KASPERSKY lab

Kaspersky Total Security

Benutzerhandbuch

Programmversion: 16.0 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.

Redaktionsdatum: 30.11.2015

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

Inhalt

Über dieses Handbuch 9
In diesem Dokument 9
Formatierung mit besonderer Bedeutung 14
Informationsquellen zum Programm 16
Quellen zur selbstständigen Recherche 16
Diskussion über die Programme von Kaspersky Lab im Forum 18
Kaspersky Total Security 19
Neuerungen 19
Lieferumfang 20
Über das Programm Kaspersky Total Security 21
Hard- und Softwarevoraussetzungen 25
Programm installieren und deinstallieren 28
Standard-Installationsmethode 28
Schritt 1. Nach neuer Programmversion suchen 30
Schritt 2. Beginn der Programminstallation 31
Schritt 3. Lizenzvereinbarung anzeigen 31
Schritt 4. Vereinbarung zum Kaspersky Security Network 31
Schritt 5. Installation 32
Schritt 6. Installation abschließen 33
Schritt 7. Programm aktivieren 33
Schritt 8. Anmeldung des Benutzers 34
Schritt 9. Aktivierung abschließen 35
Installation des Programms über die Befehlszeile 35
Programm vorbereiten 35
Upgrade einer früheren Programmversion 36
Schritt 1. Nach neuer Programmversion suchen 39
Schritt 2. Beginn der Programminstallation 39
Schritt 3. Lizenzvereinbarung anzeigen 40
Schritt 4. Vereinbarung zum Kaspersky Security Network 40
Schritt 5. Installation 41
Schritt 6. Installation abschließen 42

Programm entfernen 42
Schritt 1. Kennwort für die Programmdeinstallation eingeben 43
Schritt 2. Daten zur erneuten Verwendung speichern 43
Schritt 3. Programmdeinstallation bestätigen 44
Schritt 4. Programm entfernen. Deinstallation abschließen 45
Lizenzverwaltung des Programms 46
Über den Lizenzvertrag 46
Über die Lizenz 47
Über den eingeschränkten Funktionsmodus 48
Über den Aktivierungscode 52
Über das Abonnement 53
Über die Bereitstellung von Daten 54
Lizenz kaufen 55
Programm aktivieren 55
Lizenz verlängern 56
Mit den Benachrichtigungen des Programms arbeiten 58
Schutzstatus des Computers analysieren und Sicherheitsprobleme beheben 59
Update der Datenbanken und Programm-Module 60
Über das Update der Datenbanken und Programm-Module 60
Update der Datenbanken und Programm-Module starten 62
Untersuchung des Computers 63
Vollständige Untersuchung 63
Benutzerdefinierte Untersuchung 64
Schnelle Untersuchung 65
Schwachstellensuche 66
Objekt wiederherstellen, das vom Programm gelöscht oder desinfiziert wurde 67
Betriebssystem nach einer Infektion wiederherstellen 68
Betriebssystem nach einer Infektion wiederherstellen 68
Betriebssystem mithilfe des Wiederherstellungs-Assistenten wiederherstellen 69
Über die Notfall-CD 71
E-Mail-Schutz 72
Einstellungen für Mail-Anti-Virus 72

Unerwünschte E-Mails (Spam) blockieren 74
Schutz für persönliche Daten im Internet 75
Über den Schutz für persönliche Daten im Internet 75
Über die Bildschirmtastatur 76
Bildschirmtastatur starten 78
Anzeige des Symbols für die Bildschirmtastatur anpassen 80
Schutz von Tastatureingaben 81
Benachrichtigungen über Schwachstellen in einem WLAN-Netzwerk anpassen 83
Sicherheit einer Webseite überprüfen 84
Schutz für Finanztransaktionen und Online-Einkäufe 87
Über den Schutz von Finanztransaktionen und Online-Einkäufen 87
Einstellungen für den Sicheren Zahlungsverkehr anpassen 90
Sicheren Zahlungsverkehr für eine bestimmte Webseite anpassen 90
Automatische Aktivierung der Erweiterung Kaspersky Protection einschalten 91
Screenshot-Schutz 92
Screenshot-Schutz aktivieren 93
Schutz von Daten in der Zwischenablage 93
Kaspersky Password Manager starten 94
Schutz vor dem Sammeln von Informationen über Ihre Online-Aktivitäten 95
Über den Schutz vor Datensammlung 95
Einstellungen für den Schutz vor Datensammlung 96
Tracking-Dienste nach Kategorien blockieren 98
Datensammlung auf bestimmten Websites erlauben 98
Bericht über Anfragen an Tracking-Dienste anzeigen 99
Schutz vor Datensammlung im Browser verwalten 100
Schutz vor Bannern beim Besuch von Webseiten 101
Komponente Anti-Banner aktivieren 101
Anzeige eines Banners auf einer Webseite deaktivieren 102
Anzeige aller Banner auf einer Webseite deaktivieren 102
Aktivitätsspuren auf dem Computer und im Internet löschen 104
Kontrolle über die Aktivitäten der Benutzer auf dem Computer und im Internet 107
Kindersicherung verwenden 107
Zu den Einstellungen für die Kindersicherung wechseln 109

Kontrolle über die Verwendung des Computers 110
Kontrolle über die Verwendung des Internets 111
Kontrolle über den Start von Spielen und Programmen 114
Kontrolle über die Kommunikation in sozialen Netzwerken 116
Inhaltskontrolle für Konversationen 117
Bericht über die Aktionen eines Benutzers anzeigen 119
Fernverwaltung des Computerschutzes 120
Über die Fernverwaltung des Computerschutzes 120
Über das Benutzerkonto im Portal My Kaspersky 121
Zur Fernverwaltung des Computerschutzes wechseln 122
Betriebssystemressourcen für Computerspiele freigeben 123
Mit unbekannten Programmen arbeiten 124
Reputation eines Programms überprüfen 125
Kontrolle der Aktionen eines Programms auf dem Computer und im Netzwerk 127
Einstellungen für die Programmkontrolle anpassen 129
Zugriff von Programmen auf die Webcam 130
Einstellungen für den Zugriff von Programmen auf die Webcam anpassen 132
Zugriff eines Programms auf die Webcam erlauben 132
Über den Zugriff von Programmen auf Tonaufnahmegeräte 133
Einstellungen für den Zugriff eines Programms auf Tonaufnahmegeräte anpassen 135
Über die Überwachung von Änderungen im Betriebssystem 136
Einstellungen für die Überwachung von Änderungen im Betriebssystem anpassen 137
Modus für vertrauenswürdige Programme 139
Über den Modus für vertrauenswürdige Programme 139
Modus für vertrauenswürdige Programme aktivieren 141
Modus für vertrauenswürdige Programme deaktivieren 143
Datenvernichtung 144
Löschen von nicht benötigten Daten 147
Über das Löschen von nicht benötigten Daten 147
Vorgehen zum Löschen von nicht benötigten Daten 148

Datensicherung....150
Über die Datensicherung....150
Sicherungsaufgabe erstellen....151
Schritt 1. Dateien auswählen....152
Schritt 2. Zu sichernde Ordner auswählen....153
Schritt 3. Zu sichernde Dateitypen auswählen....153
Schritt 4. Sicherungsspeicher auswählen....153
Schritt 5. Sicherungszeitplan erstellen....154
Schritt 6. Kennwort für den Schutz von Sicherungskopien eingeben....155
Schritt 7. Einstellungen für die Sicherungsversionen von Dateien....155
Schritt 8. Name für die Sicherungsaufgabe eingeben....155
Schritt 9. Assistent abschließen....156
Sicherungsaufgabe starten....156
Daten aus einer Sicherungskopie wiederherstellen....156
Über den Online-Speicher....157
Online-Speicher aktivieren....158
Daten in Datentresoren speichern....160
Über Datentresore....160
Dateien in einen Datentresor verschieben....160
Zugriff auf Dateien im Datentresor erhalten....162
Zugriff auf die Verwaltung von Kaspersky Total Security mit einem Kennwort schützen....163
Computerschutz anhalten und fortsetzen....164
Standardeinstellungen für das Programm wiederherstellen....166
Bericht über das Programm anzeigen....167
Programmeinstellungen auf einem anderen Computer übernehmen....168
Teilnahme an Kaspersky Security Network....170
Teilnahme an Kaspersky Security Network aktivieren und deaktivieren....171
Verbindung zu Kaspersky Security Network prüfen....172
Steuerung des Programms über die Befehlszeile....173
Kontaktaufnahme mit dem Technischen Support....174
Wie Sie technischen Kundendienst erhalten....174

Technischer Support am Telefon 175
Technischer Support über das Portal My Kaspersky 175
Informationen für den Technischen Support sammeln 176
Bericht über den Zustand des Betriebssystems erstellen 177
Dateien mit Daten senden 178
Über die Zusammensetzung und Speicherung von Protokolldateien 179
AVZ-Skript ausführen 180
Einschränkungen und Warnungen 181
Glossar 188
AO Kaspersky Lab 199
Informationen über den Code von Drittherstellern 201
Markeninformationen 202
Sachregister 203

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 9

Formatierung mit besonderer Bedeutung 14

In diesem Dokument

Dieses Dokument enthält folgende Abschnitte.

Informationsquellen zum Programm (auf S. 16)

Dieser Abschnitt beschreibt Informationsquellen zum Programm.

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

Kaspersky Total Security (auf S. 19)

Dieser Abschnitt beschreibt die Funktionen, die Komponenten und den Lieferumfang von Kaspersky Total Security, und nennt die Hard- und Softwarevoraussetzungen für Kaspersky Total Security.

Programm installieren und entfernen (auf S. 28)

Dieser Abschnitt bietet genaue Anleitungen zur Installation und Deinstallation von Kaspersky Total Security.

Lizenzverwaltung des Programms (auf S. 46)

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Lizenzverwaltung für das Programm zusammenhängen.

Mit den Benachrichtigungen des Programms arbeiten (auf S. 58)

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

Schutzstatus des Computers analysieren und Sicherheitsprobleme beheben (auf S. 59)

Dieser Abschnitt enthält Informationen darüber, wie der Schutzstatus des Computers überprüft wird und Sicherheitsprobleme beseitigt werden können.

Update der Antiviren-Datenbanken und Programm-Module (auf S. 60)

Dieser Abschnitt enthält Schritt-für-Schritt-Anweisungen zum Update der Datenbanken und Programm-Module.

Untersuchung des Computers (auf S. 63)

Dieser Abschnitt enthält Schritt-für-Schritt-Anweisungen zur Untersuchung des Computers auf Viren, Schadsoftware und Schwachstellen.

Objekt wiederherstellen, das vom Programm gelöscht oder desinfiziert wurde (auf S. 67)

Dieser Abschnitt bietet Schritt-für-Schritt-Anleitungen zur Wiederherstellung eines gelöschten oder desinfizierten Objekts.

Betriebssystem nach einer Infektion wiederherstellen (auf S. 68)

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

E-Mail-Schutz (auf S. 72)

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

Schutz für persönliche Daten im Internet (auf S. 75)

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

Schutz für Finanztransaktionen und Online-Einkäufe (s. S. 87)

Dieser Abschnitt informiert darüber, wie Sie Ihre Finanztransaktionen und Online-Einkäufe mithilfe von Kaspersky Total Security schützen können.

Schutz vor dem Sammeln von Informationen über Ihre Online-Aktivitäten (s. S. 95)

Dieser Abschnitt informiert darüber, wie Kaspersky Total Security Sie vor dem Sammeln von Daten über Ihre Online-Aktivitäten schützt.

Schutz vor Bannern beim Besuch von Webseiten (auf S. 101)

Dieser Abschnitt informiert darüber, wie mithilfe von Kaspersky Total Security die Anzeige von Bannern auf Webseiten blockiert werden kann.

Aktivitätsspuren auf dem Computer und im Internet löschen (auf S. 104)

Dieser Abschnitt enthält Informationen über das Löschen von Aktivitätsspuren eines Benutzers vom Computer.

Kontrolle über die Aktivitäten der Benutzer auf dem Computer und im Internet (auf S. 107)

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

Fernverwaltung des Computerschutzes (auf S. 120)

Dieser Abschnitt informiert darüber, wie Sie den Schutz Ihres Computers über das Portal My Kaspersky fernverwalten können.

Betriebssystemressourcen für Computerspiele freigeben (s. S. 123)

Dieser Abschnitt erklärt, wie sich die Leistung des Betriebssystems für Computerspiele und andere Programme steigern lässt.

Mit unbekannten Programmen arbeiten (auf S. 124)

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

Modus für vertrauenswürdige Programme (s. S. 139)

Dieser Abschnitt enthält Informationen über den Modus für vertrauenswürdige Programme.

Datenvernichtung (auf S. 144)

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. 147)

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

Backup (auf S. 150)

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

Daten in Datentresoren speichern (auf S. 160)

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. 163)

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

Computerschutz anhalten und fortsetzen (auf S. 164)

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

Standardeinstellungen für das Programm wiederherstellen (auf S. 166)

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

Bericht über das Programm anzeigen (auf S. 167)

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

Programmeinstellungen auf einem anderen Computer übernehmen (auf S. 168)

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

Teilnahme an Kaspersky Security Network (auf S. 170)

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

Steuerung des Programms über die Befehlszeile (auf S. 173)

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

Kontaktaufnahme mit dem Technischen Support (auf S. 174)

Dieser Abschnitt beschreibt, wie Sie technische Unterstützung erhalten können und nennt die erforderlichen Voraussetzungen.

Einschränkungen und Warnungen (auf S. 181)

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

Glossar (auf S. 188)

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

AO Kaspersky Lab" (auf S. 199)

Dieser Abschnitt enthält Informationen über AO Kaspersky Lab.

Informationen über den Code von Drittherstellern (auf S. 201)

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

Markeninformationen (auf S. 202)

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

In diesem Dokument werden Formatierungen mit besonderer Bedeutung verwendet (siehe folgende Tabelle).

Tabelle 1. Formatierung mit besonderer Bedeutung

Textbeispiel	Beschreibung der Formatierung
Beachten Sie, dass ...	Warnungen sind rot hervorgehoben und eingerahmt. Warnungen informieren über Aktionen, die unerwünschte Folgen haben können.
Es wird empfohlen ...	Hinweise sind eingerahmt. Hinweise bieten zusätzliche und hilfreiche Informationen.
Beispiel:	Beispiele befinden sich in blau unterlegten Blöcken und sind mit "Beispiel" überschrieben.
Das *Update* ist ... Das Ereignis *Die Datenbanken sind veraltet* tritt ein.	Folgende Textelemente sind kursiv geschrieben: • neue Begriffe • Namen von Statusvarianten und Programmereignissen

Textbeispiel	Beschreibung der Formatierung
Drücken Sie die Taste **ENTER**. Drücken Sie die Tastenkombination **ALT**+**F4**.	Bezeichnungen von Tasten sind in fetten 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 über die Tastatur 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.

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

In diesem Abschnitt

Quellen zur selbstständigen Recherche 16

Diskussion über die Programme von Kaspersky Lab im Forum..... 18

Quellen zur selbstständigen Recherche

Sie können folgende Quellen verwenden, um nach Informationen über Kaspersky Total Security zu suchen:

- Seite für Kaspersky Total Security auf der Kaspersky-Lab-Webseite
- Seite für Kaspersky Total Security 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 "Kontaktaufnahme mit dem Technischen Support" auf S. 174).

Um die Informationsquellen auf den genannten Webseiten zu nutzen, ist eine Internetverbindung erforderlich.

Seite für Kaspersky Total Security auf der Kaspersky-Lab-Webseite

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

Diese Seite für Kaspersky Total Security bietet einen Link zum Online-Shop. Dort können Sie ein Programm kaufen oder die Nutzungsrechte für das Programm verlängern.

Seite über Kaspersky Total Security in der Wissensdatenbank

Die *Wissensdatenbank* ist ein Abschnitt der Webseite des Technischen Supports.

Auf der Seite für Kaspersky Total Security finden Sie in der Wissensdatenbank (http://support.kaspersky.com/de/kts2016) Artikel mit nützlichen 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. Die Wissensdatenbank bietet außerdem Neuigkeiten über den Technischen Support.

Elektronisches Hilfesystem

Das Programm enthält Dateien für die vollständige Hilfe und für die Kontexthilfe.

Die vollständige Hilfe bietet Informationen darüber, wie Kaspersky Total Security angepasst werden kann und verwendet wird.

In der Kontexthilfe finden Sie folgende Informationen über die Fenster von Kaspersky Total Security: Beschreibung der Einstellungen von Kaspersky Total Security und Links zu Beschreibungen für die Aufgaben, in denen diese Einstellungen verwendet werden.

Die Hilfe ist entweder im Lieferumfang des Programms enthalten oder kann auf der entsprechenden Kaspersky-Lab-Webseite online genutzt werden. Die Online-Hilfe wird im Browserfenster geöffnet. Um die Online-Hilfe nutzen zu können, ist eine Internetverbindung erforderlich.

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 Funktionen, die Komponenten und den Lieferumfang von Kaspersky Total Security, und nennt die Hard- und Softwarevoraussetzungen für Kaspersky Total Security.

In diesem Abschnitt

Neuerungen 19

Lieferumfang 20

Über das Programm Kaspersky Total Security 21

Hard- und Softwarevoraussetzungen 25

Neuerungen

Kaspersky Total Security bietet folgende Neuerungen:

- Die Einschränkungen für die Unterstützung von Microsoft® Windows® 10 wurden behoben.
- Neu: Benachrichtigungen über den Ablauf der Lizenz gemäß dem Microsoft-Standard
- In Microsoft Windows 10 werden Programmbenachrichtigungen durch Pop-up-Meldungen ersetzt, die dem Microsoft-Standard entsprechen.
- Das Programm "Protect a Friend" wurde in das Portal My Kaspersky übertragen. Registrierung und Anmeldung beim Programm "Protect a Friend" erfolgen jetzt bei der Verbindung mit dem Portal My Kaspersky. Die Seiten des Programms "Protect a Friend" können im Portal My Kaspersky eingesehen werden.
- Neu: Unterstützung des HTTP/2-Protokolls
- Neu: teilweise Unterstützung der Browser Yandex.Browser und Microsoft Edge
- Neu: Virtuelle Desktops in Microsoft Windows 10 werden unterstützt.

- Verbesserte grafische Oberfläche
- Das Symbol für die Bildschirmtastatur wurde verbessert. Das Symbol stört jetzt nicht mehr, wenn Daten in einem Eingabefeld eingegeben werden.
- Neu: Installationsratgeber Wenn Software auf dem Computer installiert wird, deaktiviert der Installationswächter automatisch die Kontrollkästchen für Angebote zur Installation zusätzlicher Programme und blockiert die Installation dieser Programme. Außerdem verhindert der Installationswächter, dass Installationsschritte angezeigt werden, die Werbung enthalten.

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.

Über das Programm Kaspersky Total Security

Kaspersky Total Security bietet einen komplexen Schutz vor unterschiedlichen Bedrohungstypen, Netzwerkangriffen, 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 unterschiedlichen Bedrohungstypen, 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 bedrohliche Programme. 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 der Verwendung von IM-Clients. Die Komponente schützt die Informationen, die über IM-Client-Protokolle auf Ihren Computer gelangen. IM-Anti-Virus gewährleistet Sicherheit bei der Verwendung unterschiedlicher Programme, die dem Austausch von Sofortnachrichten 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.

Überwachung von Änderungen im Betriebssystem

Die Komponente Überwachung von Änderungen im Betriebssystem überwacht Änderungen, die andere Programme in den Betriebssystemeinstellungen vornehmen, und benachrichtigt Sie über solche Änderungen. Zu den überwachten Einstellungen zählen beispielsweise bestimmte Browser- und Proxyserver-Einstellungen.

Zugriff auf Webcam

Die Komponente Zugriff auf Webcam blockiert den unbefugten Zugriff von Programmen auf die Webcam und zeigt eine entsprechende Meldung an.

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

Die Komponente 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.

Schutz vor Datensammlung

Die Komponente Schutz vor Datensammlung erkennt Anfragen, die ein Browser an Tracking-Dienste schickt. Außerdem kann die Komponente Anfragen an Tracking-Dienste und Antworten auf solche Anfragen modifizieren, um zu verhindern, dass Informationen über die Online-Aktivitäten des Benutzers gesammelt werden.

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 von Tastatureingaben schützt persönliche Daten, die auf Websites eingegeben werden, vor Keyloggern. Die Bildschirmtastatur 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 Informationen aus dem Kaspersky Security Network 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.

Online-Verwaltung

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.

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.

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 Installation und Aktivierung des Programms und für die Aktualisierung der Datenbanken und Programm-Module)

- Microsoft® Internet Explorer® 8.0 oder höher

  > Für das Portal My Kaspersky wird die Verwendung von Microsoft Internet Explorer 9.0 oder höher empfohlen.

- 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 verfügbar (http://support.kaspersky.com/de/12004).

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 Home, Microsoft Windows 10 Enterprise, Microsoft Windows 10 Pro:

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

Unterstützte Browser:

- Microsoft Internet Explorer Versionen 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 31.x und höher
- Google Chrome™ Versionen 36.x und höher

  > 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.

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

Anforderungen für das Programm Kaspersky Password Manager bei Installation auf Microsoft Windows XP Home (32-Bit) Service Pack 3 oder höher, Microsoft Windows XP Professional (32-Bit) Service Pack 3 oder höher, Microsoft Windows XP Professional (64-Bit) Service Pack 2 oder höher:

- Microsoft Internet Explorer (Version 8 oder höher)
- Mozilla Firefox 31 oder höher
- Google Chrome 36 oder höher
- Yandex.Browser 14.10 oder höher

Programm installieren und deinstallieren

Dieser Abschnitt bietet genaue Anleitungen zur Installation und Deinstallation von Kaspersky Total Security.

In diesem Abschnitt

Standard-Installationsmethode 28

Installation des Programms über die Befehlszeile 35

Programm vorbereiten 35

Upgrade einer früheren Programmversion 36

Programm entfernen 42

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 bei einem beliebigen Schritt abgebrochen werden. Dazu wird das Assistentenfenster geschlossen.

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 mit der Erweiterung exe.

Anschließend wird das Programm mithilfe eines standardmäßigen Installationsassistenten installiert.

In bestimmten Regionen enthält die Installations-CD kein Installationspaket für das Programm. Die Installations-CD enthält nur eine autorun-Datei, mit der ein Fenster für den Programm-Download geöffnet werden kann.

► *Um Kaspersky Total Security mithilfe der Datei autorun zu installieren, gehen Sie wie folgt vor:*

1. Klicken Sie im Download-Fenster auf **Herunterladen und installieren**.

   Bei Klick auf **Herunterladen und installieren** werden Informationen über die Version Ihres Betriebssystems an Kaspersky Lab gesendet.

2. Falls kein Download möglich ist, verwenden Sie den Link **Manuell von der Website herunterladen und installieren** und laden das Programm manuell von der Webseite herunter.

Sie können das Installationspaket für Kaspersky Total Security auch manuell aus dem Internet herunterladen. Dabei zeigt der Installationsassistent für bestimmte Sprachversionen einige zusätzliche Installationsschritte an.

Zusammen mit dem Programm werden auch Erweiterungen für die Browser installiert, die der sicheren Nutzung des Internets dienen.

Wenn Kaspersky Total Security nach der Installation zum ersten Mal gestartet wird, kann es vorkommen, dass die Wiedergabe oder Aufzeichnung von Audio- und Videodaten in entsprechenden Programmen abgebrochen wird. Dies ist erforderlich, um die Überwachung des Zugriffs von Programmen auf Tonaufnahmegeräte zu aktivieren (s. Abschnitt "Über den Zugriff von Programmen auf Tonaufnahmegeräte" auf S. 133). Der Systemdienst für die Verwaltung von Audiogeräten wird beim ersten Start von Kaspersky Total Security neu gestartet.

In diesem Abschnitt

Schritt 1. Nach neuer Programmversion suchen 30

Schritt 2. Beginn der Programminstallation..... 31

Schritt 3. Lizenzvereinbarung anzeigen..... 31

Schritt 4. Vereinbarung zu Kaspersky Security Network..... 31

Schritt 5. Installation..... 32

Schritt 6. Installation abschließen..... 33

Schritt 7. Programm aktivieren 33

Schritt 8. Anmeldung des Benutzers 34

Schritt 9. Aktivierung abschließen 35

Schritt 1. Nach neuer Programmversion suchen

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

Schritt 2. Beginn der Programminstallation

Bei diesem Schritt schlägt Ihnen der Setup-Assistent 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 Setup-Assistent 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 Bedrohungen, über laufende Programme und über geladene signierte Programme sowie Informationen zum Betriebssystem an AO 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 Speicherplatzes auf dem Laufwerk
    - Vorhandensein von Administratorrechten für den Benutzer, der die Programminstallation ausführt

    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 abgeschlossen wurde, muss das Programm manuell gestartet werden.

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

Schritt 7. Programm aktivieren

Beim ersten Start von Kaspersky Total Security wird der Aktivierungs-Assistent des Programms gestartet.

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 Variante aus und geben Sie den Aktivierungscode ein (s. Abschnitt "Über den Aktivierungscode" auf S. 52), falls 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 dann auf **Anmelden**, 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.

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

Installation des Programms über die Befehlszeile

Kaspersky Total Security kann über die Befehlszeile installiert werden.

Syntax der Befehlszeile:

```
<Pfad des Installationspakets> [Parameter]
```

Eine genaue Anleitung und eine Liste mit den Installationseinstellungen finden Sie auf der Seite des Technischen Supports (http://support.kaspersky.com/de/12003)

Programm vorbereiten

Damit die Browser in vollem Umfang von Kaspersky Total Security unterstützt werden, muss die Erweiterung Kaspersky Protection in den Browsern installiert und aktiviert sein. Mithilfe der Erweiterung Kaspersky Protection bindet Kaspersky Total Security in eine Webseite, die im Sicheren Browser geöffnet wird, und in den Datenverkehr ein Skript ein. Das Programm verwendet dieses Skript zur Interaktion mit Webseiten und zur Datenübertragung an Banken, deren Websites mithilfe der Komponente Sicherer Zahlungsverkehr geschützt werden. Die Daten, die mit dem Skript übertragen werden, werden vom Programm durch eine digitale Signatur geschützt. Kaspersky Total Security kann das Skript einbinden, ohne die Erweiterung Kaspersky Protection zu verwenden.

Kaspersky Total Security signiert die vom Skript zu übertragenden Daten mithilfe der installierten Antiviren-Datenbanken und Anfragen an Kaspersky Security Network. Das Programm überträgt Anfragen an Kaspersky Security Network unabhängig davon, ob Sie die Bedingungen der KSN-Vereinbarung akzeptiert haben oder nicht.

Die Erweiterung Kaspersky Protection wird bei der Installation von Kaspersky Total Security in die Browser installiert.

Nach der Installation von Kaspersky Total Security muss die Erweiterung Kaspersky Protection aktiviert werden:

- Um die Erweiterung im Browser Mozilla™ Firefox™ zu aktivieren, muss die Erweiterungsinstallation im Browserfenster erlaubt werden.
- Im Browser Google Chrome™ muss die Aktivierung von Kaspersky Protection erlaubt werden. Falls die Aktivierung von Kaspersky Protection abgelehnt wird, muss Kaspersky Protection später manuell installiert und aktiviert werden. In diesem Fall laden Sie die Erweiterung entweder aus dem Chrome™ Web Store oder von der Seite auf der Webseite des Technischen Supports (http://support.kaspersky.com/interactive/google/de/ktsplugin) herunter.

Im Browser Microsoft Internet Explorer wird die Erweiterung Kaspersky Protection automatisch aktiviert.

Wenn Ihr Computer das Betriebssystem Windows 10 verwendet, muss die Erweiterung Kaspersky Protection im Browser Microsoft Internet Explorer manuell installiert werden. Sie können die Benachrichtigung in der Mitteilungszentrale verwenden, um zur Installation der Erweiterung zu wechseln (s. Abschnitt "Schutzstatus des Computers analysieren und Sicherheitsprobleme beheben" auf S. 59).

Upgrade einer früheren Programmversion

Installation von Kaspersky Total Security über eine ältere Version von Kaspersky Total Security oder über Kaspersky PURE

Wenn auf Ihrem Computer bereits eine Vorgängerversion von Kaspersky Total Security oder das Programm Kaspersky PURE installiert ist, können Sie diese auf die neue Version von Kaspersky Total Security upgraden. Wenn eine aktuelle Lizenz für die Nutzung von Kaspersky PURE oder

einer Vorgängerversion von Kaspersky Total Security vorliegt, müssen Sie das Programm nicht aktivieren: Der Installationsassistent ermittelt automatisch Informationen über die Lizenz und verwendet diese Daten bei der Installation von Kaspersky Total Security.

Wenn Sie in Kaspersky PURE einen Container erstellt haben, wird der Container in einen Datentresor umgewandelt, wenn Kaspersky Total Security zum ersten Mal darauf zugreift. Die Dateien im Datentresor stehen nach der Umwandlung zur Verfügung.

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 der Vorgängerversion von 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 bei einem beliebigen Schritt abgebrochen werden. Dazu wird das Assistentenfenster geschlossen.

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 mit der Erweiterung exe.

Anschließend wird das Programm mithilfe eines standardmäßigen Installationsassistenten installiert.

In bestimmten Regionen enthält die Installations-CD kein Installationspaket für das Programm. Die Installations-CD enthält nur eine autorun-Datei, mit der ein Fenster für den Programm-Download geöffnet werden kann.

► *Um Kaspersky Total Security mithilfe der Datei autorun zu installieren, gehen Sie wie folgt vor:*

1. Klicken Sie im Download-Fenster auf **Herunterladen und installieren**.

   Bei Klick auf **Herunterladen und installieren** werden Informationen über die Version Ihres Betriebssystems an Kaspersky Lab gesendet.

2. Falls kein Download möglich ist, verwenden Sie den Link **Manuell von der Website herunterladen und installieren** und laden das Programm manuell von der Webseite herunter.

Sie können das Installationspaket für Kaspersky Total Security auch manuell aus dem Internet herunterladen. Dabei zeigt der Installationsassistent für bestimmte Sprachversionen einige zusätzliche Installationsschritte an.

Zusammen mit dem Programm werden auch Erweiterungen für die Browser installiert, die der sicheren Nutzung des Internets dienen.

Wenn Kaspersky Total Security nach der Installation zum ersten Mal gestartet wird, kann es vorkommen, dass die Wiedergabe oder Aufzeichnung von Audio- und Videodaten in entsprechenden Programmen abgebrochen wird. Dies ist erforderlich, um die Überwachung des Zugriffs von Programmen auf Tonaufnahmegeräte zu aktivieren (s. Abschnitt "Über den Zugriff von Programmen auf Tonaufnahmegeräte" auf S. 133). Der Systemdienst für die Verwaltung von Audiogeräten wird beim ersten Start von Kaspersky Total Security neu gestartet.

Das Programm-Upgrade besitzt Einschränkungen (s. Abschnitt "Einschränkungen und Warnungen" auf S. 181).

In diesem Abschnitt

Schritt 1. Nach neuer Programmversion suchen 39

Schritt 2. Beginn der Programminstallation..... 39

Schritt 3. Lizenzvereinbarung anzeigen..... 40

Schritt 4. Vereinbarung zu Kaspersky Security Network..... 40

Schritt 5. Installation..... 41

Schritt 6. Installation abschließen..... 42

Schritt 1. Nach neuer Programmversion suchen

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

Schritt 2. Beginn der Programminstallation

Bei diesem Schritt schlägt Ihnen der Setup-Assistent 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 Setup-Assistent 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 Bedrohungen, über laufende Programme und über geladene signierte Programme sowie Informationen zum Betriebssystem an AO 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 Speicherplatzes auf dem Laufwerk
  - Vorhandensein von Administratorrechten für den Benutzer, der die Programminstallation ausführt

  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.

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 entfernen

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

Kaspersky Total Security wird mit dem Installationsassistenten entfernt.

► *Um den Assistenten im Betriebssystem Microsoft Windows 7 und niedriger zu starten,*

klicken Sie im **Startmenü** auf **Alle Programme** → **Kaspersky Total Security** → **Kaspersky Total Security entfernen**.

► *Um den Assistenten im Betriebssystem Microsoft Windows 8 und höher zu starten:*

1. Klicken Sie auf dem Startbildschirm mit der rechten Maustaste auf die Kachel für Kaspersky Total Security und öffnen Sie die Symbolleiste.
2. Klicken Sie in der Symbolleiste auf **Löschen**.
3. Wählen Sie im folgenden Fenster aus der Liste Kaspersky Total Security aus.
4. Klicken Sie oben in der Liste auf **Löschen**.

In diesem Abschnitt

Schritt 1. Kennwort für die Programmdeinstallation eingeben 43

Schritt 2. Daten zur erneuten Verwendung speichern 43

Schritt 3. Programmdeinstallation bestätigen 44

Schritt 4. Programm entfernen. Deinstallation abschließen 45

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 wird nur angezeigt, falls 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 Objekten, die bereits mithilfe der iChecker-Technologie auf Viren untersucht wurden.

- **Anti-Spam-Datenbanken** – Datenbanken mit Mustern von Spam-Nachrichten, die vom Benutzer hinzugefügt wurden.

- **Virtuelle Datentresore** – Dateien, die Sie in Virtuelle Datentresore gespeichert haben.

Schritt 3. Programmdeinstallation bestätigen

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

Schritt 4. Programm entfernen. 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.

> Es kann sein, dass diese Funktionalität in bestimmten Regionen nicht verfügbar ist.

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 Lizenzverwaltung für das Programm zusammenhängen.

In diesem Abschnitt

Über den Lizenzvertrag 46

Über die Lizenz 47

Über den eingeschränkten Funktionsmodus 48

Über den Aktivierungscode 52

Über das Abonnement 53

Über die Bereitstellung von Daten 54

Lizenz kaufen 55

Programm aktivieren 55

Lizenz verlängern 56

Über den Lizenzvertrag

Der *Lizenzvertrag* ist ein rechtsgültiger Vertrag zwischen Ihnen und der AO Kaspersky Lab. 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 den Lizenzvertrag ablehnen, müssen Sie die Programminstallation abbrechen und dürfen das Programm nicht nutzen.

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 anderen Leistungen, die Ihnen von Kaspersky Lab oder den Vertriebspartnern während der Gültigkeitsdauer der Lizenz zur Verfügung gestellt werden.

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

Eine Lizenz besitzt eine beschränkte Gültigkeitsdauer. Nach Ablauf der Lizenz kann Ihnen eine Nachfrist eingeräumt werden, während der Sie weiterhin alle Programmfunktionen uneingeschränkt nutzen können.

Wenn Sie die Lizenz innerhalb der Nachfrist nicht verlängert haben (s. Abschnitt "Lizenz verlängern" auf S. 56), kann das Programm in den eingeschränkten Funktionsmodus wechseln (s. Abschnitt "Über den eingeschränkten Funktionsmodus" auf S. 48). Im eingeschränkten Funktionsmodus sind nicht alle Programmfunktionen verfügbar. Die Dauer des eingeschränkten Funktionsmodus ist von Ihrer Region und von den Lizenzbedingungen abhängig. Nach Ablauf des eingeschränkten Funktionsmodus stellt das Programm alle Funktionen ein. Informationen über die Dauer der Nachfrist und des eingeschränkten Funktionsmodus finden Sie im Fenster **Lizenzverwaltung**. Dieses Fenster wird mit dem Link **Lizenz** geöffnet, der sich unten im Hauptfenster befindet.

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.

Wenn Sie den Schutz für Ihren Computer nicht fortsetzen möchten, können Sie Kaspersky Total Security entfernen (s. Abschnitt "Programm entfernen" auf S. 42).

Über den eingeschränkten Funktionsmodus

Die folgende Tabelle informiert darüber, welche Funktionen von Kaspersky Total Security verfügbar bzw. nicht verfügbar sind, wenn das Programm im eingeschränkten Funktionsmodus läuft. Wenn in der Spalte "Eingeschränkter Funktionsmodus" der Wert "vorhanden" steht, ist die entsprechende Funktionalität im eingeschränkten Funktionsmodus verfügbar. Steht in der Spalte "Eingeschränkter Funktionsmodus" der Wert "nicht vorhanden", so ist die entsprechende Funktionalität nicht verfügbar. Die Spalte "Beschränkungen" bietet zusätzliche Informationen.

Tabelle 2. Funktionalität von Kaspersky Total Security im eingeschränkten Funktionsmodus

Funktionalität	Beschränkungen	Eingeschränkter Funktionsmodus
Datei-Anti-Virus		vorhanden
Virenuntersuchung	Die Untersuchung kann manuell gestartet werden. Die Untersuchung nach Zeitplan ist nicht verfügbar und die Untersuchungseinstellungen können nicht angepasst werden.	vorhanden
Schwachstellensuche		nicht vorhanden
Update der Datenbanken und Programm-Module	Die Einstellungen können nicht angepasst werden.	vorhanden
Schutz vor Adware und Spyware		vorhanden
Web-Anti-Virus	Funktioniert uneingeschränkt.	vorhanden

Funktionalität	Beschränkungen	Eingeschränkter Funktionsmodus
Mail-Anti-Virus	Funktioniert uneingeschränkt.	vorhanden
IM-Anti-Virus	Funktioniert uneingeschränkt.	vorhanden
Heuristische Analyse	Funktioniert uneingeschränkt.	vorhanden
Rootkit-Schutz		nicht vorhanden
Exploit-Schutz		nicht vorhanden
Aktivitätsmonitor		nicht vorhanden
Phishing-Schutz		vorhanden
Reputationsprüfung für Dateien und Links in Kaspersky Security Network	Funktioniert uneingeschränkt.	vorhanden
Zusätzliche Schutz- und Verwaltungs-Tools	Funktioniert uneingeschränkt.	vorhanden
Link-Untersuchung		nicht vorhanden
Sichere Dateneingabe		nicht vorhanden
Notfall-CD	Option zum Download über die Programmoberfläche ist verfügbar.	vorhanden
Kennwortschutz für die Programmeinstellungen	Funktioniert uneingeschränkt.	vorhanden
Leistung	Die Leistungseinstellungen für das Programm können angepasst werden.	vorhanden

Funktionalität	Beschränkungen	Eingeschränkter Funktionsmodus
Aufgabenübersicht	Die Aufgabenübersicht dient nur der Anzeige von Untersuchungsergebnissen. Die Untersuchung und die Untersuchungseinstellungen können hier nicht verwaltet werden.	vorhanden
Profil für Spiele	Funktioniert uneingeschränkt.	vorhanden
Bedrohungen und Ausnahmen	Funktioniert uneingeschränkt.	vorhanden
Selbstschutz	Funktioniert uneingeschränkt.	vorhanden
Quarantäne	Funktioniert uneingeschränkt.	vorhanden
Meldungen	Nur der Bezug von Werbenachrichten von Kaspersky Lab kann angepasst werden.	vorhanden
"Protect a Friend"	Alle Optionen zur Teilnahme am Programm "Protect a Friend" sind verfügbar.	vorhanden
Darstellungseinstellungen für das Programm	Funktioniert uneingeschränkt.	vorhanden
My Kaspersky		vorhanden
Wiederherstellung nach Infektion	Funktioniert uneingeschränkt.	vorhanden
Programmkontrolle		nicht vorhanden
Firewall		nicht vorhanden
Schutz vor Netzwerkangriffen		nicht vorhanden
Anti-Spam		nicht vorhanden
Anti-Banner		nicht vorhanden

Funktionalität	Beschränkungen	Eingeschränkter Funktionsmodus
Sicherer Zahlungsverkehr		nicht vorhanden
Sichere Suche		nicht vorhanden
Schutz vor Datensammlung		nicht vorhanden
Aktivitätsspuren löschen		nicht vorhanden
Kindersicherung		nicht vorhanden
Schutz vor Webcam-Zugriff		nicht vorhanden
Benachrichtigung bei Verbindung mit einem unsicheren WLAN-Netzwerk		nicht vorhanden
Netzwerkmonitor		nicht vorhanden
Überwachung von Änderungen des Betriebssystems		nicht vorhanden
Kaspersky Password Manager	Das Programm Kaspersky Password Manager ist verfügbar, wenn es installiert wurde, bevor der eingeschränkte Funktionsmodus aktiviert wurde. Wenn das Programm nicht installiert war, kann es im eingeschränkten Schutzmodus nicht installiert werden. Im eingeschränkten Funktionsmodus kann Kaspersky Password Manager nicht aus dem Fenster von Kaspersky Total Security gestartet werden.	nicht vorhanden
Löschen von nicht benötigten Daten		nicht vorhanden

Funktionalität	Beschränkungen	Eingeschränkter Funktionsmodus
Unwiderrufliches Löschen von Daten		nicht vorhanden
Virtuelle Datentresore	Der Zugriff ist nur auf Daten in bereits erstellten Datentresoren möglich.	nicht vorhanden
Sichern und Wiederherstellen	Es können nur Daten aus bereits vorhandenen Sicherungskopien wiederhergestellt werden.	nicht vorhanden
Fernverwaltung	Nur Anzeige und Verwaltung von Aktivierungscodes	vorhanden

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 nach der Programmaktivierung ein Aktivierungscode 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

Wenn *Kaspersky Total Security mit einem Abonnement* genutzt wird, gelten bestimmte Bedingungen für das Programm (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 Dienstanbieter kann zwei Arten von Abonnements für die Nutzung von Kaspersky Total Security anbieten: Update-Abonnement oder Update- und Schutz-Abonnement.

Ein Abonnement kann befristet (z. B. auf ein Jahr) oder unbefristet sein (ohne Ablaufdatum). Um Kaspersky Total Security weiter zu nutzen, nachdem ein befristetes Abonnement abgelaufen ist, müssen Sie das Abo manuell verlängern. Ein unbefristetes Abonnement wird automatisch verlängert, falls der vereinbarte Betrag rechtzeitig an den Dienstanbieter überwiesen wird.

Für ein befristetes 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 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 Bereitstellung von Daten

Damit der Informationsschutz verbessert und Kaspersky Total Security optimiert werden kann, stimmen Sie zu, dass automatisch die im Folgenden genannten statistischen und dienstbezogenen Informationen, einschließlich, aber nicht beschränkt auf diese Aufzählung, an Kaspersky Lab übermittelt werden: Informationen über auf dem Computer installierte Software, Lizenzdaten, Informationen über gefundene Bedrohungen und Infektionen, Prüfsummen verarbeiteter Objekte, technische Informationen über den Computer und über mit dem Computer verbundene Geräte, Informationen über die Online-Aktivitäten eines Gerätes. Ausführliche Informationen finden Sie hier (http://help.kaspersky.com/de).

Wenn Sie am Programm Kaspersky Security Network teilnehmen, stimmen Sie zu, dass automatisch folgende Informationen an Kaspersky Lab übermittelt werden (http://help.kaspersky.com/de), die bei der Nutzung von Kaspersky Total Security auf dem Computer erhalten wurden. Die Vereinbarung zu Kaspersky Security Network können Sie im Fenster **Einstellungen für zusätzliche Schutz-Tools** einsehen.

Kaspersky Lab schützt die empfangenen Informationen in Übereinstimmung mit den gesetzlichen Vorschriften und den geltenden Regeln von Kaspersky Lab.

Kaspersky Lab verwendet diese Informationen nur in anonymisierter Form und in Form von Daten für eine allgemeine Statistik. Die Daten der allgemeinen Statistik werden automatisch aus den empfangenen Quellinformationen erstellt und enthalten keine persönlichen oder sonstigen vertraulichen Informationen. Die gesammelten Quellinformationen werden regelmäßig gelöscht (einmal pro Jahr). Die Daten der allgemeinen Statistik werden unbegrenzt gespeichert.

Lizenz kaufen

Sie können eine Lizenz kaufen oder verlängern. Beim Kauf einer Lizenz erhalten Sie einen Aktivierungscode, mit dem Sie das Programm aktivieren müssen (s. Abschnitt "Programm aktivieren" auf S. 55).

► *Gehen Sie folgendermaßen vor, um eine Lizenz zu erwerben:*

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie eine der folgenden Methoden, um das Fenster **Lizenzverwaltung** zu öffnen:
   - Mit dem Link **Keine Lizenz vorhanden**, der sich im unteren Bereich des Hauptfensters befindet, wenn das Programm nicht aktiviert ist.
   - Mit dem Link **Lizenz**, der sich im unteren Bereich des Hauptfensters befindet, wenn das Programm aktiviert ist.
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. Benachrichtigungen der Komponente Programmkontrolle werden automatisch nach 500 Sekunden geschlossen. Benachrichtigungen über den Start eines Programms werden automatisch nach 1 Stunde geschlossen. 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.

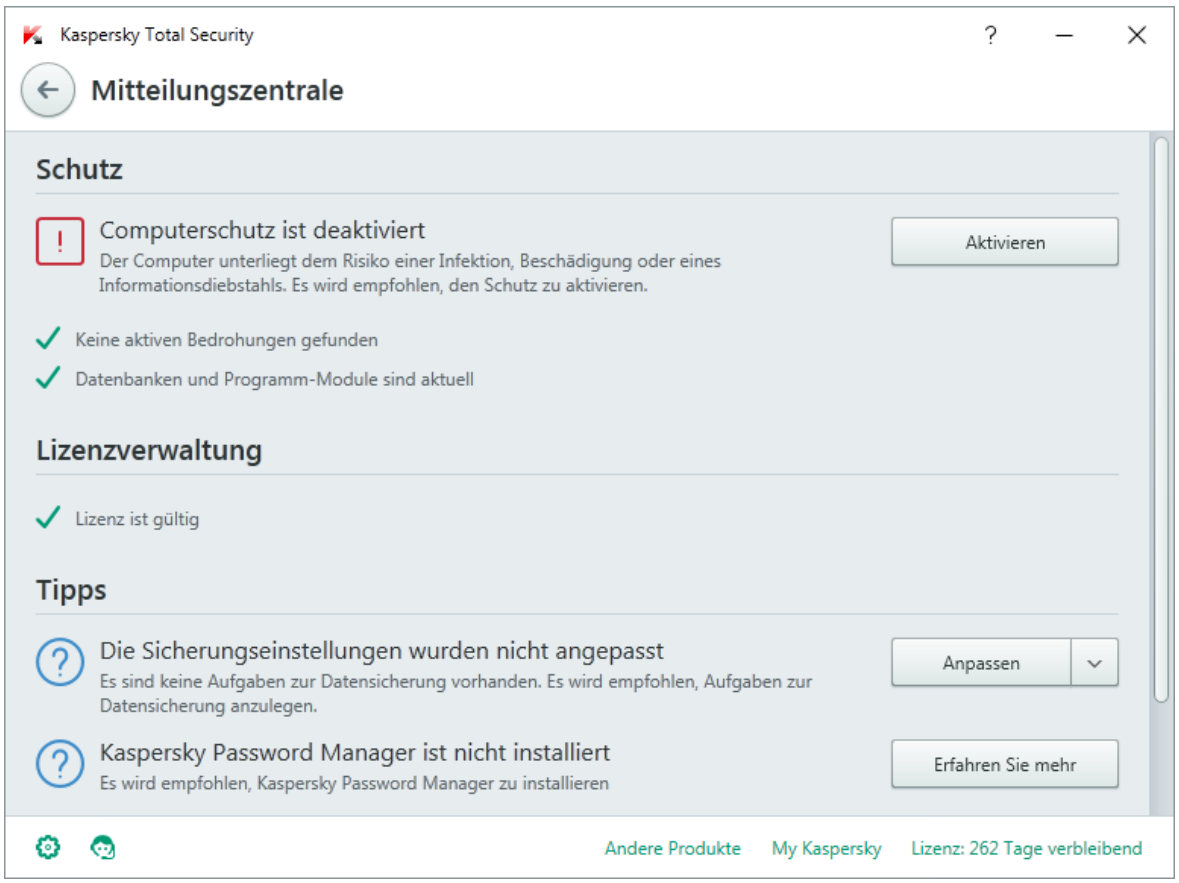

Abbildung 1. Fenster Mitteilungszentrale

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

Dieser Abschnitt enthält Informationen über das Update der Datenbanken und Programm-Module.

In diesem Abschnitt

Über das Update der Datenbanken und Programm-Module 60

Update der Datenbanken und Programm-Module starten 62

Über das Update der Datenbanken und Programm-Module

Im Installationspaket für Kaspersky Total Security sind Datenbanken und Programm-Module enthalten. Diese Programm-Datenbanken gewährleisten das *Basis-Schutzniveau*:

- Kaspersky Total Security erkennt die meisten Bedrohungen mithilfe von Kaspersky Security Network. Dafür ist eine Internetverbindung erforderlich.
- Adware, Dialer und andere legale Programme, mit denen Angreifer den Computer oder die Benutzerdaten beschädigen können, werden von Kaspersky Total Security nicht erkannt.

Um umfassenden Schutz zu gewährleisten, müssen die Datenbanken und Programm-Module sofort nach der Programminstallation aktualisiert werden.

Das Update der Datenbanken und Programm-Module verläuft wie folgt:

1. Kaspersky Total Security richtet sich beim Start des Updates der Datenbanken und Programm-Module nach den festgelegten Einstellungen: Der Start erfolgt entweder nach Zeitplan oder auf Ihren Befehl. Das Programm greift auf die Update-Quelle zu, in der das Update-Paket für die Datenbanken und Programm-Module gespeichert ist.
2. Kaspersky Total Security vergleicht die vorhandenen Datenbanken mit den Datenbanken, die in der Update-Quelle vorliegen. Wenn sich die Datenbanken unterscheiden, lädt Kaspersky Total Security den fehlenden Teil der Datenbanken herunter.

Anschließend verwendet das Programm die aktualisierten Datenbanken und Programm-Module, um den Computer auf Viren und andere bedrohliche Programme zu untersuchen.

Sie können folgende Update-Quellen verwenden:

- Kaspersky Labs Update-Server
- HTTP- oder FTP-Server
- Netzwerkordner

Für das Update der Datenbanken und Programm-Module gelten folgende Besonderheiten und Einschränkungen:

- Die Datenbanken gelten nach zwei Wochen als veraltet.
- Um ein Update-Paket von Kaspersky Labs Update-Servern herunterzuladen, ist eine Internetverbindung erforderlich.
- Das Update der Datenbanken und Programm-Module ist in folgenden Fällen nicht verfügbar:
    - Die Lizenz ist abgelaufen und eine Nachfrist oder ein eingeschränkter Funktionsmodus ist nicht vorgesehen.
    - Eine mobile Breitband-Internetverbindung wird verwendet. Diese Beschränkung gilt bei Verwendung des Betriebssystems Microsoft Windows 8 und höher, wenn der automatische Update-Modus oder der Update-Modus nach Zeitplan ausgewählt ist und für mobile Breitband-Internetverbindungen eine Beschränkung des Datenverkehrs festgelegt wurde. Damit in diesem Fall die Datenbanken und Programm-Module aktualisiert werden, deaktivieren Sie im Fenster **Einstellungen** → **Erweitert** → **Netzwerk** das Kontrollkästchen **Datenverkehr bei getakteter Verbindung beschränken**.
    - Das Programm wird im Abo genutzt und Sie haben das Abo auf der Provider-Webseite vorübergehend angehalten.

Update der Datenbanken und Programm-Module starten

► *Um das Update der Datenbanken und Programm-Module über das Kontextmenü des Programmsymbols zu starten,*

öffnen Sie im Infobereich der Taskleiste das Kontextmenü des Programmsymbols und wählen Sie den Punkt **Update** aus.

► *Um das Update der Datenbanken und Programm-Module aus dem Programmhauptfenster zu starten, gehen Sie wie folgt vor:*

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

   Das Fenster **Update** wird geöffnet.

2. Klicken Sie im Fenster **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 63

Benutzerdefinierte Untersuchung 64

Schnelle Untersuchung 65

Schwachstellensuche 66

Vollständige Untersuchung

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

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

Schwachstellensuche

Schwachstellen sind Teile eines Programmcodes, den Angreifer für ihre Ziele nutzen können, um beispielsweise 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 unten im Hauptfenster auf die Schaltfläche **Mehr Funktionen**, 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.

Für Anwendungen aus dem Windows Store, die 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 unten im Hauptfenster auf die Schaltfläche **Mehr Funktionen**, 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

Betriebssystem nach einer Infektion wiederherstellen 68

Betriebssystem mithilfe des Wiederherstellungs-Assistenten wiederherstellen 69

Über die Notfall-CD 71

Betriebssystem nach einer Infektion wiederherstellen

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 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 unten im Hauptfenster auf die Schaltfläche **Mehr Funktionen**, 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 Beschädigungen ausführen, die mit Schadsoftware-Aktivität zusammenhängen** ausgewählt ist, 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 Behebung von Beschädigungen auswählen

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. Es sind drei Gruppen vorhanden:

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

Klicken Sie links vom Namen einer Gruppe auf das Symbol ▶, um die Beschädigungen aus dieser Gruppe anzuzeigen.

Damit der Assistent eine bestimmte Beschädigung behebt, aktivieren Sie das Kontrollkästchen links von der Bezeichnung der Beschädigung. In der Grundeinstellung behebt der Assistent Beschädigungen aus den Gruppen, für die das Beheben empfohlen und ausdrücklich empfohlen ist. Falls eine bestimmte Beschädigung nicht behoben werden soll, 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. Beschädigungen beheben

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Das Beheben von Beschädigungen kann eine gewisse Zeit beanspruchen. Nachdem die Beschädigungen behoben wurden, geht der Assistent automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

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

Über die Notfall-CD

Die Notfall-CD besteht aus dem Programm Kaspersky Notfall-CD, das auf einem Wechseldatenträger (CD oder USB-Gerät) gespeichert ist. Die Notfall-CD kann verwendet werden, um den infizierten Computer zu untersuchen und zu desinfizieren, wenn eine Desinfektion mit anderen Mitteln (z. B. Antiviren-Programmen) fehlschlägt.

Wenn Sie Kaspersky Total Security in einer Box gekauft haben, enthält der Installationsdatenträger neben dem Installationspaket für Kaspersky Total Security auch Kaspersky Notfall-CD. Sie können diesen Installationsdatenträger als Notfall-CD einsetzen.

Ausführliche Informationen zur Verwendung von Kaspersky Notfall-CD finden Sie auf der Webseite des Technischen Supports (http://support.kaspersky.com/de/viruses/rescuedisk/main).

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 72

Unerwünschte E-Mails (Spam) blockieren..... 74

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 unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie links im Fenster unter **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, und führt eine heuristische Analyse mit der Genauigkeitsstufe **Mittel** aus.

    - **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, und führt eine heuristische Analyse mit der Genauigkeitsstufe **Tief** aus.

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 Backup-Kopie an und verschiebt sie in die Quarantäne (s. Abschnitt "Objekt wiederherstellen, das vom Programm gelöscht oder desinfiziert wurde" auf S. 67).

Wenn das Programm Kaspersky Total Security bei der Untersuchung im Nachrichtentext ein Kennwort für das Archiv findet, so wird das Kennwort verwendet, um den Inhalt des Archivs auf Schadsoftware zu untersuchen. Das Kennwort wird dabei nicht gespeichert. Das Archiv wird im Rahmen der Untersuchung entpackt. Sollte beim Entpacken des Archivs ein Fehler im Programm auftreten, so können Sie die Dateien, die beim Entpacken unter dem Pfad %systemroot%\temp gespeichert wurden, manuell löschen. Diese Dateien besitzen das Präfix PR.

Unerwünschte E-Mails (Spam) blockieren

Falls Sie viel Spam erhalten, aktivieren Sie die Komponente Anti-Spam und legen Sie für diese Komponente die Sicherheitsstufe **Empfohlen** fest.

► *Um Anti-Spam zu aktivieren und die Sicherheitsstufe Empfohlen auszuwählen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Programmfenster auf die Schaltfläche  .

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Schutz** aus.
4. Wählen Sie rechts im Abschnitt **Schutz** 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.

Die Komponente Anti-Spam kann protokollunabhängig nur Nachrichten analysieren, die vollständig vom Mail-Server heruntergeladen wurden.

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 75

Über die Bildschirmtastatur 76

Bildschirmtastatur starten 78

Anzeige des Symbols für die Bildschirmtastatur anpassen 80

Schutz von Tastatureingaben 81

Benachrichtigungen über Schwachstellen in einem WLAN-Netzwerk anpassen 83

Sicherheit einer Webseite überprüfen 84

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 Bankkartennummern

Kaspersky Total Security verfügt über 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 Bildschirmtastatur und der Schutz von Tastatureingaben dienen dazu, Daten, die über eine Hardwaretastatur eingegeben werden, vor Abfangversuchen 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. 107).

Über die Bildschirmtastatur

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 Daten mithilfe von Hardware-Hooks oder mit Keyloggern (Programme, die Tasteneingaben registrieren) abgefangen werden. Die Bildschirmtastatur 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 Bildschirmtastatur schützt davor, dass persönliche Daten durch das Anlegen von Bildschirmkopien (Screenshots) abgefangen werden.

Für die Bildschirmtastatur gelten folgende Besonderheiten:

- Die Tasten der Bildschirmtastatur werden mit der Maus bedient.
- Im Gegensatz zu einer echten Tastatur können auf der Bildschirmtastatur nicht mehrere Tasten gleichzeitig gedrückt werden. 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 Bildschirmtastatur mit der gleichen Tastenkombination umgeschaltet, die dafür für die gewöhnliche Tastatur in den Einstellungen des Betriebssystems 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 Bildschirmtastatur eingegeben werden, muss der Computer nach der Installation von Kaspersky Total Security neu gestartet werden.

Für die Bildschirmtastatur gelten folgende Einschränkungen:

- Die Bildschirmtastatur 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 Bildschirmtastatur geschützt.
- Die Bildschirmtastatur ist im Browser Microsoft Internet Explorer (Version 10 und 11) im neuen Windows-Design nicht verfügbar. In diesem Fall wird empfohlen, die Bildschirmtastatur über die Oberfläche von Kaspersky Total Security zu öffnen.
- Die Bildschirmtastatur kann Ihre persönlichen Daten nicht schützen, wenn Daten auf einer gehackten Webseite eingegeben werden, da die Informationen in diesem Fall direkt in die Hände des Angreifers fallen.
- Die Bildschirmtastatur verhindert nicht das Erstellen von Screenshots mithilfe der **DRUCK**-Taste und mit anderen Tastenkombinationen, die in den Einstellungen des Betriebssystems festgelegt sind.

- Wenn die Bildschirmtastatur im Browser Microsoft Internet Explorer gestartet wird, wird die Autovervollständigung für Eingabefelder deaktiviert, da die diese Funktion Betrügern die Möglichkeit zum Datendiebstahl bietet.
- Im Betriebssystem Microsoft Windows 8 und 8.1 (nur 64-Bit) funktioniert der Screenshot-Schutz von Kaspersky Total Security nicht, wenn das Fenster der Bildschirmtastatur geöffnet ist, aber der Prozess des Sicheren Browser nicht läuft.

Die oben stehende Liste enthält die wichtigsten Einschränkungen, die für die Funktionalität "Schutz der Dateneingabe" gelten. Eine vollständige Liste der Einschränkungen finden Sie im folgenden Artikel auf der Support-Website von Kaspersky Lab: http://support.kaspersky.com/de/12005.

Bildschirmtastatur starten

Die Bildschirmtastatur kann auf folgende Weise geöffnet werden:

- aus dem Kontextmenü des Programmsymbols im Infobereich der Taskleiste
- aus dem Programmfenster
- aus der Symbolleiste des Browsers Microsoft Internet Explorer, Mozilla Firefox oder Google Chrome
- mithilfe des Schnellstartsymbols für die Bildschirmtastatur in den Eingabefeldern von Webseiten

  Die Anzeige des Schnellstartsymbols in den Eingabefeldern von Webseiten lässt sich anpassen (s. Abschnitt "Anzeige des Symbols für die Bildschirmtastatur anpassen" auf S. 80).

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

- Mit einer Tastenkombination über die Hardwaretastatur.

► *Um die Bildschirmtastatur aus dem Kontextmenü des Programmsymbols im Infobereich der Taskleiste zu öffnen,*

wählen Sie den Punkt **Tools** → **Bildschirmtastatur** (s. Abb. unten).

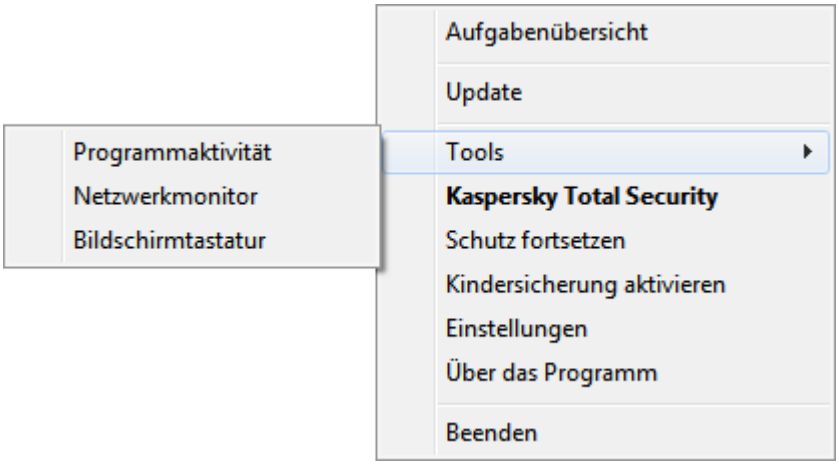

Abbildung 3. Kontextmenü von Kaspersky Total Security

► *Um die Bildschirmtastatur vom Programmfenster aus zu öffnen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Hauptfenster auf die Schaltfläche **Mehr Funktionen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie links im Fenster **Tools** auf den Link **Bildschirmtastatur**, um die Bildschirmtastatur zu öffnen.

► *Um die Bildschirmtastatur aus der Symbolleiste des Browsers Google Chrome, Microsoft Internet Explorer oder Mozilla Firefox zu öffnen, gehen Sie wie folgt vor:*

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

► *Um die Bildschirmtastatur mithilfe der Hardwaretastatur zu öffnen,*

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

Anzeige des Symbols für die Bildschirmtastatur anpassen

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

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie im Abschnitt **Erweitert** den Unterabschnitt **Sichere Dateneingabe**.

   Dieses Fenster enthält Einstellungen für die sichere Dateneingabe.
4. Aktivieren Sie, falls erforderlich, im Abschnitt **Bildschirmtastatur** das Kontrollkästchen **Bildschirmtastatur mit der Tastenkombination STRG+ALT+UMSCHALT+P öffnen**.
5. Damit das Schnellstartsymbol für die Bildschirmtastatur in Eingabefeldern auf allen Websites angezeigt wird, aktivieren Sie das Kontrollkästchen **Schnellstartsymbol in Eingabefeldern anzeigen**.
6. Damit das Schnellstartsymbol für die Bildschirmtastatur nur angezeigt wird, wenn Websites bestimmter Kategorien geöffnet werden, gehen Sie wie folgt vor:
   a. Öffnen Sie im Abschnitt **Bildschirmtastatur** mit dem Link **Kategorien ändern** das Fenster **Einstellungen für Sichere Dateneingabe**.
   b. Aktivieren Sie die Kontrollkästchen für die Webseiten-Kategorien, auf denen das Schnellstartsymbol der Bildschirmtastatur in Eingabefeldern angezeigt werden soll.

      Das Schnellstartsymbol für die Bildschirmtastatur wird angezeigt, wenn eine Webseite geöffnet wird, die zu einer der ausgewählten Kategorien gehört.
7. Um die Anzeige des Schnellstartsymbols für die Bildschirmtastatur auf einer bestimmten Webseite zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:
   a. Öffnen Sie im Abschnitt **Bildschirmtastatur** mit dem Link **Kategorien ändern** das Fenster **Einstellungen für Sichere Dateneingabe**.
   b. Öffnen Sie mit dem Link **Ausnahmen anpassen** das Fenster **Ausnahmen für die Bildschirmtastatur**.

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

d. Im folgenden Fenster kann eine Ausnahme für die Bildschirmtastatur hinzugefügt werden.

e. Tragen Sie im Feld **Maske für Webadresse** die Adresse der Webseite ein.

f. Legen Sie im Abschnitt **Geltungsbereich** fest, wo das Symbol zum Öffnen der Bildschirmtastatur angezeigt werden soll (oder nicht): auf der angegebenen Seite oder auf allen Seiten der Website.

g. Legen Sie im Abschnitt **Symbol für die Bildschirmtastatur** fest, ob das Symbol zum Öffnen der Bildschirmtastatur angezeigt werden soll oder nicht.

h. Klicken Sie auf **Hinzufügen**.

   Die angegebene Website erscheint auf der Liste im Fenster **Ausnahmen für die Bildschirmtastatur**.

Beim Öffnen der angegebenen Website wird das Schnellstartsymbol für die Bildschirmtastatur in Eingabefeldern nach den festgelegten Einstellungen angezeigt.

Schutz von Tastatureingaben

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 Tastatureingaben funktioniert nur in den Browsern Microsoft Internet Explorer, Mozilla Firefox und Google Chrome. Bei Verwendung anderer Browser 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.

Die oben stehende Liste enthält die wichtigsten Einschränkungen, die für die Funktionalität "Schutz der Dateneingabe" gelten. Eine vollständige Liste der Einschränkungen finden Sie im folgenden Artikel auf der Support-Website von Kaspersky Lab: http://support.kaspersky.com/de/12005.

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 unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
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. Klicken Sie im Abschnitt **Schutz von Tastatureingaben** unten auf den Link **Kategorien ändern**, um das Fenster **Einstellungen für Sichere Dateneingabe** zu öffnen.
6. Aktivieren Sie die Kontrollkästchen für die Webseiten-Kategorien, auf denen über die Tastatur eingegebene Daten geschützt werden sollen.
7. Um den Schutz für Tastatureingaben auf einer bestimmten Webseite zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

   a. Öffnen Sie mit dem Link **Ausnahmen anpassen** das Fenster **Ausnahmen für den Schutz von Tastatureingaben**.

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

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

d. Tragen Sie im folgenden Fenster im Feld **Maske für Webadresse** die Adresse der Website ein.

e. Wählen Sie eine Variante für den Schutz der Dateneingabe auf dieser Website aus: **Nur auf die angegebene Seite anwenden** oder **Auf die gesamte Website anwenden**.

f. Wählen Sie als Aktion für den Schutz der Dateneingabe auf dieser Website entweder **Schützen** oder **Nicht schützen** aus.

g. Klicken Sie auf **Hinzufügen**.

Die angegebene Website 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 WLAN-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 unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.

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 **Klartextübertragung eines Kennworts im Internet 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.

Sicherheit einer Webseite überprüfen

Kaspersky Total Security kann die Sicherheit einer Website überprüfen, bevor Sie einem Link zu dieser Website folgen. Für die Untersuchung von Webseiten wird die Komponente *Links untersuchen* verwendet.

> Die Link-Untersuchung ist im Browser Microsoft Internet Explorer (Version 10 und 11) im neuen Windows-Design nicht verfügbar.

Die Komponente Link-Untersuchung überprüft Links auf Webseiten, die im Browser Microsoft Internet Explorer, Google Chrome oder Mozilla Firefox geöffnet werden. Neben untersuchten Links zeigt Kaspersky Total Security 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 Daten 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 Programmfenster auf die Schaltfläche  .

   Das Fenster **Einstellungen** wird geöffnet.
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 den erweiterten Einstellungen für Web-Anti-Virus.
5. Aktivieren Sie im Abschnitt **Links untersuchen** das Kontrollkästchen **Links untersuchen**.
6. Damit Kaspersky Total Security den Inhalt aller Webseiten untersucht, wählen Sie die Variante **Auf allen Webseiten, außer den festgelegten** aus.
7. Geben Sie, falls erforderlich, im Fenster **Ausnahmen** die Webseiten an, denen Sie vertrauen. Dieses Fenster wird mit dem Link **Ausnahmen anpassen** geöffnet. Der Inhalt der angegebenen Webseiten sowie verschlüsselte Verbindungen mit den angegebenen Webseiten werden von Kaspersky Total Security nicht untersucht.

8. Damit Kaspersky Total Security nur den Inhalt bestimmter Webseiten untersucht, gehen Sie wie folgt vor:

    a. Wählen Sie die Variante **Nur auf den festgelegten Webseiten** aus.

    b. Öffnen Sie mit dem Link **Zu untersuchende Webseiten anpassen** das Fenster **Zu untersuchende Webseiten**.

    c. Klicken Sie auf **Hinzufügen**.

    d. Geben Sie eine Webadresse an, deren Inhalt untersucht werden soll.

    e. Wählen Sie einen Untersuchungsstatus für die Webseite aus (*Aktiv* – Kaspersky Total Security untersucht den Inhalt der Webseite).

    f. Klicken Sie auf **Hinzufügen**.

    Die angegebene Webseite erscheint auf der Liste im Fenster **Zu untersuchende Webseiten**. Kaspersky Total Security untersucht die Links auf dieser Webseite.

9. Um erweiterte Einstellungen für die Link-Untersuchung vorzunehmen, klicken Sie im Fenster **Erweiterte Einstellungen für Web-Anti-Virus** unter **Links untersuchen** auf den Link **Link-Untersuchung anpassen**. Das Fenster **Links untersuchen** wird geöffnet.

10. Damit Kaspersky Total Security auf allen Webseiten vor unsicheren Links warnt, wählen Sie im Abschnitt **Zu untersuchende Links** die Variante **Alle Links** aus.

11. Damit Kaspersky Total Security darüber informiert, zu welcher inhaltlichen Kategorie für Webseiten (z. B. *Obszönität*) 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.

Kaspersky Total Security untersucht die Links auf den angegebenen Webseiten und informiert über die Link-Kategorien. Dabei gelten die festgelegten Einstellungen.

Schutz für Finanztransaktionen und Online-Einkäufe

Dieser Abschnitt informiert darüber, wie Sie Ihre Finanztransaktionen und Online-Einkäufe mithilfe von Kaspersky Total Security schützen können.

In diesem Abschnitt

Über den Schutz von Finanztransaktionen und Online-Einkäufen 87

Einstellungen für den Sicheren Zahlungsverkehr anpassen 90

Sicheren Zahlungsverkehr für eine bestimmte Webseite anpassen 90

Automatische Aktivierung der Erweiterung Kaspersky Protection einschalten 91

Screenshot-Schutz 92

Screenshot-Schutz aktivieren 93

Schutz von Daten in der Zwischenablage 93

Kaspersky Password Manager starten 94

Über den Schutz von Finanztransaktionen und Online-Einkäufen

Um vertrauliche Daten zu schützen, die Sie auf den Websites von Banken und Zahlungssystemen eingeben (beispielsweise Bankkartennummern und Online-Banking-Kennwörter), und um einen Diebstahl von Zahlungsmitteln bei Online-Zahlungsvorgängen zu verhindern, schlägt Kaspersky Total Security vor, solche Websites 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. Kaspersky Total Security erstellt spezielle Profile für die Browser Mozilla Firefox und Google Chrome, um zu verhindern, dass installierte Dritthersteller-Erweiterungen den Sicheren Browser beeinflussen. Das Programm übt keinen Einfluss auf Ihre Daten aus, die Browser in den erstellten Profilen speichern können.

Browser, die den Voraussetzungen für das Programm nicht entsprechen (s. Abschnitt "Hard- und Softwarevoraussetzungen" auf S. 25), funktionieren nicht im Sicheren Browsermodus. Anstelle dieser Browser wird im Sicheren Browsermodus entweder der Internet Explorer oder jener Browser gestartet, der in den Programmeinstellungen festgelegt ist.

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.

Zur Interaktion mit geschützten Websites bindet Kaspersky Total Security ein spezielles Skript in die Seiten von Websites. Das Skript wird entweder vom Programm selbst oder mithilfe der Erweiterung Kaspersky Protection eingebunden (s. Abschnitt "Programm vorbereiten" auf S. 35). Die Erweiterung ist auch erforderlich, damit der Sichere Browser einwandfrei funktioniert. Falls die Erweiterung nicht installiert ist, bietet Ihnen der Browser beim ersten Start im Sicheren Browsermodus an, die Erweiterung zu installieren. Wenn Sie die Installation der Erweiterung Kaspersky Protection abgelehnt haben, können Sie die Erweiterung später installieren.

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

Einstellungen für den Sicheren Zahlungsverkehr anpassen

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

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
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 auf **Sicherer Zahlungsverkehr**.

   Das Fenster **Sicherer Zahlungsverkehr** wird geöffnet.
3. Klicken Sie auf den Link **Webseite zum Sicheren Zahlungsverkehr hinzufügen**, um im rechten Fensterbereich die Eingabefelder zu öffnen, mit denen Informationen über die Webseite hinzugefügt werden können.

4. Geben Sie im Feld **Website für Sicheren Zahlungsverkehr** die Adresse der Webseite an, die im Sicheren Browser geöffnet werden soll.

   > Der Webadresse muss das Protokoll HTTPS (beispielsweise https://example.com) vorangestellt sein, das standardmäßig vom Sicheren Browser verwendet wird.

5. Öffnen Sie mit dem Link **Beschreibung hinzufügen** das Feld **Beschreibung** und geben Sie eine Bezeichnung oder Beschreibung für diese Webseite an.

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 der Erweiterung Kaspersky Protection einschalten

► *Um festzulegen, dass die Erweiterung Kaspersky Protection automatisch aktiviert wird, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.

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 **Erweiterung Kaspersky Protection** das Kontrollkästchen **Erweiterung Kaspersky Protection automatisch in Browsern 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. 93).

Wenn Kaspersky Total Security auf einer 64-Bit-Version des Betriebssystems Microsoft Windows 8, Microsoft Windows 8.1 oder Microsoft Windows 10 installiert ist, verwendet das Programm die Hypervisor-Technologie für den Screenshot-Schutz.

Für die 64-Bit-Version des Betriebssystems Microsoft Windows 8, Microsoft Windows 8.1 oder Microsoft Windows 10 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 unten im Programmfenster auf die Schaltfläche  .

   Das Fenster **Einstellungen** wird geöffnet.
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**. Das Kontrollkästchen wird in der 64-Bit-Version von Windows 8 und Windows 8.1 und Windows 10 angezeigt.

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 wird unabhängig von Kaspersky Total Security installiert. Nach der Installation können Sie Kaspersky Password Manager aus dem **Startmenü** (im Betriebssystem Microsoft Windows 7 und niedriger), vom Startbildschirm aus (im Betriebssystem Microsoft Windows 8 und höher) 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**.
3. Klicken Sie im folgenden Fenster auf **Kaspersky Password Manager starten**.

Das Programmfenster von Kaspersky Password Manager wird geöffnet.

► *Um Kaspersky Password Manager herunterzuladen und zu installieren, 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 auf **Kaspersky Password Manager herunterladen und installieren**.

   Kaspersky Total Security lädt das Installationspaket für Kaspersky Password Manager herunter und installiert das Programm auf Ihren Computer.

   Das heruntergeladene Installationspaket für Kaspersky Password Manager verbleibt unabhängig davon auf Ihrem Computer, ob es zur Installation des Programms Kaspersky Password Manager verwendet wurde oder nicht.

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

Schutz vor dem Sammeln von Informationen über Ihre Online-Aktivitäten

Dieser Abschnitt informiert darüber, wie Kaspersky Total Security Sie vor dem Sammeln von Daten über Ihre Online-Aktivitäten schützt.

In diesem Abschnitt

Über den Schutz vor Datensammlung 95

Einstellungen für den Schutz vor Datensammlung 96

Tracking-Dienste nach Kategorien blockieren 98

Datensammlung auf bestimmten Websites erlauben 98

Bericht über Anfragen an Tracking-Dienste anzeigen 99

Schutz vor Datensammlung im Browser verwalten 100

Über den Schutz vor Datensammlung

Die Komponente *Schutz vor Datensammlung* schützt davor, dass Informationen über Ihre Aktivitäten im Internet gesammelt werden.

Wenn Sie im Internet sind, erkennt die Komponente Schutz vor Datensammlung Anfragen, die der Browser an Tracking-Dienste schickt, wenn Webseiten geladen werden, in denen zur Nachverfolgung dienende Programmcodes und html-Markups enthalten sind. Tracking-Dienste verwenden Informationen aus diesen Anfragen, um Ihre Aktionen zu analysieren, und können Analyseergebnisse beispielsweise nutzen, um Ihnen individualisierte Werbeangebote zu zeigen.

Im *Überwachungsmodus* bietet Ihnen die Komponente Schutz vor Datensammlung die Möglichkeit, Berichte über erkannte Anfragen an Tracking-Dienste einzusehen. Dieser Modus ist standardmäßig aktiviert.

Im *Sperrmodus* erstellt die Komponente Schutz vor Datensammlung nicht nur Berichte, sondern modifiziert auch die Anfragen an Tracking-Dienste und Antworten auf solche Anfragen, um zu verhindern, dass Informationen über Ihre Online-Aktivitäten gesammelt werden. Im Folgenden wird unter *Sperrung von Anfragen* und *Sperrung von Tracking-Diensten* die oben beschriebene Modifikation von Anfragen an Tracking-Dienste und entsprechenden Antworten verstanden.

Sie können die Komponente Schutz vor Datensammlung direkt im Browser verwalten (s. Abschnitt "Schutz vor Datensammlung im Browser verwalten" auf S. 100).

Der Schutz vor Datensammlung besitzt folgende Einschränkungen:

- Das Programm blockiert Tracking-Dienste aus der Kategorie "Kommunikationsmedien im Internet" nicht, wenn Sie sich auf der Website des entsprechenden sozialen Netzwerks befinden.
- Wenn die Webseite, von der eine Anfrage an einen Tracking-Dienst gesendet wurde, nicht ermittelt werden konnte, blockiert Kaspersky Total Security diesen Tracking-Dienst nicht und zeigt keine Informationen über die entsprechende Anfrage an.
- Wenn die Webseite, von der eine Anfrage an einen Tracking-Dienst gesendet wurde, zwar ermittelt werden konnte, sie aber nicht einer im Browser geöffneten Webseite zugeordnet werden konnte, so wendet Kaspersky Total Security auf diese Anfrage jene Aktion an, die in den Einstellungen für den Schutz vor Datensammlung festgelegt ist (Erkennen oder Blockieren). Das Programm zeigt in den Berichten Informationen über diese Anfrage an, nimmt diese Anfrage aber nicht in die Statistik für den Schutz vor Datensammlung auf, die im Browser angezeigt wird.

Einstellungen für den Schutz vor Datensammlung

► *Um den Schutz vor Datensammlung anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Schutz** aus.

   Ein Fenster mit einer Liste der Schutzkomponenten wird geöffnet. Die Komponente Schutz vor Datensammlung ist standardmäßig aktiviert.

4. Um die Komponente Schutz vor Datensammlung zu deaktivieren, schieben Sie den Schalter neben dem Element **Schutz vor Datensammlung** auf die Position  .

5. Wenn Sie die Standardeinstellungen der Komponente Schutz vor Datensammlung ändern möchten, wählen Sie rechts im Fenster das Element **Schutz vor Datensammlung** aus.

   Das Fenster **Einstellungen für den Schutz vor Datensammlung** wird geöffnet.

6. Passen Sie die Einstellungen für den Schutz vor Datensammlung auf Ihrem Computer an:

   - Wenn Sie möchten, dass das Programm Anfragen an Tracking-Dienste nur erkennt und protokolliert, die Anfragen aber nicht blockiert, belassen Sie die voreingestellte Variante **Anfragen erkennen, aber nicht blockieren**.

   - Wenn Sie möchten, dass das Programm Anfragen an Tracking-Dienste blockiert, wählen Sie die Variante **Erkannte Anfragen blockieren** aus. Der Link **Kategorien und Ausnahmen** führt in ein Fenster, in dem Sie die Kategorien für Tracking-Dienste angeben können, die blockiert werden sollen.

7. Wenn Sie nicht möchten, dass eine HTTP-Kopfzeile an Webseiten geschickt wird, um das Sammeln von Daten über Ihre Aktivitäten zu verbieten, deaktivieren Sie das Kontrollkästchen **Verbot zur Datensammlung senden**. Dieses Kontrollkästchen ist standardmäßig aktiviert.

8. Wenn Sie verbieten möchten, dass beim Besuch der Websites von Kaspersky Lab und seinen Partnern Daten über Ihre Aktivitäten gesammelt werden, deaktivieren Sie das Kontrollkästchen **Datensammlung auf Websites von Kaspersky Lab und seinen Partnern erlauben**. Standardmäßig blockiert der Schutz vor Datensammlung Anfragen an Tracking-Dienste auf Websites von Kaspersky Lab und seinen Partnern nicht.

9. Wenn Sie die Datensammlung auf Websites auch dann verbieten möchten, wenn dadurch die Funktionsfähigkeit von Websites beeinträchtigt wird, deaktivieren Sie das Kontrollkästchen **Datensammlung auf inkompatiblen Websites erlauben**. Auf Websites, die nach den Angaben von Kaspersky Lab aufgrund einer Sperrung fehlerhaft funktionieren können, werden Anfragen an Tracking-Dienste vom Schutz vor Datensammlung standardmäßig nicht blockiert.

   Die Liste der inkompatiblen Websites wird regelmäßig von Kaspersky Lab aktualisiert.

Tracking-Dienste nach Kategorien blockieren

► *Um die Sperrung von Tracking-Diensten nach Kategorien anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Schutz** aus.

   Ein Fenster mit einer Liste der Schutzkomponenten wird geöffnet. Die Komponente Schutz vor Datensammlung ist standardmäßig aktiviert.
4. Wählen Sie rechts im Fenster die Komponente **Schutz vor Datensammlung** aus.

   Das Fenster **Einstellungen für den Schutz vor Datensammlung** wird geöffnet.
5. Wählen Sie die Variante **Erkannte Anfragen blockieren** aus.
6. Wechseln Sie mit dem Link **Kategorien und Ausnahmen** ins Fenster **Kategorien und Ausnahmen**.
7. Aktivieren Sie die Kontrollkästchen für die Kategorien der Tracking-Dienste, die das Programm blockieren soll.

Datensammlung auf bestimmten Websites erlauben

► *Um die Datensammlung auf bestimmten Websites zu erlauben, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Schutz** aus.

   Ein Fenster mit einer Liste der Schutzkomponenten wird geöffnet. Die Komponente Schutz vor Datensammlung ist standardmäßig aktiviert.

4. Wählen Sie rechts im Fenster das Element **Schutz vor Datensammlung** aus.

   Das Fenster **Einstellungen für den Schutz vor Datensammlung** wird geöffnet.

5. Wählen Sie die Variante **Erkannte Anfragen blockieren** aus.

6. Wechseln Sie mit dem Link **Kategorien und Ausnahmen** ins Fenster **Kategorien und Ausnahmen**.

7. Öffnen Sie mit dem Link **Ausnahmen** das Fenster **Ausnahmen für den Schutz vor Datensammlung**.

8. Klicken Sie auf **Hinzufügen**.

9. Geben Sie im folgenden Fenster die Webadresse der Seite an, auf der die Datensammlung erlaubt werden soll, und klicken Sie auf **Hinzufügen**.

   Die angegebene Website wird zur Ausnahmeliste hinzugefügt.

Sie können die Datensammlung auch erlauben, wenn Sie eine bestimmte Website im Browser geöffnet haben (s. Abschnitt "Schutz vor Datensammlung im Browser verwalten" auf S. 100).

Bericht über Anfragen an Tracking-Dienste anzeigen

► *Um einen Bericht über die Anfragen an Tracking-Dienste anzuzeigen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie auf **Mehr Funktionen**, um das Fenster **Tools** zu öffnen.

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

   Das Fenster **Schutz der Privatsphäre** bietet im Abschnitt **Schutz vor Datensammlung** einen Kurzbericht mit Informationen über die Kategorien für Tracking-Dienste und die Anzahl der gesendeten Tracking-Anfragen.

4. Um einen ausführlichen Bericht über erkannte und blockierte Anfragen an Tracking-Dienste einzusehen, klicken Sie im Abschnitt **Schutz vor Datensammlung** auf den Link **Details**, um das Fenster **Detaillierte Berichte** zu öffnen.

Ein Bericht über erkannte Anfragen an Tracking-Dienste ist im Browser einsehbar (s. Abschnitt "Schutz vor Datensammlung im Browser verwalten" auf S. 100).

Schutz vor Datensammlung im Browser verwalten

Sie können die Komponente Schutz vor Datensammlung direkt im Browser verwalten:

- Komponente aktivieren, wenn sie deaktiviert ist
- Statistik der erkannten Anfragen an Tracking-Dienste anzeigen
- zum Konfigurationsfenster für den Schutz vor Datensammlung wechseln
- Informationen darüber anzeigen, welche Kategorien für Tracking-Dienste blockiert werden
- Anzeigen von Informationen über den Modus der Komponente (s. Abschnitt "Über den Schutz vor Datensammlung" auf S. 95) und darüber, ob Tracking-Dienste auf der im Browser geöffneten Website blockiert werden.
- Modus der Komponente ändern, sowie Sperrung von Tracking-Diensten auf der im Browser geöffneten Website erlauben oder verbieten

► *Um im Browser zur Verwaltung für die Komponente Schutz vor Datensammlung zu wechseln,*

klicken Sie in der Symbolleiste des Browsers auf die Schaltfläche **Kaspersky Protection**.

Das folgende Fenster bietet Informationen und Steuerungselemente für die Komponente.

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 101

Anzeige eines Banners auf einer Webseite deaktivieren 102

Anzeige aller Banner auf einer Webseite deaktivieren 102

Komponente Anti-Banner aktivieren

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

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
3. Gehen Sie zum Abschnitt **Schutz**.
4. Wählen Sie rechts im Fenster die Komponente Anti-Banner aus und aktivieren Sie die Komponente mithilfe des Schalters.

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. Klicken Sie unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
3. Gehen Sie zum Abschnitt **Schutz**.

4. Wählen Sie die Komponente Anti-Banner aus.

   Das Fenster **Anti-Banner-Einstellungen** wird geöffnet.

5. Aktivieren Sie die Komponente Anti-Banner mithilfe des Schalters im oberen Fensterbereich.

6. Klicken Sie im Fenster **Anti-Banner-Einstellungen** auf den Link **Verbotene Webadressen anpassen**, um das Fenster **Verbotene Webadressen** zu öffnen.

7. Klicken Sie im Fenster **Verbotene Webadressen** auf **Hinzufügen**.

8. 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*`.

9. Geben Sie für diese Webseite den Status **Aktiv** an.

10. Klicken Sie auf **Hinzufügen**.

Künftig werden Banner auf der Seite http://example.com von Kaspersky Total Security blockiert.

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 vertrauliche Daten 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 unten im Hauptfenster auf die Schaltfläche **Mehr Funktionen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie links im Fenster **Tools** auf den Link **Schutz der Privatsphäre**, um das Fenster **Schutz der Privatsphäre** zu öffnen.
4. Klicken Sie im Fenster **Schutz der Privatsphäre** 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 bietet Aktionen an, mit denen diese Spuren beseitigt werden können (s. Abb. unten).

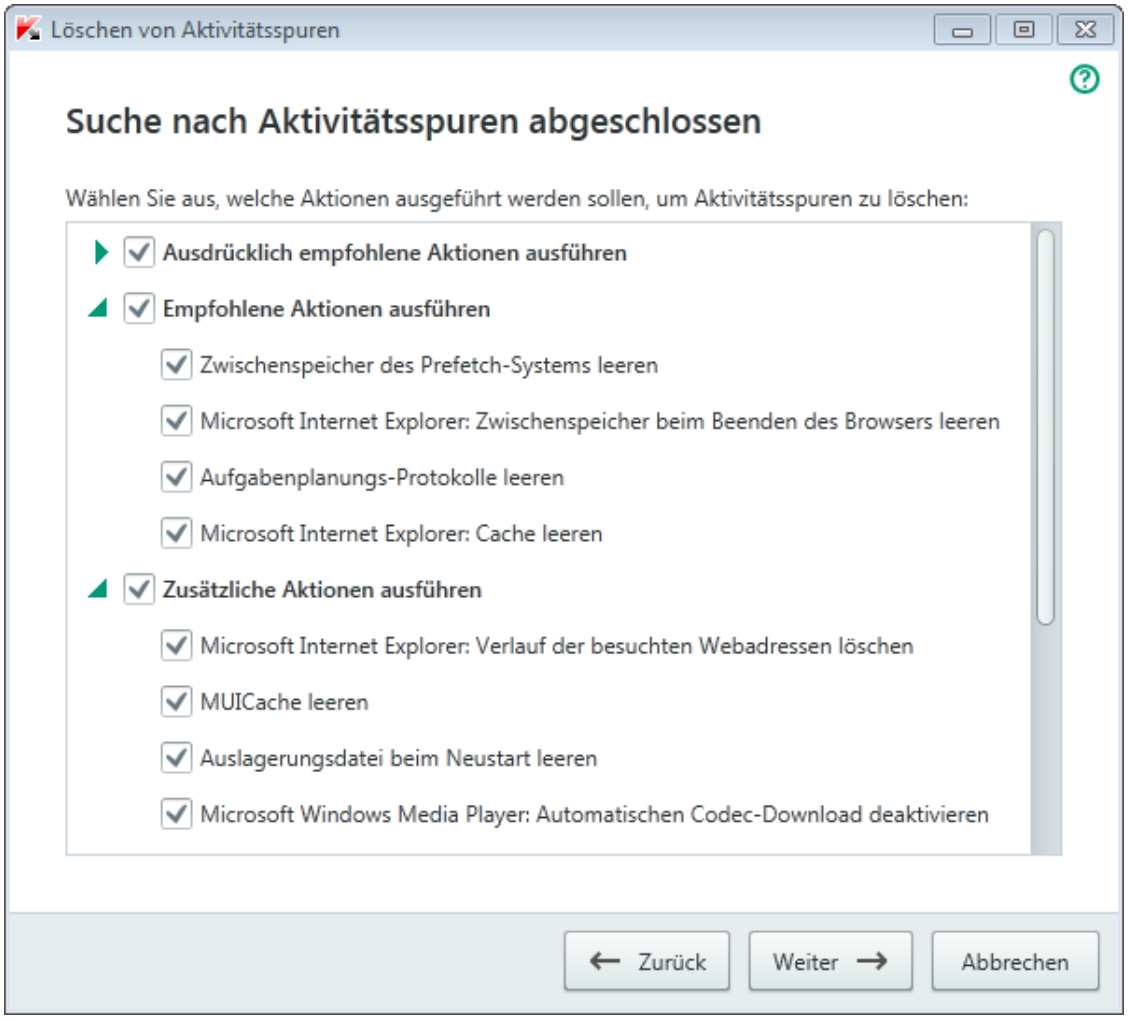

Abbildung 4. Erkannte Aktivitätsspuren und Empfehlungen zu deren Beseitigung

Klicken Sie links vom Namen einer Gruppe auf das Symbol , 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. 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 107

Zu den Einstellungen für die Kindersicherung wechseln 109

Kontrolle über die Verwendung des Computers 110

Kontrolle über die Verwendung des Internets 111

Kontrolle über den Start von Spielen und Programmen 114

Kontrolle über die Kommunikation in sozialen Netzwerken 116

Inhaltskontrolle für Konversationen 117

Bericht über die Aktionen eines Benutzers anzeigen 119

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 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 die Kommunikation in sozialen Netzwerken erlaubt oder verboten ist.
- Kontrolle des Textes von Konversationen in 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 **Kindersicherung**.
3. Falls der Zugriff auf die Einstellungen für die Kindersicherung nicht durch ein Kennwort geschützt ist, bietet Ihnen das Programm an, ein Kennwort festzulegen. Wählen Sie eine der vorgeschlagenen Varianten aus:
   - Wenn Sie den Zugriff auf die Einstellungen für die Kindersicherung durch ein Kennwort schützen möchten, gehen Sie wie folgt vor:
     a. Füllen Sie die Felder **Kennwort** und **Kennwort bestätigen** aus, und klicken Sie auf **Fortsetzen**.
     b. Klicken Sie im Fenster **Gültigkeitsbereich des Kennworts** auf **Kennwort erstellen**.
     c. Geben Sie das Kennwort im Fenster **Kennwort eingeben** erneut ein und klicken Sie auf **Anmelden**.
   - Wenn Sie den Zugriff auf die Einstellungen für die Kindersicherung nicht durch eine Kennwort schützen möchten, wechseln Sie mit dem Link **Überspringen** zu den Einstellungen für die Kindersicherung.

   Das Fenster **Kindersicherung** wird geöffnet.
4. Wählen Sie ein Konto 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 Konfigurationsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 109).

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 blockieren von**.

4. Legen Sie in der Dropdown-Liste neben dem Kontrollkästchen **Zugriff blockieren 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 maximal** 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** 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. Setzen Sie den Schalter, der sich oben im Fenster befindet, auf die Position **Die Kontrolle ist aktiviert**  .

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 Konfigurationsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 109).

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** 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** und wählen Sie in der Dropdown-Liste neben dem Kontrollkästchen eine Zeitbeschränkung aus.

5. Setzen Sie den Schalter, der sich oben im Fenster befindet, auf die Position **Die Kontrolle ist aktiviert**  .

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 Konfigurationsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 109).

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 Webseiten einschränken**.

   b. Wählen Sie die Variante **Zugriff auf Webseiten aus den ausgewählten Kategorien blockieren** aus 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 Webseiten einschränken**.

   b. Öffnen Sie mit dem Link **Ausnahmen anpassen** das Fenster **Ausnahmen**.

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

   Im folgenden Fenster kann eine neue Maske für eine Webadresse hinzugefügt werden.

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

e. Legen Sie im Abschnitt **Geltungsbereich** einen Gültigkeitsbereich 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**. Schließen Sie das Fenster **Ausnahmen**.

6. Setzen Sie den Schalter, der sich oben im Fenster befindet, auf die Position **Die Kontrolle ist aktiviert**  .

Die Kindersicherung richtet sich nach den festgelegten Einstellungen, um den Besuch von Websites zu blockieren.

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

1. Wechseln Sie zum Konfigurationsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 109).

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. Setzen Sie den Schalter, der sich oben im Fenster befindet, auf die Position **Die Kontrolle ist aktiviert**  .

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 IM-Clients) 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 Konfigurationsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 109).

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

3. Um den Start aller Spiele zu sperren, deren Inhalt nicht der Altersgruppe des Benutzers entspricht, aktivieren Sie das Kontrollkästchen **Startbeschränkung für Spiele ab** und wählen Sie in der Dropdown-Liste neben dem Kontrollkästchen eine Altersbeschränkung aus.

4. 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.

5. Kehren Sie zum Abschnitt **Programme** zurück.

6. Setzen Sie den Schalter, der sich oben im Fenster befindet, auf die Position **Die Kontrolle ist aktiviert**  .

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

1. Wechseln Sie zum Konfigurationsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 109).

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

3. Öffnen Sie mit der Schaltfläche **Programm hinzufügen** das Fenster **Öffnen** und wählen Sie eine ausführbare Programmdatei aus.

   Das ausgewählte Programm erscheint in der Liste **Folgende Programme sperren**. Kaspersky Total Security fügt die Anwendung automatisch einer bestimmten Kategorie wie z. B. *Spiele* hinzu.

4. Wenn Sie den Start des Programms blockieren möchten, wählen Sie in der Dropdown-Liste rechts vom Namen des Programms das Element **Blockieren** aus.

5. Wenn Sie den Start aller Programme einer bestimmten Kategorie blockieren möchten, aktivieren Sie in der Liste das Kontrollkästchen neben dem Namen der Kategorie (Sie können beispielsweise die Programmkategorie *Spiele* blockieren).

6. Wenn Sie die Verwendungsdauer des Programms beschränken möchten, wählen Sie in der Dropdown-Liste rechts vom Namen des Programms das Element **Nach Regeln** aus.

   Das Fenster **Verwendung des Programms einschränken** wird geöffnet.

7. Wenn Sie die Verwendungsdauer eines Programms an Werktagen und am Wochenende beschränken möchten, aktivieren Sie in den Abschnitten **Werktage** und **Wochenende** das Kontrollkästchen **Zugriff erlauben für maximal** und geben Sie in der Dropdown-Liste an, für wie viele Stunden der Benutzer das Programm pro Tag verwenden darf. Außerdem können Sie mithilfe der Tabelle **Genaue Nutzungsdauer** exakt festlegen, in welchen Zeiträumen dem Benutzer die Verwendung eines Programms erlaubt bzw. verboten ist.

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

9. Klicken Sie auf **Speichern**.

10. Setzen Sie den Schalter, der sich oben im Fenster befindet, auf die Position **Die Kontrolle ist aktiviert**  .

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 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 Konfigurationsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 109).
2. Wählen Sie im Einstellungsfenster für die Kindersicherung den Abschnitt **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. Öffnen Sie mit dem Link **Bekannte Kontakte** das Fenster **Bericht über Konversationen**.
   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 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.

      Ein Fenster mit einem Verlauf der Konversationen mit diesem Kontakt wird geöffnet.

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

4. Setzen Sie den Schalter, der sich oben im Fenster befindet, auf die Position **Die Kontrolle ist aktiviert**  .

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

Inhaltskontrolle für Konversationen

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

► *Um die Überwachung für das Senden persönlicher Daten anzupassen, gehen Sie wie folgt vor:*

1. Wechseln Sie zum Konfigurationsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 109).

2. Wählen Sie im Konfigurationsfenster für die Kindersicherung den Abschnitt **Inhaltskontrolle** aus.

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 für persönliche Daten ändern** das Fenster **Liste persönlicher Daten**.

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

   Im folgenden Fenster können persönliche Daten hinzugefügt werden.

6. Wählen Sie mit dem entsprechenden Link den Typ der persönlichen Daten aus (beispielsweise "Telefonnummer") oder geben Sie im Feld **Feldname** eine Beschreibung 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. Schließen Sie das Fenster **Liste persönlicher Daten**.

10. Setzen Sie den Schalter, der sich oben im Fenster befindet, auf die Position **Die Kontrolle ist aktiviert**  .

Die Kindersicherung überwacht und sperrt die Verwendung der angegebenen persönlichen Daten in Online-Konversationen.

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

1. Wechseln Sie zum Konfigurationsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 109).

2. Wählen Sie im Konfigurationsfenster für die Kindersicherung den Abschnitt **Inhaltskontrolle** aus.

3. Aktivieren Sie unter **Verwendung von Schlüsselwörtern kontrollieren** das Kontrollkästchen **Verwendung von Schlüsselwörtern erkennen**.

4. Öffnen Sie mit dem Link **Liste für Schlüsselwörter ändern** das Fenster **Liste für Schlüsselwörter**.

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 **Liste für Schlüsselwörter**.

7. Schließen Sie das Fenster **Liste für Schlüsselwörter**.

8. Setzen Sie den Schalter, der sich oben im Fenster befindet, auf die Position **Die Kontrolle ist aktiviert**  .

Die Kindersicherung erkennt bei Online-Konversationen Nachrichten, die eine festgelegte Schlüsselphrase enthalten, und protokolliert Informationen über solche Nachrichten.

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 Konfigurationsfenster für die Kindersicherung (s. Abschnitt "Zu den Einstellungen für die Kindersicherung wechseln" auf S. 109).

2. Wählen Sie ein Benutzerkonto aus und klicken Sie auf den Link **Bericht anzeigen**, um ins Berichtsfenster zu wechseln.

3. Öffnen Sie im Abschnitt für die erforderliche Einschränkungsart (z. B. **Internet** oder **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 120

Über das Benutzerkonto im Portal My Kaspersky 121

Zur Fernverwaltung des Computerschutzes wechseln 122

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.

Wenn die Liste für gefundene Objekte im Portal My Kaspersky mehr als 10 Elemente enthält, werden die Elemente in Gruppen angeordnet. In diesem Fall können die gefundenen Objekte über das Portal nur gemeinsam verarbeitet werden. Es ist nicht möglich, die Objekte einzeln anzuzeigen. Um einzelne Objekte anzuzeigen, kann das auf dem Computer installierte Programm verwendet werden.

Ausführliche Informationen zur Funktionsweise des Portals bietet die Hilfe für das Portal My Kaspersky https://help.kaspersky.com/KPC/1.0/de-DE/index.htm.

Über das Benutzerkonto im Portal My Kaspersky

Ein *Benutzerkonto beim Portal My Kaspersky* ist erforderlich für die Anmeldung im Portal My Kaspersky https://center.kaspersky.com/de und für die Nutzung des Portals und bestimmter Kaspersky-Lab-Programme.

Falls Sie noch kein Konto im Portal My Kaspersky besitzen, können Sie es im Portal oder von einem Programm aus erstellen, das mit dem Portal kompatibel ist. Zur Anmeldung im Portal können Sie auch die Anmeldedaten von anderen Kaspersky-Lab-Ressourcen verwenden.

Um im Portal My Kaspersky ein Benutzerkonto zu erstellen, müssen Sie eine gültige E-Mail-Adresse angeben und ein Kennwort festlegen. Das Kennwort muss mindestens 8 Zeichen lang sein und muss mindestens eine Ziffer, einen lateinischen Klein- und Großbuchstaben enthalten. Leerzeichen sind nicht zulässig.

> Falls das eingegebene Kennwort zu einfach oder leicht zu erraten ist, wird kein Konto erstellt.

Wenn Sie ein Benutzerkonto erstellen, können Sie eine Geheimfrage festlegen. Diese Frage bietet zusätzliche Sicherheit, wenn Sie ein vergessenes Kennwort wiederherstellen müssen.

Nachdem Sie ein Benutzerkonto erstellt haben, wird an die angegebene E-Mail-Adresse eine Nachricht geschickt. Diese enthält einen Link für die Aktivierung Ihres Kontos.

Aktivieren Sie Ihr Benutzerkonto innerhalb von 7 Tagen mit dem Link aus der E-Mail-Nachricht. Andernfalls wird das Konto gelöscht.

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 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.

   > Es kann vorkommen, dass aufgrund einer Störung im Portal keine Verbindung zum Portal My Kaspersky besteht. In diesem Fall meldet Kaspersky Total Security, dass im Portal My Kaspersky Probleme vorliegen, die von den Kaspersky Labs Experten behoben werden. Sollte aufgrund einer Störung keine Verbindung mit dem Portal My Kaspersky möglich sein, so wiederholen Sie den Verbindungsversuch später.

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 unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
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 125

Kontrolle der Aktionen eines Programms auf dem Computer und im Netzwerk 127

Einstellungen für die Programmkontrolle anpassen 129

Zugriff von Programmen auf die Webcam 130

Einstellungen für den Zugriff von Programmen auf die Webcam anpassen 132

Zugriff eines Programms auf die Webcam erlauben 132

Über den Zugriff von Programmen auf Tonaufnahmegeräte 133

Einstellungen für den Zugriff eines Programms auf Tonaufnahmegeräte anpassen 135

Über die Überwachung von Änderungen im Betriebssystem 136

Einstellungen für die Überwachung von Änderungen im Betriebssystem anpassen 137

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 in KSN ansehen** aus (s. Abb. unten).

Abbildung 5. Kontextmenü des Objekts

Ein Fenster mit Angaben zur Reputation des Programms in Kaspersky Security Network wird geöffnet.

Siehe auch

Teilnahme an Kaspersky Security Network 170

Kontrolle der Aktionen eines Programms auf dem Computer und im Netzwerk

Die Komponente Programmkontrolle verhindert, dass Programme Aktionen ausführen, 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 verwendet.

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 Hauptfenster von Kaspersky Total Security.
2. Klicken Sie unten im Hauptfenster auf **Mehr Funktionen**.

   Das Fenster **Tools** wird geöffnet.
3. Wählen Sie den Abschnitt **Programmkontrolle** aus.

   Das Fenster **Programmkontrolle** wird geöffnet.
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**.
6. 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. Klicken Sie in der Spalte mit den für die Ressourcen möglichen Aktionen (**Lesen**, **Schreiben**, **Löschen** oder **Erstellen**) auf das Symbol und wählen Sie im Menü den entsprechenden Wert aus (**Erlauben**, **Verbieten**, **Aktion erfragen** oder **Erben**).
7. 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. Klicken Sie in der Spalte **Aktion** auf das Symbol und wählen Sie im folgenden Menü den entsprechenden Wert aus (**Erlauben**, **Verbieten**, **Aktion erfragen** oder **Erben**).

8. 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. Markieren Sie dazu die Regel und verschieben Sie sie in der Liste nach oben oder unten.

9. Damit bestimmte Aktionen des Programms nicht von der Programmkontrolle untersucht werden, aktivieren Sie auf der Registerkarte **Ausnahmen** die Kontrollkästchen für die Aktionen, die nicht überwacht werden sollen.

10. Klicken Sie auf **Speichern**.

    Alle Ausnahmen, die in den Regeln für die Programmkontrolle erstellt wurden, stehen im Konfigurationsfenster von Kaspersky Total Security im Abschnitt **Gefahren und Ausnahmen** zur Verfügung.

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

Zugriff von Programmen auf die Webcam

Betrüger können mithilfe spezieller Programme versuchen, 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 Sicherheitsgruppen "Stark beschränkt" oder "Nicht vertrauenswürdig" gehören, blockiert Kaspersky Total Security standardmäßig den Zugriff auf die Webcam.

Im Konfigurationsfenster der Programmkontrolle können Sie den Zugriff auf die Webcam für Programme erlauben (s. Abschnitt "Zugriff eines Programms auf die Webcam erlauben" auf S. 132), 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. 132). Diese Meldung wird nicht angezeigt, wenn auf Ihrem Computer bereits Programme im Vollbildmodus laufen.

In der Dropdown-Liste der Benachrichtigung über den Videodatenempfang können Sie außerdem die Benachrichtigungsanzeige deaktivieren oder zu den Einstellungen für die Benachrichtigungsanzeige wechseln (s. Abschnitt "Einstellungen für den Zugriff von Programmen auf die Webcam anpassen" auf S. 132).

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.
- Das Programm überwacht Audiosignale, wenn diese zu einem Videostream der Webcam gehören.
- 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.

Über den Link (http://support.kaspersky.com/de/12004) 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 Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie im Abschnitt **Schutz** im rechten Fensterbereich **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 auf der Registerkarte **Schutz** im Fenster **Einstellungen** die Überwachung für den Webcam-Zugriff mithilfe des Schalters.

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 auf **Mehr Funktionen**.

   Das Fenster **Tools** wird geöffnet.

3. Klicken Sie im Fenster **Tools** unter **Programmkontrolle** auf **Details**.

   Das Fenster **Programmkontrolle** wird geöffnet.

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 den Rechtekategorien den Punkt **Änderung des Betriebssystems** → **Verdächtige Veränderungen im Betriebssystem** → **Zugriff auf Webcam** aus.

8. Klicken Sie auf das Symbol in der Spalte **Aktion** und wählen Sie im folgenden Menü den Punkt **Erlauben** aus.

9. Klicken Sie auf **Speichern**.

Der Zugriff des Programms auf die Webcam wird erlaubt.

Über den Zugriff von Programmen auf Tonaufnahmegeräte

Betrüger können mithilfe spezieller Programme versuchen, unberechtigten Zugriff auf Tonaufnahmegeräte zu erlangen. *Tonaufnahmegeräte* sind Mikrofone, die mit dem Computer verbunden oder in den Computer integriert sind, und über die Schnittstelle der Soundkarte ("Input") einen Audiodatenstrom übertragen können. Kaspersky Total Security überwacht den Zugriff von Programmen auf Tonaufnahmegeräte und schützt vor unbefugten Abfangversuchen von Audiosignalen.

Kaspersky Total Security verbietet Programmen aus den Sicherheitsgruppen "Nicht vertrauenswürdig" und "Stark beschränkt" standardmäßig den Empfang von Audiosignalen, die von mit dem Computer verbundenen Tonaufnahmegeräten stammen. Sie können den Zugriff auf Tonaufnahmegeräte manuell erlauben (s. Abschnitt "Einstellungen für den Zugriff eines Programms auf Tonaufnahmegeräte anpassen" auf S. 135).

Wenn ein Programm aus der Sicherheitsgruppe "Schwach beschränkt" auf ein Tonaufnahmegerät zugreift, zeigt Kaspersky Total Security eine Benachrichtigung an und fragt Sie, ob diesem Programm der Zugriff auf das Tonaufnahmegerät erlaubt oder verboten werden soll. Wenn Kaspersky Total Security diese Benachrichtigung nicht anzeigen kann (z. B. weil die grafische Benutzeroberfläche von Kaspersky Total Security nicht geladen ist), wird dem Programm aus der Sicherheitsgruppe "Schwach beschränkt" der Zugriff auf das Tonaufnahmegerät erlaubt.

Für alle Programme, die zur Sicherheitsgruppe "Vertrauenswürdig" gehören, ist der Zugriff auf Tonaufnahmegeräte standardmäßig erlaubt.

Die Funktionalität für den Schutz des Zugriffs von Programmen auf Tonaufnahmegeräte besitzt folgende Besonderheiten:

- Damit die Funktionalität verfügbar ist, muss die Komponente Programmkontrolle aktiviert sein.
- Wenn ein Programm bereits begonnen hat, ein Audiosignal zu empfangen, bevor die Komponente Programmkontrolle gestartet wurde, erlaubt Kaspersky Total Security dem Programm den Empfang des Audiosignals und zeigt keine Benachrichtigungen an.
- Wenn die Einstellungen für den Zugriff eines Programms auf Tonaufnahmegeräte geändert werden (Beispiel: Einem Programm wurde im Konfigurationsfenster der Programmkontrolle verboten, Audiosignale zu empfangen), muss dieses Programm neu gestartet werden, damit es keine Audiosignale mehr empfängt.
- Die Überwachung des Zugriffs auf Tonaufnahmegeräte ist von den Einstellungen für den Webcam-Schutz unabhängig.
- Wenn die grafische Programmoberfläche noch nicht geladen ist, wird Programmen, für welche die Variante "Aktion erfragen" festgelegt ist, der Empfang von Audiosignalen erlaubt.
- Kaspersky Total Security schützt nur den Zugriff auf integrierte und externe Mikrofone. Andere Tonübertragungsgeräte werden nicht unterstützt.

Für Audiosignale, die von Geräten wie DSLR-Kameras, tragbaren Videokameras und Action-Cams übertragen werden, kann das Programm keinen Schutz garantieren.

Einstellungen für den Zugriff eines Programms auf Tonaufnahmegeräte anpassen

► *Um die Einstellungen für den Zugriff eines Programms auf Tonaufnahmegeräte anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Hauptfenster auf **Mehr Funktionen**.

   Das Fenster **Tools** wird geöffnet.
3. Wählen Sie den Abschnitt **Programmkontrolle** aus.

   Das Fenster **Programmkontrolle** wird geöffnet.
4. Öffnen Sie mit dem Link **Programme verwalten** das Fenster **Programme verwalten**.
5. Wählen Sie in der Liste das Programm aus, dem Sie den Zugriff auf Tonaufnahmegeräte gewähren möchten, und öffnen Sie durch Doppelklick das Fenster **Regeln für das Programm**.
6. Wechseln Sie im Fenster **Regeln für das Programm** auf die Registerkarte **Rechte**.
7. Wählen Sie in der Liste mit den Rechtekategorien den Punkt **Änderung des Betriebssystems** → **Verdächtige Veränderungen im Betriebssystem** → **Zugriff auf Tonaufnahmegeräte** aus.
8. Klicken Sie in der Spalte **Aktion** auf das entsprechende Symbol und wählen Sie einen Menüpunkt aus:
   - Um einem Programm den Empfang von Audiosignalen zu erlauben, wählen Sie **Erlauben** aus.
   - Um einem Programm den Zugriff auf Audiosignale zu verbieten, wählen Sie **Verbieten** aus.
9. Damit Sie benachrichtigt werden, wenn einem Programm der Zugriff auf ein Audiosignal verboten oder erlaubt wurde, klicken Sie in der Spalte **Aktion** auf das Symbol und wählen Sie **Protokollieren** aus.
10. Klicken Sie auf **Speichern**.

Über die Überwachung von Änderungen im Betriebssystem

Kaspersky Total Security kontrolliert mithilfe der Komponente Überwachung von Änderungen im Betriebssystem folgende Änderungen im Betriebssystem:

- Änderung der Startseite in einem Browser
- Änderung der Suchmaschine in einem Browser
- Installation von Plug-ins, Erweiterungen und Symbolleisten in einem Browser
- Änderung des Standardbrowsers
- Änderung der Proxyserver-Einstellungen

Die hier genannte Auswahl der überwachten Änderungen gilt als minimal und wird von den Kaspersky Lab-Spezialisten garantiert. Die Auswahl der überwachten Änderungen kann beim Update der Datenbanken und Programm-Module erweitert werden.

Wenn ein Programm versucht, den Standardbrowser für das http-, ftp- oder https-Protokoll zu ändern und Sie diese Änderung im Benachrichtigungsfenster zulassen, so erlaubt Kaspersky Total Security diesem Programm künftig automatisch und ohne Benachrichtigung, den Standardbrowser für die übrigen zwei Protokolle zu ändern.

Kaspersky Total Security überwacht Änderungen des Betriebssystems nicht und zeigt keine Benachrichtigung an, wenn folgende Programme eine Änderung im Betriebssystem vornehmen:

- Browser
- standardmäßiges Tool, das zum Ändern von Browser-Einstellungen dient.
- standardmäßiges Tool des Betriebssystems, das zum Ändern von zu überwachenden Einstellungen dient, wie z. B. explorer.exe.
- Programm, das nicht mit Kaspersky Total Security kompatibel ist, falls die Überwachung oder das Verwerfen von Änderungen, die dieses Programm ausgeführt hat, darin zu Fehlern führt.
- Installationsassistent für die neue Version von Kaspersky Total Security

- Programm, das die gleichen Funktionen ausführt, wie die Komponente Überwachung von Änderungen im Betriebssystem (z. B. Browser-Manager von Yandex).
- Programme im neuen Windows-Design

Einstellungen für die Überwachung von Änderungen im Betriebssystem anpassen

► *Um die Einstellungen für Änderungen im Betriebssystem anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Programmfenster auf die Schaltfläche  .

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie links im Fenster **Einstellungen** den Abschnitt **Schutz** aus.
4. Wechseln Sie mit dem Link **Überwachung von Änderungen im Betriebssystem** in das Fenster **Änderungen im Betriebssystem**.
5. Aktivieren Sie den Schalter **Überwachung von Änderungen im Betriebssystem**, damit die Änderungen wirksam werden und die Schutzkomponente Überwachung von Änderungen im Betriebssystem ihre Arbeit aufnimmt.
6. Aktivieren Sie das Kontrollkästchen **Installationswächter verwenden**, um bei der Installation neuer Programme die Installation zusätzlicher Software zu verbieten.

   Wenn das Kontrollkästchen **Installationswächter verwenden** deaktiviert wurde, nachdem Sie die Installation eines Programms bereits gestartet hatten, so läuft der Installationswächter im Rahmen der aktuellen Installation weiter. Die Kontrollkästchen für Programme, deren Installation zusätzlich angeboten wird, werden deaktiviert, und es werden keine zusätzlichen Programme installiert. Bei der nächsten Installation von Programmen wird diese Funktionalität nicht verwendet. Zusätzliche Programme werden dann zusammen mit dem eigentlichen Programm installiert.

Die Funktionalität des Installationsratgebers ist für die Installation von 64-Bit-Programmen auf Microsoft Windows XP (x64) nicht verfügbar. Es kann sein, dass die Funktionalität des Installationsratgebers in bestimmten Installationsprogrammen nicht verfügbar ist.

7. Aktivieren Sie das Kontrollkästchen **Werbenachrichten blockieren**, um die Anzeige von Installationsschritten, die Werbung enthalten, zu verbieten, während neue Programme auf dem Computer installiert werden.

8. Aktivieren Sie das Kontrollkästchen **Änderungen überwachen**, damit Kaspersky Total Security die Einstellungen für das Betriebssystem und die Browser sowie Netzwerkeinstellungen überwacht.

9. Aktivieren Sie das Kontrollkästchen **Änderungen automatisch verbieten**, damit Kaspersky Total Security eine Änderung aller zu überwachenden Betriebssystemeinstellungen automatisch verbietet, ohne darüber zu benachrichtigen.

Modus für vertrauenswürdige Programme

Dieser Abschnitt enthält Informationen über den Modus für vertrauenswürdige Programme.

In diesem Abschnitt

Über den Modus für vertrauenswürdige Programme 139

Modus für vertrauenswürdige Programme aktivieren 141

Modus für vertrauenswürdige Programme deaktivieren 143

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, so steht dieser Modus möglicherweise nach dem Update der Datenbanken und Programm-Modulen zur Verfügung (s. Abschnitt "Update der Datenbanken und Programm-Module" auf S. 60). Nach dem Update der Datenbanken und Programm-Module können sich die Einstellungen für den Start von unbekannten Programmen und Modulen ändern.

Der Modus für vertrauenswürdige Programme kann automatisch oder manuell aktiviert werden. Wenn der Modus für vertrauenswürdige Programme manuell aktiviert wird, werden alle bereits auf Ihrem Computer installierten Programme als vertrauenswürdig eingestuft. Programme, die installiert werden, nachdem der Modus für vertrauenswürdige Programme aktiviert wurde, werden nicht als vertrauenswürdig eingestuft. Sie werden nach den allgemeinen Regeln der Programmkontrolle bearbeitet.

Sie können den Modus für vertrauenswürdige Programme auch manuell aktivieren, nachdem Kaspersky Total Security das Betriebssystem und die installierten Programme analysiert hat. Wenn Kaspersky Total Security bei der Analyse festgestellt hat, dass unbekannte Programme auf dem Computer installiert sind, wird davon abgeraten, den Modus für vertrauenswürdige Programme zu aktivieren.

Der Modus für vertrauenswürdige Programme wird automatisch aktiviert, wenn Kaspersky Total Security bei der Analyse des Betriebssystems und der installierten Programme festgestellt hat, dass auf dem Computer überwiegend vertrauenswürdige Programme verwendet werden.

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. 127), während Sie mit diesen Programmen arbeiten, und anschließend den Modus für vertrauenswürdige Programme aktivieren.

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 unten im Hauptfenster auf **Mehr Funktionen**.

   Das Fenster **Tools** wird geöffnet.
3. Klicken Sie links im Fenster **Tools** in der Tools-Liste auf den Link **Modus für vertrauenswürdige Programme**, um das Fenster **Modus für vertrauenswürdige Programme** zu öffnen.
4. Es bestehen folgende Varianten, um den Modus für vertrauenswürdige Programme zu aktivieren:

   - Klicken Sie im Fenster **Modus für vertrauenswürdige Programme** auf **Aktivieren**.

     Der Modus für vertrauenswürdige Programme wird gestartet. Bei Auswahl dieser Variante erlaubt Kaspersky Total Security den Start von Programmen, die auf Ihrem Computer installiert wurden, bevor der Modus für vertrauenswürdige Programme gestartet wurde.
   - Klicken Sie auf den Link **Aktivieren und alle installierten Programme untersuchen**. Dadurch wird eine Analyse des Betriebssystems gestartet und anschließend der Modus für vertrauenswürdige Programme aktiviert.

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.

a. Warten Sie, bis die Analyse des Betriebssystems und der installierten Programme abgeschlossen wird. Sie können das Fenster **Installierte Programme analysieren** ausblenden.

b. Im Fenster **Modus für vertrauenswürdige Programme** können Sie Informationen über die Analyseergebnisse einsehen.

   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.

   Nach Abschluss der Analyse sind im Fenster **Modus für vertrauenswürdige Programme** Informationen über nicht vertrauenswürdige Systemdateien einsehbar. Wenn der Modus für vertrauenswürdige Programme aktiviert wird, werden diese Dateien und Programme blockiert.

c. Um den Start von nicht vertrauenswürdigen Programmen und Systemdateien zu erlauben, setzen Sie im Fenster **Modus für vertrauenswürdige Programme** den Schalter in der Spalte **Start** neben dem nicht vertrauenswürdigen Programm oder der Systemdatei auf **Erlaubt**.

d. Klicken Sie auf **Modus für vertrauenswürdige Programme aktivieren**.

Der Modus für vertrauenswürdige Programme wird aktiviert. Kaspersky Total Security sperrt den Start aller Programme und Systemdateien, die nicht als vertrauenswürdig gelten. 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 unten im Hauptfenster auf **Mehr Funktionen**.

   Das Fenster **Tools** wird geöffnet.
3. Klicken Sie links im Fenster **Tools** auf den Link **Modus für vertrauenswürdige Programme**, um das Fenster **Modus für vertrauenswürdige Programme** zu öffnen.
4. Klicken Sie im Abschnitt **Der 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, Speicherkarten, 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 unten im Hauptfenster auf die Schaltfläche **Mehr Funktionen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie links im Fenster **Tools** auf den Link **Schutz der Privatsphäre**, um das Fenster **Schutz der Privatsphäre** zu öffnen.

4. Öffnen Sie im Fenster **Schutz der Privatsphäre** mit dem Link **Datenvernichtung** das Fenster **Datenvernichtung** (s. Abb. unten).

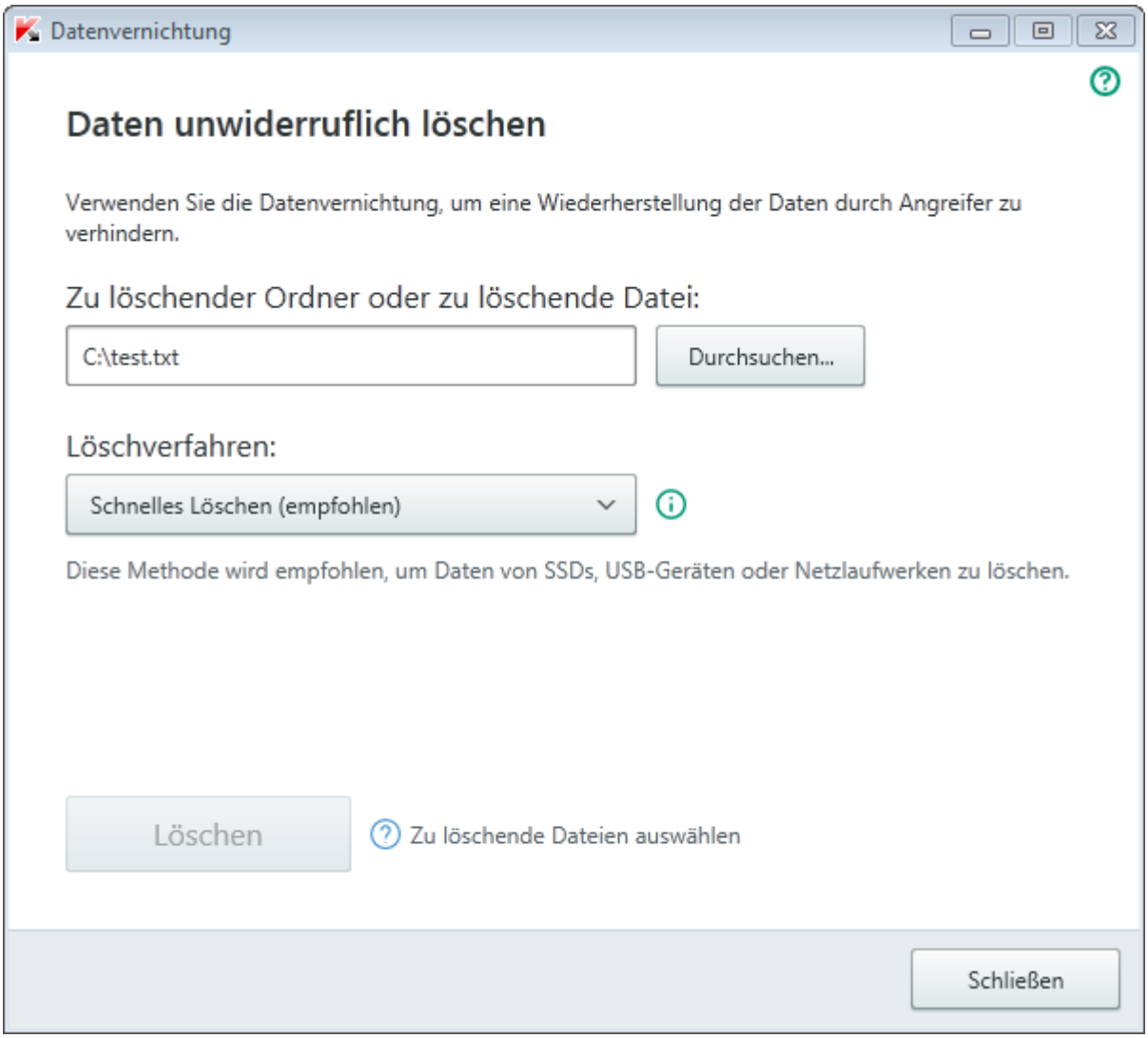

*Abbildung 6. Fenster **Datenvernichtung***

5. 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.

6. 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, Russland** 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.

7. Klicken Sie auf **Löschen**.

8. Klicken Sie im folgenden Fenster auf **Löschen**, um das Löschen zu bestätigen. 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 147

Vorgehen zum Löschen von nicht benötigten Daten 148

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 Browserdateien (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.

Vorgehen zum Löschen von nicht benötigten Daten

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

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Hauptfenster auf die Schaltfläche **Mehr Funktionen**, 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**. Der Assistent kann bei einem beliebigen Schritt 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 der Ausführung des Assistenten bestimmte Dateien vom Betriebssystem verwendet werden (beispielsweise die Berichtsdatei von Microsoft Windows oder die Berichtsdatei für Microsoft Office). Um diese Dateien zu löschen, schlägt der Assistent vor, das Betriebssystem 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.....150

Sicherungsaufgabe erstellen.....151

Sicherungsaufgabe starten.....156

Daten aus einer Sicherungskopie wiederherstellen.....156

Über den Online-Speicher.....157

Online-Speicher aktivieren.....158

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 Sicherungsaufgabe erstellen (s. Abschnitt "Sicherungsaufgabe erstellen" auf S. 151) und starten (s. Abschnitt "Sicherungsaufgabe starten" auf S. 156). 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. 157).

Sicherungsaufgabe erstellen

► *Um eine Sicherungsaufgabe 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 Sicherungsaufgabe erstellt worden ist.
   - Klicken Sie auf **Sicherungskopien für andere Dateien erstellen**, wenn bereits eine Sicherungsaufgabe vorhanden ist und Sie eine neue erstellen möchten.

   Der Assistent zum Erstellen einer Aufgabe für die 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**. Der Assistent kann bei einem beliebigen Schritt durch Klick auf **Abbrechen** abgebrochen werden.

   Details zu den einzelnen Schritten des Assistenten.

In diesem Abschnitt

Schritt 1. Dateien auswählen 152

Schritt 2. Zu sichernde Ordner auswählen 153

Schritt 3. Zu sichernde Dateitypen auswählen 153

Schritt 4. Sicherungsspeicher auswählen 153

Schritt 5. Sicherungszeitplan erstellen 154

Schritt 6. Kennwort für den Schutz von Sicherungskopien eingeben 155

Schritt 7. Einstellungen für die Sicherungsversionen von Dateien 155

Schritt 8. Name für die Sicherungsaufgabe eingeben 155

Schritt 9. Assistent abschließen 156

Schritt 1. Dateien auswählen

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

- Wählen Sie zur schnellen Konfiguration einen der voreingestellten Dateitypen aus (Dateien aus den Ordnern "Eigene Dateien" und "Desktop", Fotos und Bilder, Filme und Videos, Musikdateien). Wenn diese Variante bestätigt wird, geht der Assistent sofort zu Schritt 4. "Sicherungsspeicher auswählen".

  > Kaspersky Total Security erstellt keine Sicherungskopien für Dateien, die in den Ordnern "Desktop" und "Eigene Dateien" gespeichert sind, falls sich diese Ordner auf einem Netzlaufwerk befinden.

- Wählen Sie die Variante **Dateien aus den angegebenen Ordnern sichern** aus, um die zu sichernden Ordner manuell anzugeben.

Schritt 2. 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 im folgenden Fenster **Zu sichernden Ordner auswählen** einen Ordner aus oder ziehen Sie einen Ordner in das Programmfenster.

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

Schritt 3. Zu sichernde Dateitypen auswählen

Wenn Sie beim vorhergehenden Schritt des Assistenten das Kontrollkästchen **Zu sichernde Dateitypen angeben** aktiviert haben, aktivieren Sie beim nächsten Schritt des Assistenten die Kontrollkästchen für die zu sichernden Dateitypen.

Schritt 4. Sicherungsspeicher auswählen

Wählen Sie nun einen Sicherungsspeicher aus:

- **Online-Speicher**. Wählen Sie diese Variante aus, wenn Sie die Sicherungskopien in einem Online-Speicher bei Dropbox ablegen möchten. Der Online-Speicher muss aktiviert werden, bevor er verwendet werden kann (s. Abschnitt "Online-Speicher aktivieren" auf S. 158). Bei der Datensicherung in einem Online-Speicher legt Kaspersky Total Security keine Sicherungskopien für jene Datentypen an, die durch die Dropbox-Nutzungsregeln ausgenommen sind.

- **Lokale Festplatte**. Wenn Sie die Sicherungskopien auf einer lokalen Festplatte ablegen möchten, wählen Sie die entsprechende lokale Festplatte in der Liste aus.

- **Netzlaufwerk** Wenn Sie die Sicherungskopien auf einem Netzlaufwerk ablegen möchten, wählen Sie das entsprechende Netzlaufwerk 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 zu speichernden Sicherungsversionen und die Speicherdauer für Sicherungsversionen.

Schritt 5. Sicherungszeitplan erstellen

Führen Sie bei diesem Schritt eine der folgenden Aktionen aus:

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

Schritt 6. 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.

Schritt 7. Einstellungen für die Sicherungsversionen von Dateien

Dieser Schritt ist verfügbar, wenn Sie bei Schritt 4 "Sicherungsspeicher auswählen" das Kontrollkästchen **Erweiterte Einstellungen für den Speicher verwenden** aktiviert haben.

Passen Sie die Einstellungen für die Dateispeicherung an:

- Aktivieren Sie das Kontrollkästchen **Anzahl der Sicherungsversionen begrenzen** und legen Sie im Feld **Anzahl der zu speichernden Sicherungsversionen** fest, wie viele Sicherungsversionen einer Datei gespeichert werden sollen.
- Aktivieren Sie das Kontrollkästchen **Speicherdauer für Sicherungsversionen begrenzen** und legen Sie im Feld **Speicherdauer für eine Sicherungsversion** fest, wie viele Tage eine Sicherungsversion aufbewahrt werden soll.

Schritt 8. Name für die Sicherungsaufgabe eingeben

Führen Sie bei diesem Schritt folgende Aktionen aus:

- Geben Sie einen Namen für die Sicherungsaufgabe ein.
- Aktivieren Sie das Kontrollkästchen **Datensicherung starten, wenn der Assistent abgeschlossen wird**, damit die Datensicherung automatisch startet, sobald der Assistent abgeschlossen wird.

Schritt 9. Assistent abschließen

Klicken Sie auf **Beenden**.

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

Sicherungsaufgabe starten

► *Um eine Sicherungsaufgabe zu starten, gehen Sie wie folgt vor:*

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

Die Sicherungsaufgabe 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 Sicherungsaufgabe 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. Wenn beim Erstellen der Sicherungskopie ein Kennwort festgelegt wurde, geben Sie dieses Kennwort im Fenster **Kennwort für den Speicher eingeben** ein.
5. Wählen Sie in der Dropdown-Liste **Sicherungszeitpunkt** den Zeitpunkt aus, zu dem die Sicherungskopie erstellt wurde.
6. Aktivieren Sie das Kontrollkästchen für die Ordner, die wiederhergestellt werden sollen.
7. Wenn Sie nur bestimmte Dateitypen wiederherstellen möchten, wählen Sie diese Dateitypen in der Dropdown-Liste **Dateityp** aus.
8. Klicken Sie auf **Ausgewählte Dateien wiederherstellen**.

   Das Fenster **Dateien aus Sicherungskopien wiederherstellen** wird geöffnet.
9. 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.
10. 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.
11. 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 Webdienstes 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 Sicherungsaufgabe erstellt worden ist.
   - Klicken Sie auf **Sicherungskopien für andere Dateien erstellen**, wenn bereits eine Sicherungsaufgabe vorhanden ist.

   Dadurch wird der Assistent für neue Sicherungsaufgaben gestartet (s. Abschnitt "Sicherungsaufgabe erstellen" auf S. 151).
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....160

Dateien in einen Datentresor verschieben....160

Zugriff auf Dateien im Datentresor erhalten....162

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. Wenn Sie 10 Mal hintereinander ein falsches Kennwort eingegeben haben, wird der Zugriff auf den Datentresor für eine Stunde blockiert.

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 mit einer effektiven Schlüssellänge von 56 Bit.

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 Datentresornauf 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**.

    Der Datentresor, den Sie erstellt haben, erscheint in der Liste der Datentresore.

12. Um den Datentresor zu schließen, klicken Sie auf **Schließen**.

    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 **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 mehrere 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 entfernen

► *Um den Zugriff auf Kaspersky Total Security durch ein Kennwort zu schützen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie im linken Fensterbereich den Abschnitt **Allgemein** aus 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 Abschnitt **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. Öffnen Sie im Infobereich der Taskleiste das Kontextmenü des Programmsymbols und wählen Sie den Punkt **Schutz anhalten** aus.

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

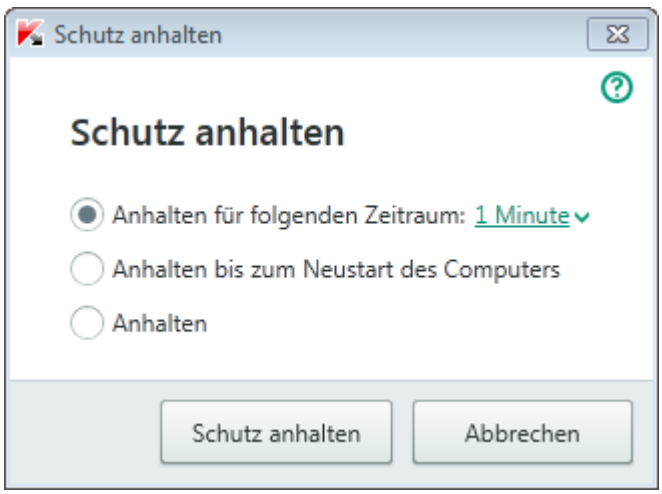

Abbildung 7. Fenster Schutz anhalten

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

   - **Anhalten für folgenden Zeitraum** – Der Schutz wird nach Ablauf des Zeitraums wieder aktiviert, der in der Dropdown-Liste festgelegt wird.
   - **Anhalten bis zum Neustart des Computers** – 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.

3. Klicken Sie auf **Schutz anhalten** und bestätigen Sie diese Aktion im folgenden Fenster.

► *Um den Computerschutz fortzusetzen,*

öffnen Sie im Infobereich der Taskleiste das Kontextmenü des Programmsymbols und klicken Sie auf **Schutz fortsetzen**.

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.

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

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
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

Bei diesem Schritt werden die Programmeinstellungen wiederhergestellt, die von Kaspersky Lab als Standard festgelegt wurden.

Schritt 3. 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 in diesem Zeitraum die Datenbanken und Programm-Module aktualisiert wurden, wie viele Spam-Nachrichten gefunden wurden, u. a.).

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

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Hauptfenster auf die Schaltfläche **Mehr Funktionen**, um das Fenster **Tools** zu öffnen.
3. Wählen Sie im Fenster **Tools** den Abschnitt **Bericht** aus, 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 **Detaillierte Berichte** sind in Tabellenform dargestellt. Die Berichtseinträge können auf unterschiedliche Weise gefiltert 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 mit 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. Klicken Sie unten im Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
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. Klicken Sie unten im Fenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
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

Um Ihren Computer effektiver zu schützen, verwendet Kaspersky Total Security die Cloud-Sicherheit. Die Cloud-Sicherheit basiert auf der Infrastruktur von Kaspersky Security Network und nutzt Daten, die von Benutzern aus der ganzen Welt stammen.

Kaspersky Security Network (KSN) ist eine Infrastruktur aus Cloud-Diensten, die Zugriff auf eine laufend aktualisierte Kaspersky-Lab-Wissensdatenbank bietet. Diese Datenbank enthält Informationen über die Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Nutzung von Daten aus 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 an Kaspersky Lab gesendet.

In diesem Abschnitt

Teilnahme an Kaspersky Security Network aktivieren und deaktivieren 171

Verbindung zu Kaspersky Security Network prüfen 172

Teilnahme an Kaspersky Security Network aktivieren und deaktivieren

Die Teilnahme an Kaspersky Security Network ist freiwillig. Die Verwendung von Kaspersky Security Network (KSN) 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 Programmfenster auf die Schaltfläche .

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie unter **Erweitert** den Abschnitt **Zusätzliche Schutz- und Verwaltungs-Tools** aus.

   Dieses Fenster enthält Informationen zu Kaspersky Security Network und Einstellungen für eine Teilnahme an Kaspersky Security Network.
4. Aktivieren oder deaktivieren Sie mithilfe der Schaltflächen **Aktivieren** / **Deaktivieren** die Teilnahme an Kaspersky Security Network:

   - Wenn Sie an Kaspersky Security Network teilnehmen möchten, klicken Sie auf **Aktivieren**.

     Ein Fenster mit dem Text der Vereinbarung zu Kaspersky Security Network wird geöffnet. Wenn Sie der Vereinbarung zustimmen, klicken Sie auf **Akzeptieren**.
   - Wenn Sie nicht an Kaspersky Security Network teilnehmen möchten, klicken Sie auf **Deaktivieren**.

Verbindung zu 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 zu Kaspersky Security Network besteht, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie unten im Hauptfenster auf die Schaltfläche **Mehr Funktionen**, um das Fenster **Tools** zu öffnen.
3. Klicken Sie links im Fenster **Tools** auf den Link **Cloud-Sicherheit**, um das Fenster **Cloud-Sicherheit** zu öffnen.

Im Fenster **Cloud-Sicherheit** wird der Status der Verbindung zu Kaspersky Security Network angezeigt.

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 erforderlichen Voraussetzungen.

In diesem Abschnitt

Wie Sie technischen Kundendienst erhalten 174

Technischer Support am Telefon 175

Technischer Support über das Portal My Kaspersky 175

Informationen für den Technischen Support sammeln 176

Wie Sie technischen Kundendienst erhalten

Wenn Sie in der Programmdokumentation und in den Informationsquellen zum Programm 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

Die Experten des Technischen Supports sind in vielen Ländern telefonisch erreichbar. Informationen darüber, wie und wo Sie in Ihrer Region technische Unterstützung erhalten können, finden Sie auf der Webseite des Technischen Supports von Kaspersky Lab (http://support.kaspersky.com/de/support/contacts).

Bitte beachten Sie die Support-Regeln, bevor Sie sich an den Technischen Support wenden (http://support.kaspersky.com/de/support/rules).

Technischer Support über das Portal My Kaspersky

My Kaspersky (https://my.kaspersky.com/de) ist eine universelle Online-Ressource, auf der Sie den Schutz Ihrer Geräte und die Aktivierungscodes für Ihre Kaspersky-Lab-Programme verwalten können. Außerdem besteht hier Zugriff auf den Technischen Support.

Sie müssen sich registrieren, um auf das Portal My Kaspersky zugreifen zu können. Dafür müssen Sie eine E-Mail-Adresse angeben und ein Kennwort festlegen.

Es bestehen folgende Möglichkeiten, um im Portal My Kaspersky technischen Support zu erhalten:

- E-Mail-Anfragen an den Technischen Support senden
- Mit dem Technischen Support kommunizieren, ohne E-Mails zu verwenden.
- Status Ihrer Anfragen in Echtzeit verfolgen.

Sie können außerdem einen vollständigen Verlauf Ihrer Anfragen an den Technischen Support einsehen.

E-Mail-Anfrage an den Technischen Support

Eine Online-Anfrage an den Technischen Support muss folgende Informationen enthalten:

- Betreff Ihrer Anfrage
- Name und Versionsnummer des Programms;
- Bezeichnung und Versionsnummer des Betriebssystems
- Problembeschreibung

Die Support-Spezialisten beantworten Ihre Frage im Portal My Kaspersky und an die E-Mail-Adresse, die Sie bei der Registrierung angegeben haben.

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 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 177

Dateien mit Daten senden 178

Über die Zusammensetzung und Speicherung von Protokolldateien 179

AVZ-Skript ausführen 180

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. Klicken Sie unten im Fenster auf die Schaltfläche .

   Das Fenster **Support** wird geöffnet.

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

4. Im folgenden Fenster können Sie mit dem Link **Wie ein Bericht über das Betriebssystem erstellt wird** im Browser einen entsprechenden Artikel aus der Wissensdatenbank öffnen.

5. Folgen Sie den Anweisungen aus dem Artikel der Wissensdatenbank.

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 die Nummer der Anfrage (s. Abschnitt "Technischer Support über das Portal My Kaspersky" auf S. 175). 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. Klicken Sie unten im Fenster auf die Schaltfläche .

   Das Fenster **Support** wird geöffnet.

3. Öffnen Sie mit dem Link **Support Tools** das Fenster **Support Tools**.

4. Klicken Sie im folgenden Fenster auf den Link **Bericht an den Technischen Support senden**, um das Fenster **Bericht senden** zu öffnen.

5. Aktivieren Sie die Kontrollkästchen für die Daten, die an den Technischen Support geschickt werden sollen.

6. Tragen Sie die Anfragenummer ein, die Sie vom Technischen Support erhalten haben.

7. Klicken Sie auf **Bericht senden**.

   Die gewählten Dateien werden komprimiert und an den Server des Technischen Supports gesendet.

Falls das Senden der Dateien nicht möglich ist, können Sie die Dateien auf Ihrem Computer speichern und 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. Klicken Sie unten im Fenster auf die Schaltfläche .

   Das Fenster **Support** wird geöffnet.
3. Klicken Sie im folgenden Fenster auf den Link **Support Tools**, um das Fenster **Support Tools** zu öffnen.
4. Klicken Sie im folgenden Fenster auf den Link **Bericht an den Technischen Support senden**, um das Fenster **Bericht senden** zu öffnen.
5. Wählen Sie den Typ der Daten aus, die auf der Festplatte gespeichert werden sollen:
   - **Informationen zum Betriebssystem**. Aktivieren Sie dieses Kontrollkästchen, wenn Sie Informationen zum Betriebssystem Ihres Computers auf der Festplatte speichern möchten.
   - **Für die Analyse ermittelte Daten**. Aktivieren Sie dieses Kontrollkästchen, wenn Sie Protokolldateien für das Programm speichern möchten. Öffnen Sie mit dem Link **<Anzahl der Dateien>, <Datenmenge>** das Fenster **Für die Analyse ermittelte Daten**. Aktivieren Sie die Kontrollkästchen für jene Protokolldateien, die gespeichert werden sollen.
6. Klicken Sie auf den Link **Bericht speichern**, um ein Fenster zum Speichern eines Archivs mit den Dateien zu öffnen.
7. 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 im Klartext auf Ihrem Computer gespeichert und werden nach der Deaktivierung der Protokollierung für sieben Tage aufbewahrt. Nach sieben Tagen werden die Protokolldateien unwiderruflich gelöscht.

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`.

Protokolldateien können vertrauliche Daten enthalten. Sie können den Inhalt einer Protokolldatei mithilfe eines Textverarbeitungsprogramms (z. B. "Notepad") einsehen.

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. Klicken Sie unten im Fenster auf die Schaltfläche  .

   Das Fenster **Support** wird geöffnet.
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**, um das Fenster **Skript ausführen** zu öffnen.
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

Das Programm kann aktualisiert werden, wenn auf Ihrem Computer eine der folgenden Versionen von Kaspersky Total Security installiert ist:

- Kaspersky PURE 2.0
- Kaspersky PURE 3.0
- Kaspersky Total Security 4.0

Ein Upgrade älterer Programmversionen wird nicht unterstützt.

Wenn eine Programmversion entfernt wird, die älter ist als Kaspersky PURE 2.0, so gehen Backup-Kopien von Dateien und Quarantäne-Objekte verloren, da ihr Format nicht unterstützt wird und nicht in das neue Format umgewandelt werden kann. Bei einem Upgrade von Kaspersky PURE 2.0 können die Backup-Kopien für Dateien und die Quarantäne-Objekte in das neue Format umgewandelt werden. Der Backup-Speicher im Format für Kaspersky CRYSTAL 3.0 wird unterstützt und muss nicht in das neue Format umgewandelt werden.

Die Funktion für das Upgrade von Kaspersky Total Security besitzt folgende Einschränkungen:

- Beim Upgrade einer älteren Programmversion von Kaspersky Total Security werden folgende Programmeinstellungen durch standardmäßige Einstellungen ersetzt:
    - Darstellungseinstellungen für Kaspersky Total Security
    - Untersuchungszeitplan
    - Teilnahme an Kaspersky Security Network
    - Schutzstufe für Datei-Anti-Virus
    - Schutzstufe für Mail-Anti-Virus
    - Update-Quellen
    - Liste der vertrauenswürdigen Webadressen

- Einstellungen für die Link-Untersuchung

- Nach dem Upgrade einer Vorgängerversion des Programms wird Kaspersky Total Security automatisch gestartet, auch wenn der automatische Programmstart in den gespeicherten Einstellungen deaktiviert ist. Bei nachfolgenden Neustarts des Betriebssystems wird Kaspersky Total Security nicht automatisch gestartet, wenn der automatische Programmstart in den gespeicherten Einstellungen deaktiviert ist.

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**.

Funktionelle Einschränkungen für die Untersuchung sicherer 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. Browser, 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. Wenn der Server nur das SPDY-Protokoll unterstützt und keine HTTPS-Verbindung aufgebaut werden kann, überwacht das Programm die hergestellte Verbindung nicht.

Das Programm Kaspersky Total Security unterstützt die Verarbeitung von Datenverkehr nicht, der über HTTPS/2 Proxy übertragen wird. Auch Datenverkehr, der über Erweiterungen des HTTP/2-Protokolls übertragen wird, wird vom Programm nicht verarbeitet.

Kaspersky Total Security überwacht nur jene sicheren Verbindungen, die vom Programm entschlüsselt werden können. Sichere Verbindungen, die auf der Ausnahmeliste stehen (Link **Webseiten** im Fenster **Netzwerkeinstellungen**), werden nicht überwacht. Verschlüsselter Datenverkehr wird standardmäßig von folgenden Komponenten untersucht und entschlüsselt:

- Web-Anti-Virus
- Sicherer Zahlungsverkehr
- Link-Untersuchung
- Kindersicherung

Bei Verwendung des Browsers Google Chrome entschlüsselt Kaspersky Total Security den verschlüsselten Datenverkehr, falls die Erweiterung Kaspersky Protection in diesem Browser nicht vorhanden oder deaktiviert ist.

Warnung für die Funktion der Komponente Anti-Spam

Die Funktionalität der Schutzkomponente Anti-Spam kann mithilfe der Konfigurationsdatei für die Komponente Anti-Spam geändert 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 Fraud Prevention 3.5
- Kaspersky Fraud Prevention 4.0
- Kaspersky Fraud Prevention 5.0
- Kaspersky Password Manager 2.0
- Kaspersky Password Manager 5.0
- Kaspersky Password Manager 7.0
- Kaspersky Password Manager 8.0

Besonderheiten bei der Verarbeitung infizierter Dateien durch die Programmkomponenten

Das Programm kann infizierte Dateien standardmäßig löschen, wenn eine Desinfektion nicht möglich ist. 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 Endpoints

Für folgende Komponenten von Kaspersky Total Security sind die Funktionen im Sicheren Browser beschränkt, wenn das Programm gemeinsam mit Kaspersky Fraud Prevention for Endpoints installiert wurde:

- Web-Anti-Virus, außer Anti-Phishing
- Kindersicherung
- Link-Untersuchung
- Anti-Banner

Warnung über eine Änderung der Funktionalität von IM-Anti-Virus und Kindersicherung

Ab Version Kaspersky Total Security 2016 untersucht die Komponente IM-Anti-Virus Nachrichten die mit dem IRC-Protokoll übertragen werden nicht mehr.

Ab Version Kaspersky Total Security 2016 untersucht die Komponente Kindersicherung Nachrichten die über IM-Clients übertragen werden nicht mehr.

Über persönliche Daten, die in Berichtsdateien enthalten sind

Berichtsdateien werden lokal auf Ihrem Computer gespeichert.

Pfad für Berichtsdateien: %allusersprofile%\Kaspersky Lab\AVP16.0.0\Report\Database

Die Berichte befinden sich in folgenden Dateien:

- reports.db
- reports.db-wal
- reports.db-shm (enthält keine persönlichen Daten)

Die Berichtsdateien sind vor unbefugtem Zugriff geschützt, wenn im Programm Kaspersky Total Security der Selbstschutz aktiviert ist. Wenn der Selbstschutz deaktiviert ist, werden die Berichtsdateien nicht geschützt.

Berichtsdateien können persönliche Daten enthalten, die von Schutzkomponenten ermittelt wurden. Zu diesen Komponenten gehören Datei-Anti-Virus, Mail-Anti-Virus, Anti-Spam und Kindersicherung.

Berichtsdateien können folgende persönlichen Daten enthalten:

- IP-Adresse des Endgeräts
- Verlauf der besuchten Websites
- Version des Browsers und des Betriebssystems
- Namen und Pfade von Cookie-Dateien und anderen Dateien
- E-Mail-Adresse, Absender, Betreff, Nachrichtentext, Benutzernamen, Kontaktliste

Funktionale Besonderheiten des Prozesses Autorun

Der Prozess autorun zeichnet seine Arbeitsergebnisse auf. Die Daten werden in einer Textdatei gespeichert. Der Dateiname folgt dem Muster "kl-autorun-<date><time>.log". Um diese Daten einzusehen, öffnen Sie das Fenster **Ausführen** (in Windows XP im **Startmenü**), geben Sie im Feld **Öffnen** den Wert %TEMP% ein und klicken Sie auf **OK**.

In den Protokolldateien werden die Pfade der Installationsdateien gespeichert, die bei der Nutzung von autorun geladen wurden. Die Daten werden gespeichert, während autorun ausgeführt wird, und werden beim Abschluss dieses Prozesses unwiderruflich gelöscht. Die Daten werden nicht versendet.

Einschränkungen für Kaspersky Total Security, wenn auf Microsoft Windows 10 der Modus Device Guard aktiviert ist:

Die Komponente Schutz vor Netzwerkangriffen kann nicht über die Programmoberfläche aktiviert werden.

Folgende Funktionalität ist teilweise einschränkt:

- Suche nach und Schutz vor Rootkits (aufgeschobene Desinfektion von Dateien beim Neustart des Computers, Erkennung von Schadsoftware, die sich in der Systemregistrierung für den Autostart eintragen)
- Heuristische Analyse (Emulation des Startens von verdächtigen Programmen)

Über Einträge im Windows-Ereignisprotokoll zu Ereignissen, die den Lizenzvertrag und Kaspersky Security Network betreffen

Einträge, die sich auf das Akzeptieren oder Ablehnen des Lizenzvertrags sowie auf das Akzeptieren oder Ablehnen der Teilnahme an Kaspersky Security Network beziehen, werden im Windows-Protokoll aufgezeichnet.

Einschränkungen für die Reputationsprüfung lokaler Adressen in Kaspersky Security Network

Links, die auf lokale Ressourcen verweisen, werden in Kaspersky Security Network nicht untersucht.

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, z. B. Aufgabe zur vollständigen Untersuchung oder Update-Aufgabe.

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. Der Bedrohungsgrad wird durch eine heuristische Analyse ermittelt, die auf zweierlei Kriterien beruht:

- Statische Kriterien (beispielsweise Informationen über die ausführbare Programmdatei: Dateigröße, Erstellungsdatum usw.).
- Dynamische Kriterien, die dazu dienen, um die Arbeit des Programms in einer virtuellen Umgebung zu modellieren (Analyse der Aufrufe von Systemfunktionen durch das Programm).

Der Bedrohungsgrad 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 * für eine beliebige Anzahl von beliebigen Zeichen und ? für ein beliebiges Einzelzeichen steht).

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

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.

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 Cloud-Diensten, die Zugriff auf eine ständig aktualisierte Wissensdatenbank von Kaspersky Lab bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Verwendung von Daten aus Kaspersky Security Network wird die Reaktion von Kaspersky Anti-Virus auf Bedrohungen beschleunigt und die Leistungsfähigkeit für bestimmte Komponenten erhöht. Außerdem verringert sich das Risiko von Fehlalarmen.

Kaspersky-Lab-Update-Server

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 implementierten 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 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 Browser. Dieser Modus ist für Finanztransaktionen und Online-Einkäufe vorgesehen. 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 in Kaspersky Security Network, 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 das Programm den Start von Skripts, fängt sie ab und untersucht sie auf Viren. Abhängig von den Untersuchungsergebnissen können Sie die Ausführung eines Skripts verbieten oder erlauben.

Spam

Unerwünschte massenhafte Versendung von E-Mail-Nachrichten, 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 in 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-Update-Servern heruntergeladen.

Update-Paket

Paket mit Dateien für das Update von Datenbanken und Programm-Modulen. Das Kaspersky-Lab-Programm kopiert ein Update-Paket von den Kaspersky-Lab-Update-Servern, 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.

AO Kaspersky Lab

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen, die Computer vor unterschiedlichen Bedrohungstypen schützen. Dazu zählt der Schutz vor Viren und anderer Schadsoftware, Spam, Netzwerk- und Hackerangriffen.

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 Angaben der IDC ist Kaspersky Lab in Russland der beliebteste Hersteller von Computerschutzsystemen für Heimanwender ("IDC Endpoint Tracker 2014").

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern, der in 31 verschiedenen Ländern über insgesamt 34 Niederlassungen verfügt. Das Unternehmen beschäftigt über 3.000 hochspezialisierte Mitarbeiter.

PRODUKTE. Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die Palette der Heimanwender-Produkte umfasst Programme für die Informationssicherheit von Desktops, Laptops, Tablets, Smartphones und anderen mobilen Geräten.

Das Unternehmen bietet Lösungen und Technologien für den Schutz von Workstations und mobilen Endgeräten, Datei- und Webservern, Mail-Gateways und Firewalls an. Im Angebot befinden sich auch spezielle Produkte für den Schutz vor DDoS-Angriffen, für den Schutz von Umgebungen für Automatisierungstechnik und für die Prävention von Finanzbetrug. In Verbindung mit Administrationstools ermöglichen es diese Lösungen, für Unternehmen jeder Größenordnung 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 Hunderttausende neuer Computerbedrohungen und entwickeln Tools, um diese Gefahren zu erkennen und zu desinfizieren. Diese Informationen fließen in die Datenbanken ein, auf welche die Kaspersky-Lab-Programme zurückgreifen.

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 Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu und ZyXEL. 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 erhielt Kaspersky Lab 2014 bei Tests des anerkannten österreichischen Antiviren-Labors AV-Comparatives neben einem anderen Hersteller die meisten Zertifikate "Advanced+" und wurde mit dem Zertifikat "Top Rated" 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 400 Millionen Anwender. Über 270.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Webseite von Kaspersky Lab:	http://www.kaspersky.com/de
Viren-Enzyklopädie:	http://www.viruslist.com/de/
Antiviren-Labor	http://newvirus.kaspersky.com/de (zur Untersuchung verdächtiger Dateien und Webseiten)
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, Chrome, YouTube sind Marken von Google, Inc.

Intel, Celeron, Atom sind in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragene Marken der Intel Corporation.

Internet Explorer, Microsoft, Windows, Bing, 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.

Skype ist eine Marke des Unternehmens Skype.

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

A

Aktivitätsspuren löschen 104

Anti-Spam 74

AO Kaspersky Lab 199

B

Berichte 167

Bildschirmtastatur 76

C

Code

- Aktivierungscode 52

D

Desinfiziertes Objekt 67

Diagnose 59

F

Fernverwaltung des Programms 120

H

Hard- und Softwarevoraussetzungen 25

K

Kaspersky Security Network 170

Keylogger
Schutz für Eingaben über eine Hardwaretastatur 81
Virtuelle Tastatur 76
Kindersicherung 107
Bericht 119
Konversationen 117
soziale Netzwerke 116
Start von Programmen 114
Start von Spielen 114
Verwendung des Computers 110
Verwendung des Internets 111
Kontrolle des Zugriffs auf das Programm 163

L

Link-Untersuchung
Web-Anti-Virus 84
Lizenz
Aktivierungscode 52
Lizenzvertrag 46

M

Mail-Anti-Virus 72
Meldungen 58
Modus für vertrauenswürdige Programme 139
My Kaspersky 175

O

Objekt wiederherstellen 67

Online-Banking 87

P

Profil für Spiele 123
Programm aktivieren 55
- Aktivierungscode 52
- Lizenz 47
- Testversion 33

Programm entfernen 42
Programm installieren 28
Programmdatenbank 60
Programmkontrolle
- Ausnahmen 127
- Rechte für den Zugriff auf Geräte 127
- Regel für ein Programm erstellen 127

Protokollierung
- Hochladen der Protokollierungsergebnisse 178

Q

Quarantäne
- Objekt wiederherstellen 67

S

Schutzstatus 59
Schwachstelle 66
Schwachstellensuche 66
Sichere Programme 139
Sicherheitsanalyse 59

Sicherheitsprobleme 59
Sicherheitsrisiken 59
Sichern und Wiederherstellen 151
Softwarevoraussetzungen 25
Spam 74
Standardparameter wiederherstellen 166
Statistik 167

U

Unbekannte Programme 124
Unerwünschte E-Mails 74
Update 60
Update-Quelle 60

V

Virtuelle Tastatur 76
Vollbildmodus für Programme 123

W

Web-Filter 84
Wiederherstellung nach Infektion 69

Z

Zusätzliche Tools
    Wiederherstellung nach Infektion 68