitt **Vollständige Untersuchung**.
4. Klicken Sie im Fenster **Vollständige Untersuchung** auf **Untersuchung starten**.

Kaspersky Total Security beginnt mit der vollständigen Untersuchung des Computers.

BENUTZERDEFINIERTE UNTERSUCHUNG

Mithilfe der benutzerdefinierten Untersuchung können Sie eine Datei, einen Ordner oder einen Datenträger auf Viren und andere bedrohliche Programme untersuchen.

Für den Start der benutzerdefinierten Untersuchung bestehen folgende Varianten:

- Aus dem Kontextmenü eines Objekts
- Aus dem Programmhauptfenster

Um die benutzerdefinierte Untersuchung über das Kontextmenü eines Objekts zu starten, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und gehen Sie in den Ordner, in dem sich das Untersuchungsobjekt befindet.
2. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt (s. Abb. unten) und wählen Sie den Punkt **Auf Viren untersuchen**.

Abbildung 2. Kontextmenü des Objekts

Um die benutzerdefinierte Untersuchung aus dem Programmhauptfenster zu starten, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.
3. Gehen Sie im Fenster **Untersuchung** zum Abschnitt **Benutzerdefinierte Untersuchung**.
4. Verwenden Sie eine der folgenden Methoden, um die Untersuchungsobjekte anzugeben:
   - Ziehen Sie die Objekte mit der Maus ins Fenster **Benutzerdefinierte Untersuchung**.
   - Klicken Sie auf **Hinzufügen** und geben Sie im folgenden Fenster eine Datei oder einen Ordner an.
5. Klicken Sie auf **Untersuchung starten**.

SCHNELLE UNTERSUCHUNG

Bei der schnellen Untersuchung scannt Kaspersky Total Security standardmäßig folgende Objekte:

- Objekte, die beim Hochfahren des Betriebssystems geladen werden.
- Systemspeicher
- Bootsektoren

- *Um die schnelle Untersuchung zu starten, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.
3. Gehen Sie im Fenster **Untersuchung** zum Abschnitt **Schnelle Untersuchung**.
4. Klicken Sie im Fenster **Schnelle Untersuchung** auf **Untersuchung starten**.

Kaspersky Total Security beginnt mit der schnellen Untersuchung des Computers.

MÖGLICHERWEISE INFIZIERTE DATEIEN UNTERSUCHEN

Wenn Sie den Verdacht haben, dass eine Datei infiziert ist, muss sie mit Kaspersky Total Security untersucht werden (s. Abschnitt "Benutzerdefinierte Untersuchung" auf S. 37).

Wenn das Programm eine Datei nach der Untersuchung als virenfrei einstuft, obwohl Sie vermuten, dass sie infiziert ist, können Sie die Datei an das *Virenlabor* schicken. Die Experten des Virenlabors untersuchen die Datei. Sollte sie tatsächlich von einem Virus oder einem anderen bedrohlichen Programm infiziert sein, so wird den Datenbanken eine Beschreibung für den neuen Virus hinzugefügt. Das Programm lädt die Datenbanken beim Update der Datenbanken und Programm-Module herunter (s. Abschnitt "Update der Datenbanken und Programm-Module" auf S. 36).

- *Um eine Datei an das Virenlabor zu schicken, gehen Sie wie folgt vor:*

1. Gehen Sie auf die Seite, die zum Senden einer Anfrage an das Virenlabor dient (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de).
2. Folgen Sie den Anweisungen, die auf dieser Seite gegeben werden, um eine Anfrage zu schicken.

SCHWACHSTELLENSUCHE

Schwachstellen sind ungeschützte Abschnitte im Programmcode, die von Angreifern ausgenutzt werden können: beispielsweise um Daten zu kopieren, die von Programmen mit ungeschütztem Code verwendet werden. Die Untersuchung Ihres Computers auf Schwachstellen erlaubt es, solche "Schwachpunkte" im Schutz des Rechners zu finden. Erkannte Schwachstellen sollten beseitigt werden.

- *Um die Schwachstellensuche zu starten, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Zusätzliche Tools anzeigen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie im Fenster **Tools** links auf den Link **Schwachstellensuche**, um das Fenster **Schwachstellensuche** zu öffnen.
4. Klicken Sie im Fenster **Schwachstellensuche** auf **Untersuchung starten**.

Kaspersky Total Security beginnt damit, Ihren Computer auf Schwachstellen zu überprüfen.

OBJEKT WIEDERHERSTELLEN, DAS VOM PROGRAMM GELÖSCHT ODER DESINFIZIERT WURDE

Kaspersky Lab warnt davor, gelöschte und desinfizierte Objekte wiederherzustellen, da diese eine Gefahr für Ihren Computer darstellen können.

Die Backup-Kopie, die vom Programm bei der Untersuchung eines Objekts angelegt wurde, dient zur Wiederherstellung eines gelöschten oder desinfizierten Objekts.

Anwendungen aus dem Windows Store werden von Kaspersky Total Security nicht desinfiziert. Wenn eine solche Anwendung bei einer Untersuchung als gefährlich eingestuft wird, wird sie von Ihrem Computer gelöscht.

Wenn Anwendungen aus dem Windows Store gelöscht werden, legt Kaspersky Total Security keine Backup-Kopien an. Zur Wiederherstellung solcher Objekte müssen entsprechende Reparatur-Tools des Betriebssystems eingesetzt werden (Nähere Informationen finden Sie in der Dokumentation zum Betriebssystem Ihres Rechners) oder die Anwendungen müssen über den Windows Store aktualisiert werden.

Gehen Sie folgendermaßen vor, um eine Datei wiederherzustellen, die vom Programm gelöscht oder desinfiziert wurde:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Zusätzliche Tools anzeigen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie im Fenster **Tools** links auf den Link **Quarantäne**, um das Fenster **Quarantäne** zu öffnen.
4. Wählen Sie im folgenden Fenster **Quarantäne** in der Liste die entsprechende Datei aus und klicken Sie auf **Wiederherstellen**.

BETRIEBSSYSTEM NACH EINER INFEKTION WIEDERHERSTELLEN

Dieser Abschnitt informiert darüber, wie das Betriebssystem nach einer Vireninfektion wiederhergestellt wird.

IN DIESEM ABSCHNITT

SO WIRD DAS BETRIEBSSYSTEM NACH EINER INFEKTION WIEDERHERGESTELLT

Wenn Sie vermuten, dass das Betriebssystem Ihres Computers durch Schadsoftware-Aktivitäten oder durch einen Systemfehler beschädigt oder verändert wurde, verwenden Sie den *Assistenten zur Wiederherstellung nach einer Infektion*, der die Spuren von schädlichen Objekten im Betriebssystem beseitigt. Die Kaspersky-Lab-Experten empfehlen außerdem, den Assistenten nach einer Desinfektion des Computers auszuführen, um sicherzustellen, dass alle aufgetretenen Bedrohungen und Beschädigungen beseitigt wurden.

Der Assistent überprüft, ob das Betriebssystem Veränderungen aufweist. Dazu können gehören: Sperrung des Zugriffs auf die Netzwerkumgebung, Veränderung der Erweiterungen von bekannten Dateiformaten und Sperrung der Systemsteuerung. Es gibt unterschiedliche Gründe für das Auftreten solcher Beschädigungen. Es kann sich um die Aktivität schädlicher Programme, ungültige Einstellungen für das Betriebssystem, Systemabstürze oder die Verwendung fehlerhaft funktionierender Optimierungsprogramme für das Betriebssystem handeln.

Nach der Untersuchung analysiert der Assistent die ermittelten Informationen, um festzustellen, ob im Betriebssystem Beschädigungen vorliegen, die sofort behoben werden müssen. Aufgrund der Untersuchungsergebnisse wird eine Liste von Aktionen erstellt, die ausgeführt werden müssen, um die Beschädigungen zu beheben. Der Assistent ordnet die Aktionen nach der Priorität der gefundenen Probleme in Kategorien an.

BETRIEBSSYSTEM NACH EINER INFEKTION MITHILFE DES WIEDERHERSTELLUNGS-ASSISTENTEN WIEDERHERSTELLEN

- *Um den Assistenten zur Wiederherstellung nach einer Infektion zu starten, gehen Sie wie folgt vor:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie im Hauptfenster unten auf den Link **Zusätzliche Tools anzeigen**, um das Fenster **Tools** zu öffnen.
  3. Klicken Sie im Fenster **Tools** links auf den Link **Wiederherstellung nach Infektion**, um den Assistenten zur Wiederherstellung nach einer Infektion zu starten.

  Das Fenster des Assistenten zur Wiederherstellung nach einer Infektion wird geöffnet.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Details zu den einzelnen Schritten des Assistenten.

Schritt 1. Wiederherstellung des Betriebssystems starten

Vergewissern Sie sich, dass im Assistentenfenster die Variante **Suche nach Problemen, die mit Malware-Aktivität zusammenhängen, ausführen** gewählt wurde, und klicken Sie auf **Weiter**.

Schritt 2. Nach Problemen suchen

Der Assistent sucht nach Problemen und möglichen Beschädigungen, die behoben werden müssen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für die Problembehebung wählen

Alle Beschädigungen, die beim vorherigen Schritt gefunden wurden, werden ihrer Gefährlichkeit nach angeordnet. Für jede Gruppe von Beschädigungen schlagen die Kaspersky-Lab-Spezialisten eine Auswahl von Aktionen vor, deren Ausführung die Beschädigungen beheben kann. Die Aktionen sind in drei Gruppen unterteilt:

- *Ausdrücklich empfohlene Aktionen* können Beschädigungen beheben, die ein ernsthaftes Problem darstellen. Es wird empfohlen, alle Aktionen dieser Gruppe auszuführen.
- *Empfohlene Aktionen* dienen zum Beheben von Beschädigungen, die ein Risiko darstellen können. Es wird empfohlen, auch alle Aktionen dieser Gruppe auszuführen.
- *Zusätzliche Aktionen* dienen dazu, momentan ungefährliche Beschädigungen des Betriebssystems zu beheben, die die Computersicherheit in Zukunft bedrohen können.

Klicken Sie links vom Namen einer Gruppe auf das Zeichen +, um die Aktionen der Gruppe anzuzeigen.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen.

Die standardmäßig aktivierten Kontrollkästchen sollten auf keinen Fall entfernt werden, da hierdurch die Sicherheit Ihres Computers bedroht wird.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Probleme beheben

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Die Problembehebung kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Problembehebung automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

E-MAIL-SCHUTZ

Dieser Abschnitt informiert darüber, wie E-Mails vor Spam, Viren und anderen bedrohlichen Programmen geschützt werden können.

IN DIESEM ABSCHNITT

EINSTELLUNGEN FÜR MAIL-ANTI-VIRUS

Kaspersky Total Security kann E-Mails auf gefährliche Objekte untersuchen. Dazu dient die Komponente Mail-Anti-Virus. Mail-Anti-Virus wird beim Start des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle E-Mail-Nachrichten, die über die Protokolle POP3, SMTP, IMAP und NNTP (sowie über geschützte Verbindungen (SSL) mit den Protokollen POP3, SMTP und IMAP) ein- und ausgehen.

Standardmäßig untersucht Mail-Anti-Virus sowohl eingehende als auch ausgehende Nachrichten. Bei Bedarf können Sie festlegen, dass nur eingehende Nachrichten untersucht werden.

Um Mail-Anti-Virus anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.

   Dieses Fenster enthält Einstellungen für Mail-Anti-Virus.
4. Vergewissern Sie sich, dass der Schalter im oberen Fensterbereich eingeschaltet ist. Der Schalter dient dazu, Mail-Anti-Virus zu aktivieren bzw. deaktivieren.
5. Wählen Sie eine Sicherheitsstufe aus:

   - **Empfohlen**. Auf dieser Sicherheitsstufe untersucht Mail-Anti-Virus ein- und ausgehende Nachrichten sowie angehängte Archive.
   - **Niedrig**. Auf dieser Sicherheitsstufe untersucht Mail-Anti-Virus nur eingehende Nachrichten. Angehängte Archive werden nicht gescannt.
   - **Hoch**. Auf dieser Sicherheitsstufe untersucht Mail-Anti-Virus ein- und ausgehende Nachrichten sowie angehängte Archive. Auf der hohen Sicherheitsstufe erfolgt eine ausführliche heuristische Analyse.
6. Wählen Sie in der Dropdown-Liste **Aktion beim Fund einer Bedrohung** aus, welche Aktion Mail-Anti-Virus ausführen soll, wenn ein infiziertes Objekt gefunden wird (z. B. Desinfizieren).

Wenn in einer E-Mail-Nachricht keine Bedrohungen gefunden oder infizierte Objekte erfolgreich neutralisiert wurden, wird der Zugriff auf die Nachricht freigegeben. Wenn ein infiziertes Objekt nicht desinfiziert werden konnte, benennt Mail-Anti-Virus das Objekt um oder löscht es aus der Nachricht und fügt dem Betreff eine Notiz darüber hinzu, dass die Nachricht von Kaspersky Total Security bearbeitet wurde. Wenn ein Objekt gelöscht wird, legt Kaspersky Total Security eine Sicherungskopie an und verschiebt sie in die Quarantäne (s. Abschnitt "Objekt wiederherstellen, das vom Programm gelöscht oder desinfiziert wurde" auf S. 40).

UNERWÜNSCHTE E-MAILS (SPAM) BLOCKIEREN

Falls Sie viel Spam erhalten, aktivieren Sie die Komponente Anti-Spam und wählen Sie die empfohlene Sicherheitsstufe.

Um Anti-Spam zu aktivieren und die empfohlene Sicherheitsstufe zu wählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf den Link **Einstellungen**, um den Abschnitt **Einstellungen** zu öffnen.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Schutz** aus.
4. Wählen Sie im Abschnitt **Schutz** rechts die Komponente **Anti-Spam** aus.

   Dieses Fenster enthält Einstellungen für Anti-Spam.
5. Verwenden Sie den Schalter im rechten Fensterbereich, um Anti-Spam zu aktivieren.
6. Vergewissern Sie sich, dass im Abschnitt **Sicherheitsstufe** die Sicherheitsstufe **Empfohlen** ausgewählt ist.

SCHUTZ FÜR PERSÖNLICHE DATEN IM INTERNET

Dieser Abschnitt informiert darüber, wie Sie sicher im Internet arbeiten und Ihre Daten vor Diebstahl schützen können.

IN DIESEM ABSCHNITT

ÜBER DEN SCHUTZ FÜR PERSÖNLICHE DATEN IM INTERNET

Mit Kaspersky Total Security können Sie Ihre persönlichen Daten vor Diebstahl schützen:

- Kennwörter, Benutzernamen und andere Anmeldedaten
- Konto- und Bankkartenummern

Kaspersky Total Security enthält Komponenten und Tools, mit denen Sie Ihre persönlichen Daten auch dann vor Diebstahl schützen können, wenn Angreifer Methoden wie Phishing und das Abfangen von Tastatureingaben einsetzen.

Für den Schutz vor Phishing ist Anti-Phishing verantwortlich, das zu den Komponenten Web-Anti-Virus, Anti-Spam und IM-Anti-Virus gehört. Aktivieren Sie diese Komponenten, um einen effektiven Schutz vor Phishing zu gewährleisten.

Die Virtuelle Tastatur und der Schutz für die Dateneingabe über eine Hardwaretastatur dienen dazu, Tastatureingaben vor dem Abfangen von Daten zu schützen.

Der Lösch-Assistent für Aktivitätsspuren dient zum Löschen von Informationen, die Rückschlüsse über die Benutzeraktionen auf dem Computer zulassen.

Die Funktionen des Sicheren Zahlungsverkehrs dienen zum Datenschutz bei der Verwendung von Online-Banking-Diensten und bei Zahlungsvorgängen in Online-Shops.

Ein Tool der Kindersicherung schützt davor, dass persönliche Daten über das Internet verschickt werden (s. Abschnitt "Kindersicherung verwenden" auf S. 61).

ÜBER DIE VIRTUELLE TASTATUR

Bei der Arbeit im Internet ist es häufig erforderlich, persönliche Daten, Benutzername und Kennwort einzugeben. Beispiele sind die Anmeldung auf Webseiten, der Besuch von Online-Shops und die Verwendung von Online-Banking.

In solchen Situationen besteht die Gefahr, dass persönliche Informationen mithilfe von Hardware-Hooks oder mit Keyloggern (Programme, die Tasteneingaben registrieren) abgefangen werden. Die virtuelle Tastatur ermöglicht es, das Abfangen von über die Tastatur eingegebenen Daten zu verhindern.

Viele Spyware-Programme besitzen Funktionen zum Anlegen von Screenshots, die an Angreifer für Analyse und Sammeln von persönlichen Benutzerdaten automatisch übergeben werden. Die Virtuelle Tastatur schützt davor, dass persönliche Daten durch das Anlegen von Bildschirmkopien (Screenshots) abgefangen werden.

Die Virtuelle Tastatur besitzt folgende Besonderheiten:

- Die Tasten der Virtuellen Tastatur werden durch Mausklick gedrückt.
- Im Gegensatz zu einer echten Tastatur ist es auf der Virtuellen Tastatur nicht möglich, mehrere Tasten gleichzeitig zu drücken. Um Tastenkombinationen zu verwenden (z. B. **ALT**+**F4**), ist es deshalb notwendig, zuerst die erste Taste (z. B. **ALT**), dann die zweite Taste (z. B. **F4**) und anschließend erneut die erste Taste zu drücken. Das wiederholte Drücken ersetzt das Loslassen einer Taste auf der echten Tastatur.
- Die Eingabesprache wird auf der Virtuellen Tastatur mit der gleichen Tastenkombination umgeschaltet, die in den Einstellungen des Betriebssystems für die gewöhnliche Tastatur eingestellt ist. Dabei muss mit der rechten Maustaste auf die zweite Taste gedrückt werden (Wenn beispielsweise in den Einstellungen des Betriebssystems zum Umschalten der Eingabesprache die Kombination **ALT LINKS**+**UMSCHALT** festgelegt ist, muss die Taste **ALT LINKS** mit der linken Maustaste und die Taste **UMSCHALT** mit der rechten Maustaste gedrückt werden).

Für den Schutz von Daten, die mithilfe der Virtuellen Tastatur eingegeben werden, muss der Computer nach der Installation von Kaspersky Total Security neu gestartet werden.

Die Verwendung der virtuellen Tastatur unterliegt folgenden Einschränkungen:

- Die Virtuelle Tastatur schützt persönliche Daten nur dann vor Diebstahlversuchen, wenn Sie den Browser Microsoft Internet Explorer, Mozilla Firefox oder Google Chrome verwenden. Bei Verwendung anderer Browser wird die Eingabe persönlicher Daten nicht von der Virtuellen Tastatur geschützt.
- Wenn in den Browser-Einstellungen das Kontrollkästchen **Erweiterten geschützten Modus aktivieren** (Enhanced Protected Mode) aktiviert ist, ist die Virtuelle Tastatur in folgenden Browsern nicht verfügbar: Microsoft Internet Explorer (Version 10 und 11) im neuen Windows-Design und Microsoft Internet Explorer (Version 10 und 11).
- Die Virtuelle Tastatur kann Ihre persönlichen Daten nicht schützen, wenn eine Webseite gehackt wurde und die Eingabe solcher Daten fordert, da die Informationen in diesem Fall dem Angreifer direkt in die Hände fallen.
- Die virtuelle Tastatur verhindert nicht das Erstellen von Screenshots mithilfe der **DRUCK**-Taste und mit anderen Tastenkombinationen, die in den Einstellungen des Betriebssystems festgelegt sind.
- Wenn die virtuelle Tastatur im Browser Microsoft Internet Explorer gestartet wird, funktioniert die Autovervollständigung für Eingabefelder nicht mehr, da die Autovervollständigung Betrügern die Möglichkeit zum Datendiebstahl bietet.
- Kaspersky Total Security schützt im Betriebssystem Microsoft Windows 8 und 8.1 (nur 64-Bit) nicht vor Screenshots, wenn das Fenster der Virtuellen Tastatur geöffnet ist, aber der Prozess des Sicheren Browser nicht läuft.
- Es kann sein, dass in bestimmten Browsern (z. B. Google Chrome) der Schutz bei der Eingabe bestimmter Datentypen nicht funktioniert (z. B. für E-Mail-Adressen oder Zahlen).

Die oben stehende Liste enthält die wichtigsten Einschränkungen, die für die Funktionalität "Schutz der Dateneingabe" gelten. Eine vollständige Liste der Einschränkungen finden Sie in folgendem Artikel auf der Seite des Technischen Supports von Kaspersky Lab http://support.kaspersky.com/de/11048.

VIRTUELLE TASTATUR STARTEN

Die Virtuelle Tastatur kann auf folgende Weise geöffnet werden:

- Aus dem Kontextmenü des Programmsymbols im Infobereich der Taskleiste
- Aus dem Programmhauptfenster
- Aus den Browserfenstern von Microsoft Internet Explorer, Mozilla Firefox oder Google Chrome mithilfe des Schnellstartsymbols der virtuellen Tastatur
- Mithilfe des Schnellstartsymbols für die Virtuelle Tastatur in den Eingabefeldern von Webseiten

  Die Anzeige des Schnellstartsymbols in den Eingabefeldern von Webseiten lässt sich anpassen (s. Abschnitt "Anzeige des Symbols für die Virtuelle Tastatur anpassen" auf S. 48).

  Wenn die Virtuelle Tastatur verwendet wird, deaktiviert Kaspersky Total Security die Autovervollständigung für Eingabefelder auf Webseiten.

- Mit einer Tastenkombination über die Hardwaretastatur.

Um die Virtuelle Tastatur aus dem Kontextmenü des Programmsymbols im Infobereich der Taskleiste zu öffnen,

wählen Sie im Kontextmenü des Programmsymbols den Punkt **Tools** → **Virtuelle Tastatur** aus (s. Abb. unten).

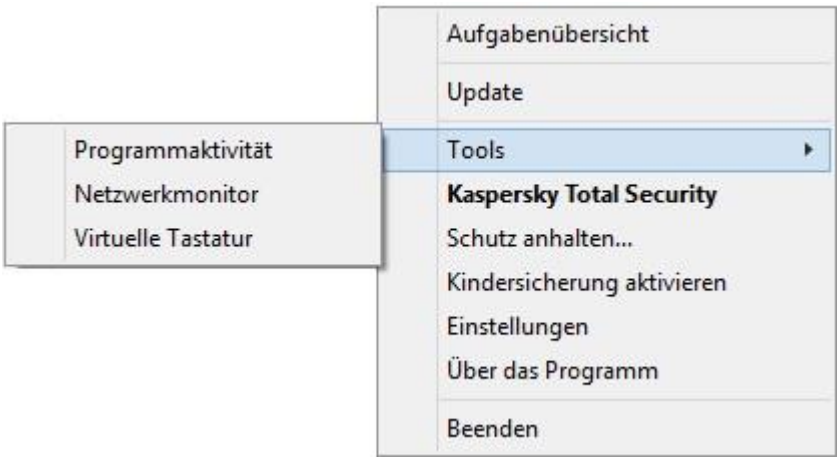

Abbildung 3. Kontextmenü von Kaspersky Total Security

Um die Virtuelle Tastatur aus dem Programmhauptfenster zu öffnen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Zusätzliche Tools anzeigen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie im Fenster **Tools** links auf den Link **Virtuelle Tastatur**, um die Virtuelle Tastatur zu öffnen.

- *Um die Virtuelle Tastatur aus dem Fenster des Browsers Microsoft Internet Explorer oder Mozilla Firefox zu öffnen,*

  klicken Sie in der Symbolleiste des Browsers auf **Virtuelle Tastatur**.

- *Um die Virtuelle Tastatur aus dem Fenster des Browsers Google Chrome zu öffnen,*

  1. Klicken Sie in der Symbolleiste des Browsers auf **Kaspersky Protection**.
  2. Wählen Sie im eingeblendeten Menü den Punkt **Virtuelle Tastatur** aus.

- *Um die Virtuelle Tastatur mithilfe der Hardwaretastatur zu öffnen,*

  verwenden Sie die Tastenkombination **STRG**+**ALT**+**UMSCHALT**+**P**.

ANZEIGE DES SYMBOLS FÜR DIE VIRTUELLE TASTATUR ANPASSEN

- *Um die Anzeige des Schnellstartsymbols für die Virtuelle Tastatur in den Eingabefeldern von Webseiten anzupassen, gehen Sie wie folgt vor:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie im unteren Fensterbereich auf den Link **Einstellungen**.
  3. Wählen Sie im folgenden Fenster **Einstellungen** im Abschnitt **Erweitert** den Unterabschnitt **Sichere Dateneingabe**.

     Dieses Fenster enthält Einstellungen für die sichere Dateneingabe.
  4. Falls erforderlich, aktivieren Sie im Abschnitt **Virtuelle Tastatur** das Kontrollkästchen **Virtuelle Tastatur mit der Tastenkombination STRG+ALT+UMSCHALT+P öffnen**.
  5. Wenn das Schnellstartsymbol für die Virtuelle Tastatur in Eingabefeldern angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Schnellstartsymbol in Eingabefeldern anzeigen**.
  6. Damit das Schnellstartsymbol für die Virtuelle Tastatur nur angezeigt wird, wenn bestimmte Webseiten geöffnet werden, gehen Sie wie folgt vor:

     a. Wählen Sie im Block **Virtuelle Tastatur** über den Link **Kategorien ändern** das Fenster **Einstellungen für die sichere Dateneingabe**.

     b. Aktivieren Sie die Kontrollkästchen für die Webseiten-Kategorien, auf denen das Schnellstartsymbol in Eingabefeldern angezeigt werden soll.

        Das Schnellstartsymbol für die Virtuelle Tastatur wird angezeigt, wenn eine Webseite geöffnet wird, die zu einer der gewählten Kategorien gehört.

     c. Um die Anzeige des Schnellstartsymbols für die Virtuelle Tastatur auf einer bestimmten Webseite zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

        a. Öffnen Sie über den Link **Ausnahmen anpassen** das Fenster **Ausnahmen für die Virtuelle Tastatur**.

        b. Klicken Sie im unteren Fensterbereich auf **Hinzufügen**.

           Ein Fenster zum Hinzufügen einer Ausnahme für die Virtuelle Tastatur wird geöffnet.

        c. Tragen Sie im Feld **Adressmaske für die Webseite** die Adresse der Webseite ein.

d. Damit das Schnellstartsymbol für die Virtuelle Tastatur nur auf der ausgewählten Webseite angezeigt wird (bzw. nicht angezeigt wird), wählen Sie im Abschnitt **Geltungsbereich** die Variante **Nur auf die angegebene Seite anwenden**.

e. Legen Sie im Abschnitt **Symbol für die Virtuelle Tastatur** fest, ob das Schnellstartsymbol für die Virtuelle Tastatur auf der angegebenen Webseite angezeigt werden soll.

f. Klicken Sie auf **Hinzufügen**.

Die angegebene Webseite erscheint auf der Liste im Fenster **Ausnahmen für die Virtuelle Tastatur**.

Beim Öffnen der angegebenen Webseite wird das Schnellstartsymbol für die Virtuelle Tastatur nach den festgelegten Einstellungen angezeigt.

SCHUTZ FÜR DIE DATENEINGABE ÜBER EINE HARDWARETASTATUR

Der Schutz für die Dateneingabe über eine Hardwaretastatur kann das Abfangen von Daten verhindern, die über eine Tastatur eingegeben werden.

Der Schutz von Tastatureingaben besitzt folgende Einschränkungen:

- Der Schutz für die Dateneingabe über eine Hardwaretastatur funktioniert nur in den Webbrowsern Microsoft Internet Explorer, Mozilla Firefox und Google Chrome. Bei Verwendung anderer Webbrowser sind Daten, die über eine Hardwaretastatur eingegeben werden, nicht vor Abfangversuchen geschützt.
- Der Schutz für die Dateneingabe ist im Browser Microsoft Internet Explorer nicht verfügbar, wenn aus dem Windows Store stammt.
- Der Schutz für die Dateneingabe über eine Hardwaretastatur kann Ihre persönlichen Daten nicht schützen, wenn eine Website gehackt wurde und die Eingabe solcher Daten fordert. In diesem Fall fallen die Informationen dem Angreifer direkt in die Hände.
- Es kann sein, dass in bestimmten Browsern (z. B. Google Chrome) der Schutz bei der Eingabe bestimmter Datentypen nicht funktioniert (z. B. für E-Mail-Adressen oder Zahlen).

Die oben stehende Liste enthält die wichtigsten Einschränkungen, die für die Funktionalität "Schutz der Dateneingabe" gelten. Eine vollständige Liste der Einschränkungen bietet ein Artikel auf der Seite des Technischen Supports von Kaspersky Lab http://support.kaspersky.com/de/11048.

Sie können den Schutz für Tastatureingaben auf bestimmten Webseiten anpassen. Nachdem der Schutz für Tastatureingaben angepasst wurde, sind bei der Dateneingabe keine zusätzlichen Aktionen erforderlich.

Um den Schutz für Tastatureingaben anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf den Link **Einstellungen**, um den Abschnitt **Einstellungen** zu öffnen.
3. Wählen Sie im Abschnitt **Erweitert** den Unterabschnitt **Sichere Dateneingabe**.

   Dieses Fenster enthält Einstellungen für die sichere Dateneingabe.
4. Aktivieren Sie im unteren Fensterbereich im Abschnitt **Schutz von Tastatureingaben** das Kontrollkästchen **Tastatureingaben schützen**.
5. Legen Sie einen Bereich für den Schutz von Tastatureingaben fest:

   a. Klicken Sie im Abschnitt **Schutz von Tastatureingaben** unten auf den Link **Kategorien ändern**, um das Fenster **Einstellungen für die sichere Dateneingabe** zu öffnen.

   b. Aktivieren Sie die Kontrollkästchen für die Webseiten-Kategorien, auf denen über die Tastatur eingegebene Daten geschützt werden sollen.

c. Um den Schutz für Tastatureingaben auf einer bestimmten Webseite zu aktivieren, gehen Sie wie folgt vor:

   a. Klicken Sie auf den Link **Ausnahmen anpassen**, um das Fenster **Ausnahmen für den Schutz von Tastatureingaben** zu öffnen.

   b. Klicken Sie im folgenden Fenster auf **Hinzufügen**.

      Ein Fenster zum Hinzufügen einer Ausnahme für die Hardwaretastatur wird geöffnet.

   c. Tragen Sie im folgenden Fenster im Feld **Maske für Webseite** die Adresse der Webseite ein.

   d. Wählen Sie eine Variante für den Schutz der Dateneingabe auf dieser Webseite aus (**Nur auf die angegebene Webseite anwenden** oder **Auf die gesamte Website anwenden**).

   e. Wählen Sie eine Aktion für den Schutz der Dateneingabe auf dieser Webseite aus (**Schützen** oder **Nicht schützen**).

   f. Klicken Sie auf **Hinzufügen**.

Die angegebene Webseite erscheint auf der Liste im Fenster **Ausnahmen für den Schutz von Tastatureingaben**. Wenn die angegebene Webseite geöffnet wird, reagiert der Schutz für die Dateneingabe gemäß den festgelegten Einstellungen.

BENACHRICHTIGUNGEN ÜBER SCHWACHSTELLEN IN EINEM WI-FI-NETZWERK ANPASSEN

Während der Arbeit in einem WLAN-Netzwerk können möglicherweise Ihre vertraulichen Daten gestohlen werden, wenn das WLAN-Netzwerk nicht ausreichend geschützt ist. Jedes Mal wenn Sie eine Verbindung mit einem WLAN-Netzwerk herstellen, überprüft Kaspersky Total Security das WLAN-Netzwerk. Wenn ein WLAN-Netzwerk nicht sicher ist (beispielsweise bei Verwendung eines verwundbaren Verschlüsselungsprotokolls oder eines populären Namens für das WLAN-Netzwerk (SSID)), so meldet das Programm, dass Sie mit einem unsicheren WLAN-Netzwerk verbunden sind. Das Benachrichtigungsfenster enthält einen Link, der zu Informationen über die sichere Nutzung von WLAN-Netzwerken führt.

Um die Benachrichtigungen über Schwachstellen in einem WLAN-Netzwerk anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf den Link **Einstellungen**, um den Abschnitt **Einstellungen** zu öffnen.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Schutz** aus.
4. Wählen Sie im Abschnitt **Schutz** rechts den Unterabschnitt **Firewall** aus.

   Dieses Fenster enthält Einstellungen für die Komponente Firewall.

5. Aktivieren Sie das Kontrollkästchen **Schwachstellen bei Verbindung mit WLAN-Netzwerk melden**, falls es deaktiviert war. Wenn Sie keine Benachrichtigungen erhalten möchten, deaktivieren Sie dieses Kontrollkästchen. Dieses Kontrollkästchen ist standardmäßig aktiviert.
6. Wenn das Kontrollkästchen **Schwachstellen bei Verbindung mit WLAN-Netzwerk melden** aktiviert ist, können Sie zusätzliche Einstellungen für die Benachrichtigungsanzeige anpassen:

   - Aktivieren Sie das Kontrollkästchen **Im Internet Kennwortübertragung im Klartext verbieten und Meldung anzeigen**, um beim Ausfüllen des Feldes **Kennwort** im Internet die Übertragung den Kennworts auf unbekannte textbasierte Art zu sperren. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

   - Stellen Sie die Werte für die Einstellungen zur Anzeige von Benachrichtigungen über die Übertragung des Kennworts auf unbekannte Art über den Link **Ausgeblendete Benachrichtigungen wiederherstellen** wieder her. Wenn Sie die Anzeige von Benachrichtigungen über die Übertragung des Kennworts auf unbekannte Art gesperrt haben, werden diese Benachrichtigungen jetzt wieder angezeigt.

SCHUTZ FÜR FINANZTRANSAKTIONEN UND ONLINE-EINKÄUFE

Um vertrauliche Daten zu schützen, die Sie auf Webseiten von Banken und Zahlungssystemen eingeben (beispielsweise Bankkartennummern und Kennwörter für Online-Banking), und um Diebstähle bei Online-Zahlungsvorgängen zu verhindern, schlägt Kaspersky Total Security vor, solche Webseiten im Sicheren Browser zu öffnen.

Der Sichere Browser ist ein spezieller Browsermodus, in dem Ihre Daten bei der Nutzung der Webseiten von Banken und Zahlungssystemen geschützt werden. Der Sichere Browser läuft in einer isolierten Umgebung. Dadurch wird verhindert, dass andere Programme in den Prozess des Sicheren Browsers eindringen können.

Im Sicheren Browser bietet das Programm Schutz vor folgenden Bedrohungsarten:

- Nicht vertrauenswürdige Module. Eine Untersuchung auf nicht vertrauenswürdige Module erfolgt jedes Mal, wenn die Webseite einer Bank oder eines Zahlungssystems geöffnet werden soll.
- Rootkits. Eine Untersuchung auf Rootkits erfolgt beim Start des Sicheren Browsers.
- Bekannte Schwachstellen im Betriebssystem Eine Untersuchung auf Schwachstellen im Betriebssystem erfolgt beim Start des Sicheren Browsers.
- Ungültige Zertifikate auf Webseiten von Banken oder Zahlungssystemen. Eine Untersuchung der Zertifikate erfolgt jedes Mal, wenn die Webseite einer Bank oder eines Zahlungssystems geöffnet werden soll. Für die Zertifikatüberprüfung wird eine Datenbank für kompromittierte Zertifikate verwendet.

Wenn Sie eine Webseite im Sicheren Browser öffnen, erhält das Browserfenster einen Rahmen. Die Farbe des Rahmens signalisiert den Schutzstatus.

Der Rahmen des Browserfensters kann folgende Farben besitzen:

- Grüner Rahmen. Bedeutet, dass alle Untersuchungen erfolgreich ausgeführt wurden. Sie können den Sicheren Browser fortsetzen.
- Gelber Rahmen. Bedeutet, dass bei den Untersuchungen Sicherheitsprobleme erkannt wurden, die behoben werden müssen.

  Das Programm kann folgende Bedrohungen und Sicherheitsprobleme erkennen:

  - Nicht vertrauenswürdiges Modul. Untersuchung des Computers und Desinfektion sind erforderlich.
  - Rootkit. Untersuchung des Computers und Desinfektion sind erforderlich.
  - Schwachstelle im Betriebssystem. Updates für das Betriebssystem müssen installiert werden.
  - Ungültiges Zertifikat der Webseite einer Bank oder eines Zahlungssystems.

  Wenn Sie die erkannten Bedrohungen nicht beheben, kann keine Sicherheit für Verbindungen mit Webseiten von Banken oder Zahlungssystemen garantiert werden. Ereignisse, die mit dem Start und der Funktion des Sicheren Browsers bei einer reduzierten Schutzstufe zusammenhängen, werden im Windows-Ereignisprotokoll aufgezeichnet.

  Ein gelber Rahmen kann auch bedeuten, dass der Start des Sicheren Browsers aufgrund technischer Einschränkungen nicht möglich ist. Dies kann der Fall sein, wenn ein Drittanbieter-Hypervisor eingesetzt wird oder wenn Ihr Computer die Hardware-Virtualisierung nicht unterstützt.

Damit der Sichere Browser einwandfrei funktioniert, müssen im Browser die Plug-ins für die Komponente Sicherer Zahlungsverkehr aktiviert sein. Die Plug-ins werden automatisch aktiviert, wenn der Browser nach der Installation von Kaspersky Total Security zum ersten Mal gestartet wird. Falls der Browser nach der Installation von Kaspersky Total Security nicht neu gestartet wurde, werden die Plug-ins nicht aktiviert.

Für die automatische Aktivierung der Plug-ins gelten folgende Einschränkungen:

- Die Integration und Aktivierung der Plug-ins erfolgt nur für Browser, die vom Programm unterstützt werden.

  Die Plug-ins für den Sicheren Zahlungsverkehr werden von folgenden Browsern unterstützt:

  - Internet Explorer Version 8.0, 9.0, 10.0 und 11.0

    Die Browser Internet Explorer 10 und Internet Explorer 11 im neuen Windows-Design werden nicht unterstützt.

  - Mozilla Firefox Versionen 19.x, 20.x, 21.x, 22.x, 23.x, 24.x, 25.x, 26.x, 27.x, 28.x, 29.x, 30.x, 31.x, 32.x, 33.x, 34.x, 35.x

  - Google Chrome Versionen 33.x, 34.x, 35.x, 36.x, 37.x, 38.x

    Kaspersky Total Security unterstützt den Browser Google Chrome der Versionen 37.x und 38.x sowohl in 32-Bit- als auch in 64-Bit-Betriebssystemen.

    In Mozilla Firefox werden die Plug-ins nicht automatisch aktiviert, wenn im Browser noch kein Benutzerprofil erstellt wurde. Um ein Benutzerprofil zu erstellen, muss der Browser neu gestartet werden.

    Wenn Google Chrome zum ersten Mal im geschützten Modus gestartet wird, schlägt Ihnen der Webbrowser vor, die Erweiterung Kaspersky Protection Plugin zu installieren, mit der die Plug-ins der Komponente Sicherer Zahlungsverkehr aktiviert werden. Wenn Sie die Erweiterung Kaspersky Protection Plugin jetzt nicht installieren möchten, können Sie das später über diesen Link http://support.kaspersky.com/interactive/google/de/kisplugin nachholen.

- Bei einer Aktualisierung des Browsers werden die Plug-ins nicht automatisch aktiviert, wenn die neue Browser-Version nicht das gleiche Aktivierungsverfahren für Plug-ins unterstützt wie die Vorgängerversion. Unterstützt die neue Browser-Version das gleiche Aktivierungsverfahren für Plug-ins wie die Vorgängerversion, so werden die Plug-ins automatisch aktiviert.

Wenn die Plug-ins beim Neustart des Browsers nicht automatisch aktiviert wurden, müssen sie manuell gestartet werden. Sie können in den Browser-Einstellungen nachsehen, ob die Plug-ins aktiviert sind, und die Plug-ins bei Bedarf manuell aktivieren. Informationen über die Plug-in-Aktivierung finden Sie in der Hilfe zu Ihrem Browser.

Sie können die automatische Plug-in-Aktivierung (s. Abschnitt "Automatische Aktivierung von Plug-ins für Sicheren Zahlungsverkehr aktivieren" auf S. 54) im Programmkonfigurationsfenster aktivieren oder deaktivieren.

Der Sichere Browser kann nicht gestartet werden, wenn das Kontrollkästchen **Selbstschutz aktivieren** deaktiviert ist, das sich im Abschnitt **Erweiterte Einstellungen**, Unterabschnitt **Selbstschutz** im Programmkonfigurationsfenster befindet.

IN DIESEM ABSCHNITT

EINSTELLUNGEN FÜR DEN SICHEREN ZAHLUNGSVERKEHR ANPASSEN

Um den Sicheren Zahlungsverkehr anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Hauptfensters auf den Link **Einstellungen**, um den Abschnitt **Einstellungen** zu öffnen.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Schutz** aus.
4. Wählen Sie im Abschnitt **Schutz** rechts den Unterabschnitt **Sicherer Zahlungsverkehr** aus.

   Dieses Fenster enthält Einstellungen für die Komponente Sicherer Zahlungsverkehr.
5. Aktivieren Sie die Komponente Sicherer Zahlungsverkehr mithilfe des Schalters im oberen Fensterbereich.
6. Aktivieren Sie das Kontrollkästchen **Schwachstellen des Betriebssystems melden**, damit vor dem Start des Sicheren Browsers gegebenenfalls eine Benachrichtigung über im Betriebssystem gefundene Schwachstellen erfolgt.

SICHEREN ZAHLUNGSVERKEHR FÜR EINE BESTIMMTE WEBSEITE ANPASSEN

Um den Sicheren Zahlungsverkehr für eine bestimmte Webseite anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf **Sicherer Zahlungsverkehr**.

   Das Fenster **Sicherer Zahlungsverkehr** wird geöffnet.
3. Klicken Sie auf **Webseite zum Sicheren Zahlungsverkehr hinzufügen**.

   In den Feldern im rechten Fensterbereich können Informationen über die Webseite hinzugefügt werden.
4. Geben Sie im Feld **Website für Sicheren Zahlungsverkehr** die Adresse der Webseite an, die im Sicheren Browser geöffnet werden soll.

   Der Adresse einer Webseite muss das Protokoll https:// vorangestellt sein. Dieses Protokoll wird standardmäßig vom Sicheren Browser verwendet.
5. Im Feld **Beschreibung** kann der Name oder eine Beschreibung für diese Webseite angegeben werden.
6. Wählen Sie aus, auf welche Weise der Sichere Browser beim Öffnen dieser Webseite gestartet werden soll:
   - Wenn die Webseite immer im Sicheren Browser gestartet werden soll, wählen Sie die Variante **Sicheren Browser starten**.
   - Damit Kaspersky Total Security fragt, welche Aktion beim Öffnen der Webseite ausgeführt werden soll, wählen Sie die Variante **Aktion erfragen**.
   - Um den Sicheren Zahlungsverkehr für diese Webseite zu deaktivieren, wählen Sie die Variante **Sicheren Browser nicht starten**.
7. Klicken Sie im rechten Fensterbereich auf **Hinzufügen**.

Die Webseite wird in der Liste im linken Fensterbereich angezeigt.

AUTOMATISCHE AKTIVIERUNG VON PLUG-INS FÜR SICHEREN ZAHLUNGSVERKEHR AKTIVIEREN

Gehen Sie folgendermaßen vor, um die Aktivierung von Plug-ins für Sicheren Zahlungsverkehr in Browsern zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Hauptfensters auf den Link **Einstellungen**, um den Abschnitt **Einstellungen** zu öffnen.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Schutz** aus.
4. Wählen Sie im Abschnitt **Schutz** rechts den Abschnitt **Web-Anti-Virus** aus.
5. Öffnen Sie im folgenden Fenster **Web-Anti-Virus-Einstellungen** über den Link **Erweiterte Einstellungen** das Fenster **Erweiterte Einstellungen für Web-Anti-Virus**.
6. Aktivieren Sie im Abschnitt **Plug-ins für Webbrowser** das Kontrollkästchen **Plug-ins für das Programm automatisch in allen Webbrowsern aktivieren**.

SCREENSHOT-SCHUTZ

Kaspersky Total Security hindert Spyware-Programme daran, unerlaubte Screenshots zu erstellen. Dadurch sind Ihre Daten bei der Verwendung von geschützten Webseiten sicher. Der Screenshot-Schutz ist standardmäßig aktiviert. Wenn der Schutz manuell deaktiviert wurde, können Sie ihn im Programmkonfigurationsfenster aktivieren (s. Abschnitt "Screenshot-Schutz aktivieren" auf S. 54).

Für den Screenshot-Schutz verwendet Kaspersky Total Security ein Hypervisor-Verfahren. Für Microsoft Windows 8 x64 besitzt die Funktionalität für den Screenshot-Schutz mithilfe des Hypervisors von Kaspersky Total Security folgende Einschränkungen:

- Die Funktionalität ist nicht verfügbar, wenn der Hypervisor eines Drittprogramms gestartet wird, z. B. der Hypervisor von Virtualisierungsprogrammen der Firma VMware™. Nachdem der Hypervisor des Drittprogramms beendet wurde, ist die Funktionalität des Screenshot-Schutzes wieder verfügbar.
- Die Funktionalität steht nicht zur Verfügung, wenn die Hardware-Virtualisierung von der CPU Ihres Computers nicht unterstützt wird. Informationen darüber, ob der Prozessor Ihres Computers die Hardware-Virtualisierung unterstützt, finden Sie in der technischen Dokumentation Ihres Computers oder auf der Webseite des Prozessor-Herstellers.
- Die Funktionalität ist nicht verfügbar, wenn beim Start des Sicheren Browsers ein laufender Drittprogramm-Hypervisor gefunden wird, z. B. der Hypervisor eines Programms der Firma VMware.

SCREENSHOT-SCHUTZ AKTIVIEREN

Um den Screenshot-Schutz zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf den Link **Einstellungen**, um den Abschnitt **Einstellungen** zu öffnen.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Schutz** aus.
4. Wählen Sie im Abschnitt **Schutz** rechts den Unterabschnitt **Sicherer Zahlungsverkehr** aus und vergewissern Sie sich, dass der Schalter für den Sicheren Zahlungsverkehr aktiviert ist.

   Das Fenster **Einstellungen für Sicheren Zahlungsverkehr** wird geöffnet.
5. Aktivieren Sie im Block **Erweitert** das Kontrollkästchen **Erstellen von Screenshots im Sicheren Browser blockieren**.

SCHUTZ VON DATEN IN DER ZWISCHENABLAGE

Kaspersky Total Security blockiert den unberechtigten Zugriff von Programmen auf die Zwischenablage während der Durchführung von Zahlungsvorgängen und verhindert so den Datendiebstahl durch Betrüger. Die Blockierung gilt nur, wenn nicht vertrauenswürdige Programme versuchen, unberechtigterweise auf die Zwischenablage zuzugreifen. Wenn Sie manuell Daten aus einem Programmfenster in ein anderes Programmfenster kopieren (beispielsweise aus Notepad in das Fenster eines Texteditors), ist der Zugriff auf die Zwischenablage erlaubt. Wenn Daten aus dem Browser Internet Explorer kopiert werden und dieser Browser im normalen Modus läuft, so können nur Daten aus der Adressleiste des Browsers in die Zwischenablage kopiert werden.

KASPERSKY PASSWORD MANAGER STARTEN

Das Programm Kaspersky Password Manager kann Kennwörter sicher speichern und zwischen allen Ihren Geräten synchronisieren. Kaspersky Password Manager muss unabhängig von Kaspersky Total Security installiert werden. Nach der Installation können Sie Kaspersky Password Manager entweder aus dem **Startmenü** oder aus dem Fenster von Kaspersky Total Security starten..

- *Um Kaspersky Password Manager zu starten, wenn dieses Programm bereits installiert ist, gehen Sie wie folgt vor:*

  1. Öffnen Sie das Programmhauptfenster von Kaspersky Total Security.
  2. Klicken Sie auf **Password Manager**.

  Das Programmfenster von Kaspersky Password Manager wird geöffnet.

- *Um Kaspersky Password Manager zu laden, wenn dieses Programm noch nicht installiert ist, gehen Sie wie folgt vor:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie auf **Password Manager**.

     Das Fenster **Password Manager** wird geöffnet.
  3. Klicken Sie im Fenster **Password Manager** auf **Laden**.

     Die Kaspersky-Lab-Webseite wird geöffnet. Von dort können Sie das Installationspaket für Kaspersky Password Manager herunterladen.

  Informationen zur Verwendung von Kaspersky Password Manager finden Sie im *Benutzerhandbuch zu Kaspersky Password Manager*.

SICHERHEIT EINER WEBSEITE ÜBERPRÜFEN

Kaspersky Total Security kann die Sicherheit einer Webseite überprüfen, bevor ein Link auf dieser Webseite geöffnet wird. Für die Untersuchung von Webseiten wird das *Modul zur Link-Untersuchung* eingesetzt, das zur Komponente Web-Anti-Virus gehört.

Das Modul zur Link-Untersuchung ist im Browser Microsoft Internet Explorer (Version 10 und 11) im Windows-8-Design nicht verfügbar.

Das Modul zur Link-Untersuchung wird in die Browser Microsoft Internet Explorer, Google Chrome und Mozilla Firefox integriert und untersucht die Links auf einer Webseite, die im Browser geöffnet wird. Kaspersky Total Security zeigt neben jedem Link eines der folgenden Symbole an:

- – Wenn die Webseite, auf die ein Link verweist, nach den Angaben von Kaspersky Lab sicher ist.
- – Wenn keine Informationen über die Sicherheit der Webseite vorliegen, auf die ein Link verweist.
- – Wenn die Webseite, auf die ein Link verweist, nach den Angaben von Kaspersky Lab gefährlich ist.

Wenn mit der Maus auf ein Symbol gezeigt wird, erscheint ein Pop-up-Fenster mit einer ausführlichen Beschreibung des Links.

Kaspersky Total Security untersucht standardmäßig nur die Links in Suchergebnissen. Die Untersuchung kann für Links auf allen Webseiten aktiviert werden.

Um die Untersuchung für Links auf Webseiten anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Hauptfenster auf den Link **Einstellungen**, um das Fenster **Einstellungen** zu öffnen.
3. Wählen Sie im Abschnitt **Schutz** den Unterabschnitt **Web-Anti-Virus** aus.

   Dieses Fenster enthält Einstellungen für Web-Anti-Virus.
4. Öffnen Sie mit dem Link **Erweiterte Einstellungen** im unteren Fensterbereich das Fenster mit erweiterten Einstellungen für Web-Anti-Virus.
5. Aktivieren Sie im Abschnitt **Modul zur Link-Untersuchung** das Kontrollkästchen **Links untersuchen**.
6. Damit Web-Anti-Virus den Inhalt aller Webseiten untersucht, wählen Sie die Variante **Auf allen Webseiten, außer den festgelegten** aus.

   Geben Sie bei Bedarf die Webseiten an, denen Sie vertrauen. Verwenden Sie dazu den Link **Ausnahmen anpassen**. Der Inhalt der angegebenen Webseiten sowie verschlüsselte Verbindungen mit den angegebenen Webseiten werden von Web-Anti-Virus nicht untersucht.
7. Damit Web-Anti-Virus nur den Inhalt bestimmter Webseiten untersucht, gehen Sie wie folgt vor:
   a. Wählen Sie die Variante **Nur auf den festgelegten Webseiten** aus.
   b. Klicken Sie auf den Link **Zu untersuchende Webseiten anpassen**.
   c. Klicken Sie im folgenden Fenster **Zu untersuchende Webseiten anpassen** auf **Hinzufügen**.
   d. Tragen Sie im folgenden Fenster **URL hinzufügen** die Adresse einer Webseite ein, deren Inhalt untersucht werden soll.
   e. Wählen Sie einen Untersuchungsstatus für die Webseite (*Aktiv* - Web-Anti-Virus untersucht den Inhalt der Webseite).
   f. Klicken Sie auf **Hinzufügen**.

      Die angegebene Webseite erscheint auf der Liste im Fenster **Zu untersuchende Adressen**. Web-Anti-Virus untersucht die Links auf dieser Webseite.
8. Um erweiterte Einstellungen für die Link-Untersuchung vorzunehmen, klicken Sie im Fenster **Erweiterte Einstellungen für Web-Anti-Virus** unter **Modul zur Link-Untersuchung** auf den Link **Modul zur Link-Untersuchung anpassen**.

   Das Fenster **Modul zur Link-Untersuchung anpassen** wird geöffnet.
9. Damit Web-Anti-Virus auf allen Webseiten vor unsicheren Links warnt, wählen Sie im Abschnitt **Zu untersuchende Links** die Variante **Alle Links** aus.
10. Damit Web-Anti-Virus darüber informiert, zu welcher inhaltlichen Kategorie für Webseiten (z. B. *Schimpfwörter*) ein Link gehört, gehen Sie wie folgt vor:
    a. Aktivieren Sie das Kontrollkästchen **Informationen über Kategorien für Webseiten-Inhalte anzeigen**.
    b. Aktivieren Sie die Kontrollkästchen für die Inhaltskategorien von Webseiten, über die in einer Anmerkung informiert werden soll.

Web-Anti-Virus untersucht die Links auf den angegebenen Webseiten und informiert über die Link-Kategorien. Dabei gelten die festgelegten Einstellungen.

SCHUTZ VOR BANNERN BEIM BESUCH VON WEBSEITEN

Die Komponente Anti-Banner schützt vor Bannern im Internet. Wenn die Komponente aktiviert ist, können Sie die Banneranzeige entweder direkt auf einer Webseite deaktivieren oder eine Webadresse oder Maske angeben, für die Kaspersky Total Security die Banneranzeige blockieren soll. Kaspersky Total Security schützt standardmäßig vor den Bannertypen, die am häufigsten vorkommen.

IN DIESEM ABSCHNITT

KOMPONENTE ANTI-BANNER AKTIVIEREN

Um die Komponente Anti-Banner zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Wechseln Sie mit dem Link **Einstellungen** ins Fenster **Einstellungen**.
3. Gehen Sie zum Abschnitt **Schutz**.
4. Aktivieren Sie die Komponente **Anti-Banner**.

ANZEIGE EINES BANNERS AUF EINER WEBSEITE DEAKTIVIEREN

Um die Anzeige eines Banners auf einer Webseite zu deaktivieren, gehen Sie wie folgt vor:

1. Wenn Sie sich auf der betreffenden Webseite befinden, zeigen Sie mit dem Mauszeiger auf das Banner, das blockiert werden soll.
2. Drücken Sie die Taste **STRG**.
3. Wählen Sie im folgenden Menü den Punkt **Zu Anti-Banner hinzufügen** aus.

   Das Fenster **Verbotene Webadressen** wird geöffnet.
4. Klicken Sie im Fenster **Verbotene Webadressen** auf **Hinzufügen**.

   Die Banneradresse wird zur Liste der verbotenen Webadressen hinzugefügt.
5. Aktualisieren Sie die Webseite im Webbrowser, damit das Banner nicht mehr angezeigt wird.

Wenn Sie diese Webseite künftig öffnen, wird das Banner nicht mehr angezeigt.

ANZEIGE ALLER BANNER AUF EINER WEBSEITE DEAKTIVIEREN

Sie können die Anzeige aller Banner auf einer bestimmten Webseite deaktivieren. Dazu wird eine Maske dieser Webseite festgelegt und zur Liste der verbotenen Webadressen hinzugefügt.

Um die Anzeige aller Banner auf einer Webseite zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Wechseln Sie mit dem Link **Einstellungen** ins Fenster **Einstellungen**.
3. Gehen Sie zum Abschnitt **Schutz**.
4. Wählen Sie die Komponente **Anti-Banner** aus.

   Das Fenster **Anti-Banner-Einstellungen** wird geöffnet.
5. Klicken Sie im Fenster **Anti-Banner-Einstellungen** auf den Link **Verbotene Webadressen anpassen**, um das Fenster **Verbotene Webadressen** zu öffnen.
6. Klicken Sie im Fenster **Verbotene Webadressen** auf **Hinzufügen**.
7. Tragen Sie im folgenden Fenster im Feld **Maske für Webadresse (URL)** die Maske der Webseite ein, auf der die Banneranzeige deaktiviert werden soll. Beispiel: `http://example.com*`.
8. Geben Sie für diese Webseite den Status **Aktiv** an.
9. Klicken Sie auf **Hinzufügen**.

Kaspersky Total Security blockiert künftig Banner auf der Seite http://example.com.

AKTIVITÄTSSPUREN AUF DEM COMPUTER UND IM INTERNET LÖSCHEN

Während der Arbeit auf dem Computer werden die Aktionen des Benutzers im Betriebssystem registriert. Dabei werden folgende Informationen gespeichert:

- Daten über Suchanfragen des Benutzers und über besuchte Webseiten
- Angaben über den Start von Programmen, Daten über das Öffnen und Speichern von Dateien
- Einträge im Systembericht von Microsoft Windows
- Sonstige Informationen über Benutzeraktionen

Angaben über Benutzeraktionen, die sensible Informationen enthalten, können Angreifern und Dritten zugänglich sein.

Kaspersky Total Security bietet einen Assistenten, der die Aktivitätsspuren des Benutzers im Betriebssystem löschen kann.

Gehen Sie folgendermaßen vor, den Assistenten zum Löschen von Aktivitätsspuren zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Zusätzliche Tools anzeigen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie im Fenster **Tools** links auf den Link **Löschen von Aktivitätsspuren**, um den Assistenten zum Löschen von Aktivitätsspuren zu starten.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Details zu den einzelnen Schritten des Assistenten.

Schritt 1. Assistent starten

Vergewissern Sie sich, dass die Variante **Suche nach Aktivitätsspuren des Benutzers ausführen** ausgewählt wurde, und klicken Sie auf **Weiter**, um den Assistenten zu starten.

Schritt 2. Suche von Aktivitätsspuren

Der Assistent führt auf Ihrem Computer die Suche nach Aktivitätsspuren aus. Die Suche kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für das Löschen von Aktivitätsspuren wählen

Nach dem Abschluss der Suche informiert der Assistent über gefundene Aktivitätsspuren und über Aktionen, mit denen diese Spuren beseitigt werden können (s. Abb. unten).

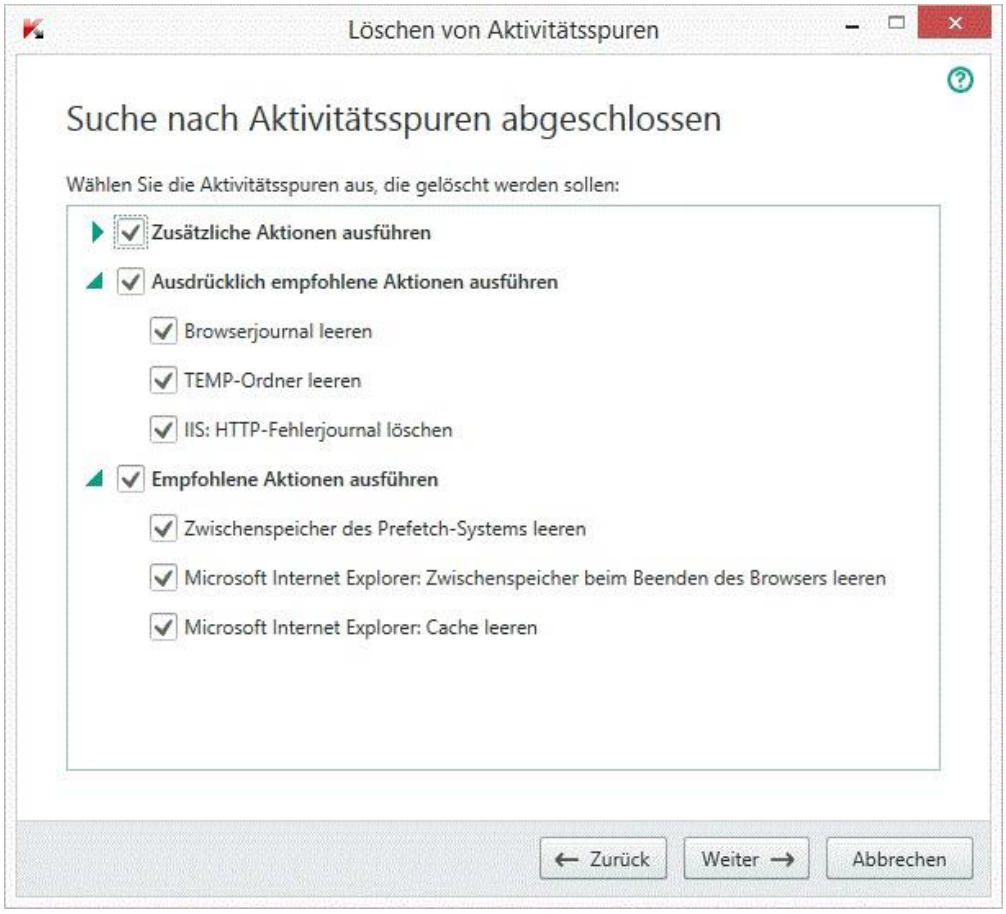

Abbildung 4. Erkannte Aktivitätsspuren und Empfehlungen zu deren Beseitigung

Um die Aktionen für eine Gruppe anzuzeigen, klicken Sie links vom Gruppennamen auf das Symbol ▸.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen.

Es wird davor gewarnt, die standardmäßig angekreuzten Kontrollkästchen zu deaktivieren. Dadurch kann die Sicherheit Ihres Computers bedroht werden.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Aktivitätsspuren löschen

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Das Löschen von Aktivitätsspuren kann eine gewisse Zeit beanspruchen. Um bestimmte Aktivitätsspuren zu löschen, kann ein Neustart des Computers erforderlich sein. Darüber werden Sie vom Assistenten informiert.

Nach Abschluss des Vorgangs wechselt der Assistent automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

KONTROLLE ÜBER DIE AKTIVITÄTEN DER BENUTZER AUF DEM COMPUTER UND IM INTERNET

Dieser Abschnitt informiert darüber, wie Kaspersky Total Security die Aktionen eines Benutzers auf dem Computer und im Internet überwacht.

IN DIESEM ABSCHNITT

KINDERSICHERUNG VERWENDEN

Die *Kindersicherung* bietet Kontrolle über die Aktionen unterschiedlicher Benutzer auf einem Computer und im Netzwerk. Mithilfe der Kindersicherung können Sie den Zugriff auf Internet-Ressourcen und Programme beschränken und Berichte über die Benutzeraktionen anzeigen.

Die Zahl der Kinder und Jugendlichen, die Zugang zu Computern und zum Internet besitzen, nimmt kontinuierlich zu. Bei der Verwendung eines Computers und des Internets droht Kindern eine ganze Reihe von Gefahren:

- Zeitverlust und / oder Geldverlust beim Besuch von Chats, Online-Spielen, Online-Shops und Auktionen.
- Zugriff auf Webressourcen, die für Erwachsene bestimmt sind (z. B. Seiten, die pornografische oder extremistische Materialien enthalten, die Themen wie Waffen, Drogen und Gewalt betreffen).
- Download von infizierten Dateien.
- Unverhältnismäßig lange Verwendung des Computers und damit verbundene gesundheitliche Risiken.
- Kontakte mit Fremden, die sich als Gleichaltrige ausgeben und persönliche Informationen über ein Kind erhalten können (beispielsweise echter Name, Adresse, Zeiträume, in denen niemand zu Hause ist).

Die Kindersicherung erlaubt es, die mit der Arbeit am Computer und im Internet verbundenen Risiken zu reduzieren. Dazu dienen folgende Funktionen:

- Zeitliche Beschränkung für die Verwendung des Computers und Internets.
- Erstellen von Listen für zum Start erlaubte und verbotene Spiele und Anwendungen sowie vorübergehende Beschränkung des Starts von erlaubten Programmen.

- Erstellen von Listen mit Webseiten, auf die der Zugriff erlaubt bzw. verboten ist. Auswahl von inhaltlichen Kategorien für Webressourcen, die nicht zur Ansicht empfohlen sind.
- Aktivieren des Modus zur sicheren Suche mit Suchmaschinen (Links zu Webseiten mit verdächtigem Inhalt werden nicht in den Suchergebnissen angezeigt).
- Beschränkung des Downloads von Dateien aus dem Internet.
- Erstellen von Listen mit Kontakten, für die Konversationen über Instant Messenger und in sozialen Netzwerken erlaubt oder verboten werden.
- Anzeige des Texts von Konversationen in Instant Messengern und sozialen Netzwerken.
- Verbot des Sendens von bestimmten persönlichen Daten.
- Suche nach bestimmten Schlüsselwörtern im Nachrichtentext.

Die Funktionen der Kindersicherung lassen sich für jedes Benutzerkonto auf dem Computer separat anpassen. Außerdem stehen für die Kindersicherung Berichte über die Aktivitäten der überwachten Computernutzer bereit.

ZU DEN EINSTELLUNGEN FÜR DIE KINDERSICHERUNG WECHSELN

Gehen Sie wie folgt vor, um zur Anpassung der Einstellungen für die Kindersicherung zu wechseln:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Programmhauptfenster auf die Schaltfläche **Kindersicherung**.
3. Beim ersten Aufruf des Fensters **Kindersicherung** schlägt das Programm vor, zum Schutz der Einstellungen für die Kindersicherung ein Kennwort anzulegen. Wählen Sie eine der vorgeschlagenen Funktionsvarianten:
   - Wenn Sie den Zugriff auf die Einstellungen für die Kindersicherung durch ein Kennwort schützen möchten, füllen Sie die Felder **Kennwort** und **Bestätigung** aus und klicken Sie auf die Schaltfläche **Fortsetzen**.
   - Wenn Sie den Zugriff auf die Einstellungen für die Kindersicherung nicht durch eine Kennwort schützen möchten, wechseln Sie über den Link **Überspringen** auf die Anpassung der Einstellungen für die Kindersicherung.

   Das Fenster **Kindersicherung** wird geöffnet.
4. Wählen Sie ein Benutzerkonto aus und wechseln Sie mit dem Link **Beschränkungen anpassen** ins Konfigurationsfenster für die Kindersicherung.

KONTROLLE ÜBER DIE VERWENDUNG DES COMPUTERS

Mit der Kindersicherung kann festgelegt werden, wie lange ein Benutzer den Computer verwenden darf. Sie können einen Zeitraum festlegen, in dem der Zugriff auf den Computer gesperrt werden soll (Nachtruhe), und die tägliche Gesamtdauer für die Verwendung des Computers beschränken. Für Werktage und für das Wochenende sind unterschiedliche Beschränkungen möglich.

Um eine Zeitbeschränkung für die Verwendung des Computers anzupassen, gehen Sie wie folgt vor:

1. Wechseln Sie zum Einstellungsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 62).
2. Wählen Sie im Einstellungsfenster für die Kindersicherung den Abschnitt **Computer**.

3. Um einen Zeitraum festzulegen, in dem die Kindersicherung den Zugriff auf den Computer sperren soll, aktivieren Sie in den Abschnitten **Werktage** und **Wochenende** das Kontrollkästchen **Zugriff sperren von**.

4. Legen Sie in der Dropdown-Liste neben dem Kontrollkästchen **Zugriff sperren von** den Beginn der Sperre fest.

5. Geben Sie in der Dropdown-Liste **bis** das Ende der Sperre an.

   Der Zeitplan für die Verwendung des Computers kann auch mithilfe einer Tabelle erstellt werden. Die Tabelle wird durch Klick auf die Schaltfläche  geöffnet.

   Der Zugriff auf den Computer wird für den Benutzer im festgelegten Zeitraum gesperrt.

6. Um die Gesamtdauer für die Verwendung des Computers zu beschränken, aktivieren Sie in den Abschnitten **Werktage** und **Wochenende** die Kontrollkästchen **Zugriff erlauben für höchstens** und wählen Sie in der Dropdown-Liste neben den Kontrollkästchen eine Zeitspanne aus.

   Der Zugriff auf den Computer wird für den Benutzer gesperrt, wenn das tägliche Limit für die Computernutzung überschritten wird.

7. Um für einen Benutzer Pausen bei der Computernutzung festzulegen, aktivieren Sie im Abschnitt **Erholungspausen** das Kontrollkästchen **Pause einlegen alle** und wählen Sie in den Dropdown-Listen neben dem Kontrollkästchen ein Intervall (z. B. jede Stunde) und eine Dauer (z. B. 10 Minuten) für die Pausen aus.

8. Aktivieren Sie im Fenster **Kindersicherung** die Optionsschaltfläche **Kindersicherung**, die sich neben dem entsprechenden Benutzerkonto befindet.

Der Zugriff auf den Computer wird für den Benutzer gemäß den festgelegten Einstellungen gesperrt.

KONTROLLE ÜBER DIE VERWENDUNG DES INTERNETS

Mithilfe der Kindersicherung können Sie die Verwendungsdauer für das Internet beschränken und einem Benutzer den Zugriff auf bestimmte Webseiten-Kategorien und festgelegte Webseiten verbieten. Außerdem kann einem Benutzer verboten werden, bestimmte Dateitypen (z. B. Archive oder Video) aus dem Internet herunterzuladen.

- *Um die Verwendungsdauer für das Internet zu beschränken, gehen Sie wie folgt vor:*

  1. Wechseln Sie zum Einstellungsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 62).

  2. Wählen Sie im Einstellungsfenster für die Kindersicherung den Abschnitt **Internet**.

  3. Um die Gesamtdauer für die Internetnutzung an Werktagen zu beschränken, aktivieren Sie im Abschnitt **Beschränkung des Internetzugriffs** das Kontrollkästchen **Zugriff an Werktagen beschränken auf <hh:mm> Stunde(n) pro Tag** und wählen Sie in der Dropdown-Liste neben dem Kontrollkästchen eine Zeitbeschränkung aus.

  4. Um die Gesamtdauer für die Internetnutzung am Wochenende zu beschränken, aktivieren Sie das Kontrollkästchen **Zugriff am Wochenende beschränken auf <hh:mm> Stunde(n) pro Tag** und wählen Sie in der Dropdown-Liste neben dem Kontrollkästchen eine Zeitbeschränkung aus.

  5. Aktivieren Sie im Fenster **Kindersicherung** die Optionsschaltfläche **Kindersicherung**, die sich neben dem entsprechenden Benutzerkonto befindet.

  Die Kindersicherung beschränkt die Gesamtdauer, für die der Benutzer das Internet nutzen darf, gemäß den festgelegten Werten.

- *Um den Besuch bestimmter Webseiten einzuschränken, gehen Sie wie folgt vor:*

  1. Wechseln Sie zum Einstellungsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 62).

  2. Wählen Sie im Einstellungsfenster für die Kindersicherung den Abschnitt **Internet**.

3. Damit in den Suchergebnissen keine Inhalte aus der Kategorie "für Erwachsene" angezeigt werden, aktivieren Sie im Abschnitt **Kontrolle des Besuchs von Webseiten** das Kontrollkästchen **Sichere Suche aktivieren**.

   Wenn auf Webseiten wie Google™, YouTube™ (nur für Benutzer, die nicht auf der Seite youtube.com angemeldet sind), Bing®, Yahoo!™, Mail.ru, VK oder Yandex nach Informationen gesucht wird, werden Ergebnisse mit "Inhalten für Erwachsene" nicht angezeigt.

4. Um den Zugriff auf bestimmte Webseiten-Kategorien zu verbieten, gehen Sie wie folgt vor:

   a. Aktivieren Sie im Abschnitt **Kontrolle des Besuchs von Webseiten** das Kontrollkästchen **Zugriff auf folgende Webseiten blockieren**.

   b. Wählen Sie die Variante **Webseiten für Erwachsene** und öffnen Sie mit dem Link **Webseiten-Kategorien wählen** das Fenster **Zugriff auf Webseiten-Kategorien sperren**.

   c. Aktivieren Sie die Kontrollkästchen für die Webseiten-Kategorien, die gesperrt werden sollen.

      Die Kindersicherung sperrt für den Benutzer alle Webseiten, deren Inhalt zu einer verbotenen Kategorie gehört.

5. Um den Zugriff auf bestimmte Webseiten zu verbieten, gehen Sie wie folgt vor:

   a. Aktivieren Sie im Abschnitt **Kontrolle des Besuchs von Webseiten** das Kontrollkästchen **Zugriff auf folgende Webseiten blockieren**.

   b. Wählen Sie die Variante **Alle Webseiten, außer den durch die Ausnahmeliste erlaubten Seiten** und öffnen Sie mit dem Link **Ausnahmen hinzufügen** das Fenster **Ausnahmen**.

   c. Klicken Sie im unteren Fensterbereich auf **Hinzufügen**.

      Das Fenster **Neue Webseite hinzufügen** wird geöffnet.

   d. Tragen Sie im Feld **Maske für Webseite** die Adresse einer Webseite ein, deren Besuch verboten werden soll.

   e. Legen Sie im Abschnitt **Geltungsbereich** einen Geltungsbereich für das Verbot fest: Gesamte Website oder Nur die angegebene Webseite.

   f. Um den Besuch einer bestimmten Webseite zu verbieten, wählen Sie im Abschnitt **Aktion** die Variante **Verbieten**.

   g. Klicken Sie auf **Hinzufügen**.

   Die angegebene Webseite erscheint auf der Liste im Fenster **Ausnahmen**.

6. Aktivieren Sie im Fenster **Kindersicherung** die Optionsschaltfläche **Kindersicherung**, die sich neben dem entsprechenden Benutzerkonto befindet.

Die Kindersicherung sperrt den Besuch von Webseiten, die auf der Liste stehen. Dabei gelten die festgelegten Einstellungen.

➡ *Um den Download von bestimmten Dateitypen aus dem Internet zu verbieten, gehen Sie wie folgt vor:*

1. Wechseln Sie zum Einstellungsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 62).

2. Wählen Sie im Einstellungsfenster für die Kindersicherung den Abschnitt **Internet**.

3. Aktivieren Sie im Abschnitt **Verbot des Downloads von Dateien** die Kontrollkästchen für jene Dateitypen, deren Download blockiert werden soll.

4. Aktivieren Sie im Fenster **Kindersicherung** die Optionsschaltfläche **Kindersicherung**, die sich neben dem entsprechenden Benutzerkonto befindet.

Die Kindersicherung sperrt den Download der angegebenen Dateitypen aus dem Internet.

KONTROLLE ÜBER DEN START VON SPIELEN UND PROGRAMMEN

Mithilfe der Kindersicherung können Sie für einen Benutzer den Start von Spielen erlauben oder verbieten. Dabei werden die Altersgruppen der Spiele berücksichtigt. Außerdem können Sie einem Benutzer den Start bestimmter Programme verbieten (z. B. Spiele und Instant Messenger) oder die Verwendungsdauer für ein Programm beschränken.

- *Um den Start von Spielen zu verbieten, deren Inhalt nicht der Altersgruppe des Benutzers entspricht, gehen Sie wie folgt vor:*

1. Wechseln Sie zum Einstellungsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 62).
2. Wählen Sie im Einstellungsfenster für die Kindersicherung den Abschnitt **Programme**.
3. Verbieten Sie im Abschnitt **Spiele nach Inhalt sperren** den Start von Spielen, die im Hinblick auf das Alter und/oder den Inhalt nicht für den ausgewählten Benutzer geeignet sind:
    a. Um den Start aller Spiele zu sperren, deren Inhalt nicht der Altersgruppe des Benutzers entspricht, aktivieren Sie das Kontrollkästchen **Spiele nach Altersstufe sperren** und wählen Sie in der Dropdown-Liste neben dem Kontrollkästchen eine Altersgruppe aus.
    b. Um den Start von Spielen mit bestimmtem Inhalt zu sperren, gehen Sie wie folgt vor:
        a. Aktivieren Sie das Kontrollkästchen **Spiele aus Kategorien für Erwachsene sperren**.
        b. Öffnen Sie mit dem Link **Spiele-Kategorien wählen** das Fenster **Spiele nach Kategorien sperren**.
        c. Aktivieren Sie die Kontrollkästchen für die zu sperrenden Inhaltskategorien für Spiele.
4. Aktivieren Sie im Fenster **Kindersicherung** die Optionsschaltfläche **Kindersicherung**, die sich neben dem entsprechenden Benutzerkonto befindet.

- *Um den Start eines bestimmten Programms einzuschränken, gehen Sie wie folgt vor:*

1. Wechseln Sie zum Einstellungsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 62).
2. Wählen Sie im Einstellungsfenster für die Kindersicherung den Abschnitt **Programme**.
3. Öffnen Sie im unteren Teil des Fensters über den Link **Programm zur Liste hinzufügen** das Fenster **Öffnen** und wählen Sie die ausführbare Datei des Programms.

    Das ausgewählte Programm erscheint auf der Liste im Abschnitt **Folgende Programme sperren**. Kaspersky Total Security fügt die Anwendung automatisch einer bestimmten Kategorie wie z. B. *Spiele* hinzu.
4. Wenn Sie den Start eines Programms sperren möchten, aktivieren Sie in der Liste das Kontrollkästchen neben dem Namen des Programms. Sie können auch den Start aller Programme einer bestimmten Kategorie sperren. Aktivieren Sie dazu in der Liste das Kontrollkästchen neben dem Namen der Kategorie (Sie können beispielsweise die Kategorie *Spiele* sperren).
5. Wenn Sie die Verwendungsdauer für ein Programm beschränken möchten, wählen Sie in der Liste ein Programm oder eine Kategorie für Programme aus und öffnen Sie mit dem Link **Regeln anpassen** das Fenster **Verwendung des Programms einschränken**.
6. Wenn Sie die Verwendungsdauer eines Programms an Werktagen und am Wochenende beschränken möchten, aktivieren Sie in den Blöcken **Werktage** und **Wochenende** das Kontrollkästchen **Zugriff erlauben für höchstens** und geben Sie in der Dropdown-Liste an, für wie viele Stunden der Benutzer das Programm pro Tag verwenden darf. Außerdem können Sie mithilfe einer Tabelle exakt festlegen, in welchen Zeiträumen dem Benutzer die Verwendung eines Programms erlaubt bzw. verboten ist. Die Tabelle wird durch Klick auf die Schaltfläche  geöffnet.

7. Um Pausen für die Nutzung eines Programms festzulegen, aktivieren Sie im Abschnitt **Erholungspausen** das Kontrollkästchen **Pause einlegen alle** und wählen Sie in den Dropdown-Listen die Häufigkeit und Dauer für die Pausen aus.

8. Klicken Sie auf **Speichern**.

9. Aktivieren Sie im Fenster **Kindersicherung** die Optionsschaltfläche **Kindersicherung**, die sich neben dem entsprechenden Benutzerkonto befindet.

Die Kindersicherung verwendet die festgelegten Einschränkungen, wenn der Benutzer mit dem Programm arbeitet.

KONTROLLE ÜBER DIE KOMMUNIKATION IN SOZIALEN NETZWERKEN

Mithilfe der Kindersicherung können Sie die Konversationen eines Benutzers in sozialen Netzwerken und in Instant Messengern überwachen und den Nachrichtenaustausch mit bestimmten Kontakten sperren.

Um die Kontrolle über die Konversationen eines Benutzers anzupassen, gehen Sie wie folgt vor:

1. Wechseln Sie zum Einstellungsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 62).

2. Wählen Sie im Einstellungsfenster für die Kindersicherung den Abschnitt **IM-Konversationen**.

3. Um die Konversationen anzusehen und, falls erforderlich, bestimmte Kontakte zu sperren, gehen Sie wie folgt vor:

   a. Wählen Sie die Variante **Alle Konversationen verbieten, außer mit erlaubten bekannten Kontakten** aus.

   b. Klicken Sie auf den Link **Bekannte Kontakte**, um das Fenster **Bericht über Konversationen** zu öffnen.

   c. Hier sehen Sie die Kontakte, mit denen sich der Benutzer unterhalten hat. Die Kontakte können in diesem Fenster auf folgende Art angezeigt werden:

      - Um die Konversationen des Benutzers in einem bestimmten sozialen Netzwerk oder Instant Messenger anzuzeigen, wählen Sie das gewünschte Element aus der Dropdown-Liste im linken Fensterbereich aus.

      - Um die Kontakte anzuzeigen, mit denen sich der Benutzer am häufigsten unterhalten hat, wählen Sie in der Dropdown-Liste die Variante **Nach Anzahl der Nachrichten**.

      - Um die Kontakte anzuzeigen, mit denen sich der Benutzer an einem bestimmten Tag unterhalten hat, wählen Sie im rechten Fensterbereich in der Dropdown-Liste die Variante **Nach Konversationsdatum**.

   d. Um die Konversationen des Benutzers mit einem bestimmten Kontakt anzuzeigen, klicken Sie in der Liste auf diesen Kontakt.

      Das Fenster **Konversationsverlauf** wird geöffnet.

   e. Um die Konversationen des Benutzers mit dem ausgewählten Kontakt zu blockieren, klicken Sie auf **Konversationen verbieten**.

4. Aktivieren Sie im Fenster **Kindersicherung** die Optionsschaltfläche **Kindersicherung**, die sich neben dem entsprechenden Benutzerkonto befindet.

In diesem Fall sperrt die Kindersicherung den Nachrichtenaustausch zwischen dem Benutzer und dem ausgewählten Kontakt.

KONTROLLE ÜBER DEN INHALT VON KONVERSATIONEN

Mithilfe der Kindersicherung können Sie überwachen, ob ein Benutzer in seinen Konversationen bestimmte persönliche Daten (z. B. Nachnamen, Telefonnummern oder Kreditkartennummern) und Schlüsselwörter (z. B. Schimpfwörter) verwendet, und Sie können die Verwendung solcher Daten und Schlüsselwörter verbieten.

Um die Überwachung der Versendung von persönlichen Daten anzupassen, gehen Sie wie folgt vor:

1. Wechseln Sie zum Einstellungsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 62).
2. Wählen Sie im Einstellungsfenster für die Kindersicherung den Abschnitt **Inhaltskontrolle**.
3. Aktivieren Sie im Abschnitt **Senden persönlicher Daten überwachen** das Kontrollkästchen **Übertragung von persönlichen Daten an Dritte verbieten**.
4. Öffnen Sie mit dem Link **Liste persönlicher Daten bearbeiten** das Fenster **Liste persönlicher Daten**.
5. Klicken Sie im unteren Fensterbereich auf **Hinzufügen**.

   Im folgenden Fenster können persönliche Daten hinzugefügt werden.
6. Wählen Sie den Typ der persönlichen Daten (beispielsweise "Telefonnummer") über den entsprechenden Link aus oder geben Sie eine Beschreibung im Feld **Feldname** ein.
7. Geben Sie im Feld **Wert** die persönlichen Daten ein (z. B. Nachname oder Telefonnummer).
8. Klicken Sie auf **Hinzufügen**.

   Die Daten erscheinen auf der Liste im Fenster **Liste persönlicher Daten**.
9. Aktivieren Sie im Fenster **Kindersicherung** die Optionsschaltfläche **Kindersicherung**, die sich neben dem entsprechenden Benutzerkonto befindet.

Die Kindersicherung überwacht und sperrt die Verwendung der angegebenen persönlichen Daten in Konversationen, die über Instant Messenger oder über Webseiten erfolgen.

Um die Überwachung für die Verwendung von Schlüsselwörtern in Konversationen anzupassen, gehen Sie wie folgt vor:

1. Wechseln Sie zum Einstellungsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 62).
2. Wählen Sie im Einstellungsfenster für die Kindersicherung den Abschnitt **Inhaltskontrolle**.
3. Aktivieren Sie unter **Verwendung von Schlüsselwörtern kontrollieren** das Kontrollkästchen **Überwachung der Verwendung von Schlüsselwörtern aktivieren**.
4. Klicken auf den Link **Liste für Schlüsselwörter bearbeiten** um das Fenster **Verwendung von Schlüsselwörtern kontrollieren** zu öffnen.
5. Klicken Sie im unteren Fensterbereich auf **Hinzufügen**.

   Im folgenden Fenster kann ein Schlüsselwort hinzugefügt werden.
6. Tragen Sie im Feld **Wert** eine Schlüsselphrase ein und klicken Sie auf **Hinzufügen**.

   Die angegebene Schlüsselphrase erscheint auf der Liste für Schlüsselwörter im Fenster **Verwendung von Schlüsselwörtern kontrollieren**.
7. Aktivieren Sie im Fenster **Kindersicherung** die Optionsschaltfläche **Kindersicherung**, die sich neben dem entsprechenden Benutzerkonto befindet.

Die Kindersicherung sperrt bei Konversationen über das Internet und über Instant Messenger das Senden von Nachrichten, die eine festgelegte Schlüsselphrase enthalten.

BERICHT ÜBER DIE AKTIONEN EINES BENUTZERS ANZEIGEN

Sie können Berichte über die Aktionen jedes Benutzers ansehen, für den die Kindersicherung aktiviert wurde. Es sind Berichte für jede Kategorie der kontrollierten Ereignisse verfügbar.

Um einen Bericht über die Aktionen eines kontrollierten Benutzers anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie zum Einstellungsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 62).

2. Wählen Sie das Benutzerkonto des Benutzers und wechseln Sie über den Link **Bericht anzeigen** auf das Berichtsfenster.

3. Öffnen Sie im Abschnitt für die erforderliche Einschränkungsart (z. B. **Internet** oder **IM-Konversationen**) mithilfe des Links **Details** einen Bericht über die zu überwachenden Aktionen.

Dieses Fenster enthält einen Bericht über die zu überwachenden Aktionen des Benutzers.

FERNVERWALTUNG DES COMPUTERSCHUTZES

Dieser Abschnitt informiert darüber, wie Sie den Schutz Ihres Computers fernverwalten können, wenn das Programm Kaspersky Total Security darauf installiert ist.

IN DIESEM ABSCHNITT

ÜBER DIE FERNVERWALTUNG DES COMPUTERSCHUTZES

Wenn das Programm Kaspersky Total Security auf einem Computer installiert ist, können Sie den Schutz für diesen Computer verwalten. Die Fernverwaltung des Computerschutzes erfolgt über das Portal My Kaspersky. Um den Computerschutz fernzuverwalten, müssen Sie sich im Portal My Kaspersky registrieren, sich mit Ihrem Konto im Portal My Kaspersky anmelden und zum Abschnitt **Geräte** gehen.

Im Portal My Kaspersky können Sie folgende Aufgaben lösen, die der Sicherheit Ihres Computers dienen:

- Liste der auf dem Computer vorhandenen Sicherheitsprobleme anzeigen und diese Probleme ferngesteuert lösen
- Computer auf Viren und andere bedrohliche Programme untersuchen
- Datenbanken und Programm-Module aktualisieren
- Programmkomponenten von Kaspersky Total Security anpassen

Wenn die Untersuchung des Computers aus dem Portal My Kaspersky gestartet wurde, verarbeitet Kaspersky Total Security gefundene Objekte im automatischen ohne Ihre Teilnahme. Wenn ein Virus oder ein anderes bedrohliches Programm gefunden wird, versucht Kaspersky Total Security, die Desinfektion ohne einen Neustart des Computers auszuführen. Wenn die Desinfektion nicht ohne einen Neustart des Computers möglich ist, erscheint im Portal My Kaspersky auf Liste der Sicherheitsprobleme eine Meldung darüber, dass zur Desinfektion des Computers ein Neustart erforderlich ist.

ZUR FERNVERWALTUNG DES COMPUTERSCHUTZES WECHSELN

Um zur Fernverwaltung des Computerschutzes zu wechseln, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Online-Verwaltung**.
3. Klicken Sie im Fenster **Online-Verwaltung** auf **Computer mit dem Portal My Kaspersky verbinden**.

   Im Fenster **Online-Verwaltung** wird ein Formular für die Verbindung zum Portal My Kaspersky geladen, falls bisher noch keine Verbindung hergestellt wurde. Füllen Sie das Formular aus und melden Sie sich im Portal My Kaspersky an.

Im Standardbrowser wird die Seite des Portals My Kaspersky im Abschnitt **Geräte** geöffnet.

BETRIEBSSYSTEMRESSOURCEN FÜR COMPUTERSPIELE FREIGEBEN

Wenn Kaspersky Total Security und bestimmte Programme (insbesondere Computerspiele) gleichzeitig laufen, können im Vollbildmodus folgende Nachteile entstehen:

- Programme und Spiele werden aufgrund fehlender Systemressourcen verlangsamt.
- Die Meldungsfenster von Kaspersky Total Security lenken vom Spiel ab.

Sie können das Spielprofil verwenden, um die Einstellungen von Kaspersky Total Security vor dem Wechsel in den Vollbildmodus nicht jedes Mal manuell zu ändern. Wenn das Spielprofil aktiviert ist, werden beim Wechsel in den Vollbildmodus automatisch die Einstellungen aller Komponenten von Kaspersky Total Security so geändert, dass in diesem Modus eine optimale Arbeit gewährleistet wird. Bei Verlassen des Vollbildmodus werden für die Einstellungen des Programms die Werte wiederhergestellt, die vor dem Wechsel in den Vollbildmodus eingestellt waren.

Um die Verwendung des Profils für Spiele zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Hauptfensters auf den Link **Einstellungen**, um den Abschnitt **Einstellungen** zu öffnen.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Leistung**.

   Dieses Fenster enthält Einstellungen für die Leistung von Kaspersky Total Security.
4. Aktivieren Sie im Abschnitt **Profil für Spiele** das Kontrollkästchen **Spielprofil verwenden**.

MIT UNBEKANNTEN PROGRAMMEN ARBEITEN

Mithilfe von Kaspersky Total Security können Sie die Risiken reduzieren, die mit der Verwendung unbekannter Programme zusammenhängen (beispielsweise das Risiko einer Infektion des Computers durch Viren und andere Schadsoftware; Risiko von unerwünschten Veränderungen am Betriebssystem).

Kaspersky Total Security bietet folgende Komponenten und Tools, mit denen die Reputation eines Programms überprüft und die Programmaktivität auf Ihrem Computer kontrolliert werden kann.

IN DIESEM ABSCHNITT

REPUTATION EINES PROGRAMMS ÜBERPRÜFEN

Kaspersky Total Security kann für ein Programm die Reputation ermitteln, die auf Daten aus der ganzen Welt basiert. Die Reputation eines Programms umfasst folgende Kriterien:

- Name des Herstellers
- Informationen zur digitalen Signatur (verfügbar, wenn eine digitale Signatur vorhanden ist).
- Informationen zur Gruppe, in die ein Programm von der Programmkontrolle oder von der Mehrheit der Benutzer des Kaspersky Security Network eingeordnet wurde.
- Anzahl der Benutzer von Kaspersky Security Network, die ein Programm verwenden (verfügbar, wenn das Programm in der Datenbank des Kaspersky Security Network zur Gruppe Vertrauenswürdig gehört).
- Zeitraum, seit dem das Programm im Kaspersky Security Network bekannt ist.
- Länder, in denen ein Programm am häufigsten vorkommt.

Die Reputationsprüfung für ein Programm ist nur möglich, wenn Sie der Teilnahme an Kaspersky Security Network zugestimmt haben.

Um die Reputation eines Programms zu ermitteln,

öffnen Sie das Kontextmenü der ausführbaren Programmdatei und wählen Sie den Punkt **Reputation im KSN ansehen** aus (s. Abb. unten).

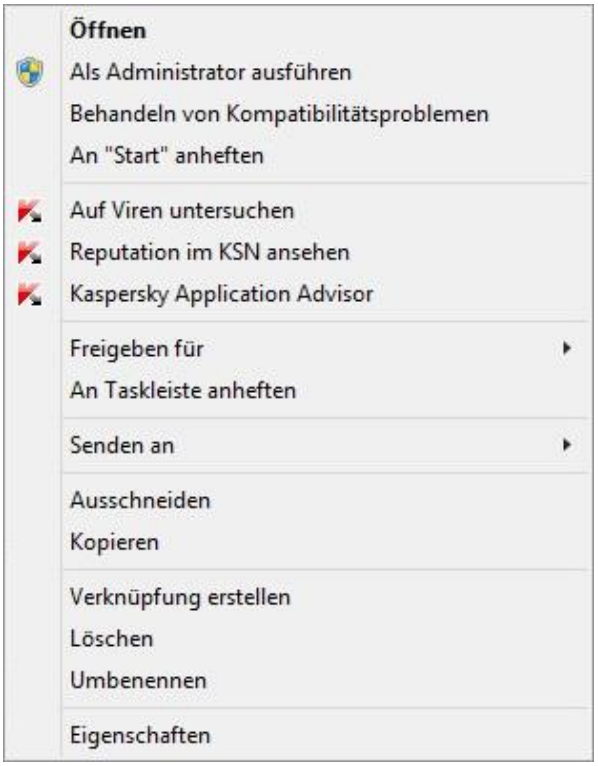

Abbildung 5. Kontextmenü des Objekts

Ein Fenster mit Angaben zur Reputation des Programms im KSN wird geöffnet.

SIEHE AUCH

Teilnahme an Kaspersky Security Network (KSN) 97

KONTROLLE DER AKTIONEN EINES PROGRAMMS AUF DEM COMPUTER UND IM NETZWERK

Die Programmkontrolle hindert Programme daran, Aktionen auszuführen, die das Betriebssystem gefährden können, und überwacht den Zugriff auf Betriebssystemressourcen und auf Ihre persönlichen Daten.

Die Programmkontrolle überwacht die Aktionen, die von auf dem Computer installierten Programmen im Betriebssystem ausgeführt werden, und reguliert die Aktivität der Programme nach entsprechenden Regeln. Diese Regeln regulieren verdächtige Aktivitäten von Programmen. Dazu zählt auch der Zugriff von Programmen auf geschützte Ressourcen (beispielsweise auf Dateien, Ordner, Registrierungsschlüssel und Netzwerkadressen).

Auf 64-Bit-Betriebssystemen können die Berechtigungen für Programme zum Ausführen folgender Aktionen nicht angepasst werden:

- Direkter Zugriff auf den physikalischen Speicher
- Verwaltung von Druckertreibern
- Erstellen eines Dienstes

- Öffnen eines Dienstes zum Lesen
- Öffnen eines Dienstes für Änderungen
- Ändern einer Dienst-Konfiguration
- Verwaltung eines Dienstes
- Starten eines Dienstes
- Löschen eines Dienstes
- Zugriff auf interne Browserdaten
- Zugriff auf kritische Objekte des Betriebssystems
- Zugriff auf den Kennwortspeicher
- Festlegen von Debugger-Rechten
- Verwendung von Programmschnittstellen des Betriebssystems
- Verwendung von Programmschnittstellen des Betriebssystems (DNS)

Auf einer 64-Bit-Version von Microsoft Windows 8 können außerdem die Berechtigungen für Programme zum Ausführen folgender Aktionen nicht angepasst werden:

- Senden von Fenstermeldungen an andere Prozesse
- Verdächtige Vorgänge
- Installation von Hooks
- Abfangen von eingehenden Ereignissen
- Erstellen von Screenshots

Die Netzwerkaktivität von Programmen wird von der Komponente Firewall überwacht.

Wenn ein Programm zum ersten Mal auf dem Computer gestartet wird, überprüft die Programmkontrolle die Sicherheit des Programms und verschiebt es in eine Gruppe (Vertrauenswürdig, Nicht vertrauenswürdig, Stark beschränkt oder Schwach beschränkt). Die Gruppe bestimmt die Regeln, die Kaspersky Total Security zur Aktivitätskontrolle dieses Programms verwenden wird.

Kaspersky Total Security verschiebt Programme nur dann in Sicherheitsgruppen (Vertrauenswürdig, Nicht vertrauenswürdig, Stark beschränkt oder Schwach beschränkt), wenn entweder die Komponente Programmkontrolle oder Firewall aktiviert ist, oder wenn beide Komponenten aktiviert sind. Wenn beide Komponenten deaktiviert sind, wird die Funktionalität, mit der Programme den Sicherheitsgruppen zugeordnet werden, nicht ausgeführt.

Die Kontrollregeln für Programmaktivitäten können manuell angepasst werden.

EINSTELLUNGEN FÜR DIE PROGRAMMKONTROLLE ANPASSEN

➡ *Um die Einstellungen für die Programmkontrolle anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Zusätzliche Tools anzeigen**, um das Fenster **Tools** zu öffnen.

3. Klicken Sie im Fenster **Tools** auf den Link **Programmkontrolle**, um das Fenster **Programmkontrolle** zu öffnen.

4. Klicken Sie im Fenster **Programmkontrolle** im Abschnitt **Programme** auf den Link **Programme verwalten**, um das Fenster **Programme verwalten** zu öffnen.

5. Wählen Sie das gewünschte Programm aus der Liste und öffnen Sie durch Doppelklicken das Fenster **Regeln für das Programm**.

   Das Fenster **Regeln für das Programm** wird geöffnet.

6. Legen Sie Regeln für die Programmüberwachung fest:

   - Gehen Sie folgendermaßen vor, um die Regeln für den Zugriff des Programms auf Betriebssystemressourcen anzupassen:

     a. Wählen Sie auf der Registerkarte **Dateien, Systemregistrierung** die entsprechende Ressourcenkategorie aus.

     b. Öffnen Sie durch Rechtsklick in der Spalte mit den für die Ressourcen möglichen Aktionen (**Lesen**, **Schreiben**, **Löschen** oder **Erstellen**) das Kontextmenü und wählen Sie dort den entsprechenden Wert aus (**Erlauben**, **Verbieten** oder **Aktion erfragen**).

   - Gehen Sie folgendermaßen vor, um die Rechte anzupassen, die dem Programm für die Ausführung bestimmter Aktionen im Betriebssystem zugewiesen werden:

     a. Wählen Sie auf der Registerkarte **Rechte** die entsprechende Rechtekategorie aus.

     b. Öffnen Sie durch Rechtsklick in der Spalte **Berechtigung** das Kontextmenü für die betreffende Regel und wählen Sie dort den entsprechenden Wert aus (**Erlauben**, **Verbieten** oder **Aktion erfragen**).

   - Gehen Sie folgendermaßen vor, um die Rechte anzupassen, die dem Programm für die Ausführung bestimmter Aktionen im Netzwerk zugewiesen werden:

     a. Klicken Sie auf der Registerkarte **Netzwerkregeln** auf **Hinzufügen**.

        Das Fenster **Netzwerkregel** wird geöffnet.

     b. Legen Sie im folgenden Fenster die entsprechenden Einstellungen für die Regel fest und klicken Sie auf **Speichern**.

     c. Weisen Sie der neuen Regel eine Priorität zu. Verschieben Sie dazu die Regel mit den Schaltflächen **Aufwärts** und **Abwärts** an die entsprechende Position der Liste.

   - Damit bestimmte Aktionen nicht von der Programmkontrolle untersucht werden, aktivieren Sie auf der Registerkarte **Ausnahmen** die Kontrollkästchen für die Aktionen, die nicht kontrolliert werden sollen.

7. Klicken Sie auf **Speichern**.

   Alle Ausnahmen, die in den Regeln für die Programmkontrolle erstellt wurden, stehen im Konfigurationsfenster des Programms im Abschnitt **Gefahren und Ausnahmen** zur Verfügung.

Die Programmkontrolle überwacht und begrenzt die Aktionen des Programms nach den festgelegten Einstellungen.

ZUGRIFF VON PROGRAMMEN AUF DIE WEBCAM

Betrüger versuchen mithilfe spezieller Programme unberechtigten Zugriff auf die Webcam zu erlangen. Kaspersky Total Security blockiert den unbefugten Zugriff von Programmen auf die Webcam und zeigt eine entsprechende Meldung an. Für Programme, die zu den Gruppen "Stark beschränkt" oder "Nicht vertrauenswürdig" gehören, blockiert Kaspersky Total Security standardmäßig den Zugriff auf die Webcam.

Im Konfigurationsfenster der Programmkontrolle (s. Abschnitt "Zugriff eines Programms auf die Webcam erlauben" auf S 76) können Sie den Zugriff auf die Webcam für Programme erlauben, die zu den Gruppen "Stark beschränkt" und "Nicht vertrauenswürdig" gehören. Wenn ein Programm, das zur Sicherheitsgruppe "Schwach beschränkt" gehört, versucht, auf die Webcam zuzugreifen, meldet Kaspersky Total Security den Vorgang und fragt Sie, ob diesem Programm der Zugriff auf die Webcam erlaubt werden soll oder nicht.

Wenn ein Programm, dem der Zugriff standardmäßig erlaubt ist, auf die Webcam zuzugreifen versucht, zeigt Kaspersky Total Security eine Meldung an. Die Meldung informiert darüber, dass ein auf dem Computer installiertes Programm (z. B. Skype) momentan Bilder von der Webcam empfängt. Die Meldung enthält eine Dropdown-Liste, mit der Sie entweder den Zugriff des Programms auf die Webcam verbieten können oder zu den Einstellungen für den Webcam-Zugriff wechseln können (s. Abschnitt "Einstellungen für den Zugriff von Programmen auf die Webcam anpassen" auf S. 75). Diese Meldung wird nicht angezeigt, wenn auf Ihrem Computer bereits Programme im Vollbildmodus laufen.

In der Dropdown-Liste der Meldung über den Videodatenempfang können Sie außerdem die Variante **Diese Meldung nicht mehr anzeigen auswählen** oder zu den Einstellungen für die Benachrichtigungsanzeige wechseln (s. Abschnitt "Einstellungen für den Zugriff von Programmen auf die Webcam anpassen" auf S. 75).

Programmen, für die Ihre Zustimmung erforderlich ist, erlaubt Kaspersky Total Security standardmäßig den Zugriff auf die Webcam, wenn die grafische Programmoberfläche geladen oder entladen wird oder nicht antwortet, und Sie deshalb den Zugriff nicht manuell erlauben können.

Die Funktionalität für den Webcam-Schutz besitzt folgende Besonderheiten und Einschränkungen:

- Das Programm überwacht Videos und statische Bilder, die auf Webcam-Daten basieren.
- Kaspersky Total Security kontrolliert nur Webcams, die über die USB-Schnittstelle oder die IEEE1394-Schnittstelle angeschlossen und im Microsoft Geräte-Manager als Gerät zur Bildverarbeitung (Imaging Device) angezeigt werden.

Hier http://support.kaspersky.com/de/10978 finden Sie eine Liste der unterstützten Webcams.

Damit der Schutz vor unbefugtem Zugriff auf die Webcam funktioniert, muss die Komponente Programmkontrolle aktiviert sein.

EINSTELLUNGEN FÜR DEN ZUGRIFF VON PROGRAMMEN AUF DIE WEBCAM ANPASSEN

Um den Zugriff von Programmen auf die Webcam anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Hauptfenster auf den Link **Einstellungen**, um das Fenster **Einstellungen** zu öffnen.
3. Wählen Sie im Abschnitt **Schutz** im rechten Fensterbereich die Komponente **Zugriff auf Webcam** aus.
4. Passen Sie die Einstellungen für den Webcam-Zugriff auf Ihrem Computer an:
   - Um den Zugriff auf die Webcam für alle Programme zu verbieten, aktivieren Sie das Kontrollkästchen **Zugriff auf Webcam für alle Programme verbieten**.
   - Damit Sie benachrichtigt werden, wenn die Webcam von einem Programm verwendet wird, dem die Verwendung erlaubt ist, aktivieren Sie das Kontrollkästchen **Meldung anzeigen, wenn ein Programm, dem dies erlaubt ist, die Webcam verwendet**.
   - Um den Zugriff auf die Webcam für alle Programme zu erlauben, deaktivieren Sie im Fenster **Einstellungen** auf der Registerkarte **Schutz** den Punkt **Zugriff auf Webcam**.

ZUGRIFF EINES PROGRAMMS AUF DIE WEBCAM ERLAUBEN

Gehen Sie folgendermaßen vor, um den Zugriff eines Programms auf die Webcam zu erlauben:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Zusätzliche Tools anzeigen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie im Fenster **Tools** auf den Link **Programmkontrolle**, um das Fenster **Programmkontrolle** zu öffnen.
4. Klicken Sie im Fenster **Programmkontrolle** im Abschnitt **Programme** auf den Link **Programme verwalten**, um das Fenster **Programme verwalten** zu öffnen.
5. Wählen Sie in der Liste das Programm aus, dem Sie Zugriff auf die Webcam gewähren möchten, und öffnen Sie durch Doppelklicken das Fenster **Regeln für das Programm**.
6. Wechseln Sie im Fenster **Regeln für das Programm** auf die Registerkarte **Rechte**.
7. Wählen Sie aus der Liste mit dem Rechte-Kategorien den Punkt **Veränderung des Systems** → **Verdächtige Veränderungen im System** → **Zugriff auf Webcam**.
8. Öffnen Sie das Kontextmenü durch Klicken mit der rechten Maustaste auf die Spalte **Berechtigung** und wählen sie den Punkt **Erlauben**.
9. Klicken Sie auf **Speichern**.

Der Zugriff des Programms auf die Webcam wird erlaubt.

MODUS FÜR VERTRAUENSWÜRDIGE PROGRAMME

Dieser Abschnitt enthält Informationen über den Modus für vertrauenswürdige Programme.

IN DIESEM ABSCHNITT

ÜBER DEN MODUS FÜR VERTRAUENSWÜRDIGE PROGRAMME

Kaspersky Total Security bietet die Möglichkeit, auf einem Computer eine sichere Umgebung zu erstellen (Modus für vertrauenswürdige Programme), in der nur vertrauenswürdige Programme gestartet werden können. Der Modus für vertrauenswürdige Programme ist geeignet, wenn Sie gewöhnlich eine Auswahl von gängigen Programmen nutzen und nur selten neue unbekannte Dateien aus dem Internet herunterladen und starten. Im Modus für vertrauenswürdige Programme sperrt Kaspersky Total Security den Start aller Programme, die laut den Informationen von Kaspersky Lab nicht als vertrauenswürdig gelten. Als Grundlage für die Entscheidung, ob ein Programm vertrauenswürdig ist oder nicht, können die aus dem Kaspersky Security Network empfangenen Informationen, Daten über die digitale Signatur des Programms, Daten über die Vertrauenswürdigkeit des Installationsprogramms und der Quelle, von der das Programm heruntergeladen wurde, dienen.

Der Modus für vertrauenswürdige Programme besitzt folgende Besonderheiten und Einschränkungen:

- Um den Modus für vertrauenswürdige Programme zu verwenden, müssen die Schutzkomponenten Programmkontrolle, Datei-Anti-Virus und Aktivitätsmonitor aktiviert sein. Wenn eine dieser Komponenten beendet wird, wird der Modus für vertrauenswürdige Programme deaktiviert.

- Es kann sein, dass der Modus für vertrauenswürdige Programme nicht verfügbar ist, wenn sich die Systemdateien in Festplattenbereichen mit einem anderen Dateisystem als NTFS befinden.

- Es kann sein, dass der Modus für vertrauenswürdige Programme in der aktuellen Version von Kaspersky Total Security fehlt oder nicht verfügbar ist. Ob der Modus für vertrauenswürdige Programme in Kaspersky Total Security vorhanden ist, hängt von Ihrem Land und Dienstanbieter ab. Erkundigen Sie sich beim Kauf des Programms, ob der Modus für vertrauenswürdige Programme enthalten ist.

- Sollte der Modus für vertrauenswürdige Programme in Ihrer Version von Kaspersky Total Security zwar vorgesehen, momentan aber nicht verfügbar sein, kann der Modus nach dem Update von Datenbanken und Programm-Modulen des Programms zur Verfügung stehen (s. Abschnitt "Update der Datenbanken und Programm-Module" auf S. 36). Nach dem Update der Datenbanken und Programm-Module können sich die Einstellungen für den Start von unbekannten Programmen und Modulen ändern.

Bevor der Modus für vertrauenswürdige Programme aktiviert wird, analysiert Kaspersky Total Security das Betriebssystem und die auf Ihrem Computer installierten Programme. Die Analyse kann lange dauern (mehrere Stunden). Wenn bei der Analyse Software gefunden wird, die nicht als vertrauenswürdig gilt, wird davor gewarnt, den Modus für vertrauenswürdige Programme zu aktivieren. Wenn der Modus für vertrauenswürdige Programme aktiviert ist, kann Kaspersky Total Security Programme blockieren, die nicht als vertrauenswürdig gelten. Sie können den Start für solche Programme erlauben (s. Abschnitt "Kontrolle der Aktionen eines Programms auf dem Computer und im Netzwerk" auf S. 72), so lange Sie mit den Programmen arbeiten, und anschließend den Modus für vertrauenswürdige Programme aktivieren.

Kaspersky Total Security kann die Analyse des Betriebssystems und der installierten Programme automatisch im Hintergrundmodus durchführen. Wenn aufgrund der Ergebnisse der Analyse durch Kaspersky Total Security erkannt wurde, dass auf dem Computer hauptsächlich vertrauenswürdige Programme verwendet werden, kann der Modus für vertrauenswürdige Programme automatisch aktiviert werden.

MODUS FÜR VERTRAUENSWÜRDIGE PROGRAMME AKTIVIEREN

Um den Modus für vertrauenswürdige Programme zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Zusätzliche Tools anzeigen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie im Fenster **Tools** auf den Link **Programmkontrolle**, um das Fenster **Programmkontrolle** zu öffnen.
4. Klicken Sie im Abschnitt **Modus für vertrauenswürdige Programme ist deaktiviert** im Fenster **Programmkontrolle** unten auf den Link **Aktivieren**.

   Falls obligatorische Schutzkomponenten deaktiviert sind, öffnet sich ein Fenster. Es informiert über die Schutzkomponenten, die für den Modus für vertrauenswürdige Programme aktiviert werden müssen.
5. Klicken Sie auf **Fortsetzen**.

   Die Analyse des Betriebssystems und der installierten Programme mit Ausnahme von temporären Dateien und Ressourcen von dll-Bibliotheken, die ausführbaren Code enthalten, wird gestartet. Das folgende Fenster **Installierte Programme analysieren** informiert über den Fortschritt der Analyse.

   Warten Sie, bis die Analyse des Betriebssystems und der installierten Programme abgeschlossen wird. Sie können das Fenster **Installierte Programme analysieren** ausblenden. Dabei wird die Analyse im Hintergrund ausgeführt. Folgen Sie dem Link **Analyse der installierten Programme (<N> %)** im Fenster **Programmkontrolle**, um Informationen zur Analyse anzuzeigen.
6. Das Fenster **Die Analyse der installierten Programme und ausführbaren Dateien wurde abgeschlossen** bietet Informationen zu den Analyseergebnissen.

   Wenn bei der Analyse Systemdateien gefunden werden, über die unzureichende Informationen vorliegen, wird davor gewarnt, den Modus für vertrauenswürdige Programme zu aktivieren. Es wird auch davon abgeraten, den Modus für vertrauenswürdige Programme zu aktivieren, wenn eine hohe Anzahl von Programmen gefunden wird, für die dem Programm Kaspersky Total Security zu wenig Informationen vorliegen, um sie als vollkommen sicher einzuordnen.

   Informationen über nicht vertrauenswürdige Systemdateien finden Sie über den Link **Liste der unbekannten Systemobjekte öffnen**. Eine Liste der nicht vertrauenswürdigen Systemdateien befindet sich im Fenster **Unbekannte Systemdateien**. Außerdem können Sie die Verwendung des Modus für vertrauenswürdige Programme mit der Schaltfläche **Modus für vertrauenswürdige Programme nicht aktivieren** ablehnen.
7. Um den Start von nicht vertrauenswürdigen Programmen und Systemdateien zu erlauben, klicken Sie im Fenster **Die Analyse der installierten Programme und ausführbaren Dateien wurde abgeschlossen** auf den Link **Start von unbekannten Systemdateien erlauben und fortfahren**.
8. Klicken Sie auf **Modus für vertrauenswürdige Programme standardmäßig aktivieren**.

Der Modus für vertrauenswürdige Programme wird aktiviert. Kaspersky Total Security sperrt den Start aller Programme und Systemdateien, die nicht als vertrauenswürdig gelten. Das Fenster **Programmkontrolle** wird geöffnet.

Nachdem der Modus für vertrauenswürdige Programme aktiviert und das Betriebssystem neu gestartet wurde, wird der Start unbekannter Programme erlaubt, bis Kaspersky Total Security gestartet wird. Nach künftigen Neustarts des Betriebssystems sperrt Kaspersky Total Security den Start von unbekannten Programmen.

MODUS FÜR VERTRAUENSWÜRDIGE PROGRAMME DEAKTIVIEREN

Um den Modus für vertrauenswürdige Programme zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Zusätzliche Tools anzeigen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie im Fenster **Tools** auf den Link **Programmkontrolle**, um das Fenster **Programmkontrolle** zu öffnen.
4. Klicken Sie im Abschnitt **Modus für vertrauenswürdige Programme ist aktiviert** im unteren Fensterbereich auf den Link **Deaktivieren**.

Der Modus für vertrauenswürdige Programme wird deaktiviert.

DATENVERNICHTUNG

Der Schutz vor unerlaubter Wiederherstellung gelöschter Informationen bietet zusätzliche Sicherheit für persönliche Daten.

Kaspersky Total Security verfügt über ein Tool zur Datenvernichtung. Daten, die auf diese Weise gelöscht wurden, können nicht mit Standard-Tools rekonstruiert werden.

Kaspersky Total Security kann Daten von folgenden Datenträgern unwiderruflich löschen:

- Lokale Festplatten und Netzlaufwerke. Das Löschen ist möglich, wenn Sie zum Schreiben und Löschen von Informationen berechtigt ist.
- Wechseldatenträger oder andere Geräte, die als Wechseldatenträger erkannt werden (z. B. Disketten, Flash Cards, USB-Sticks oder Mobiltelefone). Daten können von Speicherkarten gelöscht werden, wenn kein mechanischer Schreibschutz besteht.

Sie können jene Daten löschen, für die Ihr Benutzerkonto eine Zugriffsberechtigung besitzt. Vor der Datenvernichtung muss sicher gestellt werden, dass diese Daten nicht von laufenden Programmen verwendet werden.

Gehen Sie folgendermaßen vor, um Daten unwiderruflich zu löschen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Zusätzliche Tools anzeigen**, um das Fenster **Tools** zu öffnen.
3. Öffnen Sie im Fenster **Tools** mit dem Link **Datenvernichtung** das Fenster **Datenvernichtung** (s. Abb. unten).

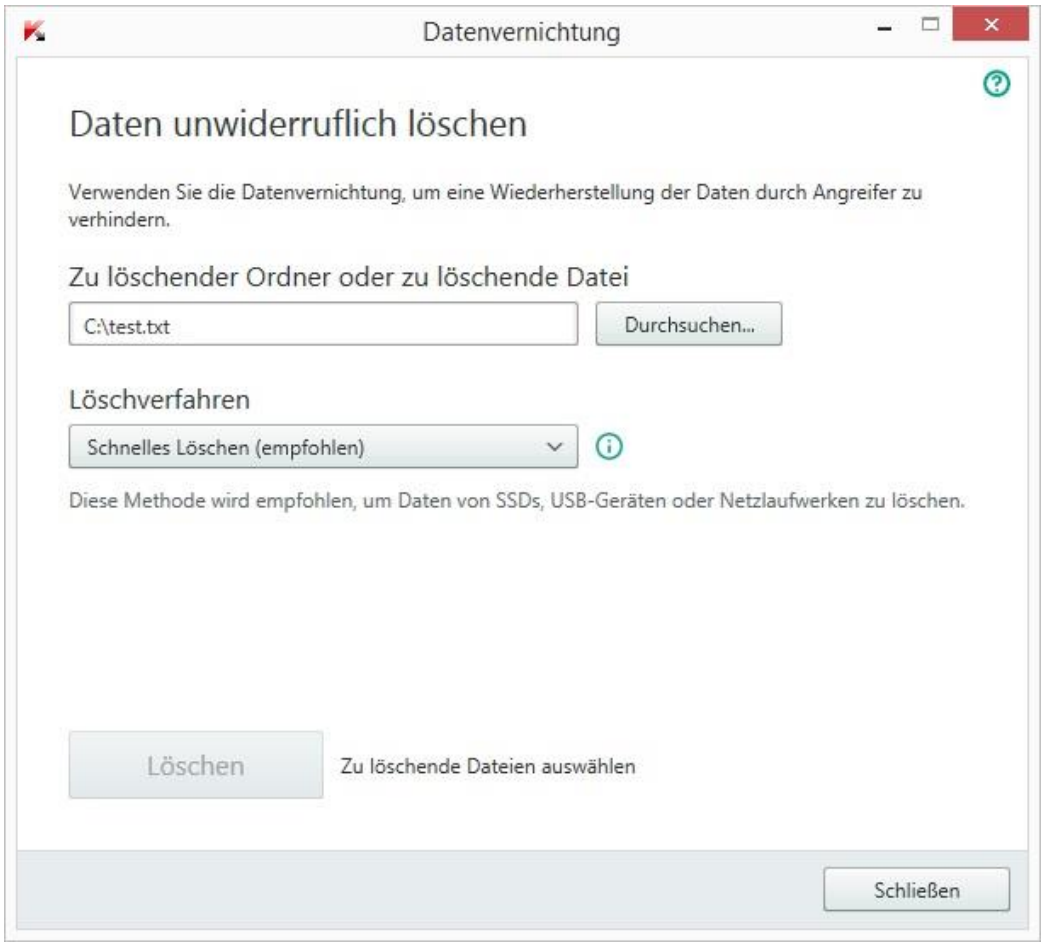

*Abbildung 6. Fenster **Datenvernichtung***

4. Klicken Sie auf **Durchsuchen** und wählen Sie im folgenden Fenster **Ordner auswählen** einen Ordner oder eine Datei für die Datenvernichtung aus.

   Das Löschen von Systemdateien kann zu Funktionsstörungen im Betriebssystem führen.

5. Wählen Sie in der Dropdown-Liste **Löschverfahren** ein Verfahren für die Datenlöschung aus.

   Es wird empfohlen, die Methoden **Schnelles Löschen** oder **GOST R 50739-95** zu verwenden, um Daten von SSD-Geräten, USB-Geräten und Netzlaufwerken zu löschen. Die übrigen Löschverfahren können zu einer Beschädigung des SSD-Geräts, USB-Geräts oder Netzlaufwerks führen.

6. Klicken Sie auf **Löschen**.

7. Bestätigen Sie im folgenden Fenster das Löschen mit **Ja**. Wenn bestimmte Dateien nicht gelöscht wurden, wiederholen Sie die Löschung durch Klick auf **Wiederholen**. Klicken Sie auf **Beenden**, um einen anderen Ordner zum Löschen auszuwählen.

LÖSCHEN VON NICHT BENÖTIGTEN DATEN

Dieser Abschnitt informiert darüber, wie temporäre und nicht benötigte Daten gelöscht werden können.

IN DIESEM ABSCHNITT

ÜBER DAS LÖSCHEN VON NICHT BENÖTIGTEN DATEN

Im Betriebssystem sammeln sich im Lauf der Zeit temporäre oder nicht benötigte Dateien an. Solche Dateien können viel Speicherplatz belegen, was die Systemeffektivität verringert. Außerdem können sie von Schadprogrammen verwendet werden.

Temporäre Dateien werden beim Start von beliebigen Programmen und beim Hochfahren des Betriebssystems erstellt. Beim Abschluss der Arbeit werden nicht alle temporären Dateien automatisch gelöscht. Im Lieferumfang von Kaspersky Total Security ist der Assistent zum Löschen von nicht benötigten Daten enthalten.

Der Assistent zum Löschen von nicht benötigten Daten kann folgende Dateien finden und löschen:

- Berichte über Systemereignisse, in denen die Namen aller geöffneten Programme protokolliert werden.
- Ereignisberichte von bestimmten Programmen oder Update-Tools (beispielsweise Windows Updater)
- Berichte über Systemverbindungen
- temporäre Webbrowser-Dateien (Cookies)
- temporäre Dateien, die nach der Installation bzw. Deinstallation von Programmen zurückbleiben.
- Inhalt des Papierkorbs
- Dateien des Ordners TEMP, dessen Umfang mehrere Gigabyte erreichen kann.

Der Assistent löscht nicht nur die nicht mehr benötigten Dateien aus dem System, er entfernt auch Dateien, die vertrauliche Daten (Kennwörter, Benutzernamen und Informationen aus Anmeldeformularen) enthalten können. Es wird trotzdem empfohlen, den Assistenten zum Löschen von Aktivitätsspuren zu verwenden, um solche Daten vollständig zu löschen.

ASSISTENT ZUM LÖSCHEN VON NICHT BENÖTIGTEN DATEN STARTEN

Gehen Sie folgendermaßen vor, um den Assistenten zum Löschen von nicht benötigten Daten zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Zusätzliche Tools anzeigen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie im folgenden Fenster auf den Link **Löschen von nicht benötigten Daten**, um den Assistenten zum Löschen von nicht benötigten Daten zu starten.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Details zu den einzelnen Schritten des Assistenten.

Schritt 1. Assistent starten

Das erste Fenster des Assistenten informiert über das Löschen von nicht benötigten Daten.

Klicken Sie auf den Link **Weiter**, um den Assistenten zu starten.

Schritt 2. Suche nach nicht benötigten Daten

Der Assistent durchsucht Ihren Computer nach nicht benötigten Daten. Die Suche kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für das Löschen von nicht benötigten Daten auswählen

Nachdem die Suche nach nicht benötigten Daten abgeschlossen wurde, wird ein Fenster mit einer Aktionsliste angezeigt.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen.

Es wird davor gewarnt, die standardmäßig angekreuzten Kontrollkästchen zu deaktivieren. Dadurch kann die Sicherheit Ihres Computers bedroht werden.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Nicht benötigte Informationen löschen

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Das Löschen von nicht mehr benötigten Informationen kann eine gewisse Zeit beanspruchen.

Nachdem das Löschen der nicht benötigten Informationen abgeschlossen wurde, geht der Assistent automatisch zum nächsten Schritt.

Es kann sein, dass während Ausführung des Assistenten bestimmte Dateien vom System verwendet werden (beispielsweise die Berichtsdatei von Microsoft Windows oder die Berichtsdatei für Microsoft Office). Um diese Dateien zu löschen, schlägt der Assistent vor, das System neu zu starten.

Schritt 5. Assistent abschließen

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

DATENSICHERUNG

Dieser Abschnitt enthält Informationen über die Datensicherung.

IN DIESEM ABSCHNITT

ÜBER DIE DATENSICHERUNG

Eine Datensicherung ist notwendig, um Ihre Daten in folgenden Fällen zu schützen: Datenverlust aufgrund von Funktionsstörungen oder Diebstahl der Hardware, irrtümliches Löschen, oder Datenverlust aufgrund von Angriffen.

Um eine Datensicherung auszuführen, müssen Sie eine Backup-Aufgabe erstellen (s. Abschnitt "Backup-Aufgabe erstellen" auf S. 84) und starten (s. Abschnitt "Backup-Aufgabe starten" auf S. 87). Die Aufgabe kann automatisch, nach Zeitplan oder manuell gestartet werden. Das Programm bietet Informationen über die Ausführung dieser Aufgaben.

Es wird empfohlen, Sicherungskopien auf Wechselmedien oder in einem Online-Speicher zu speichern.

Um mit Kaspersky Total Security Sicherungskopien anzulegen, können folgende Speichermedien verwendet werden:

- lokaler Datenträger
- Wechselmedium (z. B. externe Festplatte)
- Netzlaufwerk
- FTP-Server
- Online-Speicher (s. Abschnitt "Über den Online-Speicher" auf S. 88).

BACKUP-AUFGABE ERSTELLEN

Um eine Aufgabe zur Datensicherung zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Sichern und Wiederherstellen**.
3. Führen Sie im nächsten Fenster **Sichern und Wiederherstellen** folgende Aktionen aus:
   - Klicken Sie auf **Zu sichernde Dateien auswählen**, wenn noch keine Aufgabe zur Datensicherung erstellt worden ist.
   - Klicken Sie auf **Sicherungskopien für andere Dateien erstellen**, wenn bereits eine Aufgabe zur Datensicherung vorhanden ist und Sie eine neue erstellen möchten.

Der Assistent für neue Aufgaben zur Datensicherung wird gestartet.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Details zu den einzelnen Schritten des Assistenten.

Datentyp auswählen

Wählen Sie nun einen Datentyp aus und geben Sie die Ordner an, die gesichert werden sollen.

- Wählen Sie zur schnellen Konfiguration einen der voreingestellten Datentypen aus (Dateien aus den Ordnern "Eigene Dateien" und "Desktop", Fotos und Bilder, Filme und Videos, Musikdateien).
- Wählen Sie die Variante **Dateien aus den angegebenen Ordnern sichern** aus, um die zu sichernden Ordner manuell anzugeben.

Zu sichernde Ordner auswählen

Wenn Sie beim vorhergehenden Schritt des Assistenten die Variante **Dateien aus den angegebenen Ordnern sichern** ausgewählt haben, klicken Sie auf **Ordner hinzufügen** und wählen Sie entweder den Ordner im folgenden Fenster **Ordner auswählen** aus oder ziehen Sie den Ordner in das Programmfenster.

Aktivieren Sie das Kontrollkästchen **Zusätzlich Dateitypen angeben**, wenn Sie für die angegebenen Ordner die zu sichernden Dateikategorien festlegen möchten.

Kategorien für die zu sichernden Dateien auswählen

Wenn Sie beim vorhergehenden Schritt des Assistenten das Kontrollkästchen **Zusätzlich Dateitypen angeben** aktiviert haben, aktivieren Sie im folgenden Fenster die Kontrollkästchen für die zu sichernden Dateikategorien.

Sicherungsspeicher auswählen

Wählen Sie nun einen Sicherungsspeicher aus:

- **Online-Speicher**. Wählen Sie diese Variante aus, wenn Sie die Sicherungskopien in einem Online-Speicher ablegen möchten. Bevor Sie einen Online-Speicher verwenden können, muss der Online-Speicher aktiviert werden (s. Abschnitt "Online-Speicher aktivieren" auf S. 88). Bei der Datensicherung in einem Online-Speicher legt Kaspersky Total Security keine Sicherungskopien für jene Datentypen an, die durch die Dropbox-Nutzungsregeln ausgenommen sind.
- **Lokales Laufwerk (C:)**. Wählen Sie diese Variante aus, wenn Sie die Sicherungskopien auf der lokalen Festplatte ablegen möchten.
- **Netzwerkspeicher**. Wenn Sie die Sicherungskopien in einem Netzwerkspeicher ablegen möchten, wählen Sie den entsprechenden Netzwerkspeicher in der Liste aus.
- **Wechselmedium**. Wenn Sie die Sicherungskopien auf einem Wechselmedium ablegen möchten, wählen Sie das entsprechenden Wechselmedium in der Liste aus.

Um die Daten besser zu schützen, wird empfohlen, einen Online-Speicher zu verwenden oder die Sicherungsspeicher auf Wechselmedien anzulegen.

Um einen Netzwerkspeicher hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Netzwerkspeicher hinzufügen**, um das Fenster **Netzwerkspeicher hinzufügen** zu öffnen, und wählen Sie einen Typ für den Netzwerkspeicher aus: Netzlaufwerk oder FTP-Server.
2. Geben Sie die Daten an, die für die Verbindung mit dem Netzwerkspeicher erforderlich sind
3. Klicken Sie auf **OK**.

Um ein Wechselmedium als Sicherungsspeicher hinzuzufügen, gehen Sie wie folgt vor:

1. Mit dem Link **Vorhandenen Speicher verbinden** wird das Fenster **Speicher verbinden** geöffnet.
2. Wählen Sie den Abschnitt **Wechselmedium** aus.
3. Klicken Sie auf **Durchsuchen** und geben Sie im folgenden Fenster das Wechselmedium an, auf dem die Sicherungskopien gespeichert werden sollen.

Aktivieren Sie das Kontrollkästchen **Erweiterte Einstellungen für den Speicher verwenden**, um die Einstellungen für die Dateispeicherung anzupassen. Zu diesen Einstellungen gehören die Anzahl der für eine Datei zu speichernden Sicherungskopien und die Speicherdauer für Sicherungskopien.

Sicherungszeitplan erstellen

Führen Sie bei diesem Schritt eine der folgenden Aktionen aus:

- Legen Sie einen Startzeitplan für die Aufgabe zur Datensicherung an, wenn die Aufgabe automatisch gestartet werden soll.
- Wählen Sie in der Dropdown-Liste **Sicherung starten** die Variante **manuell** aus, wenn die Aufgabe manuell gestartet werden soll.

Kennwort für den Schutz von Sicherungskopien eingeben

Aktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren** und füllen Sie die Felder **Kennwort für den Zugriff auf Sicherungskopien** und **Kennwort bestätigen** aus, wenn Sie den Zugriff auf Sicherungskopien durch ein Kennwort schützen möchten.

Einstellungen für die Dateispeicherung

Dieser Schritt ist verfügbar, wenn Sie beim vorherigen Schritt das Kontrollkästchen **Erweiterte Einstellungen für den Speicher verwenden** aktiviert haben.

Passen Sie die Einstellungen für die Dateispeicherung an:

- Aktivieren Sie das Kontrollkästchen **Anzahl der Dateiversionen begrenzen** und legen Sie im Feld **Anzahl der zu speichernden Versionen** fest, wie viele Sicherungskopien einer Datei gespeichert werden sollen.
- Aktivieren Sie das Kontrollkästchen **Speicherdauer für Dateiversionen begrenzen** und legen Sie im Feld **Speicherdauer für die Dateiversion** fest, wie viele Tage die Sicherungskopie einer Datei aufbewahrt werden soll.

Name für die Aufgabe zur Datensicherung eingeben

Führen Sie bei diesem Schritt folgende Aktionen aus:

1. Geben Sie einen Namen für die Aufgabe zur Datensicherung ein.
2. Aktivieren Sie das Kontrollkästchen **Sicherung starten, wenn der Assistent abgeschlossen wird**, damit die Sicherung startet, sobald der Assistent abgeschlossen wird.

Assistent abschließen

Klicken Sie auf **Beenden**.

Die Aufgabe zur Datensicherung wird erstellt. Die erstellte Aufgabe wird im Fenster **Sichern und Wiederherstellen** angezeigt.

AUFGABE ZUR DATENSICHERUNG STARTEN

Gehen Sie folgendermaßen vor, um eine Aufgabe zur Datensicherung zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Sichern und Wiederherstellen**.
3. Wählen Sie im folgenden Fenster **Sichern und Wiederherstellen** eine Aufgabe zur Datensicherung aus und klicken Sie auf **Sicherung starten**.

Die Aufgabe zur Datensicherung wird gestartet.

DATEN AUS EINER SICHERUNGSKOPIE WIEDERHERSTELLEN

Gehen Sie folgendermaßen vor, um Daten aus einer Sicherungskopie wiederherzustellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Sichern und Wiederherstellen**.
3. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie neben der entsprechenden Aufgabe zur Datensicherung auf **Dateien wiederherstellen**.
   - Klicken Sie auf den Link **Speicher verwalten** und klicken Sie dann im folgenden Fenster neben dem entsprechenden Sicherungsspeicher auf **Dateien wiederherstellen**.
4. Wählen Sie in der Dropdown-Liste **Gesichert am** das Erstellungsdatum der Sicherungskopie aus.
5. Aktivieren Sie das Kontrollkästchen für die Ordner, die wiederhergestellt werden sollen.
6. Wenn Sie nur bestimmte Dateikategorien wiederherstellen möchten, wählen Sie diese Dateikategorien in der Dropdown-Liste Dateityp aus.
7. Klicken Sie auf **Ausgewählte Dateien wiederherstellen**.

   Das Fenster **Datenwiederherstellung aus einer Sicherungskopie** wird geöffnet.
8. Wählen Sie eine der zwei Varianten aus:
   - **Im ursprünglichen Ordner**. Bei Auswahl dieser Variante stellt das Programm die Daten im ursprünglichen Ordner wiederher.
   - **Im folgenden Ordner**. Bei Auswahl dieser Variante stellt das Programm die Daten im angegebenen Ordner wiederher. Klicken Sie auf **Durchsuchen**, um einen Ordner auszuwählen, in dem die Daten wiederhergestellt werden sollen.
9. Legen Sie in der Dropdown-Liste **Bei gleichen Dateinamen** fest, wie das Programm vorgehen soll, wenn der Name der wiederherzustellenden Datei mit dem Namen einer Datei übereinstimmt, die sich im angegebenen Wiederherstellungsordner befindet.
10. Klicken Sie auf **Wiederherstellen**.

    Die für die Wiederherstellung ausgewählten Dateien werden aus der Sicherungskopie wiederhergestellt und im angegebenen Ordner gespeichert.

ÜBER DEN ONLINE-SPEICHER

Das Programm Kaspersky Total Security bietet die Möglichkeit, Sicherungskopien Ihrer Daten in einem Online-Speicher zu speichern, der sich auf einem Remote-Server des Webdiensts Dropbox befindet.

Für die Verwendung eines Online-Speichers gelten folgende Voraussetzungen:

- Stellen Sie sicher, dass der Computer mit dem Internet verbunden ist.
- Erstellen Sie auf der Webseite des Cloud-Anbieters ein Konto.
- Aktivieren Sie den Online-Speicher.

Sie können ein einziges Dropbox-Konto verwenden, um Daten von unterschiedlichen Geräten in einem Online-Speicher zu sichern. Auf diesen Geräten muss das Programm Kaspersky Total Security installiert sein.

Das Volumen des Online-Speichers ist vom Cloud-Anbieter abhängig, in unserem Fall vom Webdienst Dropbox. Ausführliche Informationen über die Nutzungsbedingungen für den Webdienst finden Sie auf der Dropbox-Website https://www.dropbox.com/.

ONLINE-SPEICHER AKTIVIEREN

Gehen Sie folgendermaßen vor, um den Online-Speicher zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Sichern und Wiederherstellen**.
3. Führen Sie im nächsten Fenster **Sichern und Wiederherstellen** folgende Aktionen aus:
   - Klicken Sie auf **Zu sichernde Dateien auswählen**, wenn noch keine Aufgabe zur Datensicherung erstellt worden ist.
   - Klicken Sie auf **Sicherungskopien für andere Dateien erstellen**, wenn bereits eine Aufgabe zur Datensicherung vorhanden ist.

   Dadurch wird der Assistent für neue Backup-Aufgaben gestartet (s. Abschnitt "Backup-Aufgabe erstellen" auf S. 84).
4. Wählen Sie im Fenster Datentyp eine Datenkategorie aus oder geben Sie die zu sichernden Dateien manuell an.
5. Wählen Sie im Auswahlfenster einen Online-Speicher aus und klicken Sie auf **Aktivieren**.

   Um einen Online-Speicher zu erstellen, ist eine Internetverbindung erforderlich.

   Ein Fenster für die Anmeldung im Dropbox-Konto wird geöffnet.
6. Führen Sie im nächsten Fenster eine der folgenden Aktionen aus:
   - Falls Sie kein Dropbox-Konto besitzen, registrieren Sie sich auf der Dropbox-Webseite.
   - Wenn Sie bereits auf der Dropbox-Webseite registriert sind, melden Sie sich mit Ihrem Dropbox-Konto an.
7. Um die Aktivierung des Online-Speichers abzuschließen, bestätigen Sie, dass Kaspersky Total Security Ihr Dropbox-Konto für die Datensicherung und für die Datenwiederherstellung aus einer Sicherungskopie verwenden darf. Kaspersky Total Security speichert die Sicherungskopien für Daten in einem separaten Ordner, der im Dropbox-Anwendungsordner angelegt wird.

   Nach dem Abschluss der Aktivierung des Online-Speichers öffnet sich ein Fenster zur Auswahl eines Speichers. Der Online-Speicher ist für die Auswahl verfügbar. Für den aktivierten Online-Speicher wird die Größe des belegten Speichers und des freien Speichers angezeigt, der für die Speicherung von Daten verfügbar ist.

DATEN IN DATENTRESOREN SPEICHERN

Dieser Abschnitt informiert darüber, wie Sie Ihre Daten mithilfe von Datentresoren schützen können.

IN DIESEM ABSCHNITT

ÜBER DATENTRESORE

Datentresore dienen dem Schutz Ihrer sensiblen Daten vor unbefugtem Zugriff. Ein *Datentresor* ist ein Datenspeicher auf Ihrem Computer, den Sie mithilfe eines Kennworts entsperren oder verriegeln können. Das Kennwort ist nur Ihnen bekannt. Um Dateien zu ändern, die in einem verriegelten Datentresor gespeichert sind, muss das Kennwort eingegeben werden.

Falls Sie das Kennwort verlieren oder vergessen, können die Daten nicht wiederhergestellt werden.

Beim Erstellen von Datentresoren verwendet Kaspersky Total Security folgende Algorithmen für die Datenverschlüsselung: AES XTS 256, DRBG-SHA2-256, PBKDF-SHA2-256.

DATEIEN IN EINEN DATENTRESOR VERSCHIEBEN

Um Dateien in einen Datentresor zu verschieben, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf **Virtuelle Datentresore**.
3. Führen Sie im folgenden Fenster **Virtuelle Datentresore** eine der folgenden Aktionen aus:
   - Klicken Sie auf **Neuen Datentresor erstellen**, wenn Sie noch keinen Datentresor besitzen.
   - Klicken Sie auf **Datentresor erstellen**, wenn Sie bereits einen Datentresor erstellt haben.
4. Öffnen Sie mit dem Link **Dateien und Ordner zum Datentresor hinzufügen** den Explorer und geben Sie die Dateien an, die in den Datentresor verschoben werden sollen.

   Die ausgewählten Dateien werden im Fenster **Virtuelle Datentresore** angezeigt.
5. Klicken Sie auf **Fortsetzen**.
6. Geben Sie entweder den Namen und den Ort des Datentresors oder verwenden Sie die entsprechenden Standardwerte.
7. Um den schnellen Zugriff auf den Datentresor zu ermöglichen, aktivieren Sie das Kontrollkästchen **Verknüpfung für den Datentresor auf dem Desktop erstellen**.
8. Klicken Sie auf **Fortsetzen**.

9. Füllen Sie die Felder **Kennwort** und **Kennwort bestätigen** aus, und klicken Sie auf **Fortsetzen**.
10. Legen Sie fest, was mit den Originaldateien außerhalb des Datentresors geschehen soll:
    - Um die Originaldateien außerhalb des Datentresors zu löschen, klicken Sie auf **Löschen**.
    - Um die Originaldateien außerhalb des Datentresors beizubehalten, klicken Sie auf **Überspringen**
11. Klicken Sie auf **Beenden**.

    Ihre Datentresore enthält eine Liste der von Ihnen erstellten Datentresore.
12. Um den Datentresor zu schließen, klicken Sie auf **Datentresor verriegeln**.

    Die Daten in einem verriegelten Datentresor sind nur nach Eingabe des Kennworts verfügbar.

ZUGRIFF AUF DATEIEN IM DATENTRESOR ERHALTEN

Um Zugriff auf die Dateien in einem Datentresor zu erhalten, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster
2. Klicken Sie auf **Virtuelle Datentresore**.
3. Klicken Sie im folgenden Fenster **Virtuelle Datentresore** neben dem entsprechenden Datentresor auf **Datentresor öffnen**.
4. Geben Sie das Kennwort ein und klicken Sie auf **Datentresor im Windows Explorer öffnen**.

Die Dateien, die im Datentresor gespeichert sind, werden im Explorer-Fenster angezeigt. Sie können die Dateien entsprechend ändern und den Datentresor anschließend wieder verriegeln.

Um Datentresore zu öffnen, die in einer älteren Programmversion erstellt worden sind, müssen die Datentresore in das neue Format konvertiert werden. Das Programm schlägt Ihnen eine Konvertierung vor, wenn Sie versuchen, einen Datentresor in Kaspersky Total Security zu öffnen.

Die Umwandlung von Datentresoren in das neue Format ist von der Größe des Datentresors abhängig und kann relativ viel Zeit beanspruchen.

ZUGRIFF AUF DIE VERWALTUNG VON KASPERSKY TOTAL SECURITY MIT EINEM KENNWORT SCHÜTZEN

Es kann sein, dass ein Rechner von mehreren Benutzern verwendet wird, deren Kenntnisse und Erfahrungen im Umfang mit Computern sehr unterschiedlich sind. Das Sicherheitsniveau des Computers kann beeinträchtigt werden, wenn verschiedene Benutzer uneingeschränkten Zugriff auf die Verwaltung und auf die Einstellungen von Kaspersky Total Security besitzen.

Um den Zugriff auf das Programm einzuschränken, können Sie ein Administrator-Kennwort festlegen und angeben, für welche Aktionen diese Kennwort abgefragt werden soll:

- Programmeinstellungen anpassen
- Programm beenden
- Programm deinstallieren

Gehen Sie folgendermaßen vor, um den Zugriff auf Kaspersky Total Security durch ein Kennwort zu schützen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Hauptfensters auf den Link **Einstellungen**, um den Abschnitt **Einstellungen** zu öffnen.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Allgemein** und öffnen Sie mit dem Link **Kennwortschutz einrichten** das Fenster **Kennwortschutz**.
4. Füllen Sie im folgenden Fenster die Felder **Neues Kennwort** und **Kennwort bestätigen** aus.
5. Geben Sie im Block **Gültigkeitsbereich des Kennworts** an, welche Vorgänge durch das Kennwort geschützt werden sollen.

Ein vergessenes Kennwort kann nicht wiederhergestellt werden. Wenn Sie das Kennwort vergessen haben, müssen Sie sich an den Technischen Support wenden, um erneut Zugriff auf die Einstellungen von Kaspersky Total Security zu erhalten.

COMPUTERSCHUTZ ANHALTEN UND FORTSETZEN

Das Anhalten des Schutzes bedeutet, dass alle Komponenten für einen bestimmten Zeitraum ausgeschaltet werden.

Wenn der Schutz angehalten ist oder Kaspersky Total Security ausgeschaltet ist, funktioniert weiterhin die Aktivitätsüberwachung für die Programme, die auf Ihrem Computer laufen. Informationen über die Ergebnisse der Aktivitätsüberwachung für Programme werden im Betriebssystem gespeichert. Wenn der Schutz wieder gestartet oder fortgesetzt wird, verwendet Kaspersky Total Security diese Informationen, um Ihren Computer vor schädlichen Aktionen zu schützen, die ausgeführt werden konnten, während der Schutz angehalten oder Kaspersky Total Security deaktiviert war. Die Informationen über die Ergebnisse der Aktivitätsüberwachung für Programme werden für unbegrenzte Zeit aufbewahrt. Diese Informationen werden gelöscht, wenn Kaspersky Total Security von Ihrem Computer entfernt wird.

Gehen Sie folgendermaßen vor, um den Computerschutz anzuhalten:

1. Wählen Sie im Kontextmenü des Programmsymbols im Infobereich der Taskleiste den Punkt **Schutz anhalten** aus.

   Das Fenster **Schutz anhalten** wird geöffnet (s. Abb. unten).

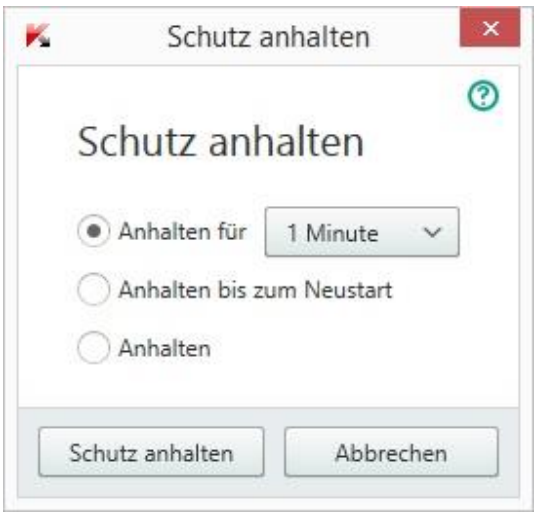

Abbildung 7. Fenster Schutz anhalten

2. Wählen Sie im Fenster **Schutz anhalten** den Zeitraum, nach dem der Schutz wieder aktiviert werden soll:

   - **Anhalten für** – Der Schutz wird nach Ablauf des Zeitraums wieder aktiviert, der in der Dropdown-Liste festgelegt wird.
   - **Anhalten bis zum Neustart** – Der Schutz wird nach dem Neustart des Programms oder des Betriebssystems aktiviert (unter der Bedingung, dass der automatische Programmstart aktiviert ist).
   - **Anhalten** – Der Schutz wird wieder aktiviert, wenn Sie ihn fortsetzen.

Um den Computerschutz fortzusetzen,

wählen Sie im Kontextmenü des Programmsymbols im Infobereich der Taskleiste den Punkt **Schutz fortsetzen** aus.

STANDARDEINSTELLUNGEN FÜR DAS PROGRAMM WIEDERHERSTELLEN

Sie können jederzeit die von Kaspersky Lab empfohlenen Einstellungen für Kaspersky Total Security wiederherstellen. Die Wiederherstellung der Einstellungen erfolgt mit Hilfe des *Konfigurationsassistenten für das Programm*.

Der Assistent stellt für alle Schutzkomponenten die Sicherheitsstufe *Empfohlen* ein. Wenn Sie die empfohlene Sicherheitsstufe wiederherstellen, können Sie die benutzerdefinierten Einstellungswerte für die Programmkomponenten beibehalten.

Gehen Sie folgendermaßen vor, den Konfigurationsassistenten für das Programm zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf den Link **Einstellungen**.

   Dieses Fenster enthält den Abschnitt **Einstellungen**.
3. Wählen Sie den Abschnitt **Allgemein**.

   Dieses Fenster enthält Einstellungen für Kaspersky Total Security.
4. Wählen Sie im unteren Fensterbereich aus der Dropdown-Liste **Einstellungen verwalten** die Variante **Einstellungen wiederherstellen** .

Details zu den einzelnen Schritten des Assistenten.

Schritt 1. Assistent starten

Klicken Sie auf den Link **Weiter**, um den Assistenten fortzusetzen.

Schritt 2. Einstellungen wiederherstellen

Das Fenster enthält die Schutzkomponenten von Kaspersky Total Security, deren Einstellungen vom Benutzer geändert oder von Kaspersky Total Security beim Training der Komponenten Firewall und Anti-Spam gesammelt wurden. Wenn für eine bestimmte Komponente individuelle Einstellungen festgelegt wurden, werden diese ebenfalls in diesem Fenster genannt (s. Abb. unten).

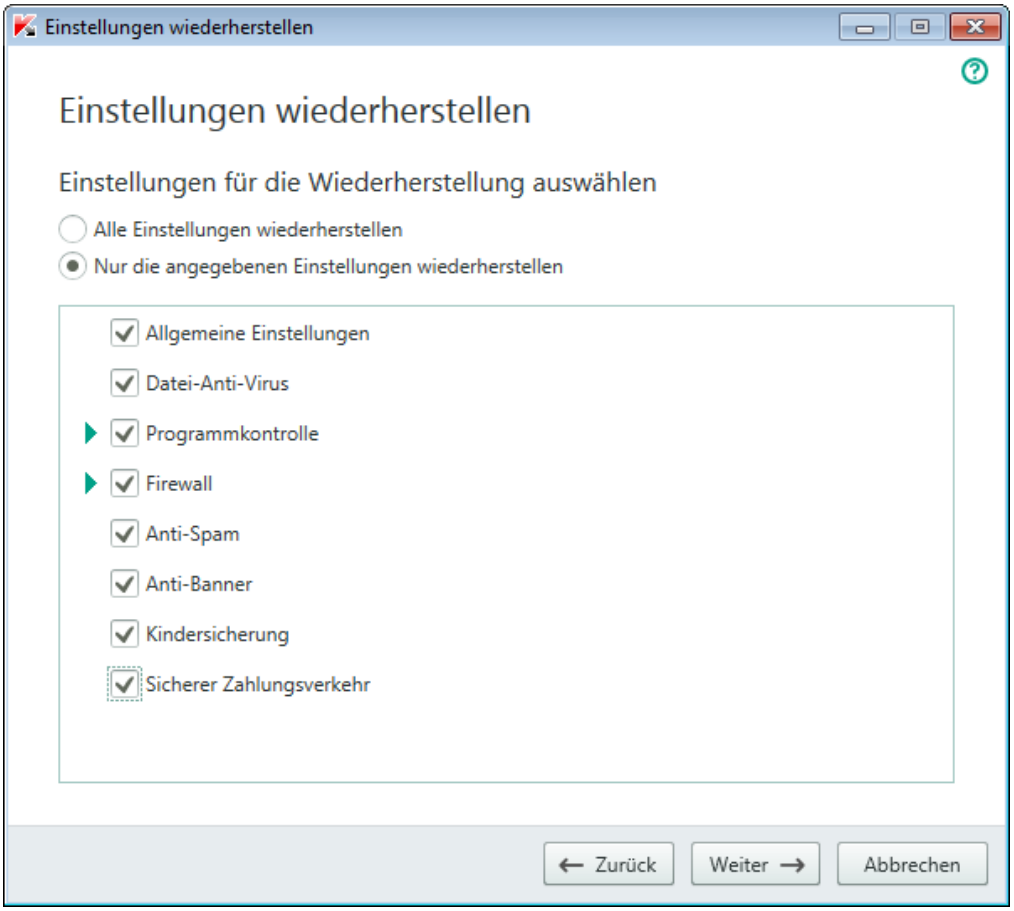

Abbildung 8. Fenster Einstellungen wiederherstellen

Als eindeutige Einstellungen gelten: Listen mit erlaubten und verbotenen Phrasen und Adressen für die Komponente Anti-Spam, Listen mit vertrauenswürdigen Internetadressen und Telefonnummern von Internetprovidern, Ausnahmeregeln für die Programmkomponenten, Firewall-Filterregeln für Pakete und Programme.

Die Einstellungen werden bei der Arbeit von Kaspersky Total Security festgelegt. Dabei werden individuelle Aufgaben und Sicherheitsanforderungen berücksichtigt. Kaspersky Lab empfiehlt, die individuellen Einstellungen zu speichern, wenn die ursprünglichen Programmeinstellungen wiederhergestellt werden.

Aktivieren Sie die Kontrollkästchen für die Einstellungen, die gespeichert werden sollen, und klicken Sie auf **Weiter**.

Schritt 3. Analyse des Betriebssystems

Bei diesem Schritt werden Informationen über Programme gesucht, die zu Microsoft Windows gehören. Diese Programme werden in die Liste der vertrauenswürdigen Anwendungen aufgenommen, deren Aktionen im Betriebssystem nicht beschränkt werden.

Der Assistent geht nach Abschluss der Analyse automatisch zum nächsten Schritt.

Schritt 4. Wiederherstellung abschließen

Klicken Sie auf **Beenden**, um die Arbeit des Assistenten abzuschließen.

BERICHT ÜBER DAS PROGRAMM ANZEIGEN

Kaspersky Total Security führt Berichte über die Arbeit aller Schutzkomponenten. Der Bericht bietet statistische Informationen über das Programm (Sie können beispielsweise nachsehen, wie viele schädliche Objekte das Programm in einem bestimmten Zeitraum gefunden und neutralisiert hat, wie oft das Programm in diesem Zeitraum aktualisiert wurde, wie viele Spam-Mails gefunden wurden, u. a.). Die Berichte werden in verschlüsselter Form aufgezeichnet.

Um einen Bericht über die Programmarbeit anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Zusätzliche Tools anzeigen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie im Fenster **Tools** auf den Link **Bericht**, um das Fenster **Berichte** zu öffnen.

   Das Fenster **Berichte** enthält Berichte über das Programm für den aktuellen Tag (im linken Fensterbereich) und für einen bestimmten Zeitraum (im rechten Fensterbereich).
4. Um einen ausführlichen Programmbericht anzusehen, öffnen Sie das Fenster **Detaillierte Berichte**. Klicken Sie dazu auf den Link **Detaillierte Berichte**, der sich im oberen Bereich des Fensters **Berichte** befindet.

Die Daten im Fenster **Detallierte Berichte** sind in Tabellenform dargestellt. Die Berichtseinträge können auf unterschiedliche Weise angeordnet werden.

PROGRAMMEINSTELLUNGEN AUF EINEM ANDEREN COMPUTER ÜBERNEHMEN

Sie können Ihre Programmeinstellungen für ein anderes Exemplar von Kaspersky Total Security übernehmen, das auf einem anderen Computer installiert ist. Auf diese Weise sind die Einstellungen des Programms auf beiden Computern identisch.

Die Programmeinstellungen werden in einer Konfigurationsdatei gespeichert, die Sie von Computer zu Computer übertragen können.

Die Übertragung von Einstellungen für Kaspersky Total Security von einem Computer auf einen anderen erfolgt in drei Schritten:

1. Programmeinstellungen in einer Konfigurationsdatei speichern.
2. Konfigurationsdatei auf einen anderen Computer übertragen (beispielsweise per E-Mail oder auf einem Wechseldatenträger).
3. Einstellungen aus der Konfigurationsdatei in ein auf einem anderen Computer installiertes Programm importieren.

Um die Programmeinstellungen zu exportieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie über den Link **Einstellungen** im unteren Teil des Fensters das Fenster **Einstellungen**.
3. Wählen Sie im Fenster **Einstellungen** den Abschnitt **Allgemein**.
4. Wählen Sie in der Dropdown-Liste **Einstellungen verwalten** das Element **Einstellungen exportieren**.

   Das Fenster **Speichern unter** wird angezeigt.
5. Geben Sie den Namen der Konfigurationsdatei an und klicken Sie auf die Schaltfläche **Speichern**.

Die Programmeinstellungen werden in der Konfigurationsdatei gespeichert.

Sie können die Programmeinstellungen auch mithilfe der Befehlszeile exportieren. Verwenden Sie dazu den Befehl `avp.com EXPORT <Dateiname>`.

Um Einstellungen in ein auf einem anderen Computer installiertes Programm zu importieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster von Kaspersky Total Security auf dem anderen Computer.
2. Öffnen Sie über den Link **Einstellungen** im unteren Teil des Fensters das Fenster **Einstellungen**.
3. Wählen Sie im Fenster **Einstellungen** den Abschnitt **Allgemein**.
4. Wählen Sie in der Dropdown-Liste **Einstellungen verwalten** das Element **Einstellungen importieren**.

   Das Fenster **Öffnen** wird geöffnet.
5. Geben Sie die Konfigurationsdatei an und klicken Sie auf **Öffnen**.

Die Einstellungen werden in das auf dem anderen Computer installierte Programm importiert.

TEILNAHME AN KASPERSKY SECURITY NETWORK (KSN)

Um Ihren Computer effektiver zu schützen, verwendet Kaspersky Total Security die Cloud-Sicherheit. Die Cloud-Sicherheit basiert auf der Infrastruktur des Kaspersky Security Network und nutzt Daten, die von Benutzern aus der ganzen Welt stammen.

Kaspersky Security Network (KSN) ist eine Infrastruktur der Online-Dienste und -Services, die den Zugriff auf die aktuelle Wissensdatenbank von Kaspersky Lab über den "Ruf" der Dateien, Internet-Ressourcen und Programme bietet. Durch die Verwendung der Daten aus dem Kaspersky Security Network wird die Reaktion von Kaspersky Total Security auf unbekannte Bedrohungen beschleunigt und die Leistungsfähigkeit einiger Schutzkomponenten erhöht. Außerdem reduziert sich das Risiko von Fehlalarmen.

Die Teilnahme von Benutzern an Kaspersky Security Network ermöglicht es, schnell Informationen über neue Bedrohungen und Bedrohungsquellen zu ermitteln, Neutralisierungsmethoden zu entwickeln und die Anzahl von Fehlalarmen zu reduzieren. Durch eine Teilnahme an Kaspersky Security Network erhalten Sie Zugriff auf die Reputations-Datenbanken für Programme und Webseiten.

Wenn Sie an Kaspersky Security Network teilnehmen, werden automatisch Informationen über die Konfiguration Ihres Betriebssystems sowie über den Start- und Endzeitpunkt der Prozesse von Kaspersky Total Security (s. Abschnitt "Über die Zurverfügungstellung von Daten" auf S. 31) an Kaspersky Lab gesendet.

IN DIESEM ABSCHNITT

TEILNAHME AN KASPERSKY SECURITY NETWORK AKTIVIEREN UND DEAKTIVIEREN

Die Teilnahme an Kaspersky Security Network ist freiwillig. Die Verwendung von Kaspersky Security Network kann bei der Installation von Kaspersky Total Security oder jederzeit nach der Programminstallation aktiviert oder deaktiviert werden.

Um die Teilnahme an Kaspersky Security Network zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Hauptfenster auf den Link **Einstellungen**, um das Fenster **Einstellungen** zu öffnen.
3. Wählen Sie im Abschnitt **Erweitert** den Unterabschnitt **Feedback**.

   Dieses Fenster enthält Informationen zum Kaspersky Security Network (KSN) und Einstellungen für eine Teilnahme an KSN.
4. Aktivieren oder deaktivieren Sie mithilfe der Schaltflächen **Aktivieren** / **Deaktivieren** die Teilnahme an Kaspersky Security Network:

   - Wenn Sie an KSN teilnehmen möchten, klicken Sie auf **Aktivieren**.
   - Wenn Sie nicht an KSN teilnehmen möchten, klicken Sie auf **Deaktivieren**.

VERBINDUNG ZUM KASPERSKY SECURITY NETWORK PRÜFEN

Mögliche Gründe, warum keine Verbindung mit dem Kaspersky Security Network besteht:

- Sie nehmen nicht an Kaspersky Security Network teil.
- Ihr Computer ist nicht mit dem Internet verbunden.
- Der aktuelle Schlüsselstatus erlaubt keine Verbindung mit dem Kaspersky Security Network.

Der aktuelle Schlüsselstatus wird im Fenster **Lizenzverwaltung** angezeigt.

Um zu prüfen, ob eine Verbindung zum Kaspersky Security Network besteht, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Hauptfenster auf den Link **Einstellungen**, um das Fenster **Einstellungen** zu öffnen.
3. Wählen Sie im Abschnitt **Erweitert** den Unterabschnitt **Feedback**.

Dieses Fenster zeigt den Status der Verbindung zum Kaspersky Security Network.

STEUERUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE

Kaspersky Total Security kann über die Befehlszeile gesteuert werden.

Syntax der Befehlszeile:

```
avp.com <Befehl> [Parameter]
```

Um Hilfeinformationen zur Syntax der Befehlszeile anzuzeigen, verwenden Sie folgenden Befehl:

```
avp.com [ /? | HELP ]
```

Durch diesen Befehl erhalten Sie eine vollständige Liste der Befehle, die für die Steuerung von Kaspersky Total Security über die Befehlszeile zulässig sind.

Um Hilfeinformationen zur Syntax einer konkreten Befehlszeile anzuzeigen, verwenden Sie einen der folgenden Befehle:

```
avp.com <Befehl> /?
avp.com HELP <Befehl>
```

Um über die Befehlszeile auf das Programm zuzugreifen, wechseln Sie entweder in den Zielordner des Programms oder geben Sie den vollständigen Pfad für avp.com an.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Dieser Abschnitt beschreibt, wie Sie technische Unterstützung erhalten können und nennt die Voraussetzungen, die dafür erfüllt sein müssen.

IN DIESEM ABSCHNITT

WIE SIE TECHNISCHEN KUNDENDIENST ERHALTEN

Wenn Sie in der Programmdokumentation und in den Informationsquellen zum Programm (s. Abschnitt "Informationsquellen zum Programm" auf S. 12) keine Lösung für Ihr Problem finden können, empfehlen wir Ihnen, sich an den Technischen Support von Kaspersky Lab zu wenden. Die Support-Mitarbeiter beantworten Ihre Fragen zur Installation und Verwendung des Programms.

Beachten Sie die Support-Richtlinien (http://support.kaspersky.com/de/support/rules), bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- Telefonisch. Sie können sich am telefonisch von den Spezialisten des lokalen oder internationalen Technischen Supports beraten lassen.
- Anfrage senden über das Portal My Kaspersky. Sie können sich über ein Webformular an die Support-Experten wenden.

Der Technische Support steht nur den Benutzern zur Verfügung, die eine Lizenz für die Programmnutzung gekauft haben. Die Benutzer von Testversionen haben keinen Anspruch auf technischen Kundendienst.

TECHNISCHER SUPPORT AM TELEFON

Bei dringenden Problemen können Sie den lokalen oder internationalen Technischen Support anrufen (http://support.kaspersky.com/de/support/international).

Beachten Sie die Support-Richtlinien (http://support.kaspersky.com/de/support/rules), bevor Sie sich an den Technischen Support wenden. Dadurch können unsere Spezialisten Ihnen möglichst schnell helfen.

TECHNISCHER SUPPORT ÜBER DAS PORTAL MY KASPERSKY

My Kaspersky ist Ihr persönlicher Bereich (https://my.kaspersky.com/de) auf der Seite des Technischen Supports.

Um auf das Portal My Kaspersky zugreifen zu können, müssen Sie sich auf der Registrierungsseite registrieren (https://my.kaspersky.com/de/registration). Geben Sie Ihre E-Mail-Adresse und das Kennwort für den Zugriff auf das Portal My Kaspersky an.

Das Portal My Kaspersky bietet folgende Möglichkeiten:

- Anfragen an den Technischen Support und an das Virenlabor senden.
- Mit dem Technischen Support kommunizieren, ohne E-Mails zu verwenden.
- Status Ihrer Anfragen in Echtzeit verfolgen.
- Vollständigen Verlauf Ihrer Anfragen an den Technischen Support ansehen.
- Kopie einer Schlüsseldatei erhalten, falls die Schlüsseldatei verloren gegangen ist oder gelöscht wurde.

E-Mail-Anfrage an den Technischen Support

Anfragen an den Technischen Support können per E-Mail auf Deutsch, Englisch, Französisch, Spanisch oder Russisch gestellt werden.

Füllen Sie folgende Felder des elektronischen Formulars aus:

- Typ der Anfrage.
- Name und Versionsnummer des Programms;
- Anfragetext.
- Kundennummer und Kennwort.
- E-Mail-Adresse.

Die Support-Spezialisten antworten über das Portal My Kaspersky und an die E-Mail-Adresse, die Sie in der Anfrage angegeben haben.

Elektronische Anfrage an das Virenlabor

Beachten Sie, dass für die Bearbeitung bestimmter Anfragen nicht der Technische Support, sondern das Virenlabor verantwortlich ist.

Sie können Anfragen zur Analyse von verdächtigen Dateien oder Webressourcen an das Virenlabor schicken. Sie können sich auch an das Virenlabor wenden, wenn Sie einen Fehlalarm von Kaspersky Total Security vermuten und die betroffenen Dateien oder Webressourcen für sicher halten.

Anfragen an das Virenlabor sind auch über ein Anfrageformular auf der Support-Seite (http://support.kaspersky.ru/virlab/helpdesk.html) möglich. Dazu ist keine Registrierung beim Portal My Kaspersky notwendig. Die Angabe eines Aktivierungscodes für das Programm ist dabei nicht erforderlich.

INFORMATIONEN FÜR DEN TECHNISCHEN SUPPORT SAMMELN

Wenn Sie sich mit einem Problem an den Technischen Support wenden, bitten die Support-Experten Sie möglicherweise darum, einen Bericht über den Systemzustand zu erstellen und den Bericht an den Technischen Support zu schicken. Es kann sein, dass die Support-Experten zusätzlich eine Protokolldatei von Ihnen anfordern. Eine Protokolldatei ermöglicht eine schrittweise Prüfung von ausgeführten Programmbefehlen. Dadurch lässt sich erkennen, auf welcher Etappe ein Fehler aufgetreten ist.

Aufgrund einer Analyse der von Ihnen eingesandten Daten können die Support-Experten ein AVZ-Skript erstellen, das dann an Sie geschickt wird. Mithilfe von AVZ-Skripten können laufende Prozesse auf schädlichen Code analysiert, das System auf schädlichen Code untersucht, infizierte Dateien desinfiziert bzw. gelöscht, und ein Bericht über die Ergebnisse der Systemuntersuchung erstellt werden.

Es kann es sein, dass Sie von den Support-Experten dazu aufgefordert werden, die Programmeinstellungen vorübergehend zu ändern. Eine solche Maßnahme dient dazu, den Support effektiver zu gestalten und eine Fehlerdiagnose vorzunehmen. Dafür können folgende Aktionen erforderlich sein:

- Aktivieren der Funktion zum Sammeln erweiterter Diagnoseinformationen.
- Anpassen spezieller Einstellungen für bestimmte Programmkomponenten, die über die standardmäßige Programmoberfläche nicht verfügbar sind.
- Ändern der Einstellungen für das Speichern und Senden von gesammelten Diagnoseinformationen.
- Einstellungen für das Abfangen und Speichern von Daten über den Netzwerkverkehr.

Alle Informationen, die für die oben genannten Aktionen erforderlich sind (Anleitungen, zu ändernde Einstellungen, Konfigurationsdateien, Skripte, erweiterte Optionen für die Befehlszeile, Debug-Module und spezielle Tools), sowie Informationen über den Umfang der im Rahmen der Fehlersuche zu sammelnden Daten werden Ihnen von den Support-Experten mitgeteilt. Die zusätzlich gesammelten Diagnoseinformationen werden auf dem Benutzercomputer gespeichert. Gesammelte Daten werden nicht automatisch an Kaspersky Lab gesendet.

Die oben genannten Aktionen dürfen nur unter Anleitung eines Support-Experten erfolgen. Wenn die Programmeinstellungen auf andere Weise geändert werden, als im Administratorhandbuch oder in den Anleitungen der Support-Experten beschrieben, kann es sein, dass die Funktion des Betriebssystems verlangsamt oder gestört wird, das Sicherheitsniveau des Computers sinkt, und die Verfügbarkeit und Integrität der verarbeiteten Informationen gestört werden.

IN DIESEM ABSCHNITT

BERICHT ÜBER DEN ZUSTAND DES BETRIEBSSYSTEMS ERSTELLEN

Gehen Sie folgendermaßen vor, um einen Bericht über den Zustand des Betriebssystems zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Support** im unteren Fensterbereich das Fenster **Support**.

3. Klicken Sie im folgenden Fenster auf den Link **Support Tools**.

   Das Fenster **Support Tools** wird geöffnet.

4. Klicken Sie im folgenden Fenster auf den Link **Bericht über das Betriebssystem erstellen**.

Der Bericht über den Zustand des Betriebssystems wird in den Formaten html und xml erstellt und im Archiv sysinfo.zip gespeichert. Nachdem die Ermittlung von Daten über das Betriebssystem abgeschlossen wurde, können Sie einen Bericht ansehen.

Gehen Sie folgendermaßen vor, um einen Bericht anzuzeigen:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Support** im unteren Fensterbereich das Fenster **Support**.
3. Klicken Sie im folgenden Fenster auf den Link **Support Tools**.

   Das Fenster **Support Tools** wird geöffnet.

4. Klicken Sie im folgenden Fenster auf den Link **Bericht anzeigen**.

   Microsoft Windows Explorer wird geöffnet.

5. Öffnen Sie im folgenden Fenster das Archiv sysinfo.zip. Es enthält die Berichtsdateien.

DATEIEN MIT DATEN SENDEN

Nachdem die Protokolldateien und der Bericht über den Zustand des Betriebssystems erstellt wurden, müssen diese an den Technischen Support von Kaspersky Lab geschickt werden.

Um die Dateien auf den Server des Technischen Supports hochzuladen, benötigen Sie eine Anfragenummer. Diese Nummer ist im Portal My Kaspersky verfügbar, wenn eine aktive Anfrage vorliegt.

Gehen Sie folgendermaßen vor, um die Dateien mit den Daten auf den Server des Technischen Supports hochzuladen:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Support** im unteren Fensterbereich das Fenster **Support**.
3. Klicken Sie im folgenden Fenster auf den Link **Support Tools**.

   Das Fenster **Support Tools** wird geöffnet.

4. Klicken Sie im folgenden Fenster auf den Link **Bericht an den Technischen Support senden**.

   Das Fenster **Bericht senden** wird geöffnet.

5. Aktivieren Sie die Kontrollkästchen für die Daten, die an den Technischen Support geschickt werden sollen.
6. Klicken Sie auf **Bericht senden**.

   Die gewählten Dateien werden komprimiert und an den Server des Technischen Supports gesendet.

Falls kein Kontakt mit dem Technischen Support möglich ist, können Sie diese Dateien auf Ihrem Computer speichern und sie später aus dem Portal My Kaspersky absenden.

Gehen Sie folgendermaßen vor, um die Dateien mit Daten auf der Festplatte zu speichern:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Support** im unteren Fensterbereich das Fenster **Support**.
3. Klicken Sie im folgenden Fenster auf den Link **Support Tools**.

4. Das Fenster **Support Tools** wird geöffnet.

5. Klicken Sie im folgenden Fenster auf den Link **Bericht an den Technischen Support senden**.

   Das Fenster **Bericht senden** wird geöffnet.

6. Wählen Sie den Typ der Daten aus, die Sie senden möchten:

   - **Informationen zum Betriebssystem**. Aktivieren Sie dieses Kontrollkästchen, wenn Sie Informationen zum Betriebssystem Ihres Computers an den Technischen Support senden möchten.

   - **Für die Analyse gesammelte Daten** Aktivieren Sie dieses Kontrollkästchen, wenn Sie Protokolldateien an den Technischen Support senden möchten. Öffnen Sie mit dem Link **<Anzahl der Dateien>, <Datenmenge>** das Fenster **Für die Analyse gesammelte Daten**. Aktivieren Sie die Kontrollkästchen für jene Protokolldateien, die gesendet werden sollen.

7. Klicken Sie auf den Link **Bericht speichern**.

   Ein Fenster zum Speichern des Archivs wird geöffnet.

8. Geben Sie einen Namen für das Archiv an und bestätigen Sie das Speichern.

Das fertige Archiv können Sie über das Portal My Kaspersky an den Technischen Support senden.

ÜBER DIE ZUSAMMENSETZUNG UND SPEICHERUNG VON PROTOKOLLDATEIEN

Protokolldateien werden während der gesamten Nutzungsdauer des Programms in verschlüsselter Form auf Ihrem Computer gespeichert. Sie werden unwiderruflich gelöscht, wenn das Programm entfernt wird.

Protokolldateien werden im Ordner ProgramData\Kaspersky Lab abgelegt.

Protokolldateien werden nach folgendem Prinzip benannt:
`KAV<Versionsnummer_dateXX.XX_timeXX.XX_pidXXX.><Typ der Protokolldatei>.log.enc1.`

Alle Protokolldateien enthalten folgende allgemeine Daten:

- Ereigniszeitpunkt
- Thread-Nummer
- Programmkomponente, auf die das Ereignis zurückgeht.
- Ereigniskategorie (informativ, Warnung, kritisch, Fehler)
- Ereignisbeschreibung für den Befehl der Programmkomponente und Ausführungsergebnis für diesen Befehl.

Inhalt der Protokolldateien SRV.log, GUI.log und ALL.log

In den Protokolldateien SRV.log und GUI.log können folgende Informationen aufgezeichnet werden:

- Persönliche Daten wie Nachname und Vorname, falls diese Daten Bestandteil eines Dateipfads auf dem lokalen Computer sind.

- Benutzername und Kennwort, falls diese im Klartext übertragen wurden. Diese Daten können bei der Untersuchung des Internet-Datenverkehrs in den Protokolldateien gespeichert werden. Der Datenverkehr wird nur aus trafmon2.ppl in Protokolldateien aufgezeichnet.

- Benutzername und Kennwort, Cookie-Dateien, falls diese in HTTP-Kopfzeilen enthalten sind.

- Benutzername für die Anmeldung bei Microsoft Windows, falls der Name des Benutzerkontos Bestandteil eines Dateinamens ist.
- Ihre E-Mail-Adresse oder Webadresse mit Benutzername und Kennwort, falls diese im Namen eines gefundenen Objekts enthalten sind.
- Webseiten, die Sie besuchen, sowie Links von diesen Webseiten. Diese Daten werden in Protokolldateien aufgezeichnet, wenn das Programm Webseiten untersucht.
- Adresse des Proxyservers, Computername, Port, IP-Adresse, Benutzername, der bei der Autorisierung auf dem Proxyserver verwendet wird. Diese Daten werden in Protokolldateien aufgezeichnet, wenn das Programm einen Proxyserver verwendet.
- Externe IP-Adressen, mit denen eine Verbindung zu Ihrem Computer aufgebaut wurde.
- Nachrichtenbetreff, ID, Name des Absenders und Webadresse des Nachrichtenabsenders in einem sozialen Netzwerk. Diese Daten werden in Protokolldateien aufgezeichnet, wenn die Komponente Kindersicherung aktiviert ist.

Inhalt der Protokolldateien HST.log, BL.log, Dumpwriter.log

Die Protokolldatei HST enthält Informationen über die Aktualisierung der Datenbanken und Programm-Module.

Die Protokolldatei BL enthält Informationen über Ereignisse, die im Programm auftreten, sowie Daten, die im Programm zur Problembehebung benötigt werden. Diese Datei wird erstellt, wenn das Programm mit dem Schlüssel avp.exe –bl gestartet wird.

Die Protokolldatei dumpwriter.log enthält Verwaltungsinformationen, die zur Behebung von Problemen benötigt werden, die bei der Protokollierung von Speicherdumpdateien auftreten.

Inhalt der Protokolldateien für die Programm-Plug-ins

Die Protokolldateien für die Programm-Plug-ins enthalten folgende Informationen:

- VirtualKeyboard (VKB.log) enthält Verwaltungsinformationen über das Plug-in und Daten, die im Plug-in zur Problembehebung benötigt werden.
- Online Banking (OB.log) enthält Verwaltungsinformationen über das Plug-in, darunter auch Informationen über Ereignisse bei der Untersuchung von Webseiten und über Ergebnisse dieser Untersuchung, über Verbindungen mit Remote-IP-Adressen, Proxyserver-Einstellungen und Cookie-Dateien. Die Datei enthält außerdem Daten, die im Plug-in zur Problembehebung benötigt werden.
- ContentBlocker (CB.log) enthält Verwaltungsinformationen über das Plug-in, darunter auch Informationen über Ereignisse bei der Untersuchung von Webseiten, über Untersuchungsergebnisse, über Verbindungen mit Remote-IP-Adressen, Proxyserver-Einstellungen. Die Datei enthält außerdem Daten, die im Plug-in zur Problembehebung benötigt werden.
- Office Anti-Virus (OA.log) enthält Informationen über die Untersuchung von Microsoft-Office-Dokumenten. Diese Datei enthält außerdem Informationen zum vollständigen Pfad des Dokuments oder zur Adresse der Webseite, von der dieses Dokument heruntergeladen wurde.
- Protokolldatei des Plug-ins für den Start der Untersuchungsaufgabe aus dem Kontextmenü (shellex.dll.log). Enthält Informationen über die Ausführung der Untersuchungsaufgabe und Daten, die im Plug-in zur Problembehebung benötigt werden.
- Protokolldateien für das Plug-in für Microsoft Outlook:
  - mcouas.OUTLOOK.EXE Plug-in für Anti-Spam
  - mcou.OUTLOOK.EXE Plug-in für Mail-Anti-Virus

  Die Dateien können Teile von E-Mail-Nachrichten enthalten, darunter auch Adressen.
- Die Protokolldatei des Plug-ins für die Registrierung der Erweiterung für Google Chrome (NativeMessagingHost.log) enthält Verwaltungsinformationen für das Plug-in.

AVZ-SKRIPT AUSFÜHREN

Es wird davor gewarnt, den Text eines Skripts, das Ihnen von den Support-Spezialisten geschickt wurde, zu verändern. Falls bei der Skript-Ausführung Probleme auftreten sollten, wenden Sie sich bitte an den Technischen Support.

Gehen Sie folgendermaßen vor, um ein AVZ-Skript auszuführen:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Support** im unteren Fensterbereich das Fenster **Support**.
3. Klicken Sie im folgenden Fenster auf den Link **Support Tools**.

   Das Fenster **Support Tools** wird geöffnet.
4. Klicken Sie im folgenden Fenster auf den Link **Skript ausführen**.

   Das Fenster **Skript-Ausführung** wird geöffnet.
5. Kopieren Sie den Text des Skripts, das Sie vom Technischen Support erhalten haben, fügen Sie den Text im folgenden Fenster ins Eingabefeld ein und klicken Sie auf **Ausführen**.

Die Skript-Ausführung wird gestartet.

Wenn das Skript erfolgreich ausgeführt wurde, wird der Assistent automatisch abgeschlossen. Falls bei der Skript-Ausführung Störungen auftreten, zeigt der Assistent eine entsprechende Meldung an.

EINSCHRÄNKUNGEN UND WARNUNGEN

Kaspersky Total Security besitzt eine Reihe von nicht kritischen Einschränkungen.

Einschränkungen beim Upgrade einer älteren Programmversion

- Beim Upgrade einer älteren Programmversion von Kaspersky Total Security werden folgende Programmeinstellungen durch standardmäßige Einstellungen ersetzt: Update-Quellen, Liste für vertrauenswürdige Webadressen, Einstellungen für das Modul zur Link-Untersuchung.

- Wenn die neue Version von Kaspersky Total Security über eine ältere Version als Kaspersky PURE 2.0 installiert wird, so gehen Sicherungskopien von Dateien sowie die Quarantäne- und Backup-Objekte verloren, da ihr Format nicht unterstützt wird und nicht in das neue Format umgewandelt werden kann. Bei einem Programm-Upgrade der Version Kaspersky PURE 2.0 können die Sicherungskopien für Dateien sowie die Quarantäne- und Backup-Objekte umgewandelt werden. Der Backup-Speicher im Format für Kaspersky CRYSTAL 3.0 wird unterstützt und muss nicht in das neue Format umgewandelt werden.

Einschränkungen für bestimmte Komponenten und für die automatische Dateiverarbeitung

Infizierte Dateien werden automatisch nach den Regeln verarbeitet, die von den Kaspersky-Lab-Experten erstellt wurden. Sie können diese Regeln nicht manuell ändern. Die Regeln werden beim Update der Antiviren-Datenbanken und Programm-Module aktualisiert. Daneben werden auch die Regeln für die Firewall, für die Programmkontrolle und für den Modus für vertrauenswürdige Programme automatisch aktualisiert.

Einschränkungen für die Untersuchung von Dateien und Webseiten-Zertifikaten

Das Programm kann bei der Untersuchung einer Datei und eines Webseiten-Zertifikats auf Informationen aus dem Kaspersky Security Network zugreifen. Wenn die Anfrage beim Kaspersky Security Network keine Daten ergibt, entscheidet das Programm anhand der lokalen Antiviren-Datenbanken darüber, ob die Datei infiziert oder das Zertifikat nicht vertrauenswürdig ist.

Funktionelle Einschränkungen für den Aktivitätsmonitor

Die Funktionalität zur Abwehr von Verschlüsselungsprogrammen (Verschlüsselung von Benutzerdateien durch Schadsoftware) besitzt folgende Einschränkungen:

- Für diese Funktionalität wird der Systemordner Temp verwendet. Falls auf dem Systemlaufwerk, auf dem sich der Temp-Ordner befindet, nicht genügend freier Platz für die temporären Dateien vorhanden ist, wird der Schutz vor Verschlüsselungsprogrammen nicht ausgeführt. In diesem Fall erfolgt keine Meldung darüber, dass eine Datensicherung nicht vorgenommen wird (bzw. der Schutz nicht ausgeführt wird).

- Die temporären Dateien werden automatisch gelöscht, wenn Kaspersky Total Security beendet oder wenn die Komponente Aktivitätsmonitor deaktiviert wird.

- Wenn Kaspersky Total Security unvorhergesehen beendet wird, werden die temporären Dateien nicht automatisch gelöscht. Die temporären Dateien müssen dann manuell gelöscht werden. Öffnen Sie dazu das Fenster **Ausführen** (in Windows XP im **Startmenü**) und geben Sie im Feld **Öffnen** den Wert `%TEMP%` ein. Klicken Sie auf **OK**.

Warnung über das Sammeln von Diagnoseinformationen

Diagnoseinformationen über das Programm, die Sie für den Technischen Support sammeln, werden verschlüsselt. Die Verschlüsselung kann bei Bedarf deaktiviert werden.

Funktionelle Einschränkungen für Sichere Verbindungen

Aufgrund technischer Einschränkungen der Untersuchungsalgorithmen werden bei der Untersuchung sicherer Verbindungen bestimmte Erweiterungen des Protokolls TLS 1.0 und höher nicht unterstützt (insbesondere NPN und ALPN). Eine Verbindung unter Verwendung dieser Protokolle kann eingeschränkt sein. Internetbrowser, die das SPDY-Protokoll unterstützen, verwenden anstelle von SPDY das HTTP-Protokoll mit TLS, auch wenn der Server, zu dem eine Verbindung hergestellt wird, SPDY unterstützt. Die Sicherheit der Verbindung wird dadurch nicht reduziert.

Warnung für die Funktion der Komponente Anti-Spam

Die Funktionalität der Schutzkomponente Anti-Spam kann mithilfe der Konfigurationsdatei für die Komponente Anti-Spam angepasst werden.

Einschränkungen für die Komponente Sichern und Wiederherstellen

Für die Komponente Sichern und Wiederherstellen gelten folgende Einschränkungen:

- Ein Online-Speicher für Sicherungskopien ist nicht mehr verfügbar, wenn eine andere Festplatte ausgewählt oder ein neuer Computer verwendet wird. Informationen darüber, wie die Verbindung zu einem Online-Speicher beim Austausch der Hardware wiederhergestellt wird, finden Sie auf der Webseite des Technischen Support von Kaspersky Lab.

- Änderungen in den Dienstdateien eines Sicherungsspeichers können dazu führen, dass Sie den Zugriff auf den Sicherungsspeicher verlieren und Ihre Daten nicht wiederherstellen können.

Funktionelle Einschränkungen für Virtuelle Datentresore

Für einen Datentresor, der auf einem FAT32-Dateisystem erstellt werden soll, darf die Datentresordatei maximal 4 GB groß sein.

Besonderheiten bei der Rootkit-Untersuchung des Kernelspeichers im Sicheren Browser

Wenn bei der Arbeit im Sicheren Browser ein nicht vertrauenswürdiges Modul gefunden wird, öffnet sich im Browser eine neue Registerkarte mit einer Meldung über den Schadsoftware-Fund. Für diesen Fall wird empfohlen, den Browser zu beenden und den Computer vollständig zu untersuchen.

Besonderheiten beim Schutz von Daten in der Zwischenablage

In folgenden Fällen erlaubt Kaspersky Total Security einem Programm den Zugriff auf die Zwischenablage:

- Ein Programm mit einem aktiven Fenster versucht, Daten in die Zwischenablage einzufügen. Ein Fenster gilt als aktiv, wenn Sie gerade damit arbeiten.

- Ein geschützter Programmprozess versucht, Daten in die Zwischenablage einzufügen.

- Ein geschützter Programmprozess oder ein Prozess mit einem aktiven Fenster versucht, Daten aus der Zwischenablage zu lesen.

- Ein Programmprozess versucht, Daten aus der Zwischenablage zu lesen, die er vorher selbst in die Zwischenablage eingefügt hat.

Warnung zur Kompatibilität mit Kaspersky-Lab-Programmen

Das Programm Kaspersky Total Security ist mit folgenden Kaspersky-Lab-Programmen kompatibel:

- Kaspersky Fraud Prevention 2.0

- Kaspersky Fraud Prevention 2.5

- Kaspersky Fraud Prevention 3.0
- Kaspersky Password Manager 2.0
- Kaspersky Password Manager 5.0
- Kaspersky Password Manager 7.0

Besonderheiten bei der Verarbeitung von Schadsoftware durch die Programmkomponenten

Das Programm kann irreparable Dateien standardmäßig löschen. Das standardmäßige Löschen kann bei der Dateiverarbeitung durch Komponenten wie Programmkontrolle, Mail-Anti-Virus oder Datei-Anti-Virus, im Rahmen von Untersuchungsaufgaben sowie beim Erkennen von gefährlichen Programmaktivitäten durch die Komponente Aktivitätsmonitor erfolgen.

Einschränkungen für bestimmte Komponenten bei gleichzeitiger Installation mit dem Programm Kaspersky Fraud Prevention for Endpoint

Für folgende Komponenten von Kaspersky Total Security sind die Funktionen im Sicheren Browser beschränkt, wenn das Programm gemeinsam mit Kaspersky Fraud Prevention for Endpoint installiert wurde:

- Web-Anti-Virus, außer Anti-Phishing
- Kindersicherung
- Modul zur Link-Untersuchung
- Anti-Banner

Funktionale Einschränkungen von Kaspersky Total Security auf Microsoft Windows 10

Wenn Sie das Programm auf dem Betriebssystem Microsoft Windows 10 installiert haben, steht folgende Funktionalität nicht zur Verfügung:

- Screenshot-Schutz
- Schutz von Daten in der Zwischenablage
- Schutz vor Webcam-Zugriff
- Aktive Desinfektion

Bei der Installation des Programms auf dem Betriebssystem Microsoft Windows 10 ist auch folgende Funktionalität teilweise eingeschränkt:

- Selbstschutz. Der Selbstschutz der grafischen Programmoberfläche funktioniert auch dann nicht, wenn er aktiviert ist.
- Aktivitätsmonitor.
- Schutz vor Verschlüsselungsprogrammen und Ransomware. Das Programm kann nur die einfache Verschlüsselungsprogramme und Ransomware erkennen.
- Programmkontrolle. Vom Benutzer erstellte Regeln für Programme funktionieren nicht. Die Kategorisierung von Programmen im neuen Windows-Design wird fehlerhaft ausgeführt.

GLOSSAR

A

AKTIVIERUNGSCODE

Code, den Sie beim Kauf einer Lizenz für die Nutzung von Kaspersky Total Security erhalten. Dieser Code ist für die Programmaktivierung erforderlich.

Ein Aktivierungscode besteht aus einer Folge von zwanzig Ziffern und lateinischen Buchstaben im Format XXXXX-XXXXX-XXXXX-XXXXX.

ANTIVIREN-DATENBANKEN

Datenbanken mit Informationen über Computer-Bedrohungen, die Kaspersky Lab beim Erscheinen der Antiviren-Datenbanken bekannt sind. Mithilfe der Einträge in den Antiviren-Datenbanken wird in den Untersuchungsobjekten schädlicher Code identifiziert. Die Antiviren-Datenbanken werden von den Kaspersky-Lab-Spezialisten gepflegt und stündlich aktualisiert.

AUFGABE

Funktionen, die das Kaspersky-Lab-Programm ausführen kann und die als Aufgaben realisiert sind. Beispiele: Echtzeitschutz für Dateien, Vollständige Untersuchung des Computers, Datenbank-Update.

AUFGABENEINSTELLUNGEN

Parameter für die Arbeit des Programms, die für jeden Aufgabentyp individuell sind.

AUTOSTART-OBJEKTE

Programme, die für den Start und die korrekte Funktionsweise des Betriebssystems und der Software auf Ihrem Computer erforderlich sind. Diese Objekte werden jedes Mal beim Hochfahren des Betriebssystems gestartet. Es gibt Viren, die speziell Autostart-Objekte infizieren können. Dadurch kann beispielsweise das Hochfahren des Betriebssystems blockiert werden.

B

BEDROHUNGSSTUFE

Index für die Wahrscheinlichkeit, mit der ein Computerprogramm eine Bedrohung für das Betriebssystem darstellt. Die Bedrohungsstufe wird durch eine heuristische Analyse ermittelt, die auf zweierlei Kriterien beruht:

- Statische Kriterien (z. B. Informationen über die ausführbare Programmdatei: Dateigröße, Erstellungsdatum usw.).
- Dynamische Kriterien, die dazu dienen, die Arbeit des Programms in einer virtuellen Umgebung zu modellieren (Analyse der Aufrufe von Systemfunktionen durch das Programm).

Die Bedrohungsstufe erlaubt es, ein für Schadprogramme typisches Verhalten zu identifizieren. Je geringer der Bedrohungsgrad, desto mehr Aktionen werden einem Programm im Betriebssystem erlaubt.

D

DATEIMASKE

Darstellung eines Dateinamens durch Platzhalter. Die wichtigsten Zeichen, die in Dateimasken verwendet werden, sind * und ? (wobei * - eine beliebige Anzahl von beliebigen Zeichen und ? – ein beliebiges Zeichen).

DATENBANK FÜR PHISHING-WEBADRESSEN

Eine Liste der Webressourcen, die von den Kaspersky-Lab-Spezialisten als Phishing-Adressen eingestuft wurden. Die Datenbank wird regelmäßig aktualisiert und gehört zum Lieferumfang des Kaspersky-Lab-Programms.

DATENBANK FÜR SCHÄDLICHE WEBADRESSEN

Eine Liste der Webressourcen, deren Inhalt als gefährlich eingestuft werden kann. Die Liste ist von den Kaspersky-Lab-Spezialisten angelegt, wird regelmäßig aktualisiert und gehört zum Lieferumfang des Programms.

DATENSICHERUNG

Erstellen von Sicherungskopien für Daten, die auf dem Computer gespeichert sind. Sicherungskopien werden erstellt, um vor einem Datenverlust aufgrund von Diebstahl, Hardware-Funktionsstörungen oder Angriffen zu schützen.

DIGITALE SIGNATUR

Verschlüsselter Datenblock, der zu einem Dokument oder Programm gehört. Eine digitale Signatur dient dazu, den Autor eines Dokuments oder Programms zu identifizieren. Zum Erstellen einer digitales Signatur benötigt der Autor eines Dokuments oder Programms ein digitalen Zertifikat, das die Identität des Autors bestätigt.

Mit einer digitalen Signatur können Quelle und Integrität von Daten überprüft werden. Dies bietet Schutz vor Fälschungen.

F

FEHLALARM

Situation, in der ein virenfreies Objekt von der Kaspersky-Lab-Anwendung als infiziert eingestuft wird, weil sein Code Ähnlichkeit mit einem Virus aufweist.

G

GEPACKTE DATEI

Archivdatei, die ein Extrahierprogramm und für das Betriebssystem bestimmte Extrahierbefehle enthält.

GÜLTIGKEITSDAUER DER LIZENZ

Zeitraum, für den Sie die Programmfunktionen und Zusatzleistungen nutzen dürfen.

H

HEURISTISCHE ANALYSE

Technologie zur Erkennung von Bedrohungen, die noch nicht in den Datenbanken von Kaspersky Lab verzeichnet sind. Die heuristische Analyse erkennt Objekte, deren Verhalten eine Sicherheitsbedrohung für das Betriebssystem darstellen kann. Objekte, die mithilfe der heuristischen Analyse gefunden werden, werden als möglicherweise infiziert eingestuft. Als möglicherweise infiziert kann beispielsweise ein Objekt gelten, das eine Befehlsfolge enthält, die für schädliche Objekte als charakteristisch gilt (Datei öffnen, in Datei schreiben).

HYPERVISOR

Programm, das die Arbeit mehrerer Betriebssysteme auf einem Computer ermöglicht.

I

INFIZIERTES OBJEKT

Objekt, das einen Codeabschnitt enthält, der mit dem Codeabschnitt eines bekannten Programms, das eine Bedrohung darstellt, übereinstimmt. Die Kaspersky-Lab-Experten warnen davor, mit solchen Objekten zu arbeiten.

INKOMPATIBLES PROGRAMM

Antiviren-Programm eines Drittherstellers oder Kaspersky-Lab-Programm, das nicht mit Kaspersky Total Security verwaltet werden kann.

K

KASPERSKY SECURITY NETWORK (KSN)

Eine Infrastruktur von Online-Diensten und -Services, die Zugriff auf eine aktuelle Wissensdatenbank von Kaspersky Lab bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Verwendung von Daten aus dem Kaspersky Security Network wird die Reaktion von Kaspersky Anti-Virus auf unbekannte Bedrohungen beschleunigt und die Leistungsfähigkeit für bestimmte Komponenten erhöht. Außerdem verringert sich das Risiko von Fehlalarmen.

KASPERSKY-LAB-UPDATESERVER

HTTP-Server von Kaspersky Lab, von denen das Kaspersky-Lab-Programm die Updates für Datenbanken und Programm-Module herunterlädt.

KEYLOGGER

Ein Programm, das dazu dient, die Tastatureingaben des Benutzers an einem Computer heimlich zu protokollieren. Keylogger werden auch Tasten-Rekorder genannt.

L

LAUFWERKSBOOTSEKTOR

Ein Bootsektor ist ein spezieller Sektor auf der Festplatte eines Computers, auf einer Diskette oder auf einem anderen Gerät zur Datenspeicherung. Er enthält Angaben über das Dateisystem des Datenträgers und ein Bootprogramm, das für den Start des Betriebssystems verantwortlich ist.

Laufwerksbootsektoren können von so genannten Bootviren infiziert werden. Die Kaspersky-Lab-Anwendung erlaubt es, Bootsektoren auf Viren zu untersuchen und infizierte Sektoren zu desinfizieren.

M

MÖGLICHER SPAM

E-Mail, die sich nicht eindeutig als Spam einstufen lässt, die aber bestimmte Spam-Merkmale aufweist (betrifft beispielsweise bestimmte Arten von Massenmails und Werbenachrichten).

MÖGLICHERWEISE INFIZIERTES OBJEKT

Objekt, das einen modifizierten Codeabschnitt einer bekannten Bedrohung enthält, oder ein Objekt, dessen Verhalten dem Verhalten dieser Bedrohung ähnelt.

O

OBJEKT BLOCKIEREN

Der Zugriff externer Programme auf ein Objekt wird verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt, verändert oder gelöscht werden.

P

PHISHING

Typ des Internetbetrugs, bei dem versucht wird, unberechtigten Zugriff auf sensible Benutzerdaten zu erhalten.

PROGRAMM AKTIVIEREN

Freischalten aller Programmfunktionen. Die Aktivierung wird während oder nach der Programminstallation vom Benutzer ausgeführt. Zur Aktivierung des Programms benötigt der Benutzer einen Aktivierungscode.

PROGRAMM-MODULE

Dateien, die zum Lieferumfang des Installationspakets für ein Kaspersky-Lab-Programm gehören und zur Realisierung der wichtigsten Aufgaben dienen. Jedem Typ der im Programm realisierten Aufgaben (Schutz, Untersuchung, Update der Datenbanken und Programm-Module) entspricht ein spezielles Programm-Modul.

PROTOKOLL

Genau definierte und standardisierte Kombination von Regeln, die das Verhältnis zwischen Client und Server regulieren. Bekannte Protokolle und die entsprechenden Dienste sind beispielsweise: z. B. HTTP, FTP und NNTP.

PROTOKOLLIERUNG

Aufzeichnung und Anzeige der Ergebnisse eines einzelnen Befehls bei der Ausführung des Programms im Debug-Modus.

Q

QUARANTÄNE

Spezielle Datenablage, in der das Programm Sicherungskopien für Dateien speichert, die bei einer Desinfektion verändert oder gelöscht wurden. Die Kopien von Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr für den Computer dar.

R

ROOTKIT

Programm oder Programmbausatz, mit dem die Spuren eines Angreifers oder einer Schadsoftware im Betriebssystem verborgen werden.

Im Kontext von Windows-Betriebssystemen versteht man unter Rootkit ein Programm, das sich im Betriebssystem einnistet und Windows-Systemfunktionen (Windows API) abfängt. Das Abfangen und die Modifikation von Low-Level-API-Funktionen ermöglichen es einem solchen Programm, seine Existenz im Betriebssystem effektiv zu verbergen. Außerdem kann ein Rootkit meist alle Prozesse, Verzeichnisse und Dateien auf einem Laufwerk, sowie Schlüssel in der Registrierung verbergen, die im Betriebssystem vorhanden und in der Rootkit-Konfiguration beschrieben sind. Viele Rootkits installieren eigene Treiber und Dienste im Betriebssystem (die ebenfalls "unsichtbar" sind).

S

SCHUTZKOMPONENTEN

Komponenten von Kaspersky Total Security, die dazu dienen, den Computer vor bestimmten Bedrohungsarten zu schützen (beispielsweise Anti-Spam und Anti-Phishing). Die einzelnen Schutzkomponenten sind relativ autonom und können separat deaktiviert oder angepasst werden.

SCHWACHSTELLE

Fehler in einem Betriebssystem oder Programm, der von Schadsoftware-Autoren ausgenutzt werden kann, um in ein Betriebssystem oder Programm einzudringen oder seine Integrität zu beschädigen. Wenn ein Betriebssystem viele Schwachstellen aufweist, wird es unzuverlässig, weil Viren eindringen und im Betriebssystem oder in den installierten Programmen Störungen verursachen können.

SICHERER BROWSER

Spezieller Modus für einen normalen Webbrowser, der für Finanztransaktionen und Online-Einkäufe vorgesehen ist. Mithilfe des Sicheren Browsers schützt das Programm sensible Daten, die auf Webseiten von Banken und Zahlungssystemen eingegeben werden (z. B. Bankkartennummern und Kennwörter für Online-Banking), und verhindert Diebstähle bei Online-Zahlungsvorgängen. Dabei wird im normalen Browser, in dem versucht wurde, auf die Webseite zuzugreifen, eine Meldung über den Start des Sicheren Browsers angezeigt.

SICHERHEITSGRUPPE

Gruppe, in die Kaspersky Total Security ein Programm oder einen Prozess unter Berücksichtigung folgender Kriterien verschiebt: Vorhandensein einer digitalen Signatur des Programms, Reputation des Programms im KSN, Vertrauenswürdigkeit für die Quelle des Programms, und potenzielles Risiko der Aktionen, die ein Programm oder ein Prozess ausführt. Aufgrund der Zugehörigkeit zu einer Sicherheitsgruppe kann Kaspersky Total Security Beschränkungen für die Aktivität des betreffenden Programms im Betriebssystem festlegen.

In Kaspersky Total Security werden folgende Sicherheitsgruppen verwendet: Vertrauenswürdig, Schwach beschränkt, Stark beschränkt, Nicht vertrauenswürdig.

SICHERHEITSSTUFE

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für die Arbeit einer Programmkomponente verstanden.

SKRIPT

Ein kleines Computerprogramm oder ein unabhängiger Programmteil (Funktion), das/der in der Regel dazu dient, eine konkrete Aufgabe auszuführen. Meistens werden sie bei Programmen, die in Hypertext integriert sind, verwendet. Skripte werden beispielsweise gestartet, wenn Sie bestimmte Websites öffnen.

Wenn der Echtzeitschutz aktiviert ist, überwacht die Anwendung den Start von Skripts, fängt sie ab und untersucht diese auf Viren. Abhängig von den Untersuchungsergebnissen können Sie die Ausführung eines Skripts verbieten oder erlauben.

SPAM

Unerwünschte massenhafte Versendung von E-Mails, die meistens Werbung enthalten.

U

UNBEKANNTER VIRUS

Neuer Virus, über den noch keine Informationen in den Datenbanken vorhanden sind. In der Regel werden unbekannte Viren vom Programm in den Objekten mithilfe der heuristischen Analyse erkannt. Diesen Objekten wird der Status möglicherweise infiziert zugewiesen.

UNTERSUCHUNG DES DATENVERKEHRS

Untersuchung von Objekten, die mit beliebigen Protokollen übertragen werden (beispielsweise HTTP und FTP). Die Untersuchung erfolgt im Echtzeitmodus unter Verwendung der aktuellen (letzten) Datenbankversion.

UPDATE

Vorgang, bei dem vorhandene Dateien (Datenbanken oder Programm-Module) durch neue Dateien ersetzt bzw. neue Dateien hinzugefügt werden. Die neuen Dateien werden von den Kaspersky-Lab-Updateservern heruntergeladen.

UPDATEPAKET

Paket mit Dateien für das Update von Datenbanken und Programm-Modulen. Das Kaspersky-Lab-Programm kopiert ein Updatepaket von den Kaspersky-Lab-Updateservern, um das Paket anschließend automatisch zu installieren und zu übernehmen.

V

VERTRAUENSWÜRDIGER PROZESS

Programmprozess, dessen Dateioperationen im Echtzeitschutz-Modus nicht von der Kaspersky-Lab-Anwendung kontrolliert werden. Wenn Kaspersky Total Security in einem vertrauenswürdigen Prozess eine verdächtige Aktivität erkennt, wird dieser Prozess aus der vertrauenswürdigen Liste ausgeschlossen und seine Aktionen werden gesperrt.

VIRTUELLER DATENTRESOR

Spezieller Datenspeicher, in dem Daten in verschlüsselter Form gespeichert werden. Für den Zugriff auf solche Dateien muss das Kennwort eingegeben werden. Virtuelle Datentresore dienen dazu, den unberechtigten Zugriff auf Benutzerdaten zu verhindern.

VIRUS

Ein Programm, das andere Programme infiziert. Es fügt seinen Code ein, um beim Start von infizierten Dateien die Kontrolle zu übernehmen. Aus dieser einfachen Definition ergibt sich die wichtigste Aktion, die von einem Virus ausgeführt wird – die Infektion.

I

ICHECKER-TECHNOLOGIE

Diese Technologie erlaubt eine Erhöhung der Untersuchungsgeschwindigkeit. Dabei werden jene Objekte von der Untersuchung ausgeschlossen, die seit dem vorherigen Scannen nicht verändert wurden, wobei vorausgesetzt wird, dass die Untersuchungsparameter (Programm-Datenbanken und Einstellungen) gleich geblieben sind. Informationen darüber werden einer speziellen Datenbank aufgezeichnet. Die Technologie wird sowohl für den Echtzeitschutz als auch für den Scan auf Befehl verwendet.

Beispiel: Eine Archivdatei wurde vom Programm untersucht und ihr wurde der Status virenfrei zugewiesen. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungseinstellungen geändert oder die Programm-Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

Einschränkungen für die Technologie iChecker:

- Die Technologie funktioniert nicht mit großen Dateien, da die Untersuchung der gesamten Datei in diesem Fall weniger Zeit beansprucht, als zu ermitteln, ob sie seit der letzten Untersuchung verändert wurde.

- Diese Technologie unterstützt eine begrenzte Anzahl von Formaten.

KASPERSKY LAB ZAO

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen, die Computer vor Viren und anderer Schadsoftware, Spam, Netzwerk- und Hackerangriffen schützen.

Seit 2008 gehört Kaspersky Lab international zu den vier führenden Unternehmen im Bereich der IT-Sicherheit für Endbenutzer (Rating des "IDC Worldwide Endpoint Security Revenue by Vendor"). Nach einer Studie des Marktforschungsinstituts COMCON TGI-Russia war Kaspersky Lab 2009 in Russland der beliebteste Hersteller von Schutzsystemen für Heimanwender.

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern mit Hauptsitz in Moskau und verfügt über fünf regionale Niederlassungen, die in Russland, West- und Osteuropa, im Nahen Osten, in Afrika, Nord- und Südamerika, Japan, China und anderen Ländern aktiv sind. Das Unternehmen beschäftigt über 2.000 hoch spezialisierte Mitarbeiter.

PRODUKTE. Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die Palette der Heimanwender-Produkte umfasst Antiviren-Programme für Desktops, Laptops, Tablet-PCs, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Programme und Services für den Schutz von Workstations, Datei- und Webservern, Mail-Gateways und Firewalls. In Verbindung mit Administrationstools ermöglichen es diese Lösungen, netzwerkweit einen effektiven automatisierten Schutz vor Computerbedrohungen aufzubauen. Die Produkte von Kaspersky Lab sind durch namhafte Testlabore zertifiziert, mit den Programmen der meisten Softwarehersteller kompatibel und für die Arbeit mit unterschiedlichen Hardwareplattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Sie finden und analysieren jeden Tag Hunderte neuer Computerbedrohungen. Mit diesem Wissen entwickeln sie Mittel, um Gefahren zu erkennen und zu desinfizieren. Diese Informationen fließen in die Datenbanken ein, auf die Kaspersky-Programme zurückgreifen. *Die Antiviren-Datenbanken von Kaspersky Lab werden stündlich aktualisiert*, *die Anti-Spam-Datenbanken im 5-Minuten-Takt*.

TECHNOLOGIEN. Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Softwarehersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Openwave Messaging (Irland), D-Link (Taiwan), M86 Security (USA), GFI Software (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), Netasq+Arkoon (France), NETGEAR (USA), Parallels (USA), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

AUSZEICHNUNGEN. Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So wurde Kaspersky Anti-Virus 2010 in Tests des anerkannten österreichischen Antiviren-Labors AV-Comparatives mehrfach mit dem Premium-Award Advanced+ ausgezeichnet. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 300 Millionen Anwender. Über 200.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Webseite von Kaspersky Lab:	http://www.kaspersky.de
Viren-Enzyklopädie:	http://www.securelist.com/de/
Antiviren-Labor	newvirus@kaspersky.com (nur zum Einsenden von möglicherweise infizierten Dateien, die zuvor archiviert wurden)
Webforum von Kaspersky Lab:	http://forum.kaspersky.com

INFORMATIONEN ÜBER DEN CODE VON DRITTHERSTELLERN

Die Informationen über den Code von Drittherstellern sind in der Datei legal_notices.txt enthalten, die sich im Installationsordner des Programms befindet.

MARKENINFORMATIONEN

Eingetragene Marken und Dienstleistungszeichen sind Eigentum der jeweiligen Rechteinhaber.

Dropbox ist eine Marke der Dropbox, Inc.

Google, Google Chrome, YouTube sind Marken von Google, Inc.

Intel, Celeron, Atom und Pentium sind in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragene Marken der Intel Corporation.

Internet Explorer, Microsoft, Windows, DirectX, Bing, Outlook, Windows Vista sind in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragene Marken der Microsoft Corporation.

Mozilla und Firefox sind Marken der Mozilla Foundation.

OpenGL ist eine eingetragene Marke von SGI.

VMware ist eine Marke von VMware, Inc oder eine in den USA und/oder anderen Ländern eingetragene Marke von VMware, Inc.

Mail.ru ist eine eingetragene Marke, deren Rechteinhaber die OOO "Mail.Ru" ist.

SACHREGISTER