

Kaspersky PURE

KASPERSKY **pure**

Benutzerhandbuch

PROGRAMMVERSION: 3.0

Sehr geehrter Benutzer!

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

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

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

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

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

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

Redaktionsdatum: 04.12.2012

© 2013 Kaspersky Lab ZAO. Alle Rechte vorbehalten.

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

INHALT

ÜBER DIESES HANDBUCH.....	6
In diesem Handbuch.....	6
Formatierung mit besonderer Bedeutung	7
INFORMATIONSQLLEN ZUM PROGRAMM.....	9
Informationsquellen zur selbstständigen Recherche	9
Diskussion über die Programme von Kaspersky Lab im Webforum	10
Kontaktaufnahme mit der Vertriebsabteilung.....	10
Kontaktaufnahme mit der Abteilung für Lokalisierung und technische Dokumentation	10
KASPERSKY PURE	11
Neuerungen.....	11
Hauptfunktionen des Programms	12
Lieferumfang.....	14
Service für Benutzer	15
Hard- und Softwarevoraussetzungen	15
PROGRAMM INSTALLIEREN UND DEINSTALLIEREN	17
Installation des Programms auf einem Computer.....	17
Schritt 1. Nach neuer Programmversion suchen.....	18
Schritt 2. Beginn der Programminstallation.....	18
Schritt 3. Lizenzvereinbarung anzeigen	18
Schritt 4. Erklärung zur Verwendung von Kaspersky Security Network	18
Schritt 5. Installation.....	18
Schritt 6. Installation abschließen	19
Schritt 7. Programm aktivieren.....	19
Schritt 8. Anmeldung des Benutzers.....	20
Schritt 9. Aktivierung abschließen.....	20
Upgrade einer Vorgängerversion von Kaspersky PURE	20
Schritt 1. Nach neuer Programmversion suchen.....	21
Schritt 2. Beginn der Programminstallation.....	21
Schritt 3. Lizenzvereinbarung anzeigen	21
Schritt 4. Erklärung zur Verwendung von Kaspersky Security Network	22
Schritt 5. Installation.....	22
Schritt 6. Installation abschließen	22
Programm deinstallieren.....	23
Schritt 1. Daten zur erneuten Verwendung speichern.....	23
Schritt 2. Löschen bestätigen.....	24
Schritt 3. Programm deinstallieren Deinstallation abschließen	24
LIZENZIERUNG DES PROGRAMMS.....	25
Über den Lizenzvertrag	25
Über die Lizenz.....	25
Über die Zurverfügungstellung von Daten	26
Über den Aktivierungscode.....	27
LÖSUNGEN FÜR TYPISCHE AUFGABEN	28
Programm aktivieren	29
Lizenz kaufen oder verlängern	30

Mit den Benachrichtigungen des Programms arbeiten	30
Schutzstatus des Computers analysieren und Sicherheitsprobleme beheben	31
Update der Datenbanken und Programm-Module	32
Untersuchung wichtiger Computerbereiche auf Viren	33
Vollständige Untersuchung des Computers auf Viren	33
Virenuntersuchung einer Datei, eines Ordners oder eines anderen Objekts	34
Untersuchung des Computers auf Schwachstellen	35
Ein vom Programm gelöscht oder desinfiziertes Objekt wiederherstellen	35
Betriebssystem nach einer Infektion wiederherstellen	37
Unerwünschte E-Mails (Spam) blockieren	39
E-Mail untersuchen und E-Mail-Anhänge filtern	39
Sicherheit einer Webseite überprüfen	40
Zugriff auf Websites bestimmter Regionen sperren	41
Fernverwaltung für den Schutz des Heimnetzwerks	41
Mit unbekanntem Programmen arbeiten	42
Kontrolle der Aktionen eines Programms auf dem Computer und im Netzwerk	42
Reputation eines Programms überprüfen	44
Persönliche Daten vor Diebstahl schützen	45
Sicherer Zahlungsverkehr	45
Schutz vor Phishing	46
Virtuelle Tastatur verwenden	47
Schutz für die Dateneingabe über eine Hardwaretastatur	49
Schutz für Kennwörter	51
Hinzufügen von Anmeldedaten für die automatische Authentifizierung	51
Kennwort-Generator verwenden	52
Neues Benutzername/Kennwort-Paar hinzufügen	53
Daten verschlüsseln	54
Löschen von nicht benötigten Daten	56
Unwiderrufliches Löschen von Daten	58
Aktivitätsspuren löschen	60
Backup	62
Datensicherung	62
Daten aus einer Sicherheitskopie wiederherstellen	63
Verwendung eines Online-Speichers	64
Kennwortschutz für die Einstellungen von Kaspersky PURE	65
Kindersicherung verwenden	66
Kindersicherung anpassen	67
Bericht über die Aktionen eines Benutzers anzeigen	68
Computerschutz anhalten und fortsetzen	68
Bericht über den Computerschutz anzeigen	69
Standardeinstellungen für das Programm wiederherstellen	70
Import der Programmeinstellungen für Kaspersky PURE auf einen anderen Computer	72
Notfall-CD erstellen und verwenden	73
Notfall-CD erstellen	73
Hochfahren eines Computers mithilfe der Notfall-CD	75
KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT	76
Wie Sie technischen Kundendienst erhalten	76
Technischer Support am Telefon	76

Technischen Support erhalten über Mein Kaspersky Account	77
Bericht über den Systemstatus erstellen und AVZ-Skript verwenden.....	78
Bericht über den Systemzustand erstellen.....	78
Technische Informationen über die Arbeit des Programms sammeln.....	79
Dateien mit Daten senden.....	79
Skript ausführen.....	80
GLOSSAR.....	82
KASPERSKY LAB.....	89
INFORMATIONEN ÜBER DEN CODE VON DRITTHERRSTELLERN	90
MARKENINFORMATIONEN.....	90

ÜBER DIESES HANDBUCH

Dieses Dokument ist das Benutzerhandbuch für Kaspersky PURE.

Um Kaspersky PURE zu bedienen, sollte sich der Benutzer mit der Benutzeroberfläche und den grundlegenden Funktionen des verwendeten Betriebssystems auskennen und die Arbeit mit E-Mails und Internet beherrschen.

Das Handbuch dient folgenden Zwecken:

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

IN DIESEM ABSCHNITT

In diesem Handbuch	6
Formatierung mit besonderer Bedeutung.....	7

IN DIESEM HANDBUCH

Dieses Dokument enthält folgende Abschnitte.

Informationsquellen zum Programm

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

Kaspersky PURE

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

Programm installieren und deinstallieren

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

Lizenzierung des Programms

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

Lösungen für typische Aufgaben

Dieser Abschnitt bietet genaue Anleitungen für die wichtigsten Aufgaben, die der Benutzer mit dem Programm lösen kann.

Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt beschreibt die Kontaktaufnahme mit dem Technischen Support.

Anhänge

Dieser Abschnitt enthält Informationen, die den Haupttext des Dokuments ergänzen.

Glossar

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

Kaspersky Lab ZAO

Dieser Abschnitt enthält Informationen über ZAO Kaspersky Lab.

Informationen über den Code von Drittherstellern

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

Markeninformationen

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

Sachregister

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

FORMATIERUNG MIT BESONDERER BEDEUTUNG

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

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

Tabelle 1. Formatierung mit besonderer Bedeutung

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

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
<p>Das <i>Update</i> ist ...</p> <p>Das Ereignis <i>Die Datenbanken sind veraltet</i> tritt ein.</p>	<p>Folgende Textelemente sind kursiv geschrieben.</p> <ul style="list-style-type: none"> • neue Begriffe • Namen von Statusvarianten und Programmereignissen
<p>Drücken Sie die Taste ENTER.</p> <p>Drücken Sie die Tastenkombination ALT+F4.</p>	<p>Bezeichnungen von Tasten sind halbfett und in Großbuchstaben geschrieben.</p> <p>Tastenbezeichnungen, die durch ein Pluszeichen verbunden sind, bedeuten eine Tastenkombination. Die genannten Tasten müssen gleichzeitig gedrückt werden.</p>
<p>Klicken Sie auf Aktivieren.</p>	<p>Die Namen von Elementen der Programmoberfläche sind halbfett geschrieben (z. B. Eingabefelder, Menüpunkte, Schaltflächen).</p>
<p>➔ <i>Gehen Sie folgendermaßen vor, um den Aufgabenzeitplan anzupassen:</i></p>	<p>Der erste Satz einer Anleitung ist kursiv geschrieben und wird durch einen Pfeil markiert.</p>
<p>Geben Sie in der Befehlszeile den Text <code>help</code> ein.</p> <p>Es erscheint folgende Meldung:</p> <p>Geben Sie das Datum im Format <code>TT:MM:JJ</code> an.</p>	<p>Folgende Textarten werden durch eine spezielle Schriftart hervorgehoben:</p> <ul style="list-style-type: none"> • Text einer Befehlszeile • Text von Nachrichten, die das Programm auf dem Bildschirm anzeigt. • Daten, die vom Benutzer eingegeben werden müssen.
<p><Benutzername></p>	<p>Variable stehen in eckigen Klammern. Eine Variable muss durch einen entsprechenden Wert ersetzt werden. Dabei fallen die eckigen Klammern weg.</p>

INFORMATIONSQLUELLEN ZUM PROGRAMM

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

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

IN DIESEM ABSCHNITT

Informationsquellen zur selbstständigen Recherche	9
Diskussion über die Programme von Kaspersky Lab im Webforum.....	10
Kontaktaufnahme mit der Vertriebsabteilung	10
Kontaktaufnahme mit der Abteilung für Lokalisierung und technische Dokumentation	10

INFORMATIONSQLUELLEN ZUR SELBSTSTÄNDIGEN RECHERCHE

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

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

Wenn Sie keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky Lab (s. Abschnitt "Technischer Support am Telefon" auf S. [76](#)).

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

Seite auf der Webseite von Kaspersky Lab

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

Auf der Seite (<http://www.kaspersky.de/kaspersky-pure>) finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

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

Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

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

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

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

Elektronisches Hilfesystem

Das elektronische Hilfesystem des Programms umfasst verschiedene Hilfedateien.

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

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

Dokumentation

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

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

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

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

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf des Programms sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung über ein Kontaktformular unter <http://www.kaspersky.de/kontakt> zur Verfügung.

Die Beratung kann auf Deutsch oder Englisch erfolgen.

KONTAKTAUFNAHME MIT DER ABTEILUNG FÜR LOKALISIERUNG UND TECHNISCHE DOKUMENTATION

Wenn Sie Fragen zu dieser Programmdokumentation haben, können Sie sich an unsere Abteilung für Handbücher und Hilfesysteme wenden. Sie können uns gerne ein Feedback zu dieser Dokumentation schicken.

KASPERSKY PURE

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

IN DIESEM ABSCHNITT

Neuerungen	11
Hauptfunktionen des Programms.....	12
Lieferumfang	14
Service für Benutzer.....	15
Hard- und Softwarevoraussetzungen.....	15

NEUERUNGEN

Kaspersky PURE verfügt über folgende Neuerungen:

- Die neue Komponente Sicherer Zahlungsverkehr (s. S. [45](#)) bietet Schutz bei der Verwendung von Online-Banking und Zahlungssystemen sowie bei Zahlungsvorgängen in Online-Shops.
- Der Schutz gegen Keylogger wurde verbessert. Keylogger können persönliche Informationen abfangen, die auf Webseiten eingegeben werden.
 - Neu: Schutz für die Dateneingabe über eine Hardwaretastatur (auf S [49](#)).
 - Das Programm fügt in Eingabefeldern für Kennwörter auf Webseiten automatisch eine Schaltfläche zum Start der virtuellen Tastatur hinzu (s. Abschnitt "Virtuelle Tastatur verwenden" auf S. [47](#)).
- Neu: Verwendung eines Online-Speichers (s. Abschnitt "Verwendung eines Online-Speichers" auf S. [64](#)) zum Speichern von Sicherungskopien für Dateien. Durch den Einsatz von Cloud-Technologien wird die Sicherheit bei der Datenspeicherung erhöht und der Datenzugriff vereinfacht.
- Exploit-Schutz ist eine neue Funktion der Komponente Aktivitätsmonitor, die dem Schutz gegen einen Missbrauch von Software-Schwachstellen dient.
- Der Password Manager wurde verbessert. Die Kennwort-Datenbank kann jetzt auf Remoteservern gespeichert werden. Durch die Synchronisierung stehen aktuelle Kennwörter und persönliche Daten auf allen Ihren Notebooks und PCs zur Verfügung, auf denen Kaspersky PURE installiert ist.
- Verbesserungen der Benutzeroberfläche von Kaspersky PURE: Quickinfos mit nützlichen Hinweisen über das Programm wurden hinzugefügt.
- Das Vorgehen für die Programminstallation wurde vereinfacht (s. Abschnitt "Programm installieren und deinstallieren" auf S. [17](#)). Neue Option zur automatischen Installation der neuesten Version von Kaspersky PURE mit den aktuellen Updates für die Programm-Datenbanken.
- Der Umfang der Programm-Datenbanken wurde verringert. Dadurch wird die herunterzuladende Datenmenge reduziert und die Installation von Updates beschleunigt.

- Die heuristische Analyse, die der Untersuchung von Webseiten auf Phishing-Merkmale dient, wurde optimiert.
- Meldungen, die Kindern von der Kindersicherung angezeigt werden, wurden angepasst. Die Genauigkeit der Kindersicherung wurde erhöht: Diese Komponente nutzt jetzt Cloud-Technologien, um Webseiten auf unerwünschte Inhalte zu überprüfen.

HAUPTFUNKTIONEN DES PROGRAMMS

Kaspersky PURE bietet Ihrem Computer einen umfassenden Schutz. Der Schutz umfasst den Schutz des Computers, der Daten und der Benutzer. Des Weiteren bezieht er sich auf die Fernverwaltung der Funktionen von Kaspersky PURE auf Netzwerkcomputern. In Kaspersky PURE sind unterschiedliche Funktionen und Schutzkomponenten für die einzelnen Aufgaben des umfassenden Schutzes verantwortlich.

Computerschutz

Die *Schutzkomponenten* schützen Ihrem Computer vor bekannten und neuen Bedrohungen, Netzwerkangriffen und Betrugsversuchen, Spam und anderen unerwünschten Informationen. 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 eine regelmäßige *Untersuchung* Ihres Computers empfohlen. 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 PURE auf dem neuesten Stand zu halten, ist ein *Update* der Datenbanken und Programm-Module erforderlich, die bei der Arbeit des Programms verwendet werden.

Programme, an deren Sicherheit Sie zweifeln, können in der speziellen *Sicheren Umgebung* gestartet werden.

Einige spezifische Aufgaben, die nicht regelmäßig, sondern nur gelegentlich anfallen, werden mithilfe *zusätzlicher Tools und Assistenten* ausgeführt: Dazu zählen beispielsweise die Konfiguration des Browsers Microsoft® Internet Explorer® oder das Löschen von Aktivitätsspuren des Benutzers im System.

Der Echtzeitschutz Ihres Computers wird durch folgende Schutzkomponenten gewährleistet:

Im Folgenden werden die Schutzkomponenten von Kaspersky PURE 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 PURE fängt jeden Zugriff auf eine Datei ab und untersucht die Datei nach bekannten Viren. 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 im Backup abgelegt oder in der Quarantäne 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 Skripten, die sich auf Webseiten befinden, ab und blockiert sie, falls Sie gefährlich sind. Web-Anti-Virus kontrolliert auch den Web-Datenverkehr und blockiert den gesamten Zugriff auf bekannte gefährliche Webseiten.

IM-Anti-Virus

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

Proaktiver Schutz

Der Proaktive Schutz erlaubt es, ein neues Schadprogramm zu erkennen, bevor es Schaden anrichten kann. Die Arbeit der Komponente basiert auf der Kontrolle und Analyse des Verhaltens aller auf Ihrem Computer installierten Programme. Abhängig von den auszuführenden Aktionen entscheidet Kaspersky PURE, ob ein Programm potenziell gefährlich ist. So ist Ihr Computer nicht nur vor bekannten Viren, sondern auch vor neuen, bisher unbekannt Viren geschützt.

Programmkontrolle

Programmkontrolle registriert die Aktionen, die von Programmen im System ausgeführt werden können, und reguliert in Abhängigkeit von der Gruppe, zu der ein Programm gehört, seine Aktivität. Für jede Gruppe von Programmen ist eine Auswahl von Regeln vorgegeben. Diese Regeln steuern den Zugriff von Programmen auf unterschiedliche Ressourcen des Betriebssystems.

Firewall

Firewall gewährleistet Sicherheit bei der in lokalen Netzwerken und im Internet. Diese Komponente führt die Filterung der gesamten Netzwerkaktivität durch, wozu zwei Arten von Regeln dienen: *Regeln für Programme* und *Paketregeln*.

Netzwerkmonitor

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

Schutz vor Netzwerkangriffen

Der Schutz wird vor Netzwerkangriffen beim Hochfahren des Betriebssystems gestartet und überwacht den eingehenden Datenverkehr auf für Netzwerkangriffe charakteristische Aktivität. Wenn ein Angriffsversuch auf den Computer erkannt wird, blockiert Kaspersky PURE 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 zu den Listen für schädliche und Phishing-Webadressen. Diese Komponente wird in Web-Anti-Virus, Anti-Spam und IM-Anti-Virus integriert.

Anti-Banner

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

Sicherer Zahlungsverkehr

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

Informationsschutz

Die Funktionen Backup, Verschlüsselung und Password Manager schützen die Daten vor Verlust, unbefugtem Zugriff und Diebstahl.

Backup

Es gibt unterschiedliche Gründe für den Verlust oder die Beschädigung von Daten auf einem Computer: beispielsweise eine Vireninfektion, Veränderungen oder das Löschen von Informationen durch andere Benutzer. Um den Verlust wichtiger Daten zu vermeiden, ist eine regelmäßige Datensicherung unerlässlich.

Mit der Backup-Funktion lassen sich auf einem ausgewählten Datenträger in einem speziellen Speicher Sicherungskopien von Daten anlegen. Zu diesem Zweck werden Update-Aufgaben erstellt. Eine Aufgabe kann entweder manuell oder automatisch nach Zeitplan gestartet werden und dient dazu, in einem Speicher Sicherungskopien ausgewählter Dateien anzulegen. Bei Bedarf kann eine gespeicherte Datei in der erforderlichen Version aus einer Sicherungskopie wiederhergestellt werden.

Datenverschlüsselung

Vertrauliche Informationen, die in elektronischer Form gespeichert sind, erfordern einen zusätzlichen Schutz vor unbefugtem Zugriff. Dazu dient die Speicherung der Daten in einem verschlüsselten Container.

Die Datenverschlüsselung erlaubt es, auf einem ausgewählten Datenträger verschlüsselte Spezialcontainer zu erstellen. Diese Container werden im System als virtuelle Wechseldatenträger dargestellt. Für den Zugriff auf die Daten, die in einem verschlüsselten Container gespeichert sind, ist die Eingabe des Kennworts erforderlich.

Password Manager

Der Zugriff auf eine Vielzahl von Diensten und Internetressourcen erfolgt durch die Anmeldung des Benutzers und die Eingabe von Benutzerdaten zum Zweck der Authentifizierung. Aus Sicherheitsgründen wird empfohlen, für die Anmeldung auf unterschiedlichen Websites verschiedene Benutzerkonten zu verwenden und den Benutzernamen sowie das Kennwort nicht aufzuschreiben.

Der Password Manager kann unterschiedliche Arten persönlicher Daten (z. B. Benutzernamen, Kennwörter, Adressen, Telefon- und Kreditkartennummern) in verschlüsselter Form speichern. Der Zugriff auf die Daten wird durch ein einziges Master-Kennwort geschützt. Nach Eingabe des Master-Kennworts ermöglicht Password Manager das automatische Ausfüllen von Feldern unterschiedlicher Authentifizierungsformulare auf Websites. Mit einem Master-Kennwort können Sie alle Benutzerkonten auf Websites verwalten.

Kindersicherung

Die Funktionen der Kindersicherung dienen dazu, Kinder und Jugendliche vor Gefahren zu schützen, die bei der Arbeit am Computer und im Internet bestehen.

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

Verwaltung

Die Sicherheitsverwaltung eines lokalen Netzwerks wird erschwert, weil es aus mehreren Computern besteht. Schwachstellen, die zunächst nur einen Computer betreffen, können schnell das gesamte Netzwerk bedrohen.

Die Verwaltung bietet folgende Funktionen: Netzwerkweite Untersuchungsaufgabe oder Update-Aufgabe starten, Datensicherung verwalten, von einem lokalen Computer aus die Kindersicherung für alle Netzwerkcomputer anpassen. Dadurch lässt sich die Sicherheit für alle Computer, die zu einem lokalen Netzwerk gehören, fernverwalten.

LIEFERUMFANG

Sie können das Programm folgendermaßen kaufen:

- **In einer Box.** Verkauf über unsere Vertriebspartner.
- **Über den Online-Shop.** Verkauf über Online-Shops von Kaspersky Lab (beispielsweise <http://www.kaspersky.com/de/store>, Abschnitt **Online-Shop**) oder die Online-Shops unserer 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 PURE in einem Online-Shop kaufen, kopieren Sie das Programm von der Seite des Online-Shops. Sie erhalten die zur Programmaktivierung erforderlichen Informationen nach Eingang des Rechnungsbetrags per E-Mail.

Ausführliche Informationen zum Kauf und Lieferumfang erhalten Sie bei unserer Vertriebsabteilung unter der Adresse sales@kaspersky.com.

SERVICE FÜR BENUTZER

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

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

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

HARD- UND SOFTWAREVORAUSSETZUNGEN

Um die Funktionsfähigkeit von Kaspersky PURE zu gewährleisten, muss der Computer folgende Voraussetzungen erfüllen:

Allgemeine Anforderungen:

- 700 MB freier Speicherplatz auf der Festplatte
- CD / DVD-ROM-Laufwerk (zur Installation von Kaspersky PURE von einer Installations-CD)
- Maus
- Internetverbindung (für die Aktivierung des Programms und für das Update der Datenbanken und Programm-Module)
- Microsoft Internet Explorer 8.0 oder höher
- Microsoft Windows® Installer 3.0

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 Intel® Pentium® 800 MHz 32-Bit (x86) / 64-Bit (x64) oder höher (oder ein kompatibler Prozessor).
- 512 MB freier Arbeitsspeicher.

Anforderungen für die Betriebssysteme Microsoft Windows Vista® Home Basic (Service Pack 2 oder höher), Microsoft Windows Vista Home Premium (Service Pack 2 oder höher), Microsoft Windows Vista Business (Service Pack 2 oder höher), Microsoft Windows Vista Enterprise (Service Pack 2 oder höher), Microsoft Windows Vista Ultimate (Service Pack 2 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, Windows 8 Enterprise oder höher (x32 und x64):

- Prozessor Intel Pentium 1 GHz 32-Bit (x86) / 64-Bit (x64) oder höher (oder ein kompatibler Prozessor).
- 1 GB freier Arbeitsspeicher für 32-Bit-Betriebssysteme, 2 GB freier Arbeitsspeicher für 64-Bit-Betriebssysteme

Anforderungen für Netbooks:

- Prozessor Intel Atom™ 1,6 GHz (Z520) oder ein kompatibler Prozessor
- 1 GB freier Arbeitsspeicher.
- Grafikkarte Intel GMA950 mit Videospeicher von mindestens 64 MB (oder kompatibel)
- Bildschirmdiagonale mindestens 10.1 Zoll

Für 64-Bit-Versionen der Betriebssysteme wird die Verwendung des Password Managers nicht unterstützt.

PROGRAMM INSTALLIEREN UND DEINSTALLIEREN

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

IN DIESEM ABSCHNITT

Installation des Programms auf einem Computer	17
Upgrade einer Vorgängerversion von Kaspersky PURE	20
Programm deinstallieren	23

INSTALLATION DES PROGRAMMS AUF EINEM COMPUTER

Kaspersky PURE wird auf dem Computer interaktiv mit einem Installationsassistenten 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**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

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

➔ *Um Kaspersky PURE auf Ihrem Computer zu installieren,*

starten Sie auf der Produkt-CD die Installationsdatei (Datei mit der Erweiterung .exe).

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

IN DIESEM ABSCHNITT

Schritt 1. Nach neuer Programmversion suchen	18
Schritt 2. Beginn der Programminstallation	18
Schritt 3. Lizenzvereinbarung anzeigen	18
Schritt 4. Erklärung zur Verwendung von Kaspersky Security Network	18
Schritt 5. Installation	18
Schritt 6. Installation abschließen	19
Schritt 7. Programm aktivieren	19
Schritt 8. Anmeldung des Benutzers	20
Schritt 9. Aktivierung abschließen	20

SCHRITT 1. NACH NEUER PROGRAMMVERSION SUCHEN

Vor der Installation wird geprüft, ob neuere Versionen von Kaspersky PURE auf den Updateservern von Kaspersky Lab vorhanden sind.

Wenn keine neuere Version des Programms auf den Updateservern von Kaspersky Lab gefunden wurde, wird der Installationsassistent für diese Version gestartet.

Wenn auf den Updateservern eine neuere Version von Kaspersky PURE vorgefunden wurde, werden Ihnen Download und Installation vorgeschlagen. Es wird empfohlen, die neue Programmversion zu installieren, da neue Versionen den Schutz Ihres Computers optimieren. Sollten Sie die neuere Version ablehnen, wird der Installationsassistent der laufenden Version gestartet. Sollten Sie die Installation der neueren Version annehmen, werden die Programmdateien auf Ihren Computer kopiert und der Installationsassistent wird automatisch gestartet. Eine weitere Beschreibung zur Installation einer neueren Version finden Sie in der Dokumentation zur entsprechenden Programmversion.

SCHRITT 2. BEGINN DER PROGRAMMINSTALLATION

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

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

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

SCHRITT 3. LIZENZVEREINBARUNG ANZEIGEN

In dieser Phase müssen Sie die Lizenzvereinbarung lesen, die zwischen Ihnen und Kaspersky Lab eingegangen 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 der Lizenzvertrag nicht akzeptiert wird, wird die Programminstallation abgebrochen.

SCHRITT 4. ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK

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

Lesen Sie sich die Erklärung zur Verwendung von Kaspersky Security Network gründlich durch. Wenn Sie mit allen Punkten einverstanden sind, aktivieren Sie im Assistentenfenster das Kontrollkästchen **Ich möchte am Programm Kaspersky Security Network (KSN) teilnehmen**.

Klicken Sie auf **Weiter**, um die Programminstallation fortzusetzen.

SCHRITT 5. 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 PURE führt bei der Installation eine Reihe von Untersuchungen aus. Im Rahmen dieser Untersuchungen können folgende Probleme erkannt werden:

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

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

- **Vorhandensein von inkompatiblen Programmen auf dem Computer.** Werden inkompatible Programme gefunden, so wird eine entsprechende Liste auf dem Bildschirm angezeigt und Sie werden aufgefordert, die Programme zu entfernen. Programme, die nicht automatisch von Kaspersky PURE entfernt werden können, müssen manuell deinstalliert werden. Bei der Deinstallation inkompatibler Programme wird das System neu gestartet. Anschließend wird die Installation von Kaspersky PURE automatisch fortgesetzt.
- **Vorhandensein von schädlichen Anwendungen auf dem Computer.** Wenn auf dem Computer schädliche Anwendungen 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 manuell herunterzuladen. Dazu wird ein Link angegeben.

SCHRITT 6. INSTALLATION ABSCHLIEßEN

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

In einigen Fällen kann ein Neustart des Betriebssystems erforderlich sein, um die Installation abzuschließen. Wenn das Kontrollkästchen **Kaspersky PURE starten** aktiviert ist, wird das Programm nach einem Reboot automatisch gestartet.

Wenn Sie vor dem Beenden des Assistenten das Kontrollkästchen **Kaspersky PURE starten** deaktiviert haben, muss das Programm künftig manuell gestartet werden.

SCHRITT 7. PROGRAMM AKTIVIEREN

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

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

Um das Programm zu aktivieren, ist eine Internetverbindung erforderlich.

Für die Aktivierung von Kaspersky PURE bestehen folgende Möglichkeiten:

- **Kommerzielle Version aktivieren.** Wählen Sie diese Variante aus und geben Sie einen Aktivierungscode ein (s. Abschnitt "Über den Aktivierungscode" auf S. 27), wenn Sie eine kommerzielle Programmversion erworben haben.
- **Testversion aktivieren.** Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion des Programms installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Für die Gültigkeitsdauer der Testlizenz können Sie das Programm im vollen Funktionsumfang verwenden. Nach Ablauf der Lizenz ist es nicht möglich, erneut eine Testlizenz zu aktivieren.

SCHRITT 8. ANMELDUNG DES BENUTZERS

Dieser Schritt ist nur bei der Aktivierung einer kommerziellen Programmversion verfügbar. Bei der Aktivierung einer Testversion wird der Schritt übersprungen.

Registrierten Benutzern stehen folgende Leistungen zur Verfügung: Senden von Anfragen an den Technischen Support und an das Virenlabor (über Mein Kaspersky Account auf der Kaspersky-Lab-Webseite); bequeme Verwaltung von Aktivierungscodes; regelmäßige Informationen über neue Produkte und Sonderangebote.

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

SCHRITT 9. AKTIVIERUNG ABSCHLIEßEN

Der Assistent informiert Sie darüber, dass die Aktivierung von Kaspersky PURE erfolgreich abgeschlossen wurde. Außerdem werden in diesem Fenster Informationen über die aktuelle Lizenz angezeigt: Typ der Lizenz (kommerzielle oder Testlizenz), Gültigkeitsdauer der Lizenz sowie Anzahl der Computer, für die die Lizenz gültig ist.

Bei der Verwendung eines Abonnements werden anstelle des Ablaufdatums für die Lizenz Informationen zum Abo-Status angezeigt.

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

UPGRADE EINER VORGÄNGERVERSION VON KASPERSKY PURE

Wenn auf Ihrem Computer eine ältere Version von Kaspersky PURE installiert ist, müssen Sie das Programm auf die neue Version von Kaspersky PURE aktualisieren. Wenn eine aktuelle Lizenz für die Nutzung von Kaspersky PURE vorliegt, müssen Sie das Programm nicht aktivieren: Der Installationsassistent erhält automatisch die Informationen über die Lizenz für die Nutzung von Kaspersky PURE und übernimmt diese beim Installationsvorgang.

Kaspersky PURE wird auf dem Computer interaktiv mit einem Installationsassistenten 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**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

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

➔ *Um Kaspersky PURE auf Ihrem Computer zu installieren,*

starten Sie auf der Produkt-CD die Installationsdatei (Datei mit der Erweiterung .exe).

Sie können auch ein Programmpaket, das Sie über das Internet erhalten haben, für die Installation von Kaspersky PURE verwenden. Dabei zeigt der Installationsassistent für bestimmte Sprachversionen einige zusätzliche Installationschritte an.

IN DIESEM ABSCHNITT

Schritt 1. Nach neuer Programmversion suchen	21
Schritt 2. Beginn der Programminstallation	21
Schritt 3. Lizenzvereinbarung anzeigen	21
Schritt 4. Erklärung zur Verwendung von Kaspersky Security Network	22
Schritt 5. Installation	22
Schritt 6. Installation abschließen.....	22

SCHRITT 1. NACH NEUER PROGRAMMVERSION SUCHEN

Vor der Installation wird geprüft, ob neuere Versionen von Kaspersky PURE auf den Updateservern von Kaspersky Lab vorhanden sind.

Wenn keine neuere Version des Programms auf den Updateservern von Kaspersky Lab gefunden wurde, wird der Installationsassistent für diese Version gestartet.

Wenn auf den Updateservern eine neuere Version von Kaspersky PURE vorgefunden wurde, werden Ihnen Download und Installation vorgeschlagen. Es wird empfohlen, die neue Programmversion zu installieren, da neue Versionen den Schutz Ihres Computers optimieren. Sollten Sie die neuere Version ablehnen, wird der Installationsassistent der laufenden Version gestartet. Sollten Sie die Installation der neueren Version annehmen, werden die Programmdateien auf Ihren Computer kopiert und der Installationsassistent wird automatisch gestartet. Eine weitere Beschreibung zur Installation einer neueren Version finden Sie in der Dokumentation zur entsprechenden Programmversion.

SCHRITT 2. BEGINN DER PROGRAMMINSTALLATION

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

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

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

SCHRITT 3. LIZENZVEREINBARUNG ANZEIGEN

In dieser Phase müssen Sie die Lizenzvereinbarung lesen, die zwischen Ihnen und Kaspersky Lab eingegangen 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 der Lizenzvertrag nicht akzeptiert wird, wird die Programminstallation abgebrochen.

SCHRITT 4. ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK

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

Lesen Sie sich die Erklärung zur Verwendung von Kaspersky Security Network gründlich durch. Wenn Sie mit allen Punkten einverstanden sind, aktivieren Sie im Assistentenfenster das Kontrollkästchen **Ich möchte am Programm Kaspersky Security Network (KSN) teilnehmen**.

Klicken Sie auf **Weiter**, um die Programminstallation fortzusetzen.

SCHRITT 5. 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 PURE führt bei der Installation eine Reihe von Untersuchungen aus. Im Rahmen dieser Untersuchungen können folgende Probleme erkannt werden:

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

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

- **Vorhandensein von inkompatiblen Programmen auf dem Computer.** Werden inkompatible Programme gefunden, so wird eine entsprechende Liste auf dem Bildschirm angezeigt und Sie werden aufgefordert, die Programme zu entfernen. Programme, die nicht automatisch von Kaspersky PURE entfernt werden können, müssen manuell deinstalliert werden. Bei der Deinstallation inkompatibler Programme wird das System neu gestartet. Anschließend wird die Installation von Kaspersky PURE automatisch fortgesetzt.
- **Vorhandensein von schädlichen Anwendungen auf dem Computer.** Wenn auf dem Computer schädliche Anwendungen 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 manuell herunterzuladen. Dazu wird ein Link angegeben.

SCHRITT 6. INSTALLATION ABSCHLIEßEN

Dieses Fenster des Assistenten informiert über den Abschluss der Programminstallation.

Zum Abschluss der Installation muss das Betriebssystem neu gestartet werden.

Wenn das Kontrollkästchen **Kaspersky PURE starten** aktiviert ist, wird das Programm nach einem Reboot automatisch gestartet.

Wenn Sie vor dem Beenden des Assistenten das Kontrollkästchen **Kaspersky PURE starten** deaktiviert haben, muss das Programm manuell gestartet werden.

PROGRAMM DEINSTALLIEREN

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

Kaspersky PURE wird mit dem Installationsassistenten entfernt.

➤ Um den Assistenten zu starten,

wählen Sie im **Startmenü** den Punkt **Programme** → **Kaspersky PURE** → **Kaspersky PURE löschen** aus.

IN DIESEM ABSCHNITT

Schritt 1. Daten zur erneuten Verwendung speichern.....	23
Schritt 2. Löschen bestätigen.....	24
Schritt 3. Programm deinstallieren Deinstallation abschließen.....	24

SCHRITT 1. 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 (z. B. Installation einer neueren Version) wiederzuverwenden.

Sie können folgende Datentypen zur späteren Verwendung auswählen:

- **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.
- **Quarantäneobjekte** – Dateien, die vom Programm untersucht und im Backup und in der Quarantäne gespeichert wurden.

Wenn Kaspersky PURE vom Computer entfernt wird, besteht kein Zugriff mehr auf die Quarantänedateien. Kaspersky PURE muss installiert werden, um mit diesen Dateien zu arbeiten.

- **Funktionsparameter des Programms** – Parameterwerte für die Programmfunktion, die im Verlauf der Programmkonfiguration eingestellt 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.

- **iChecker-Daten** – Dateien mit Informationen zu den Objekten, die bereits mithilfe der iChecker-Technologie auf Viren untersucht wurden.
- **Verschlüsselte Container (mit Daten)** – Dateien, die mithilfe der Funktion Datenverschlüsselung in verschlüsselte Container verschoben wurden.
- **Datenbank für Password Manager (für alle Benutzer)** – Benutzerkonten, persönliche Notizen, Lesezeichen und Visitenkarten, die mit der Funktion Password Manager erstellt wurden.
- **Anti-Spam-Datenbanken** – Datenbanken, die Muster von Spam-Mails enthalten, die das Programm erhalten und gespeichert hat.

Das Programm schlägt standardmäßig vor, die Aktivierungsinformationen zu speichern.

➤ *Um Daten zur erneuten Verwendung zu speichern,*

aktivieren Sie die Kontrollkästchen der zu speichernden Daten.

SCHRITT 2. LÖSCHEN BESTÄTIGEN

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

SCHRITT 3. PROGRAMM DEINSTALLIEREN DEINSTALLATION

ABSCHLIEßEN

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

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 herunter- und hochgefahren wird.

LIZENZIERUNG DES PROGRAMMS

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

IN DIESEM ABSCHNITT

Über den Lizenzvertrag	25
Über die Lizenz	25
Über die Zurverfügungstellung von Daten	26
Über den Aktivierungscode	27

ÜBER DEN LIZENZVERTRAG

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

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

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

ÜBER DIE LIZENZ

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

Die Lizenz berechtigt zur Nutzung folgender Leistungen:

- Verwendung des Programms auf einem oder mehreren Geräten.

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

- Kontaktaufnahme mit dem Technischen Support von Kaspersky Lab
- Nutzung von sonstigen Leistungen, die Ihnen von Kaspersky Lab oder den Vertriebspartnern für die Gültigkeitsdauer der Lizenz angeboten werden (s. Abschnitt "Service für Benutzer" auf S. [15](#)).

Der Umfang der verfügbaren Leistungen und die Nutzungsdauer des Programms sind vom Typ der Lizenz abhängig, mit der das Programm aktiviert wurde.

Es sind folgende Lizenztypen vorgesehen

- *Testlizenz* – Kostenlose Lizenz, die zum Kennenlernen des Programms gedacht ist.

Eine Testlizenz besitzt gewöhnlich eine kurze Gültigkeitsdauer. Nach Ablauf der Testlizenz stellt Kaspersky PURE alle Funktionen ein. Es muss eine kommerzielle Lizenz gekauft werden, um das Programm weiter zu verwenden.

- *Kommerziell* – Gekaufte Lizenz, die beim Kauf eines Programms zur Verfügung gestellt wird.

Nach Ablauf der kommerziellen Lizenz funktioniert das Programm weiterhin, wobei aber der Funktionsumfang eingeschränkt wird (dann sind beispielsweise das Update und der Dienst Kaspersky Security Network nicht mehr verfügbar). Sie können weiterhin alle Programmkomponenten verwenden und eine Untersuchung auf Viren und andere bedrohliche Programme ausführen, allerdings nur mit den Datenbanken, die beim Ablauf der Lizenz installiert waren. Die kommerzielle Lizenz muss verlängert werden, um Kaspersky PURE mit der vollen Funktionalität weiter zu verwenden.

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

ÜBER DIE ZURVERFÜGUNGSTELLUNG VON DATEN

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

- Informationen über die Kontrollsummen verarbeiteter Dateien (MD5)
- Informationen für die Ermittlung der URL-Reputation
- Statistik über die Verwendung von Benachrichtigungen des Produkts
- statistische Daten für den Spam-Schutz
- Daten zur Aktivierung und zur eingesetzten Version von Kaspersky PURE
- Informationen über die Typen von gefundenen Bedrohungen
- Informationen über die verwendeten digitalen Zertifikate und Informationen, die zur Authentifizierung der Zertifikate erforderlich sind.

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

Bei der Teilnahme am Programm Kaspersky Security Network werden automatisch folgende Informationen an Kaspersky Lab übermittelt, die von Kaspersky PURE auf dem Computer gesammelt werden:

- Informationen über die installierte Hard- und Software
- Informationen über den Status des Antiviren-Schutzes auf dem Computer, Informationen über alle potenziell gefährlichen Objekte, riskanten Aktionen und Entscheidungen im Hinblick auf diese Objekte und Aktionen.
- Informationen über geladene und gestartete Programme
- Informationen über Fehler und über die Verwendung der Benutzeroberfläche von Kaspersky PURE
- Informationen über die Version der verwendeten Programm-Datenbanken
- Statistik über Updates und über Verbindungen mit den Kaspersky-Lab-Servern
- Statistik für die tatsächliche Zeitdauer, die die Programmkomponenten für die Objektuntersuchung aufgewendet haben.

Für eine zusätzliche Untersuchung können außerdem Dateien (oder Dateiteile) an Kaspersky Lab geschickt werden, die von Angreifern zur Beschädigung des Computers oder der Daten verwendet werden können.

Diese Informationen werden von Kaspersky Lab in Übereinstimmung mit den gesetzlichen Anforderungen geschützt. Kaspersky Lab verwendet diese Informationen nur in Form einer allgemeinen Statistik. Die Daten der allgemeinen Statistik werden automatisch aus den gesammelten Quellinformationen ermittelt und enthalten keinerlei persönliche oder sonstige vertrauliche Informationen. Die gesammelten Quellinformationen werden in verschlüsselter Form gespeichert und regelmäßig gelöscht (2 Mal jährlich). Die Daten der allgemeinen Statistik werden unbegrenzt gespeichert.

ÜBER DEN AKTIVIERUNGSCODE

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

Ein Aktivierungscode besteht aus einer unikal 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 PURE 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 PURE 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 PURE auf mehreren Geräten genutzt werden kann, so beginnt die Laufzeit der Lizenz, wenn der Aktivierungscode zum ersten Mal verwendet wird.

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

LÖSUNGEN FÜR TYPISCHE AUFGABEN

Dieser Abschnitt bietet genaue Anleitungen für die wichtigsten Aufgaben, die der Benutzer mit dem Programm lösen kann.

IN DIESEM ABSCHNITT

Programm aktivieren	29
Lizenz kaufen oder verlängern	30
Mit den Benachrichtigungen des Programms arbeiten.....	30
Schutzstatus des Computers analysieren und Sicherheitsprobleme beheben.....	31
Update der Datenbanken und Programm-Module.....	32
Untersuchung wichtiger Computerbereiche auf Viren	33
Vollständige Untersuchung des Computers auf Viren	33
Virenuntersuchung einer Datei, eines Ordners oder eines anderen Objekts.....	34
Computer auf Schwachstellen untersuchen	35
Eine vom Programm gelöschte oder desinfizierte Datei wiederherstellen.....	35
Betriebssystem nach einer Infektion wiederherstellen	37
Unerwünschte E-Mails (Spam) blockieren	39
E-Mail untersuchen und E-Mail-Anhänge filtern	39
Sicherheit einer Webseite überprüfen	40
Zugriff auf Websites bestimmter Regionen sperren	41
Fernverwaltung für den Schutz des Heimnetzwerks	41
Mit unbekanntem Programmen arbeiten	42
Persönliche Daten vor Diebstahl schützen.....	45
Backup	62
Kennwortschutz für die Einstellungen von Kaspersky PURE	65
Kindersicherung verwenden.....	66
Computerschutz anhalten und fortsetzen.....	68
Bericht über den Computerschutz anzeigen	69
Standardeinstellungen für das Programm wiederherstellen	70
Import der Programmeinstellungen für Kaspersky PURE auf einen anderen Computer	72
Notfall-CD erstellen und verwenden.....	73

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 PURE durch entsprechende Meldungen im Infobereich der Taskleiste daran erinnert. Kaspersky PURE wird mit dem Aktivierungsassistenten aktiviert.

➤ *Gehen Sie folgendermaßen vor, um den Aktivierungsassistenten für Kaspersky PURE zu starten:*

- Klicken Sie im Meldungsfenster von Kaspersky PURE, das im Infobereich der Taskleiste erscheint, auf den Link **Aktivieren**.
- Verwenden Sie im unteren Bereich des Programmhauptfensters den Link **Lizenz**. Klicken Sie im folgenden Fenster **Lizenzierung** auf **Programm aktivieren**.

Im Assistenten für die Programmaktivierung müssen einige Einstellungen angegeben werden.

Schritt 1. Aktivierungscode eingeben

Geben Sie im entsprechenden Feld den Aktivierungscode ein (s. Abschnitt "Über den Aktivierungscode" auf S. [27](#)) und klicken Sie auf **Weiter**.

Schritt 2. Aktivierungsanfrage

Nach einer erfolgreichen Aktivierungsabfrage geht der Assistent automatisch zum nächsten Schritt.

Schritt 3. Anmeldeinformationen eingeben

Registrierten Benutzern stehen folgende Leistungen zur Verfügung:

- Senden von Anfragen an den Technischen Support und an das Virenlabor (über Mein Kaspersky Account auf der Kaspersky-Lab-Homepage)
- AktivierungsCodes verwalten
- Empfang von Informationen über neue Produkte und Sonderangebote von Kaspersky Lab

Geben Sie Ihre Anmeldeinformationen an und klicken Sie dann auf **Weiter**.

Schritt 4. Aktivierung

Wenn die Programmaktivierung erfolgreich verlaufen ist, geht der Assistent automatisch zum nächsten Fenster.

Schritt 5. Assistent abschließen

Dieses Fenster des Assistenten informiert über die Aktivierungsergebnisse.

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

LIZENZ KAUFEN ODER VERLÄNGERN

Wenn Sie Kaspersky PURE installiert haben und keine kommerzielle Lizenz besitzen, können Sie nach der Programminstallation eine Lizenz erwerben. Beim Kauf einer kommerziellen Lizenz erhalten Sie einen Aktivierungscode, mit dem das Programm aktiviert werden muss (s. Abschnitt "Programm aktivieren" auf S. [29](#)).

Wenn die Gültigkeit einer Lizenz bald abläuft, können Sie diese verlängern. Dazu können Sie im Programm einen Reserve-Aktivierungscode hinzufügen, bevor die Lizenz abläuft. Wenn die Lizenz abläuft, wird Kaspersky PURE automatisch mit dem Reserve-Aktivierungscode aktiviert.

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

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

Die Webseite des Online-Shops wird geöffnet. Dort können Sie eine Lizenz erwerben.

➤ *Gehen Sie folgendermaßen vor, um einen Reserve-Aktivierungscode einzugeben:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Lizenz**, um das Fenster **Lizenzverwaltung** zu öffnen.
3. Klicken Sie im folgenden Fenster auf **Programm aktivieren**.

Das Fenster des Assistenten zur Programmaktivierung wird geöffnet.

4. Tragen Sie in die entsprechenden Felder den Aktivierungscode ein und klicken Sie auf **Weiter**.

Kaspersky PURE schickt die Daten zur Überprüfung an den Aktivierungsserver. Wenn die Überprüfung erfolgreich verläuft, geht der Aktivierungsassistent automatisch weiter zum nächsten Schritt.

5. Klicken bei Abschluss des Assistenten auf **Beenden**.

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 System). 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 System). 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 von Kaspersky Lab empfohlene Variante.

SCHUTZSTATUS DES COMPUTERS ANALYSIEREN UND SICHERHEITSPROBLEME BEHEBEN

Ist die Computersicherheit gefährdet, so wird dies durch ein Farbsignal im Hauptfenster von Kaspersky PURE angezeigt (s. Abb. unten). Die Farbe des Indikators ist vom Status des Computerschutzes abhängig: Grün bedeutet, dass der Computer sicher ist. Gelb signalisiert, dass der Schutz Probleme aufweist, und Rot warnt vor einer ernsthaften Bedrohung für die Computersicherheit. Es wird empfohlen, Sicherheitsprobleme sofort zu lösen und Bedrohungen zu beheben.



Abbildung 1. Roter Farbindikator im Hauptfenster

Wenn die Computersicherheit bedroht ist, befindet sich auf dem Statusindikator rechts oben im Programmhauptfenster die Schaltfläche **Korrigieren** (s. Abb. oben). Durch Klick auf die Schaltfläche **Korrigieren** können Sie das Fenster **Sicherheitsprobleme** öffnen (s. Abb. unten). Es enthält ausführliche Angaben zum Schutzstatus des Computers und bietet unterschiedliche Aktionen zur Lösung von Sicherheitsproblemen und zum Beheben von Bedrohungen.

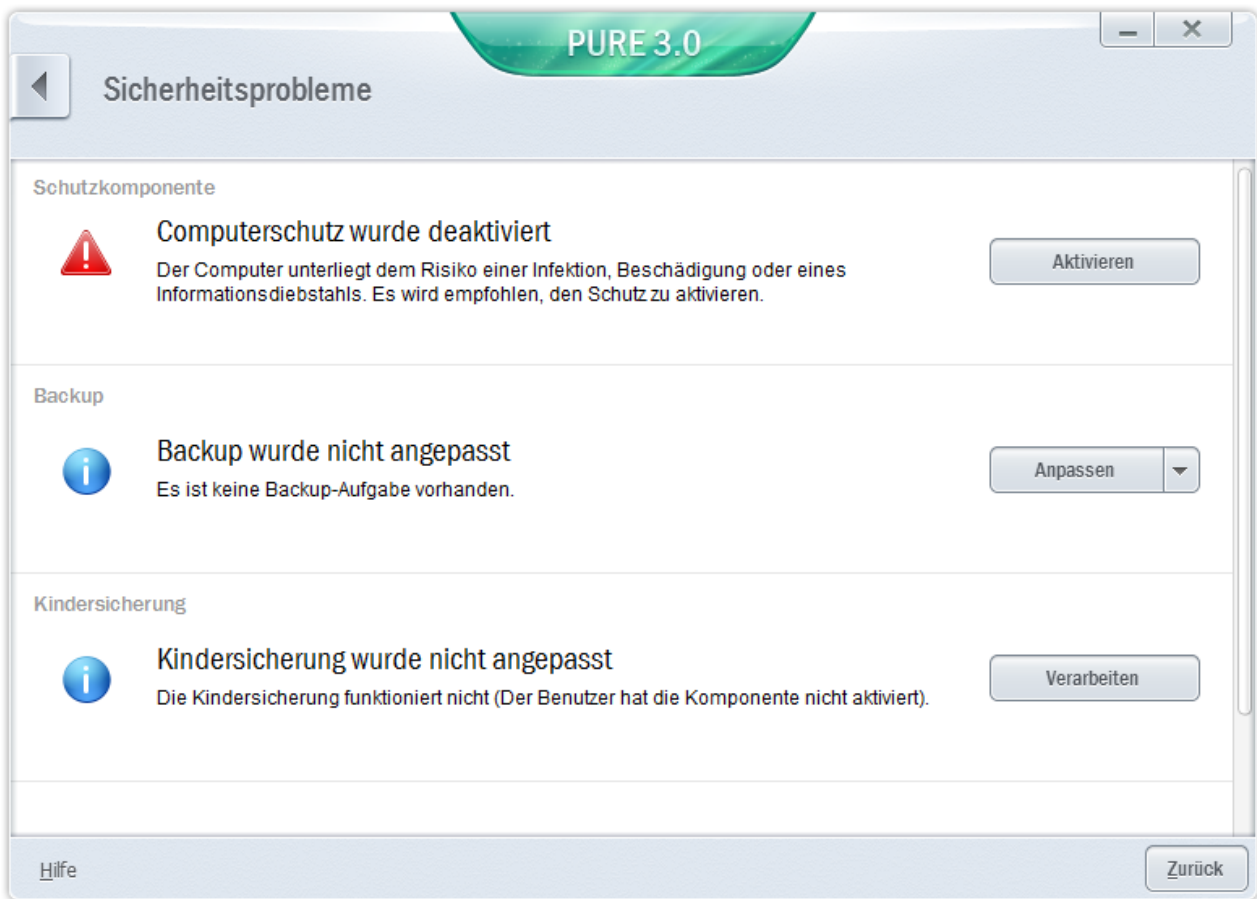


Abbildung 2. Fenster **Sicherheitsprobleme**

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

Eine Überprüfung des Schutzstatus auf anderen Computern des Heimnetzwerks ist mithilfe der Verwaltung möglich (s. Abschnitt "Fernverwaltung für den Schutz des Heimnetzwerks" auf S. 41).

UPDATE DER DATENBANKEN UND PROGRAMM-MODULE

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

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

- Um das Update aus dem Kontextmenü des Programmsymbols im Infobereich der Taskleiste zu starten, wählen Sie im Kontextmenü des Programmsymbols den Punkt **Update** aus.

➤ Gehen Sie folgendermaßen vor, um das Update aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Starten Sie im Block **Computersicherheit** mit dem Link **Update** die Aktualisierung der Datenbanken.


UNTERSUCHUNG WICHTIGER COMPUTERBEREICHE AUF VIREN

Die Untersuchung wichtiger Bereiche umfasst folgende Objekte:

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

➤ Gehen Sie folgendermaßen vor, um die Untersuchung der wichtigen Bereiche aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Wählen Sie im linken Bereich den Abschnitt **Untersuchung**.

3. Klicken Sie im rechten Fensterbereich unter **Untersuchung wichtiger Bereiche** auf .

VOLLSTÄNDIGE UNTERSUCHUNG DES COMPUTERS AUF VIREN

Bei einer vollständigen Untersuchung scannt Kaspersky PURE standardmäßig folgende Objekte:

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

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

➤ Gehen Sie folgendermaßen vor, um die vollständige Untersuchung aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie im Block **Computersicherheit** mit dem Link **Untersuchung** eine Liste der Untersuchungsaufgaben.
3. Starten Sie mit dem Link **Vollständige Untersuchung** eine vollständige Untersuchung.

VIRENUNTERSUCHUNG EINER DATEI, EINES ORDNERS ODER EINES ANDEREN OBJEKTS

Ein bestimmtes Objekt kann folgendermaßen auf Viren untersucht werden:

- aus dem Kontextmenü eines Objekts
- aus dem Programmhauptfenster

➤ Gehen Sie folgendermaßen vor, um eine Virenuntersuchung aus dem Kontextmenü eines Objekts zu starten:

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**.

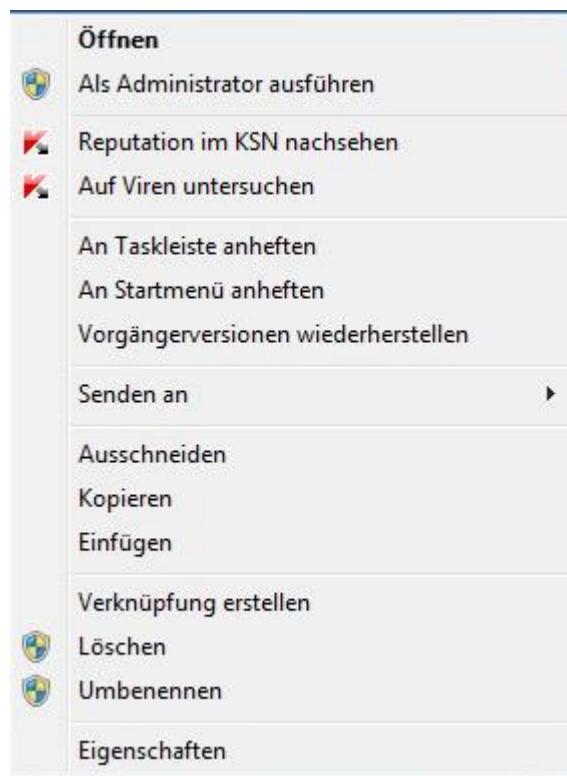


Abbildung 3. Kontextmenü einer ausführbaren Datei

➤ Gehen Sie folgendermaßen vor, um die Untersuchung eines Objekts aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Wählen Sie im linken Bereich den Abschnitt **Untersuchung**.
3. Verwenden Sie eine der folgenden Methoden, um ein Untersuchungsobjekt anzugeben:
 - Öffnen Sie mit dem Link **wählen**, der sich unten rechts im Fenster befindet, das Fenster **Benutzerdefinierte Untersuchung** und aktivieren Sie die Kontrollkästchen für die Ordner und Laufwerke, die untersucht werden sollen.

Gehen Sie folgendermaßen vor, wenn ein Objekt, das untersucht werden soll, nicht in diesem Fenster vorhanden ist:

- a. Klicken Sie links unten auf den Link **Hinzufügen**, um das Fenster **Untersuchungsobjekt auswählen** zu öffnen.
 - b. Wählen Sie im folgenden Fenster **Untersuchungsobjekt wählen** ein Untersuchungsobjekt.
- Ziehen Sie ein Untersuchungsobjekt mit der Maus in den dafür vorgesehenen Bereich (s. Abb. unten).




Abbildung 4. Bereich im Abschnitt **Untersuchung**, in den ein Objekt gezogen wird, um es zu untersuchen.

UNTERSUCHUNG DES COMPUTERS AUF SCHWACHSTELLEN

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

➤ Gehen Sie folgendermaßen vor, um die Schwachstellensuche aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Wählen Sie im linken Bereich den Abschnitt **Untersuchung**.

3. Klicken Sie im folgenden Fenster unter **Schwachstellensuche** auf .

EIN VOM PROGRAMM GELÖSCHTES ODER DESINFIZIERTES OBJEKT WIEDERHERSTELLEN

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

Die Sicherungskopie, die vom Programm bei der Untersuchung einer Datei angelegt wurde, dient zur Wiederherstellung einer gelöschten oder desinfierten Datei.

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

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

2. Klicken Sie im linken Bereich des folgenden Fensters auf den Link **Quarantäne: <Anzahl der Dateien>** (s. Abb. unten).



Abbildung 5. Fenster **Computersicherheit**

3. Wählen Sie im folgenden Fenster **Quarantäne** in der Liste die entsprechende Datei aus und klicken Sie auf **Wiederherstellen** (s. Abb. unten).

Kaspersky PURE stellt die angegebene Datei im Ordner wieder her, in dem die vom Programm gelöschte und desinfizierte Datei gespeichert wurde.

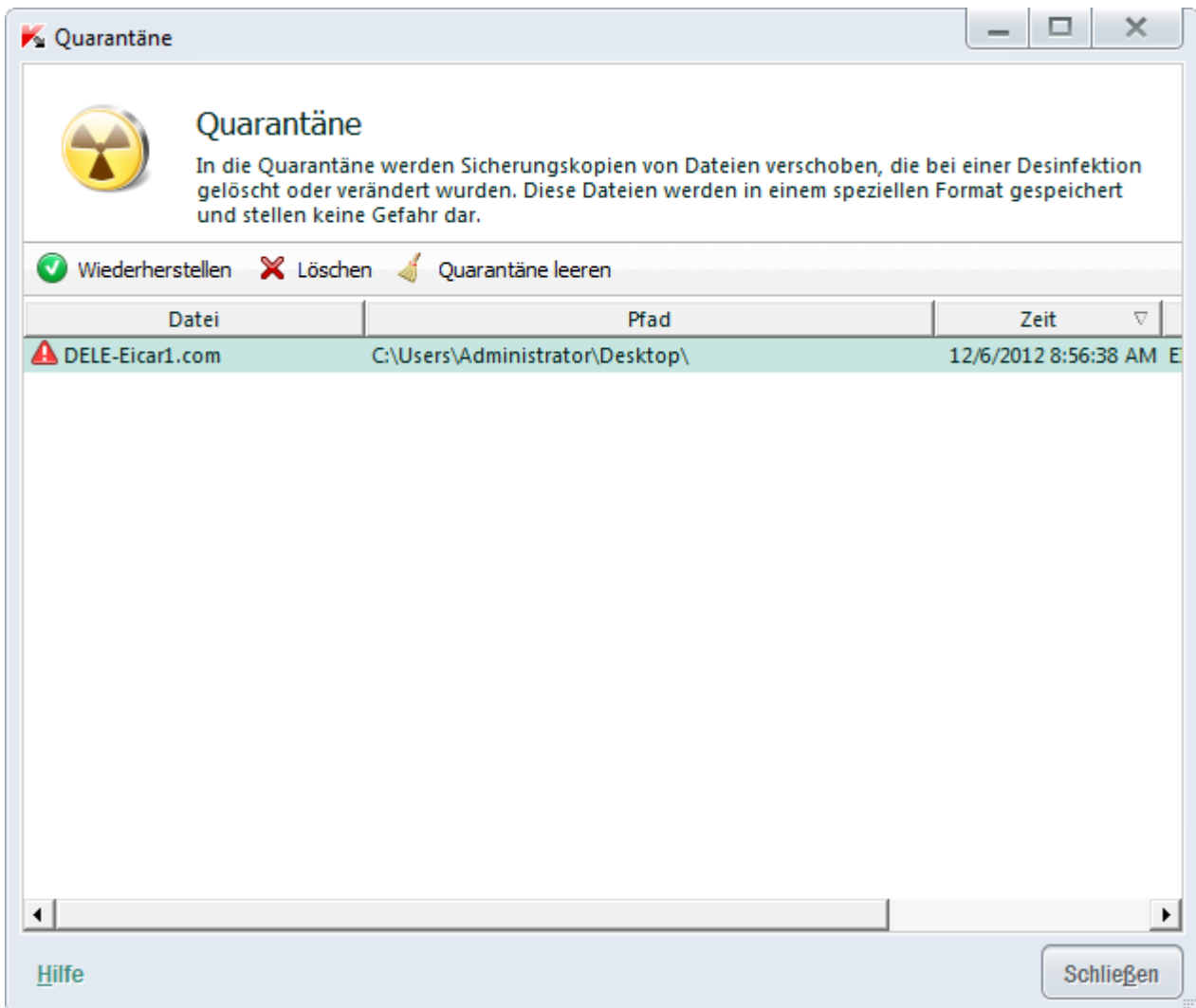


Abbildung 6. Fenster **Quarantäne**

BETRIEBSSYSTEM NACH EINER INFEKTION WIEDERHERSTELLEN

Wenn Sie vermuten, dass das Betriebssystem Ihres Computers durch Malware-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 System 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 prüft, ob im System Veränderungen vorliegen. Dazu zählen beispielsweise: blockierter Zugriff auf die Netzwerkumgebung, veränderte Dateierweiterungen bekannter Formate und blockierte Systemsteuerung. Es gibt unterschiedliche Gründe für das Auftreten solcher Beschädigungen. Es kann sich um die Aktivität schädlicher Programme, ungültige Systemeinstellungen, Systemabstürze oder die Verwendung fehlerhaft funktionierender Systemoptimierungsprogramme handeln.

Nach der Untersuchung analysiert der Assistent die gesammelten Informationen, um festzustellen, ob im System 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.

➤ *Gehen Sie folgendermaßen vor, den Assistenten zur Systemwiederherstellung zu starten:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Zusätzliche Funktionen**.
3. Klicken Sie im folgenden Fenster im Block **Wiederherstellung nach Infektion** auf **Ausführen**.

Das Fenster des Systemwiederherstellungs-Assistenten 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. Systemwiederherstellung starten

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

Schritt 2. Nach Problemen suchen

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

Schritt 3. Aktionen für die Problembehebung wählen

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

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

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

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

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

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

Schritt 4. Probleme beheben

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

Schritt 5. Assistent abschließen

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

UNERWÜNSCHTE E-MAILS (SPAM) BLOCKIEREN

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

➤ *Gehen Sie folgendermaßen vor, um Anti-Spam zu aktivieren und die empfohlene Sicherheitsstufe zu wählen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz** die Komponente **Anti-Spam**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Anti-Spam aktivieren**.
5. Vergewissern Sie sich, dass im Block **Sicherheitsstufe** die Sicherheitsstufe **Empfohlen** ausgewählt ist.

Sollte die Sicherheitsstufe **Niedrig** oder **Benutzerdefiniert** gewählt sein, so klicken Sie auf **Standard**. Die Sicherheitsstufe erhält automatisch den Wert **Empfohlen**.

E-MAIL UNTERSUCHEN UND E-MAIL-ANHÄNGE FILTERN

Kaspersky PURE 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 die E-Mail-Nachrichten der Protokolle POP3, SMTP, IMAP, MAPI und NNTP (einschließlich geschützter Verbindungen (SSL) mit den Protokollen POP3, SMTP und IMAP).

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

➤ *Gehen Sie folgendermaßen vor, damit nur eingehende Nachrichten untersucht werden:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

Das Fenster **Mail-Anti-Virus** wird geöffnet.

5. Wählen Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Schutzbereich** die Variante **Nur eingehende Nachrichten**.

Wenn in einer E-Mail-Nachricht keine Bedrohungen gefunden wurden oder infizierte Objekte erfolgreich neutralisiert wurden, wird der Zugriff auf die E-Mail-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 PURE bearbeitet wurde. Wenn ein Objekt gelöscht wird, legt Kaspersky PURE eine Sicherungskopie an und verschiebt sie in die Quarantäne.

Schädliche Programme können sich über E-Mail-Anhänge ausbreiten. Sie können die Filterung von E-Mail-Anhängen aktivieren. Mit der Filterung können angehängte Dateien der festgelegten Typen automatisch umbenannt oder gelöscht werden.

➔ Gehen Sie folgendermaßen vor, um die Anlagenfilterung in E-Mail-Nachrichten zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

Das Fenster **Mail-Anti-Virus** wird geöffnet.

5. Wählen Sie im folgenden Fenster auf der Registerkarte **Anlagenfilterung** einen Modus für die Anlagenfilterung aus (**Anhänge der ausgewählten Typen umbenennen** oder **Anhänge der ausgewählten Typen löschen**).
6. Wählen Sie in der Liste der Dateitypen (Erweiterungen) die Typen der Anlagen aus, die gefiltert werden sollen.

Gehen Sie folgendermaßen vor, um eine Maske für einen neuen Dateityp hinzuzufügen:




- a. Öffnen Sie mit dem Link **Hinzufügen** im unteren Fensterbereich das Fenster **Maske für Dateinamen**.
 - b. Geben Sie im folgenden Fenster die entsprechende Maske für den Dateityp an.
7. Klicken Sie im Fenster **Einstellungen** auf **Übernehmen**.

SICHERHEIT EINER WEBSEITE ÜBERPRÜFEN

Kaspersky PURE kann die Sicherheit einer Website überprüfen, bevor ein Link auf dieser Website geöffnet wird. Dazu dient das *Modul zur Link-Untersuchung*.

Das Modul zur Link-Untersuchung ist in Microsoft Internet Explorer 10 im Metro-Stil und in Microsoft Internet Explorer 10 nicht verfügbar, wenn in den Browser-Einstellungen das Kontrollkästchen **Erweiterten geschützten Modus aktivieren** (Enhanced Protected Mode) aktiviert ist.

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

-  – Wenn die Webseite, auf die ein Link verweist, nach den Angaben von Kaspersky Lab sicher ist.
-  – Wenn keine Informationen über die Sicherheit der Webseite vorliegen, auf die ein Link verweist.
-  – Wenn die Webseite, auf die ein Link verweist, nach den 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 PURE untersucht standardmäßig nur die Links in Suchergebnissen. Die Untersuchung kann für Links auf allen Websites aktiviert werden.

➔ Gehen Sie folgendermaßen vor, um die Untersuchung für Links auf allen Websites zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie im folgenden Fenster **Einstellungen** im Abschnitt **Schutz-Center** den Unterabschnitt **Web-Anti-Virus** aus und klicken Sie auf **Einstellungen**.

Das Fenster **Web-Anti-Virus** wird geöffnet.

4. Klicken Sie im folgenden Fenster auf der Registerkarte **Web-Filter** unter **Modul zur Link-Untersuchung** auf **Einstellungen**.

Das Fenster **Modul zur Link-Untersuchung anpassen** wird geöffnet.

5. Wählen Sie im folgenden Fenster unter **Untersuchungsmodus** die Variante **Alle Links** aus.
6. Klicken Sie im Fenster **Einstellungen** auf **Übernehmen**.

ZUGRIFF AUF WEBSITES BESTIMMTER REGIONEN SPERREN

Statistisch betrachtet unterscheidet sich der Kontaminationsgrad von Websites in verschiedenen Ländern. Kaspersky PURE kann den Zugriff auf Websites verbieten, die regionalen Domains mit einem hohem Kontaminationsgrad angehören. Dazu dient die Komponente Geo-Filter.

Wenn der Geo-Filter aktiviert ist, erlaubt oder verbietet Kaspersky PURE den Zugriff auf regionale Domains oder fragt nach einer Zugriffserlaubnis. Das Vorgehen ist von Ihrer Auswahl abhängig.

➔ *Gehen Sie folgendermaßen vor, um den Geo-Filter zu aktivieren und anzupassen:*

1. Öffnen Sie das Programmfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie im folgenden Fenster **Einstellungen** im Abschnitt **Schutz-Center** den Unterabschnitt **Web-Anti-Virus** aus und klicken Sie auf **Einstellungen**.
Das Fenster **Web-Anti-Virus** wird geöffnet.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Geo-Filter** das Kontrollkästchen **Filterung nach regionalen Domains aktivieren**.
5. Im unteren Fensterbereich befindet sich eine der Liste der kontrollierten Domains. Geben Sie hier die Domains an, auf die der Zugriff erlaubt oder verboten werden soll oder für die eine Zugriffserlaubnis erfragt werden soll.
6. Klicken Sie im Fenster **Einstellungen** auf **Übernehmen**.

FERNVERWALTUNG FÜR DEN SCHUTZ DES HEIMNETZWERKS

Mit der Komponente Verwaltung lässt sich Kaspersky PURE von einem Administratorarbeitsplatz aus auf den Computern eines Heimnetzwerks fernverwalten.

Mit der Verwaltung können folgende Aufgaben gelöst werden, um die Sicherheit des Heimnetzwerks zu gewährleisten:

- Liste der auf einem bestimmten Netzwerkcomputer vorliegenden Sicherheitsprobleme anzeigen und bestimmte Probleme ferngesteuert beheben.
- Auf mehreren Computern des Heimnetzwerks gleichzeitig nach Viren suchen.
- Datenbanken gleichzeitig auf mehreren Computern des Heimnetzwerks aktualisieren.

➤ *Gehen Sie folgendermaßen vor, um eine Liste der Sicherheitsprobleme anzuzeigen, die auf einem bestimmten Netzwerkcomputer vorliegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Fensterbereich auf **Verwaltung**.
2. Wählen Sie im Bereich des folgenden Fensters **Verwaltung** den Computer aus, für den eine Problemliste angezeigt werden soll, und gehen Sie zum Abschnitt **Informationen**.
3. Klicken Sie auf der rechten Fensterseite unter **Probleme** auf **Liste**.

Das Fenster **Probleme** wird geöffnet. Es enthält Informationen über die Sicherheitsprobleme auf dem ausgewählten Computer.

➤ *Gehen Sie folgendermaßen vor, um mehrere Netzwerkcomputer auf Viren zu untersuchen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Fensterbereich auf **Verwaltung**.
Öffnen Sie das Fenster **Verwaltung**.
2. Öffnen Sie mit dem Link **Auf Viren untersuchen** das Fenster **Gruppenweiser Start der Untersuchung**.
3. Wählen Sie im Fenster **Gruppenweiser Start der Untersuchung** die Registerkarte mit dem erforderlichen Untersuchungstyp aus (**Vollständige Untersuchung** oder **Untersuchung wichtiger Bereiche**).
4. Wählen Sie aus, welche Computer untersucht werden sollen, und klicken Sie auf **Untersuchung starten**.

➤ *Gehen Sie folgendermaßen vor, um die Datenbanken gleichzeitig auf mehreren Netzwerkcomputern zu aktualisieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Fensterbereich auf **Verwaltung**.
Öffnen Sie das Fenster **Verwaltung**.
2. Öffnen Sie mit dem Link **Datenbanken aktualisieren** das Fenster **Gruppenweiser Start des Updates**.
3. Wählen Sie im Fenster **Gruppenweiser Start des Updates** die Computer aus, auf denen die Datenbanken aktualisiert werden sollen, und klicken Sie auf **Update starten**.

MIT UNBEKANNTEN PROGRAMMEN ARBEITEN

Mit Hilfe von Kaspersky PURE können Sie die Risiken reduzieren, die mit der Verwendung unbekannter Programme zusammenhängen (beispielsweise die Risiken einer Vireninfektion des Computers und unerwünschter Veränderungen am Betriebssystem).

Kaspersky PURE enthält Komponenten und Tools, mit denen die Reputation von Programmen ermittelt und ein Programm in einer sicheren Umgebung gestartet werden kann, die vom Betriebssystem getrennt ist.

KONTROLLE DER AKTIONEN EINES PROGRAMMS AUF DEM COMPUTER UND IM NETZWERK

Die Programmkontrolle hindert Programme daran, systemgefährliche Aktionen auszuführen, und kontrolliert den Zugriff auf Betriebssystemressourcen und auf Ihre persönlichen Daten.

Die Komponente verfolgt die Aktionen, die von auf dem Computer installierten Programmen im System ausgeführt werden, und reguliert ihre Aktivität entsprechend den Regeln der Programmkontrolle. Diese Regeln beziehen sich auf Aktivitäten, die Einfluss auf die Computersicherheit haben können. Dazu zählt auch der Zugriff von Programmen auf geschützte Ressourcen (beispielsweise Dateien, Ordner, Registrierungsschlüssel und Netzwerkadressen).

Die Netzwerkaktivität von Programmen wird von der Komponente Firewall kontrolliert.

Wenn ein Programm zum ersten Mal auf dem Computer gestartet wird, untersucht 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 PURE zur Aktivitätskontrolle dieses Programms verwenden wird.

Die Kontrollregeln für Programmaktivitäten können manuell angepasst werden.

➔ *Gehen Sie folgendermaßen vor, um eine Regel für die Programmkontrolle manuell zu ändern:*

1. Öffnen Sie das Programmhauptfenster.
 2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
 3. Wählen Sie im folgenden Fenster **Einstellungen** im Abschnitt **Schutz-Center** den Unterabschnitt **Programmkontrolle** aus.
 4. Klicken Sie im rechten Fensterbereich unter **Anpassen von Regeln für Programme, Schutz für persönliche Daten und andere Ressourcen auf Programme**.
 5. Wählen Sie im folgenden Fenster **Programme** das betreffende Programm aus der Liste und klicken Sie auf **Ändern**.
 6. Legen Sie im folgenden Fenster **Regeln für das Programm** die Kontrollregeln für das Programm fest:
 - Gehen Sie folgendermaßen vor, um die Regeln für den Zugriff des Programms auf Betriebssystemressourcen anzupassen:
 - a. Wählen Sie auf der Registerkarte **Dateien, Systemregistrierung** die entsprechende Ressourcenkategorie aus.
 - b. Öffnen Sie durch Rechtsklick in der Spalte mit den für die Ressourcen möglichen Aktionen (**Lesen, Schreiben, Löschen** oder **Erstellen**) das Kontextmenü und wählen Sie dort den entsprechenden Wert aus (**Erlauben, Verbieten** oder **Aktion erfragen**).
 - Gehen Sie folgendermaßen vor, um die Rechte anzupassen, die dem Programm für die Ausführung bestimmter Aktionen im Betriebssystem zugewiesen werden:
 - a. Wählen Sie auf der Registerkarte **Rechte** die entsprechende Rechtekategorie aus.
 - b. Öffnen Sie durch Rechtsklick in der Spalte **Erlaubnis** das Kontextmenü für die betreffende Regel und wählen Sie dort den entsprechenden Wert aus (**Erlauben, Verbieten** oder **Aktion erfragen**).
 - Gehen Sie folgendermaßen vor, um die Rechte anzupassen, die dem Programm für die Ausführung bestimmter Aktionen im Netzwerk zugewiesen werden:
 - a. Klicken Sie auf der Registerkarte **Netzwerkregeln** auf **Hinzufügen**.
Das Fenster **Netzwerkregel** wird geöffnet.
 - b. Legen Sie im folgenden Fenster die entsprechenden Einstellungen für die Regel fest und klicken Sie auf **OK**.
 - c. Weisen Sie der neuen Regel eine Priorität zu. Verschieben Sie dazu die Regel mit den Schaltflächen **Aufwärts** und **Abwärts** an die entsprechende Position der Liste.
 - Damit bestimmte Aktionen nicht von der Programmkontrolle untersucht werden, aktivieren Sie auf der Registerkarte **Ausnahmen** die Kontrollkästchen für die Aktionen, die nicht kontrolliert werden sollen.
- Alle Ausnahmen, die in den Regeln für Programme erstellt wurden, stehen im Konfigurationsfenster des Programms im Abschnitt **Gefahren und Ausnahmen** zur Verfügung.
7. Klicken Sie im Fenster **Einstellungen** auf **Übernehmen**.

REPUTATION EINES PROGRAMMS ÜBERPRÜFEN

Kaspersky PURE 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 am Kaspersky Security Network zugestimmt haben.

➔ Um die Reputation eines Programms zu ermitteln,

wählen Sie im Kontextmenü der ausführbaren Programmdatei den Punkt **Reputation im KSN nachsehen** aus (s. Abb. unten).

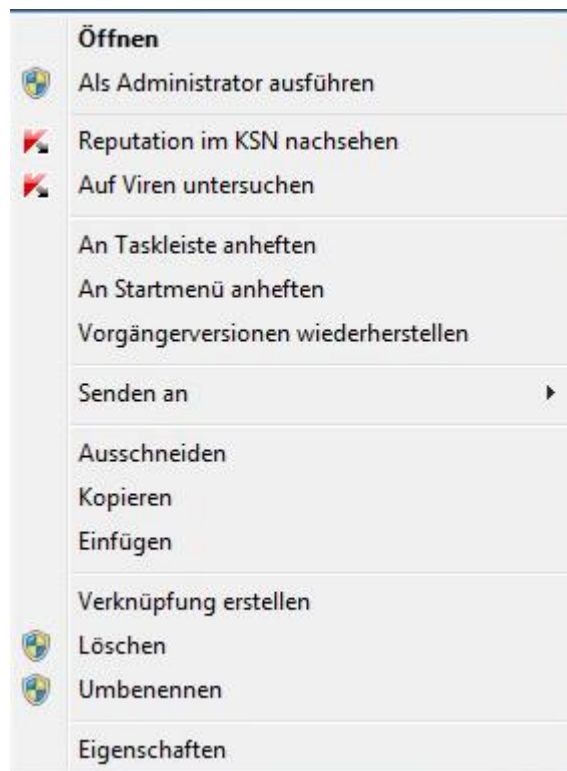


Abbildung 7. Kontextmenü für ein Objekt in Microsoft Windows

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

PERSÖNLICHE DATEN VOR DIEBSTAHL SCHÜTZEN

Mit Kaspersky PURE können Sie Ihre persönlichen Daten vor Diebstahl schützen:

- Kennwörter, Benutzernamen und andere Anmeldedaten
- Konto- und Kreditkartennummern
- vertrauliche Dateien

Kaspersky PURE enthält Komponenten und Tools, mit denen Ihre persönlichen Daten vor Diebstahl geschützt werden können, wenn Angreifer Methoden wie Phishing und das Abfangen von Daten, die über die Tastatur eingegeben werden, einsetzen.

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

Für den Schutz vor Phishing ist Anti-Phishing verantwortlich, das zu den Komponenten Web-Anti-Virus, Anti-Spam und IM-Anti-Virus gehört.

Die Virtuelle Tastatur, der Schutz von Tastatureingaben und Password Manager dienen dazu, Tastatureingaben vor dem Abfangen von Daten zu schützen.

Die Datenverschlüsselung schützt Dateien vor unbefugtem Zugriff.

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

IN DIESEM ABSCHNITT

Sicherer Zahlungsverkehr	45
Schutz vor Phishing	46
Virtuelle Tastatur verwenden.....	47
Schutz für die Dateneingabe über eine Hardwaretastatur.....	49
Schutz für Kennwörter.....	51
Datenverschlüsselung.....	54
Löschen von nicht benötigten Daten	56
Unwiderrufliches Löschen von Daten	58
Aktivitätsspuren löschen.....	60

SICHERER ZAHLUNGSVERKEHR

Zum Schutz vertraulicher Daten, die Sie auf Websites von Banken und Zahlungssystemen eingeben (beispielsweise Kreditkartennummern, Kennwörter für Online-Banking) und zur Verhinderung des Diebstahls von Zahlungsmitteln bei Online-Zahlungsvorgängen schlägt Kaspersky PURE vor, solche Websites im sicheren Browser zu öffnen.

Der sichere Browser kann nicht gestartet werden, wenn das Kontrollkästchen **Selbstschutz aktivieren** im Abschnitt **Erweiterte Einstellungen**, Unterabschnitt **Selbstschutz** des Programmkonfigurationsfensters deaktiviert ist.

Sie können den Sicheren Zahlungsverkehr so einstellen, dass Webseiten von Banken und Zahlungssystemen automatisch erkannt werden.

Sicherer Zahlungsverkehr ist in Microsoft Internet Explorer 10 im Windows-8-Stil und in Microsoft Internet Explorer 10 nicht verfügbar, wenn in den Browser-Einstellungen das Kontrollkästchen **Erweiterten geschützten Modus aktivieren** (Enhanced Protected Mode) aktiviert ist. Sie können den Modus für den Sicherer Browser aus der Oberfläche von Kaspersky PURE starten.

➤ Gehen Sie folgendermaßen vor, um den Sicherer Zahlungsverkehr anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie im folgenden Fenster **Einstellungen** im Abschnitt **Schutz-Center** den Unterabschnitt **Sicherer Zahlungsverkehr** aus.
4. Aktivieren Sie das Kontrollkästchen **Sicherer Zahlungsverkehr aktivieren**.
5. Aktivieren Sie das Kontrollkästchen **Schwachstellen des Betriebssystems melden**, damit vor dem Start des sicheren Browsers gegebenenfalls eine Benachrichtigung über im Betriebssystem gefundene Schwachstellen erfolgt.
6. Gehen Sie folgendermaßen vor, um den Sicherer Zahlungsverkehr für eine bestimmte Webseite anzupassen:
 - a. Klicken Sie in der Liste **Webseiten von Banken und Zahlungssystemen** auf **Hinzufügen**.
Das Fenster **Website für Sicherer Zahlungsverkehr** wird geöffnet.
 - b. Geben Sie im folgenden Fenster im Feld **Website der Bank oder des Zahlungssystems** die Adresse der Website an, die im sicheren Browser geöffnet werden soll.

Der Adresse einer Webseite muss das Protokoll <https://> vorangestellt werden, das standardmäßig vom sicheren Browser verwendet wird.

- c. Im Feld **Beschreibung** kann der Name oder eine Beschreibung für diese Webseite angegeben werden.
- d. Wählen Sie aus, auf welche Weise der sichere Browser beim Öffnen dieser Website gestartet werden soll:
 - Wählen Sie die Variante **Aktion erfragen** aus, damit Kaspersky PURE jedes Mal vorschlägt, den sicheren Browser zu starten, wenn diese Website geöffnet wird.
 - Wählen Sie die Variante **Sicherer Browser automatisch starten** aus, damit Kaspersky PURE diese Website automatisch im sicheren Browser öffnet.
 - Wählen Sie die Variante **Sicherer Browser nicht starten** aus, um den Sicherer Zahlungsverkehr für diese Website zu deaktivieren.
7. Klicken Sie im Fenster **Einstellungen** auf **Übernehmen**.

SCHUTZ VOR PHISHING

Für den Schutz vor Phishing dient die Komponente Anti-Phishing, die 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.

Der Phishing-Schutz der Komponenten Web-Anti-Virus und IM-Anti-Virus kann zusätzlich angepasst werden.

➤ Gehen Sie folgendermaßen vor, um den Phishing-Schutz für Web-Anti-Virus anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie im folgenden Fenster **Einstellungen** unter **Schutz** den Abschnitt **Web-Anti-Virus** aus und klicken Sie auf **Einstellungen**.

Das Fenster **Web-Anti-Virus** wird geöffnet.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Links untersuchen** das Kontrollkästchen **Webseiten auf Phishing prüfen**.
5. Wenn in Anti-Phishing zur Untersuchung von Webseiten die heuristische Analyse verwendet werden soll, klicken Sie auf **Erweitert**.

Das Fenster **Anti-Phishing anpassen** wird geöffnet.

6. Aktivieren Sie im folgenden Fenster das Kontrollkästchen **Heuristische Analyse zur Phishing-Prüfung von Webseiten verwenden** und legen Sie eine Genauigkeitsstufe für die Untersuchung fest.
7. Klicken Sie im Fenster **Einstellungen** auf **Übernehmen**.

➡ Gehen Sie folgendermaßen vor, um den Phishing-Schutz für IM-Anti-Virus anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie im folgenden Fenster **Einstellungen** unter **Schutz** den Abschnitt **IM-Anti-Virus** aus.
4. Aktivieren Sie auf der rechten Fensterseite im Block **Untersuchungsmethoden** das Kontrollkästchen **Links mit der Datenbank für Phishing-Webadressen untersuchen**.
5. Klicken Sie im Fenster **Einstellungen** auf **Übernehmen**.

VIRTUELLE TASTATUR VERWENDEN

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

In solchen Situationen besteht die Gefahr, dass persönliche Informationen mithilfe von Hardware-Hooks oder mit Keyloggern (Programme, die Tasteneingaben registrieren) abgefangen werden.

Die virtuelle Tastatur ermöglicht es, das Abfangen von über die Tastatur eingegebenen Daten zu verhindern.

Die Virtuelle Tastatur schützt persönliche Daten nur dann vor Diebstahlversuchen, wenn Sie den Internetbrowser Microsoft Internet Explorer, Mozilla Firefox oder Google Chrome verwenden. Die Virtuelle Tastatur schützt nur bei Verwendung der genannten Internetbrowser davor, dass persönliche Daten bei der Eingabe abgefangen werden können.

Die virtuelle Tastatur ist in Microsoft Internet Explorer 10 im Metro-Stil und in Microsoft Internet Explorer 10 nicht verfügbar, wenn in den Browser-Einstellungen das Kontrollkästchen **Erweiterten geschützten Modus aktivieren** (Enhanced Protected Mode) aktiviert ist. In diesem Fall wird empfohlen, die virtuelle Tastatur über die Oberfläche von Kaspersky PURE zu öffnen.

Die Virtuelle Tastatur kann Ihre persönlichen Daten nicht schützen, wenn eine Webseite gehackt wurde und die Eingabe solcher Daten fordert, da die Informationen in diesem Fall dem Angreifer direkt in die Hände fallen.

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

Folgende Aktionen können nicht von der Virtuellen Tastatur verhindert werden: Erstellen von Screenshots mithilfe der **Druck**-Taste und mit anderen Tastenkombinationen, die in den Einstellungen des Betriebssystems festgelegt sind, sowie Erstellen von Screenshots mithilfe der DirectX-Technologie.

Die Virtuelle Tastatur besitzt folgende Besonderheiten:

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

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

Die Virtuelle Tastatur kann auf folgende Weise geöffnet werden:

- aus dem Kontextmenü des Programmsymbols im Infobereich der Taskleiste
- aus dem Programmhauptfenster
- aus dem Fenster des Browsers Microsoft Internet Explorer, Mozilla Firefox oder Google Chrome
- Mithilfe des Schnellstartsymbols der Virtuellen Tastatur im Eingabefeld auf Webseiten

Die Anzeige des Schnellstartsymbols in den Eingabefeldern von Webseiten kann angepasst werden.

- Mit einer Tastenkombination über eine Hardwaretastatur.

- ➔ *Um die Virtuelle Tastatur aus dem Kontextmenü des Programmsymbols im Infobereich der Taskleiste zu öffnen, wählen Sie im Kontextmenü des Programmsymbols den Punkt **Tools** → **Virtuelle Tastatur** aus (s. Abb. unten).*

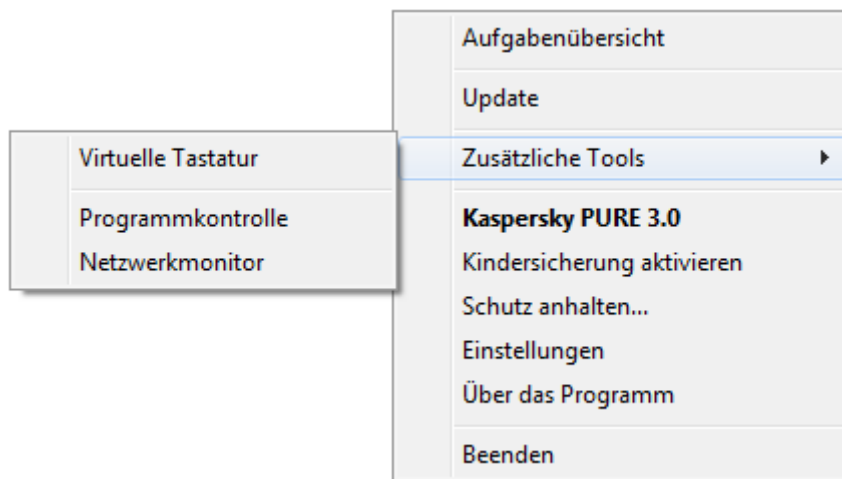



Abbildung 8. Kontextmenü des Symbols von Kaspersky PURE

- ➔ *Gehen Sie folgendermaßen vor, um die Virtuelle Tastatur vom Programmhauptfenster aus zu öffnen:*

1. Wählen Sie unten im Hauptfenster den Abschnitt **Password Manager**.
2. Klicken Sie im folgenden Fenster unten auf **Virtuelle Tastatur**.

- Um die virtuelle Tastatur von einem Browserfenster aus zu öffnen,

klicken Sie in der Symbolleiste von Microsoft Internet Explorer, Mozilla Firefox oder Google Chrome auf die Schaltfläche  **Virtuelle Tastatur**.

- Um die virtuelle Tastatur mithilfe der Computertastatur zu öffnen,

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

- Gehen Sie folgendermaßen vor, um die Anzeige des Schnellstartsymbols für die Virtuelle Tastatur in den Eingabefeldern von Webseiten anzupassen:

1. Öffnen Sie das Programmfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie im folgenden Fenster **Einstellungen** im Abschnitt **Schutz-Center** den Unterabschnitt **Sichere Dateneingabe** aus.
4. Aktivieren Sie auf der rechten Fensterseite im Block **Virtuelle Tastatur** das Kontrollkästchen **Schnellstartsymbol in Eingabefeldern anzeigen** und klicken Sie auf die Schaltfläche **Einstellungen**.

Das Fenster **Virtuelle Tastatur** wird geöffnet.

5. Legen Sie im folgenden Fenster fest, nach welchen Regeln das Schnellstartsymbol angezeigt werden soll.
 - Aktivieren Sie auf der Registerkarte **Kategorien** die Kontrollkästchen für die Webseiten-Kategorien, auf denen das Schnellstartsymbol in Eingabefeldern angezeigt werden soll.
 - Damit das Schnellstartsymbol in den Eingabefeldern der Webseiten angezeigt wird, die im sicheren Browser bei Verwendung des Sicheren Zahlungsverkehrs geöffnet werden, aktivieren Sie auf der Registerkarte **Kategorien** das Kontrollkästchen **Schnellstartsymbol in den Eingabefeldern für Sicheren Zahlungsverkehr anzeigen**.
 - Gehen Sie folgendermaßen vor, um die Anzeige des Schnellstartsymbols in den Eingabefeldern einer bestimmten Webseite zu aktivieren:
 - a. Klicken Sie auf der Registerkarte **Ausnahmen** in der Liste **Schnellstartsymbol auf folgenden Webseiten anzeigen** auf **Hinzufügen**.
Das Fenster **Schnellstartsymbol anzeigen** wird geöffnet.
 - b. Geben Sie im folgenden Fenster im Feld **Webadresse** die Adresse der Webseite an und wählen Sie aus, auf welche Weise das Schnellstartsymbol auf dieser Webseite angezeigt werden soll (**Schnellstartsymbol nur auf der angegebenen Webseite anzeigen** oder **Symbol auf der ganzen Website anzeigen**).

6. Klicken Sie im Fenster **Einstellungen** auf **Übernehmen**.

SCHUTZ FÜR DIE DATENEINGABE ÜBER EINE HARDWARETASTATUR

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

In solchen Situationen besteht die Gefahr, dass persönliche Informationen mithilfe von Hardware-Hooks oder mit Keyloggern (Programme, die Tasteneingaben registrieren) abgefangen werden.

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

Der Schutz für die Dateneingabe über eine Hardwaretastatur funktioniert nur in den Webbrowsern Microsoft Internet Explorer, Mozilla Firefox und Google Chrome. Bei Verwendung anderer Webbrowser sind Daten, die über eine Hardwaretastatur eingegeben werden, nicht vor Abfangversuchen geschützt.

Der Schutz für die Dateneingabe ist in Microsoft Internet Explorer 10 im Metro-Stil und in Microsoft Internet Explorer 10 nicht verfügbar, wenn in den Browser-Einstellungen das Kontrollkästchen **Erweiterten geschützten Modus aktivieren** (Enhanced Protected Mode) aktiviert ist.

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.

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.

Für den Schutz von Daten, die mithilfe einer Hardwaretastatur eingegeben werden, muss der Computer nach der Installation von Kaspersky PURE neu gestartet werden.

➤ Gehen Sie folgendermaßen vor, um den Schutz für Tastatureingaben anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie im folgenden Fenster **Einstellungen** im Abschnitt **Schutz-Center** den Unterabschnitt **Sichere Dateneingabe** aus.
4. Aktivieren Sie auf der rechten Fensterseite im Block **Schutz von Tastatureingaben** das Kontrollkästchen **Tastatureingaben schützen** und klicken Sie auf **Einstellungen**.

Das Fenster **Schutz für Tastatureingaben** wird geöffnet.

5. Legen Sie im folgenden Fenster einen Bereich für den Schutz von Tastatureingaben fest:
 - Aktivieren Sie auf der Registerkarte **Kategorien** die Kontrollkästchen für die Website-Kategorien, auf denen über die Tastatur eingegebene Daten geschützt werden sollen.
 - Damit Tastatureingaben auf jenen Websites geschützt werden, die im sicheren Browser im Modus Sicherer Zahlungsverkehr geöffnet werden, aktivieren Sie auf der Registerkarte **Kategorien** das Kontrollkästchen **Tastatureingaben für Sicheren Zahlungsverkehr schützen**.
 - Damit Tastatureingaben in Feldern zur Kennworteingabe auf allen Websites geschützt werden, aktivieren Sie auf der Registerkarte **Kategorien** das Kontrollkästchen **Kennwort-Eingabefelder auf allen Websites schützen**.
 - Gehen Sie folgendermaßen vor, um den Schutz für Tastatureingaben auf einer bestimmten Webseite zu aktivieren:
 - a. Klicken Sie auf der Registerkarte **Ausnahmen** in der Liste **Tastatureingaben auf folgenden Websites schützen** auf **Hinzufügen**.

Das Fenster **Geschützte Website** wird geöffnet.

- b. Geben Sie im folgenden Fenster im Feld **Webadresse** die Adresse der Website an und wählen Sie eine Variante für den Schutz von Tastatureingaben auf dieser Website aus (**Schutz nur auf der angegebenen Webseite aktivieren** oder **Schutz auf der ganzen Website aktivieren**).
6. Klicken Sie im Fenster **Einstellungen** auf **Übernehmen**.

SCHUTZ FÜR KENNWÖRTER

Kaspersky PURE speichert und schützt Ihre persönlichen Daten (beispielsweise Kennwörter, Benutzernamen, Kontaktdaten, finanzielle Informationen). Kaspersky PURE assoziiert Kennwörter und Benutzerkonten mit Anwendungen oder mit Webseiten, auf denen diese zur Autorisierung verwendet werden. Persönliche Daten werden in verschlüsselter Form in einem Speicher aufbewahrt, der durch ein Master-Kennwort geschützt ist. Wenn der Speicher entsperrt ist, können Sie ganz einfach Zugriff auf Ihre Kennwörter und Daten erhalten. Bei der Autorisierung auf Webseiten oder in Anwendungen können Kennwort, Benutzername und andere persönliche Daten mithilfe von Kaspersky PURE schnell und einfach eingegeben werden. Es besteht außerdem die Möglichkeit einer automatischen Anmeldung.

Ein Zugriff auf ihre persönlichen Daten ist von jedem Ihrer Geräte möglich. Dazu muss das Programm auf dem Gerät installiert sein und es muss eine Internetverbindung bestehen. Wenn ein Gerät nicht mit dem Internet verbunden ist, können Sie Ihre Kennwörter und Daten auf dem Gerät speichern. Wenn das Gerät wieder mit dem Internet verbunden wird, schlägt Kaspersky PURE Ihnen vor, Ihre Kennwörter und Daten mit der Kennwort-Datenbank auf den Remote-Servern zu synchronisieren.

Außerdem können Sie folgende Funktionen von Kaspersky PURE nutzen:

- Sichere Kennwörter für Benutzerkonten mithilfe des Kennwort-Generators erstellen.
- Aktuelle Kennwörter und persönliche Daten mit allen Ihren Geräten synchronisieren, auf denen Kaspersky PURE installiert ist.

IN DIESEM ABSCHNITT

Anmeldedaten für die automatische Anmeldung hinzufügen	51
Kennwort-Generator verwenden	52
Neues Benutzername/Kennwort-Paar hinzufügen	53

HINZUFÜGEN VON ANMELDEDATEN FÜR DIE AUTOMATISCHE AUTHENTIFIZIERUNG

Mithilfe des Programms können Sie eine automatische Anmeldung (Eingabe von Benutzername und Kennwort) auf Websites und in Anwendungen ausführen. Für die automatische Anmeldung verwendet das Programm Benutzerkonten.

Sie können zwei Arten von Benutzerkonten erstellen:

- Internet-Benutzerkonten, die zur Autorisierung auf Webseiten dienen.
- Benutzerkonten für Anwendungen, die zur Anmeldung in Anwendungen wie, beispielsweise, Mailprogrammen dienen.

➡ *Gehen Sie folgendermaßen vor, um vom Hauptfenster von Kaspersky PURE aus ein neues Benutzerkonto hinzuzufügen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Password Manager**.

Das Fenster des Password Managers wird geöffnet.

2. Klicken Sie auf **Kennwörter und Daten**.

Der Inhalt der Datenbank für den Password Manager wird angezeigt.

3. Öffnen Sie im Fenster des Password Managers den Abschnitt **Internet**.

Im rechten Fensterbereich erscheint ein Feld zur Angabe von Daten für das Benutzerkonto.

4. Geben Sie im oberen Fensterbereich im Feld **Kontoname** den Namen des Benutzerkontos ein. Klicken Sie auf die Schaltfläche .

Der Kontoname wird gespeichert.

5. Geben Sie im Feld **Link** die Adresse der Webseite an, auf der das Konto zur Anmeldung verwendet werden soll.
6. Geben Sie im Feld **Benutzername** den Benutzernamen ein, der auf dieser Website zur Anmeldung verwendet werden soll.
7. Geben Sie im Feld **Kennwort** das Kennwort für das Benutzerkonto ein. Um automatisch ein neues Kennwort zu erstellen, klicken Sie auf den Link **Kennwort-Generator**.
8. Klicken Sie im unteren Fensterbereich auf **Hinzufügen**.

Das neue Benutzerkonto erscheint in der Kontenliste im Abschnitt **Internet**.

➤ *Gehen Sie folgendermaßen vor, um ein neues Benutzerkonto für eine Anwendung hinzuzufügen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Password Manager**.

Das Fenster des Password Managers wird geöffnet.

2. Klicken Sie auf **Kennwörter und Daten**.

Der Inhalt der Datenbank für den Password Manager wird angezeigt.

3. Öffnen Sie den Abschnitt **Anwendungen**. Klicken Sie auf **Programm-Benutzerkonto hinzufügen**.

4. Geben Sie im oberen Fensterbereich im Feld **Kontoname** den Namen des Benutzerkontos ein. Klicken Sie auf die Schaltfläche .

Der Kontoname wird gespeichert.

5. Geben Sie im Feld **Anwendung** den Pfad der ausführbaren Datei der Anwendung an, in der das Benutzerkonto zur Anmeldung verwendet werden soll.
6. Geben Sie im Feld **Benutzername** den Benutzernamen ein, der in dieser Anwendung zur Anmeldung verwendet werden soll.
7. Geben Sie im Feld **Kennwort** das Kennwort für das Benutzerkonto ein. Um automatisch ein neues Kennwort zu erstellen, klicken Sie auf den Link **Kennwort-Generator**.
8. Klicken Sie im unteren Fensterbereich auf **Hinzufügen**.

Das neue Benutzerkonto erscheint in der Kontenliste im Abschnitt **Anwendungen**.

KENNWORT-GENERATOR VERWENDEN

Die Datensicherheit ist direkt von der Stärke der Kennwörter abhängig. In folgenden Fällen können Daten einem Risiko unterliegen:

- Es wird ein Kennwort für alle Benutzerkonten verwendet.
- Das verwendete Kennwort ist zu einfach.
- Als Kennwort werden Informationen verwendet, die sich leicht erraten lassen (z. B. Namen von Familienmitgliedern oder ihre Geburtstage).

Um die Datensicherheit zu gewährleisten, kann Kaspersky PURE mithilfe eines Kennwort-Generators individuelle und sichere Kennwörter für Benutzerkonten generieren.

Ein Kennwort gilt als sicher, wenn es aus mehr als vier Zeichen besteht und Sonderzeichen, Ziffern, Groß- und Kleinbuchstaben darin verwendet werden.

➔ *Gehen Sie folgendermaßen vor, um mit dem Kennwort-Generator ein sicheres Kennwort zu erstellen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Password Manager**.

Das Fenster des Password Managers wird geöffnet.

2. Klicken Sie auf **Kennwort-Generator**.

Der Kennwort-Generator kann auch direkt beim Festlegen eines Kennworts für ein Benutzerkonto eingesetzt werden. Verwenden Sie den Link **Kennwort-Generator** im Kontoverwaltungsbereich neben dem Feld zur Kennworteingabe, um den Kennwort-Generator zu öffnen.

3. Geben Sie im folgenden Fenster **Kennwort-Generator** im Feld **Länge des Kennworts** an, aus wie vielen Zeichen das Kennwort bestehen soll.

Das Kennwort darf 4 bis 99 Zeichen lang sein. Je länger ein Kennwort ist, desto sicherer ist es.

4. Passen Sie bei Bedarf zusätzliche Einstellungen für den Kennwort-Generator an. Aktivieren / deaktivieren Sie dazu im Abschnitt **Erweiterte Einstellungen** die entsprechenden Kontrollkästchen.

5. Klicken Sie auf **Generieren**.

Das erstellte Kennwort wird im Feld **Kennwort** angezeigt.

NEUES BENUTZERNAME/KENNWORT-PAAR HINZUFÜGEN

Es kann notwendig sein, auf einer Webseite bzw. in einer Anwendung mehrere Benutzername-/Kennwort-Paare für die Anmeldung zu verwenden. Beispielsweise können Sie mehrere Postfächer bei einem E-Mail-Server nutzen oder mehrere Benutzer eines Computers können Konten im gleichen sozialen Netzwerk besitzen. In solchen Fällen kann mit Kaspersky PURE ein Benutzerkonto erstellt werden, das mit einer bestimmten Webseite oder Anwendung verknüpft wird, und für dieses Konto können mehrere Benutzername-/Kennwort-Paare angegeben werden.

Wenn die angegebene Webseite oder Anwendung geladen wird, bietet Kaspersky PURE die entsprechenden Benutzername-/Kennwort-Paare zur Auswahl an, um die Berechtigungsfelder auszufüllen.

Kaspersky PURE erkennt einen neuen Benutzernamen automatisch, wenn dieser zum ersten Mal verwendet wird, und schlägt vor, ihn zum Benutzerkonto für diese Anwendung bzw. Webseite hinzuzufügen. Ein neues Benutzername-/Kennwort-Paar für ein Konto kann manuell hinzugefügt und später geändert werden. Außerdem können Sie das gleiche Benutzername-/Kennwort-Paar für unterschiedliche Konten verwenden.

➔ *Gehen Sie folgendermaßen vor, um eine neues Benutzername/Kennwort-Paar für ein Benutzerkonto hinzuzufügen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Password Manager**.

Das Fenster des Password Managers wird geöffnet.

2. Klicken Sie auf **Kennwörter und Daten**.


Der Inhalt der Datenbank für den Password Manager wird angezeigt.

3. Öffnen Sie den Abschnitt **Internet** oder **Anwendungen**, je nachdem, zu welchem Konto Sie den Benutzernamen und das Kennwort hinzufügen möchten.

4. Wählen Sie in der Liste das erforderliche Benutzerkonto aus und klicken Sie auf die Schaltfläche .

5. Wählen Sie im folgenden Menü den Punkt **Benutzername hinzufügen**.

6. Tragen Sie im Feld **Benutzername** den Benutzernamen und im Feld **Kennwort** das Kennwort ein.

Um einen Benutzernamen und ein Kennwort hinzuzufügen, die bereits in anderen Konten verwendet werden, klicken Sie auf die Schaltfläche  im Feld **Benutzername**. Wählen Sie im folgenden Fenster **Benutzerkonten für die Verknüpfung auswählen** ein Konto aus, das den entsprechenden Benutzernamen enthält, und klicken Sie auf **Verknüpfen**.

7. Wenn Sie möchten, dass der Password Manager den Benutzernamen und das Kennwort, die hinzugefügt wurden, automatisch auf einer Webseite oder in einer Anwendung zum Ausfüllen verwendet, aktivieren Sie das Kontrollkästchen **Automatische Anmeldung** unten im Kontoverwaltungsbereich.

Wenn der Password Manager den Benutzernamen und das Kennwort nicht zum automatischen Ausfüllen von Berechtigungsfeldern verwenden soll, deaktivieren Sie das Kontrollkästchen **Automatische Anmeldung**. Um das automatische Ausfüllen zu verwenden, müssen Sie in diesem Fall den hinzugefügten Benutzernamen und das Kennwort aus dem Kontextmenü des Programmsymbols oder der Titelleisten-Schaltfläche auswählen.

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

Die Anzahl der Benutzernamen, die zu einem Konto hinzugefügt worden sind, wird in der Kontenliste angezeigt.

DATEN VERSCHLÜSSELN

Um private Daten vor unbefugtem Zugriff zu schützen, wird empfohlen, diese in verschlüsselter Form in einem Spezialcontainer zu speichern.

In der Grundeinstellung steht Ihnen nach der Installation von Kaspersky PURE ein vordefinierter Container mit Standardeinstellungen zur Verfügung. Es muss ein Kennwort festgelegt werden, um diesen Container zu verwenden. Sie können Container mit entsprechenden Einstellungen erstellen.

Um Daten zu schützen, müssen sie in einen Container verschoben und verschlüsselt werden. Danach ist für den Zugriff auf Daten, die sich in diesem Container befinden, die Eingabe des Kennworts erforderlich.

➔ *Gehen Sie folgendermaßen vor, um einen verschlüsselten Container anzulegen:*

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

2. Klicken Sie im folgenden Fenster auf die die Schaltfläche **Container erstellen** (s. Abb. unten).

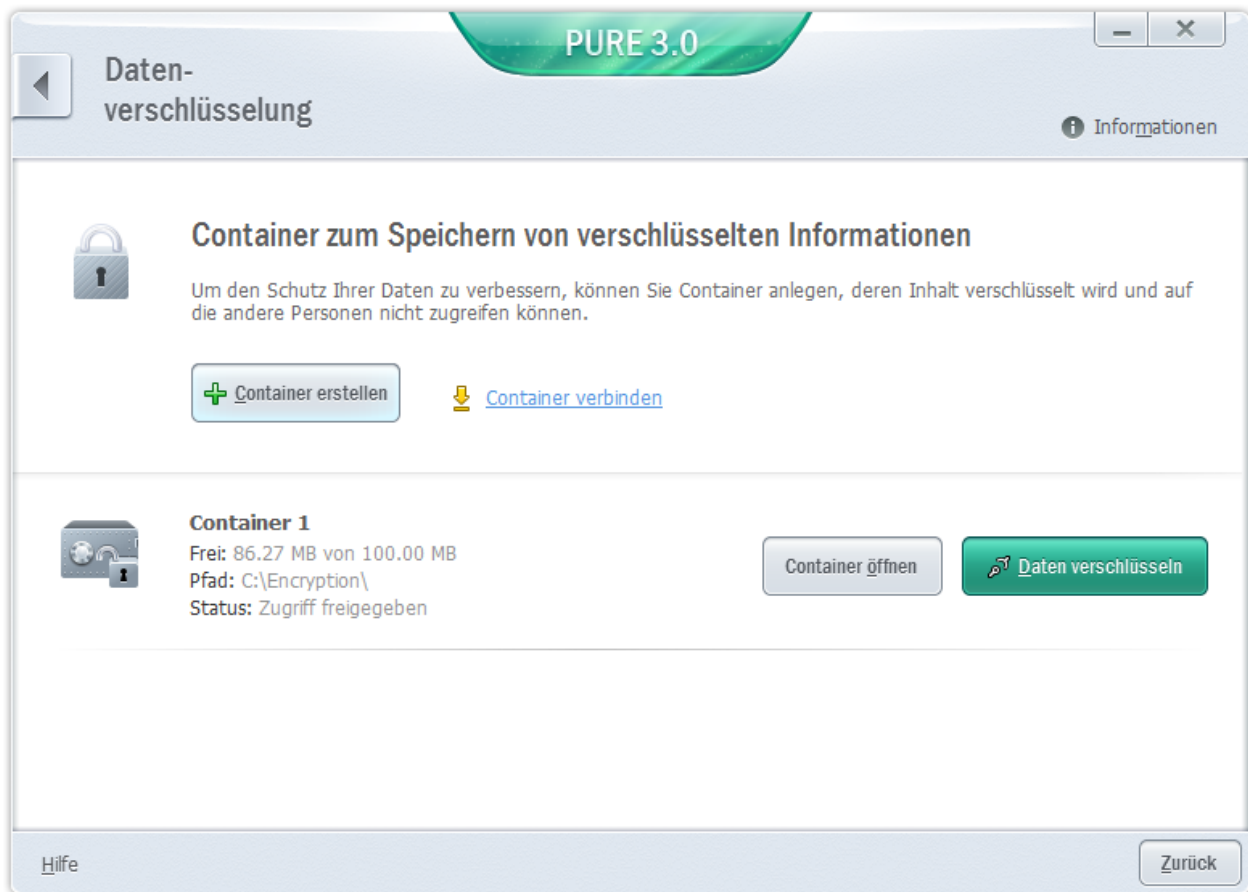


Abbildung 9. Fenster **Datenverschlüsselung**

3. Geben Sie im folgenden Fenster **Verschlüsselten Container erstellen** die Einstellungen für den neuen Container an.
 4. Klicken Sie auf **OK**.
- *Gehen Sie folgendermaßen vor, um Daten in einem Container zu speichern:*
1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
 2. Wählen Sie im folgenden Fenster einen Container aus der Liste aus und klicken Sie auf **Container öffnen**.
Der Container wird im Fenster von Microsoft Windows Explorer geöffnet.
 3. Speichern Sie die Daten, die verschlüsselt werden sollen, in dem Container.
 4. Klicken Sie im Fenster **Datenverschlüsselung** auf **Daten verschlüsseln**.
- *Gehen Sie folgendermaßen vor, um Zugriff auf die Daten in einem Container zu erhalten:*
1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
 2. Wählen Sie im folgenden Fenster einen Container aus der Liste aus und klicken Sie auf **Daten entschlüsseln**.
 3. Geben Sie im folgenden Fenster das Kennwort für den Zugriff auf den Container ein.
 4. Klicken Sie im Fenster **Datenverschlüsselung** auf **Container öffnen**.

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 PURE ist der Assistent zum Löschen von nicht benötigten Daten enthalten.

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

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

Der Assistent löscht nicht nur die nicht mehr benötigten Dateien aus dem System, er entfernt auch Dateien, die vertrauliche Daten (Kennwörter, Benutzernamen und Informationen aus Anmeldeformularen) enthalten können. Trotzdem wird empfohlen, den Assistenten zum Löschen von Aktivitätsspuren (s. S. [60](#)) zu verwenden, um solche Daten vollständig zu entfernen.

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

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Zusätzliche Funktionen**.

Das Fenster **Zusätzliche Funktionen** wird geöffnet (s. Abb. unten).

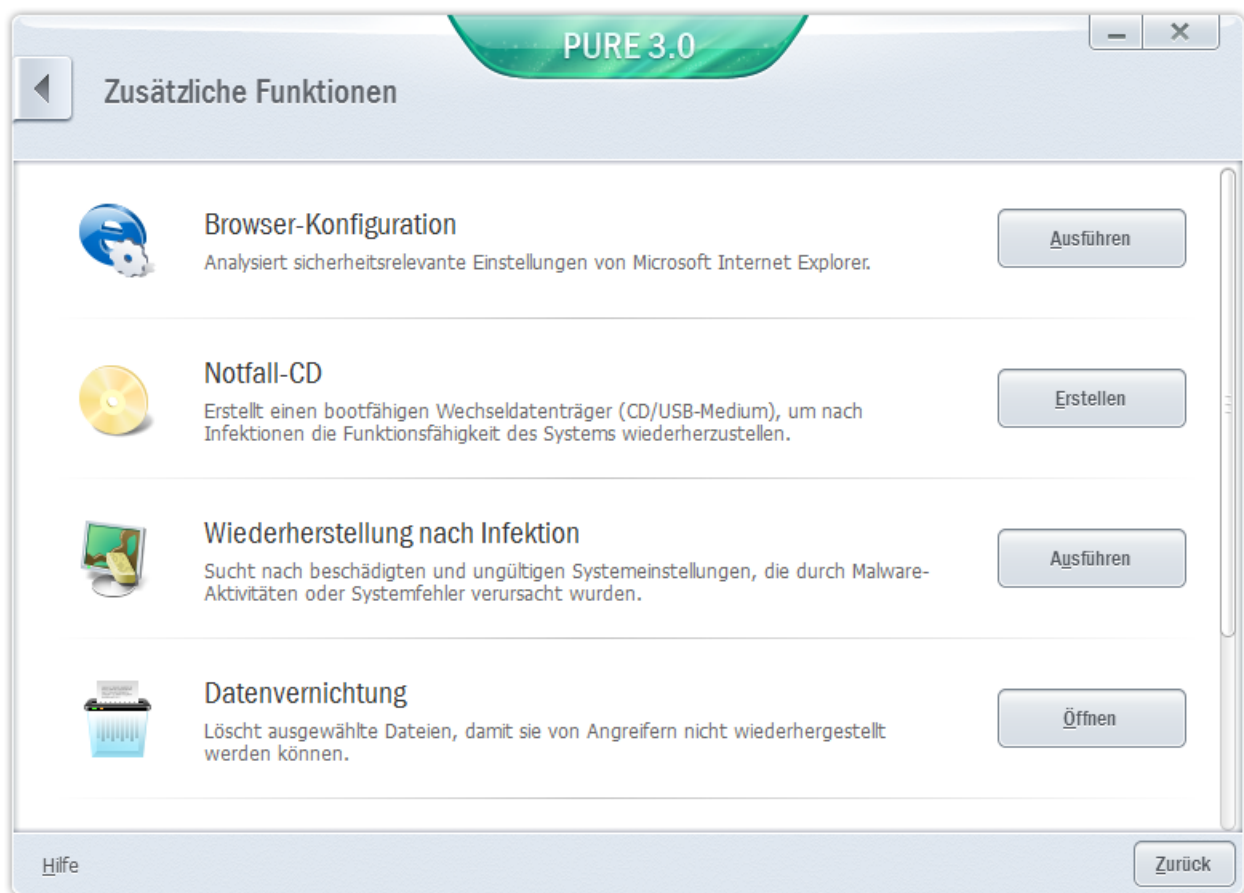


Abbildung 10. Fenster **Zusätzliche Funktionen**

3. Klicken Sie im folgenden Fenster unter **Löschen von nicht benötigten Daten** auf **Ausführen**.

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

Details zu den einzelnen Schritten des Assistenten.

Schritt 1. Assistent starten

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

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

Schritt 2. Suche nach nicht benötigten Daten

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

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

Nachdem die Suche nach nicht benötigten Daten abgeschlossen wurde, zeigt der Assistent eine Liste mit möglichen Aktionen an.

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

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

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

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

Schritt 4. Nicht benötigte Informationen löschen

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

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

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

Schritt 5. Assistent abschließen

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

UNWIDERRUFLICHES LÖSCHEN VON DATEN

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

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

Kaspersky PURE kann Daten von folgenden Datenträgern unwiderrufflich löschen:

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

Sie können jene Daten löschen, für die Ihr Benutzerkonto eine Zugriffsberechtigung besitzt. Vergewissern Sie sich vor dem Löschen von Daten, dass diese Daten nicht von anderen Programmen verwendet werden.

➤ *Gehen Sie folgendermaßen vor, um Daten unwiderrufflich zu löschen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Zusätzliche Funktionen**.

Das Fenster **Datenvernichtung** wird geöffnet (s. Abb. unten).

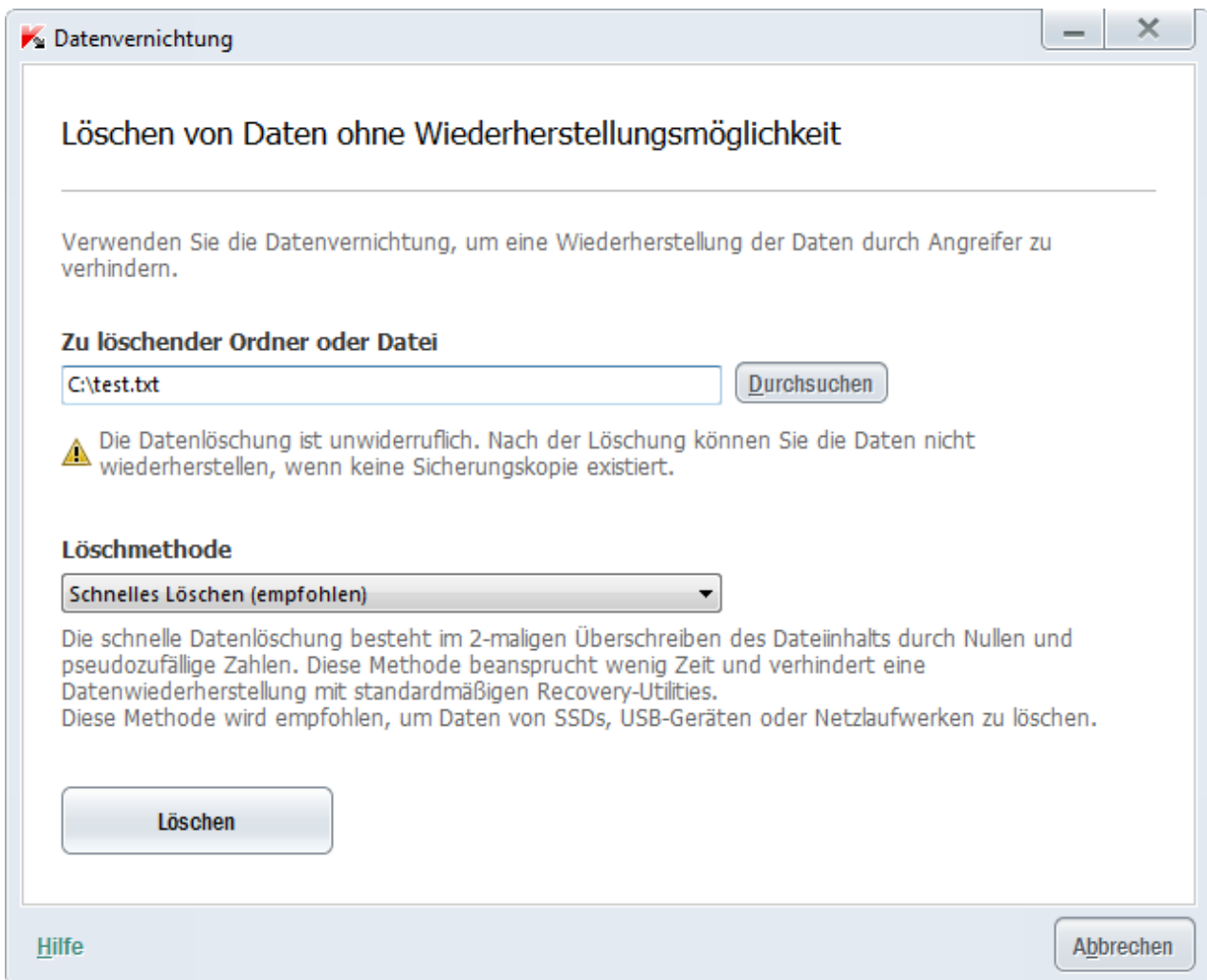


Abbildung 11. Fenster **Datenvernichtung**

3. Klicken Sie im folgenden Fenster unter **Datenvernichtung** auf **Öffnen**.
4. Klicken Sie im folgenden Fenster **Datenvernichtung** auf **Durchsuchen** und wählen Sie im folgenden Fenster **Datei oder Ordner auswählen** ein Objekt aus.

Das Löschen von Systemdateien kann zu Funktionsstörungen im Betriebssystem führen. Wenn Systemdateien oder Ordner zum Löschen ausgewählt werden, fordert das Programm eine zusätzliche Bestätigung an.

5. Werden Sie in der Dropdown-Liste **Löschmethode** einen Algorithmus zur Datenlöschung aus.

Es wird empfohlen, die Methoden **Schnelles Löschen** oder **GOST R 50739-95** zu verwenden, um Daten von **SSDs, USB-Geräten und Netzlaufwerken** zu löschen. Die übrigen Lösch-Algorithmen können zu einer **Beschädigung von Netzlaufwerken oder Wechselmedien** führen.

6. Bestätigen Sie das Löschen von Daten im folgenden Fenster durch Klick auf **OK**. Wenn bestimmte Dateien nicht gelöscht wurden, wiederholen Sie die Löschung durch Klick auf **Wiederholen**. Klicken Sie auf **Beenden**, um ein anderes Objekt zum Löschen auszuwählen.

AKTIVITÄTSSPUREN 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 Websites
- Angaben über den Start von Programmen, Daten über das Öffnen und Speichern von Dateien
- Einträge im Systembericht von Microsoft Windows
- Sonstige Informationen über Benutzeraktionen

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

Kaspersky PURE bietet einen Assistenten, der die Aktivitätsspuren des Benutzers im System löschen kann.

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

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Zusätzliche Funktionen**.
3. Klicken Sie im folgenden Fenster im Block **Löschen von Aktivitätsspuren** auf die Schaltfläche **Ausführen**.

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 **Diagnose der Spuren von Benutzeraktivität durchführen** gewählt wurde, und klicken Sie auf **Weiter**, um den Assistenten zu starten.

Schritt 2. Nach Aktivitätsspuren suchen

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 die gefundenen Aktivitätsspuren und mögliche Aktionen, um sie zu beseitigen (s. Abb. unten).

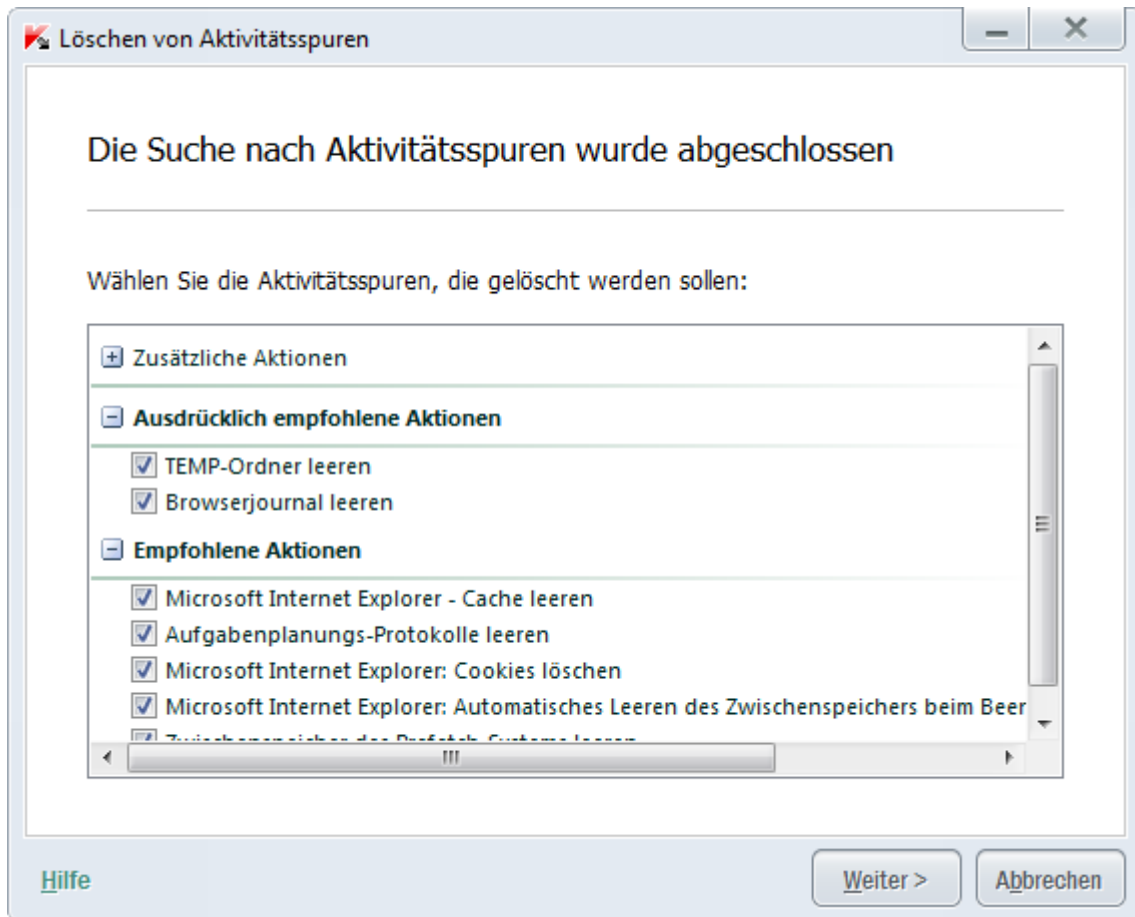


Abbildung 12. Erkannte Aktivitätsspuren und Empfehlungen zu deren Beseitigung

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

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

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

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

Schritt 4. Aktivitätsspuren löschen

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

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

Schritt 5. Assistent abschließen

Damit das Löschen von Aktivitätsspuren in Zukunft automatisch erfolgt, wenn Kaspersky PURE beendet wird, aktivieren Sie beim letzten Schritt des Assistenten das Kontrollkästchen **Löschen von Aktivitätsspuren jedes Mal beim Beenden von Kaspersky PURE ausführen**. Wenn Sie planen, die Aktivitätsspuren künftig selbst zu beseitigen, lassen Sie dieses Kontrollkästchen deaktiviert.

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

BACKUP

Die wichtigste Maßnahme, um wichtige Daten vor Verlust zu schützen, besteht in der Sicherung auf einem zuverlässigen Datenträger. Kaspersky PURE erlaubt es, in einem festgelegten Speicher automatisch Sicherungskopien von ausgewählten Daten anzulegen. Die Sicherung erfolgt nach Zeitplan oder manuell.

Mithilfe der Verwaltung (s. Abschnitt "Fernverwaltung für den Schutz des Heimnetzwerks" auf S. 41) können Sie Backup-Aufgaben auf den Computern des Heimnetzwerks starten sowie den Ausführungsstatus dieser Aufgaben kontrollieren.

Zum Anlegen von Sicherungskopien können Sie folgende Speicherarten verwenden:

- lokaler Datenträger
- Wechselmedium (z. B. externe Festplatte)
- Netzlaufwerk
- FTP-Server
- Online-Speicher

IN DIESEM ABSCHNITT

Datensicherung	62
Daten aus einer Sicherheitskopie wiederherstellen	63
Verwendung eines Online-Speichers	64

DATENSICHERUNG

➔ *Gehen Sie folgendermaßen vor, um eine Sicherung auszuführen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.
2. Klicken Sie im folgenden Fenster **Backup** auf **Backup-Aufgabe erstellen**.

Dadurch wird der Assistent für neue Backup-Aufgaben gestartet.

Details zu den einzelnen Schritten des Assistenten:

- a. Führen Sie im Fenster zur Auswahl des Datentyps eine der folgenden Aktionen aus:
 - Wählen Sie für eine schnelle Konfiguration einen der voreingestellten Datentypen aus (Dateien aus den Ordner Meine Dokumente und Desktop, Video, Bilder, Musikdateien).
 - Wählen Sie die Variante **Benutzerdefinierte Dateien** aus, um die zu sichernden Dateien manuell auszuwählen.

- b. Wenn Sie beim vorherigen Schritt die Variante **Benutzerdefinierte Dateien** ausgewählt haben, geben Sie im Fenster zur Auswahl der Dateien die zu sichernden Dateien oder Dateikategorien an.

Bei einer Sicherung unter Verwendung eines Online-Speichers legt Kaspersky PURE keine Sicherungskopien für jene Dateitypen an, die durch die Dropbox-Nutzungsregeln ausgenommen sind (s. Abschnitt "Verwendung eines Online-Speichers" auf S. 64).

- c. Führen Sie im Fenster Speicher auswählen eine der folgenden Aktionen aus:

- Wählen Sie einen voreingestellten Speicher aus, in dem Sicherungskopien angelegt werden sollen.

Standardmäßig erlaubt Kaspersky PURE das Anlegen von Sicherungskopien auf lokalen Datenträgern und Wechselmedien sowie im Online-Speicher.

Bevor Sie einen Online-Speicher zur Sicherung Ihrer Daten nutzen, muss der Online-Speicher aktiviert werden (s. Abschnitt "Verwendung eines Online-Speichers" auf S. 64).

- Wählen Sie einen vorhandenen Netzwerk-Speicher aus.
- Klicken Sie auf **Speicher hinzufügen**, um einen neuen Netzwerk-Speicher zu erstellen.

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

- d. Legen Sie im Fenster Zeitplan die Startbedingungen für die Aufgabe fest.

Wenn Sie eine einmalige Sicherung vornehmen möchten, aktivieren Sie das Kontrollkästchen **Automatisch nach Zeitplan starten** nicht.

- e. Geben Sie im Fenster **Übersicht** einen Namen für die neue Aufgabe an, aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten** und klicken Sie auf **Beenden**.

DATEN AUS EINER SICHERHEITSKOPIE WIEDERHERSTELLEN

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

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.
2. Wählen Sie den Abschnitt **Daten wiederherstellen** aus.
3. Wählen Sie den Speicher, in dem sich die erforderlichen Sicherungskopien befinden, und klicken Sie auf **Daten wiederherstellen**.

Das Fenster **Daten wiederherstellen aus Speicher** wird geöffnet.

4. Führen Sie im nächsten Fenster folgende Aktionen aus:
 - a. Wählen Sie in der Dropdown-Liste **Backup-Aufgabe** die Aufgabe aus, bei deren Ausführung die erforderlichen Sicherungskopien erstellt wurden.
 - b. Wählen Sie in der Dropdown-Liste **Datum** den Zeitpunkt aus, zu dem die erforderlichen Sicherungskopien erstellt wurden.
 - c. Wählen Sie in der Dropdown-Liste **Kategorie** den Typ der Dateien aus, die wiederhergestellt werden sollen.

- Wählen Sie in der Liste der Dateien im unteren Fensterbereich die Dateien aus, die wiederhergestellt werden sollen. Aktivieren Sie dazu in der Liste die Kontrollkästchen der entsprechenden Dateien.

Kaspersky PURE kann Daten nicht aus einem Online-Speicher wiederherstellen, wenn diese Daten über die Dropbox-Weboberfläche gelöscht wurden.

- Klicken Sie auf **Daten wiederherstellen**.

Das Fenster **Wiederherstellung** wird geöffnet.

- Wählen Sie im Fenster **Wiederherstellung** aus, wo die wiederherzustellenden Dateien gespeichert werden sollen (im Ausgangsordner oder in einem angegebenen Ordner).

- Klicken Sie auf **Ausgewählte Daten wiederherstellen**.

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

Beim Fund einer anderen Version einer für die Wiederherstellung ausgewählten Datei schlägt das Programm vor, die vorhandene Datei durch eine Sicherungskopie zu ersetzen bzw. die beiden Dateien zu speichern.

VERWENDUNG EINES ONLINE-SPEICHERS

Der Online-Speicher ermöglicht das Speichern der Sicherheitskopien Ihrer Daten auf einem Remote-Server mithilfe des Webdienstes Dropbox.

Um einen Online-Speicher verwenden zu können, muss auf der Dropbox-Webseite ein Benutzerkonto angelegt werden. Dropbox ist ein Anbieter für Backup-Dienste.

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

Ein standardmäßiges Dropbox-Konto bietet bis zwei Gigabyte Speicherplatz auf einem Remote-Server. Bei Bedarf können Sie die Größe des Online-Speichers zu Bedingungen vergrößern, die vom Backup-Dienstleister festgelegt werden. Ausführliche Informationen über die Nutzungsbedingungen für den Webdienst finden Sie auf der Dropbox-Website.

Bevor Sie einen Online-Speicher zur Sicherung Ihrer Daten nutzen, muss der Online-Speicher aktiviert werden.

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

- Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.
- Klicken Sie im folgenden Fenster **Backup** auf **Backup-Aufgabe erstellen**.
Dadurch wird der Assistent für neue Backup-Aufgaben gestartet.
- Wählen Sie im Fenster Datentyp eine Datenkategorie aus oder geben Sie die zu sichernden Dateien manuell an.
- Wählen Sie im Fenster Speicher auswählen einen Online-Speicher aus und klicken Sie auf **Jetzt aktivieren**.

Ein Fenster für die Anmeldung im Dropbox-Konto wird geöffnet.

- Führen Sie hier eine der folgenden Aktionen aus:
 - Falls Sie noch kein Dropbox-Konto besitzen, registrieren Sie sich auf der Dropbox-Webseite.

b. Wenn Sie schon auf der Dropbox-Webseite registriert sind, melden Sie sich mit Ihrem Dropbox-Konto an.

Um die Aktivierung des Online-Speichers abzuschließen, bestätigen Sie, dass Kaspersky PURE Ihr Dropbox-Benutzerkonto für die Ausführung des Backups und Datenwiederherstellung verwenden darf. Kaspersky PURE speichert die Sicherungskopien gespeicherter Daten in einem separaten Ordner, der im Ordner für Anwendungen von Dropbox 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.

KENNWORTSCHUTZ FÜR DIE EINSTELLUNGEN VON KASPERSKY PURE

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

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

- Programmeinstellungen anpassen
- Backup verwalten
- Fernverwaltung der Sicherheit auf den Computern eines Heimnetzwerks (Das Kennwort muss auf allen Computern identisch sein.)
- Kindersicherung verwalten
- Programm beenden
- Programm deinstallieren

➡ *Gehen Sie folgendermaßen vor, um den Zugriff auf Kaspersky PURE durch ein Kennwort zu schützen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie rechts oben auf den Link **Einstellungen**.

Das Programmkonfigurationsfenster wird geöffnet.

3. Wählen Sie im Programmkonfigurationsfenster oben die Registerkarte **Kennwort** aus (s. Abb. unten).

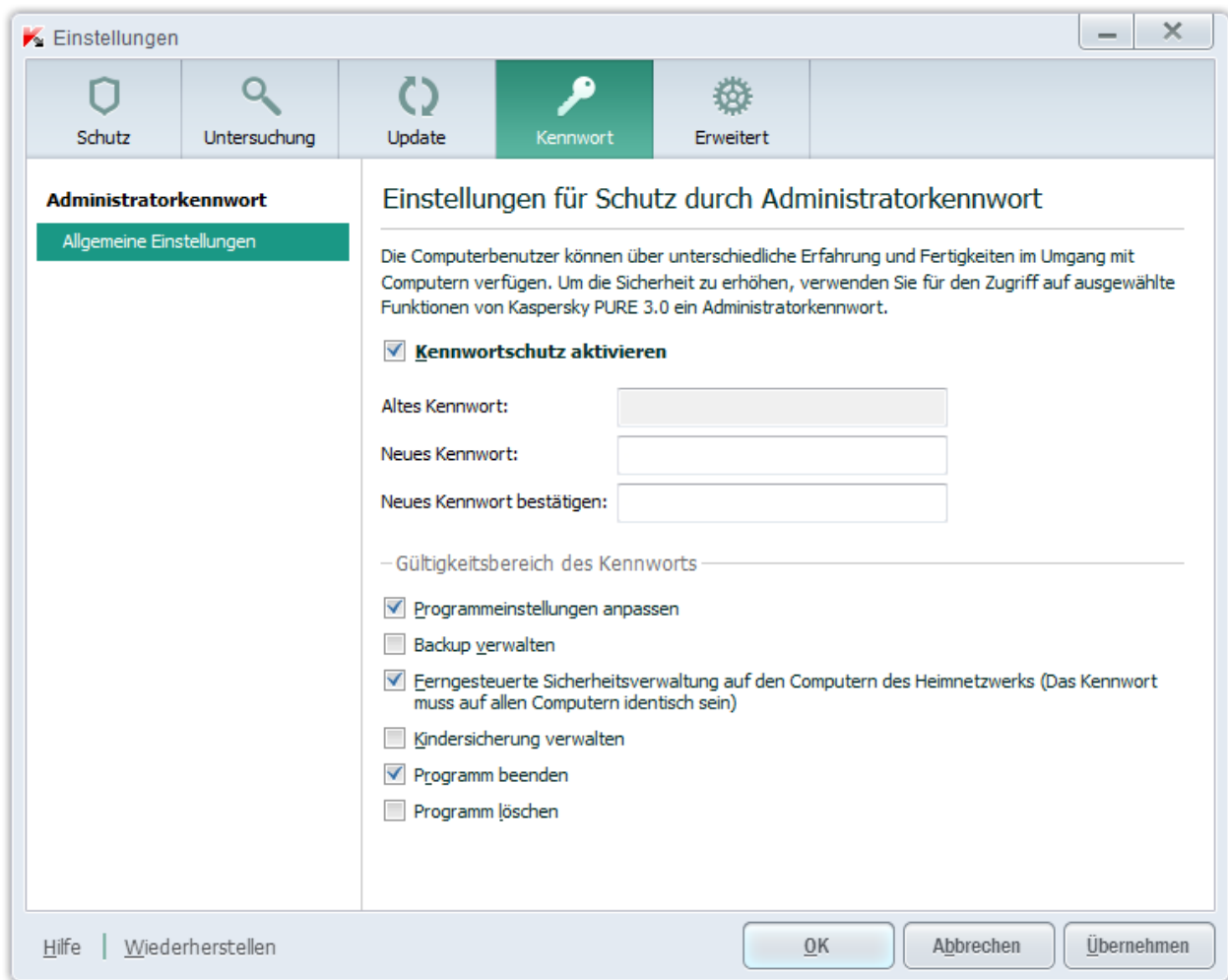


Abbildung 13. Fenster **Einstellungen**, Abschnitt **Kennwort**

4. Aktivieren Sie im rechten Fensterbereich das Kontrollkästchen **Kennwortschutz aktivieren** und füllen Sie die Felder **Neues Kennwort** und **Kennwort bestätigen** aus.
5. Wenn Sie ein vorhandenes Kennwort ändern möchten, tragen Sie es im Feld **Altes Kennwort** ein.
6. Geben Sie im Block **Gültigkeitsbereich des Kennworts** an, welche Vorgänge durch das Kennwort geschützt werden sollen.
7. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Ein vergessenes Kennwort kann nicht wiederhergestellt werden. Sollten Sie das Kennwort vergessen, so muss Kontakt mit dem Technischen Support aufgenommen werden, um erneut Zugriff auf Kaspersky PURE zu erhalten.

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 drohen 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 Dateien, die von Malware infiziert sind.
- unverhältnismäßig lange Verwendung des Computers und damit verbundene gesundheitliche Risiken.
- Kontakte mit Fremden, die sich als Gleichaltrige ausgeben und persönliche Informationen über ein Kind erhalten können (beispielsweise echter Name, Adresse, Zeiträume, in denen niemand zu Hause ist).

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

- Zeitliche Beschränkung für die Verwendung des Computers und Internets.
- Erstellen von Listen für zum Start erlaubte und verbotene Programme sowie vorübergehende Beschränkung des Starts von erlaubten Programmen.
- Erstellen von Listen mit Websites, 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 Websites 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 über Instant Messenger und in sozialen Netzwerken erlaubt oder verboten wird.
- Kontrolle des Texts von Nachrichten, die mit Instant Messengern und in sozialen Netzwerken ausgetauscht werden.
- Verbot des Sendens von bestimmten persönlichen Daten.
- Suche nach bestimmten Schlüsselwörtern im Nachrichtentext.

Die Beschränkungen können einzeln aktiviert werden, wodurch sich die Kindersicherung flexibel auf unterschiedliche Benutzer anpassen lässt. Für jedes Benutzerkonto können Berichte angezeigt werden, die Ereignisse der kontrollierten Kategorien für einen bestimmten Zeitraum umfassen.

IN DIESEM ABSCHNITT

Kindersicherung anpassen.....	67
Bericht über die Aktionen eines Benutzers anzeigen	68

KINDERSICHERUNG ANPASSEN

Wenn der Zugriff auf die Einstellungen von Kaspersky PURE noch nicht durch ein Kennwort geschützt wurde (s. S. [65](#)), schlägt Kaspersky PURE beim ersten Start der Kindersicherung vor, ein Kennwort festzulegen, damit die Kontrolleinstellungen nicht von Unbefugten geändert werden können. Anschließend können Sie Beschränkungen anpassen, die die Verwendung des Computers und des Internets für alle Benutzerkonten des Computers regulieren.

➤ *Gehen Sie folgendermaßen vor, um die Kindersicherung für ein Benutzerkonto anzupassen:*

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

Das Fenster **Computerbenutzer** wird geöffnet. Es enthält alle Benutzerkonten, die auf dem Computer angelegt wurden.

2. Klicken Sie für das entsprechende Benutzerkonto auf die Schaltfläche **Kontrollstufe auswählen**.

3. Führen Sie im folgenden Fenster **Kindersicherung** eine der folgenden Aktionen aus:

- Wählen Sie eine vordefinierte Kontrollstufe aus (**Datenerfassung**, **Profil "Kind"** oder **Profil "Jugendlicher"**).
- Legen Sie die Einschränkungen manuell fest:
 - a. Wählen Sie den Punkt **Benutzerdefinierte Einschränkungen** aus.

- b. Klicken Sie auf **Einstellungen**.

Das Fenster **Kindersicherung** wird geöffnet

- c. Wählen Sie im folgenden Fenster auf der Registerkarte **Einstellungen** auf der linken Seite einen Beschränkungstyp aus und passen Sie rechts die Kontrolleinstellungen an.

- d. Klicken Sie auf **OK**, um die vorgenommenen Änderungen zu speichern.

4. Klicken Sie im Fenster **Kindersicherung** auf **OK**.

BERICHT ÜBER DIE AKTIONEN EINES BENUTZERS ANZEIGEN

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

➤ *Gehen Sie folgendermaßen vor, um einen Bericht über die Aktionen eines kontrollierten Benutzers anzuzeigen:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.

3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf die Schaltfläche



Das Fenster **Kindersicherung** wird geöffnet

4. Wählen Sie die Registerkarte **Berichte**.
5. Wählen Sie links im Fenster einen Abschnitt mit dem Namen einer Kategorie für kontrollierte Aktionen oder Inhalte aus (z. B. **Verwendung des Internets** oder **Persönliche Daten**).

Auf der rechten Fensterseite befindet sich ein Bericht über die kontrollierten Aktionen und Inhalte.

COMPUTERSCHUTZ ANHALTEN UND FORTSETZEN

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

➤ *Gehen Sie folgendermaßen vor, um den Computerschutz anzuhalten:*

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

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

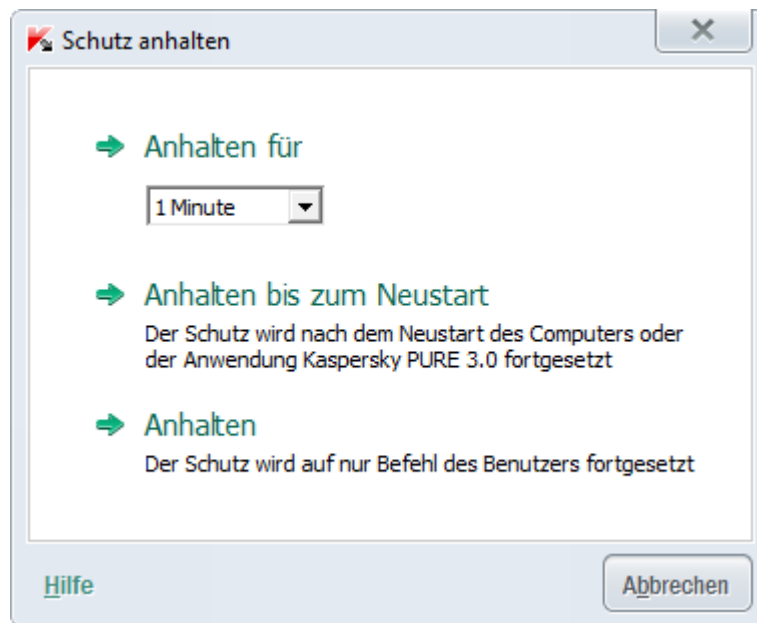


Abbildung 14. Fenster **Schutz anhalten**

2. Wählen Sie im Fenster **Schutz anhalten** den Zeitraum, nach dem der Schutz wieder aktiviert werden soll:
 - **Anhalten für...** – Der Schutz wird nach Ablauf des Zeitraums wieder aktiviert, der in der Dropdown-Liste festgelegt wird.
 - **Anhalten bis zum Neustart** – Der Schutz wird nach dem Neustart des Programms oder des Systems aktiviert (unter der Bedingung, dass der automatische Programmstart aktiviert ist).
 - **Anhalten** – Der Schutz wird wieder aktiviert, wenn Sie ihn fortsetzen.

➔ Um den Computerschutz fortzusetzen,

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

BERICHT ÜBER DEN COMPUTERSCHUTZ ANZEIGEN

Kaspersky PURE führt Berichte über die Arbeit der einzelnen Schutzkomponenten. Der Bericht bietet statistische Informationen über den Computerschutz (Sie können beispielsweise nachsehen, wie viele schädliche Objekte in einem bestimmten Zeitraum gefunden und neutralisiert wurden, wie oft das Programm in diesem Zeitraum aktualisiert wurde und wie viele Spam-Mails gefunden wurden).

➔ Gehen Sie folgendermaßen vor, um einen Bericht über den Computerschutz anzuzeigen:

1. Klicken Sie im Programmhauptfenster auf **Computersicherheit**.

Das Fenster **Computersicherheit** wird geöffnet.

2. Klicken Sie im oberen Fensterbereich auf den Link **Berichte**, um das Fenster für Berichte über die Computersicherheit zu öffnen.

Im Block **Berichte** werden die Berichte über den Computerschutz als Diagramme angezeigt.

3. Klicken Sie unten im Fenster **Bericht** auf **Detaillierter Bericht**, um einen ausführlichen Bericht über die Arbeit des Programms zu öffnen (z. B. über die Arbeit der einzelnen Programmkomponenten).

Das Fenster **Detaillierter Bericht** wird geöffnet. Hier werden die Daten in Tabellenform dargestellt. Die Berichtseinträge können auf unterschiedliche Weise angeordnet werden.

STANDARDEINSTELLUNGEN FÜR DAS PROGRAMM WIEDERHERSTELLEN

Sie können jederzeit die von Kaspersky Lab empfohlenen Einstellungen für Kaspersky PURE wiederherstellen. Die Wiederherstellung der Einstellungen erfolgt mithilfe des Konfigurationsassistenten für das Programm.

Der Assistent stellt für alle Schutzkomponenten die Sicherheitsstufe *Empfohlen* ein. Wenn die empfohlene Sicherheitsstufe wiederhergestellt wird, können Sie Einstellungsänderungen beibehalten, die zuvor für die Programmkomponenten angepasst wurden.

➔ *Gehen Sie folgendermaßen vor, um die empfohlenen Programmeinstellungen wiederherzustellen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Verwenden Sie eine der folgenden Methoden, um im folgenden Fenster **Einstellungen** den Konfigurationsassistenten für das Programm zu starten:
 - Klicken Sie links unten auf den Link **Wiederherstellen**.
 - Wählen Sie im oberen Fensterbereich den Abschnitt **Erweitert**, Unterabschnitt **Einstellungen verwalten** aus und klicken Sie unter **Standardeinstellungen wiederherstellen** auf **Wiederherstellen** (s. Abb. unten).

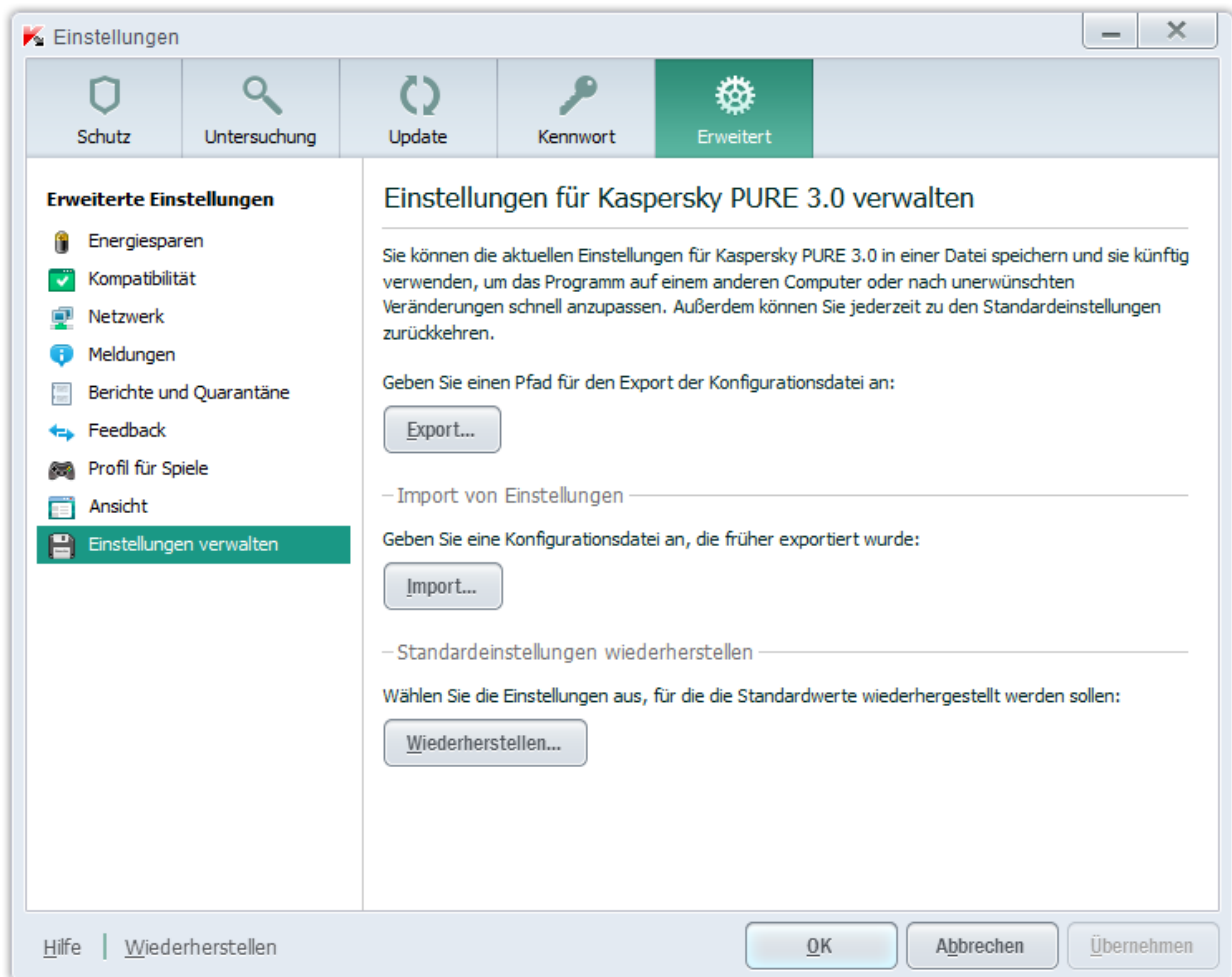


Abbildung 15. Fenster **Einstellungen**, Abschnitt **Einstellungen verwalten**

Details zu den einzelnen Schritten des Assistenten.

Schritt 1. Assistent starten

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

Schritt 2. Einstellungen wiederherstellen

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

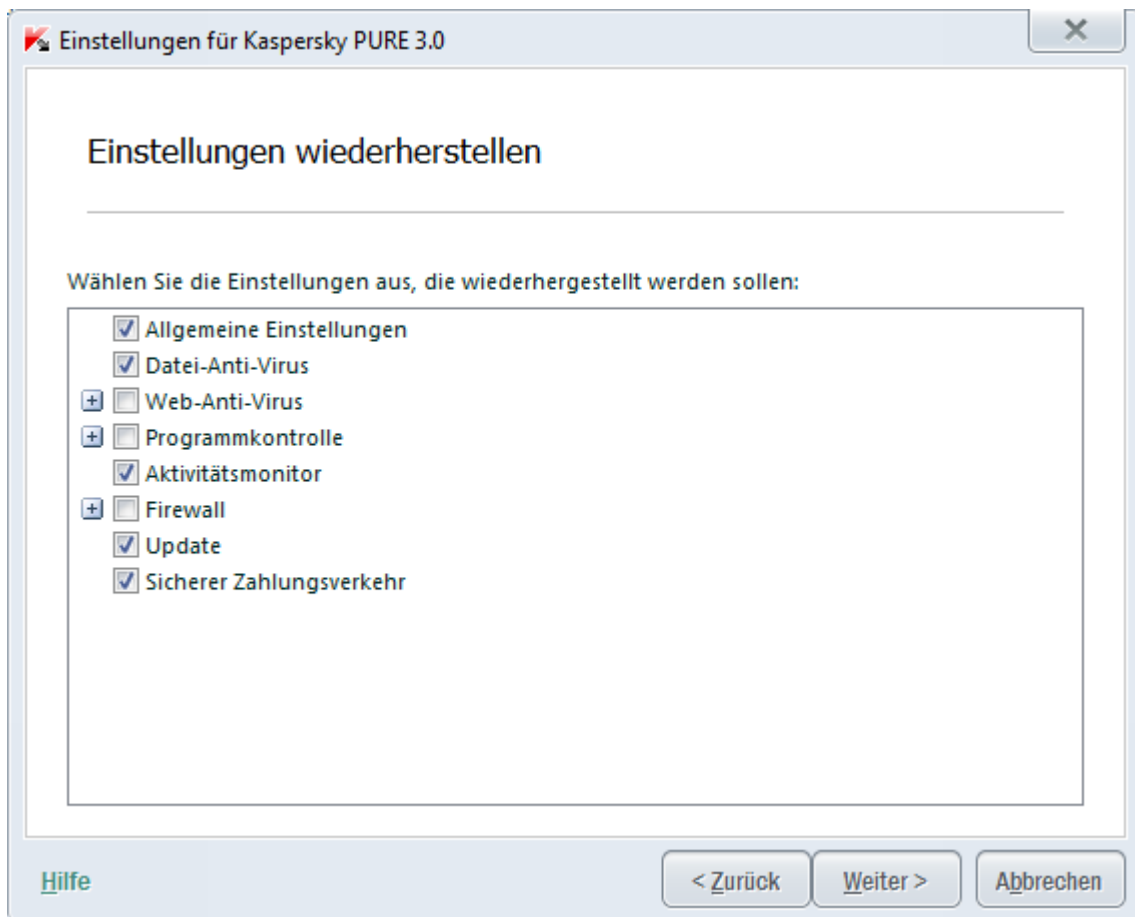


Abbildung 16. Fenster **Einstellungen wiederherstellen**

Als Einstellungen gelten: Erlaubnisliste und Verbotsliste mit Phrasen und Adressen für die Komponente Anti-Spam, Listen mit vertrauenswürdigen Internetadressen und Telefonnummern von Internet Providern, Ausnahmeregeln für die Programmkomponenten, Firewall-Filterregeln für Pakete und Programme.

Spezifische Einstellungen werden bei der Arbeit von Kaspersky PURE erstellt. Dabei werden individuelle Aufgaben und Sicherheitsanforderungen berücksichtigt. Kaspersky Lab empfiehlt, die unikalenen Einstellungen zu speichern, wenn die ursprünglichen Programmeinstellungen wiederhergestellt werden.

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

Schritt 3. Systemanalyse

Auf dieser Etappe werden Informationen über Programme, die zu Microsoft Windows gehören, gesammelt. Diese Programme werden in die Liste der vertrauenswürdigen Anwendungen aufgenommen, deren Aktionen im System nicht beschränkt werden.

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

Schritt 4. Wiederherstellung abschließen

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

IMPORT DER PROGRAMMEINSTELLUNGEN FÜR KASPERSKY PURE AUF EINEN ANDEREN COMPUTER

Sie können Ihre Programmeinstellungen für ein anderes Exemplar von Kaspersky PURE übernehmen, das auf einem anderen Computer installiert ist. Auf diese Weise sind die Einstellungen des Programms auf beiden Computern identisch. Diese Option kann beispielsweise von Nutzen sein, wenn Sie Kaspersky PURE auf Ihrem PC zuhause und im Büro installiert haben.

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

1. Programmeinstellungen in eine Konfigurationsdatei exportieren.
2. Konfigurationsdatei auf einen anderen Computer übertragen (beispielsweise per E-Mail oder auf einem Wechseldatenträger).
3. Einstellungen aus einer Konfigurationsdatei in das Programm übernehmen, das auf einem anderen Computer installiert ist.

➡ *Gehen Sie folgendermaßen vor, um die Einstellungen für Kaspersky PURE in einer Konfigurationsdatei zu speichern:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie im oberen Bereich des Fensters **Einstellungen** unter **Erweitert** den Abschnitt **Einstellungen verwalten** aus.
4. Klicken Sie im Abschnitt **Einstellungen verwalten** auf **Export**.
5. Geben Sie im folgenden Fenster einen Namen für die Konfigurationsdatei an und wählen Sie einen Speicherort dafür aus.
6. Klicken Sie auf **OK**.

➡ *Gehen Sie folgendermaßen vor, um Einstellungen aus einer Konfigurationsdatei für ein Programm zu übernehmen, das auf einem anderen Computer installiert ist:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie im oberen Bereich des Fensters **Einstellungen** unter **Erweitert** den Abschnitt **Einstellungen verwalten** aus.
4. Klicken Sie im Abschnitt **Einstellungen verwalten** auf **Import**.
5. Wählen Sie im folgenden Fenster eine Datei, aus der Sie die Einstellungen für Kaspersky PURE importieren möchten.
6. Klicken Sie auf **OK**.

NOTFALL-CD ERSTELLEN UND VERWENDEN

Eine Notfall-CD besteht aus dem Programm Notfall-CD, das auf einem Wechseldatenträger gespeichert ist (CD oder USB-Gerät).

Die Notfall-CD kann verwendet werden, um einen infizierten Computer zu untersuchen und zu desinfizieren, wenn eine Desinfektion mit anderen Mitteln (z. B. Antiviren-Programmen) fehlschlägt.

IN DIESEM ABSCHNITT

Notfall-CD erstellen	73
Hochfahren eines Computers mithilfe der Notfall-CD.....	75

NOTFALL-CD ERSTELLEN

Beim Anlegen einer Notfall-CD wird ein Disc-Abbild (Datei im ISO-Format) mit einer aktuellen Version des Programms Notfall-CD erstellt und auf einen Wechseldatenträger gespeichert.

Ein Original des Disc-Abbilds kann vom Kaspersky-Lab-Server heruntergeladen oder aus einer lokalen Quelle kopiert werden.

Eine Notfall-CD wird mit dem Notfall-CD-Assistenten erstellt. Die vom Assistenten angelegte Abbild-Datei rescuecd.iso wird auf der Festplatte Ihres Computers gespeichert:

- im Betriebssystem Microsoft Windows XP – im Ordner Dokumente und Einstellungen\All Users\Application Data\Kaspersky Lab\AVP12\Data\Rdisk\.
- in den Betriebssystemen Microsoft Windows Vista, Microsoft Windows 7 und Microsoft Windows 8 – im Ordner ProgramData\Kaspersky Lab\AVP13\Data\Rdisk\.

➤ *Gehen Sie folgendermaßen vor, um eine Notfall-CD zu erstellen:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Zusätzliche Funktionen**.
3. Klicken Sie im folgenden Fenster **Notfall-CD** auf **Erstellen**.

Das Fenster **Notfall-CD-Assistent** 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. Assistent starten Suche nach einem existierenden Festplattenabbild

Das erste Fenster des Assistenten informiert über das Programm Notfall-CD.

Wenn der Assistent in dem dafür vorgesehenen Ordner (s. oben) ein früher erstelltes Notfall-CD-Abbild findet, wird im ersten Fenster des Assistenten das Kontrollkästchen **Vorhandenes Abbild verwenden** angezeigt. Aktivieren Sie dieses Kontrollkästchen, um die gefundene Datei als Grundlage für das Disc-Abbild zu verwenden und direkt zum Schritt **Abbild-Datei aktualisieren** weiterzugehen (s. unten). Deaktivieren Sie dieses Kontrollkästchen, wenn Sie das gefundene Disc-Abbild nicht verwenden möchten. Der Assistent geht weiter zum Fenster **Quelle für das Abbild wählen**.

Schritt 2. Quelle für das Abbild wählen

Wenn Sie im ersten Fenster des Assistenten das Kontrollkästchen **Vorhandenes Abbild verwenden**, aktiviert haben, wird dieser Schritt übersprungen.

Bei diesem Schritt muss aus folgenden Varianten eine Quelle für das Disc-Abbild ausgewählt werden:

- Wählen Sie die Variante **Abbild von lokaler Festplatte oder Netzlaufwerk kopieren**, wenn Sie über eine gespeicherte Notfall-CD verfügen oder auf Ihrem Computer bzw. in einer Ressource des lokalen Netzwerks ein Disc-Abbild (Datei im ISO-Format) bereitliegt.
- Wählen Sie die Variante **Abbild von Kaspersky-Lab-Server herunterladen**, wenn Sie nicht über eine Abbild-Datei für die Notfall-CD verfügen und die Abbild-Datei vom Kaspersky-Lab-Server herunterladen möchten (Dateigröße ca. 175 MB).

Schritt 3. Disc-Abbild kopieren (herunterladen)

Wenn Sie im ersten Fenster des Assistenten das Kontrollkästchen **Vorhandenes Abbild verwenden**, aktiviert haben, wird dieser Schritt übersprungen.

Wenn Sie beim vorherigen Schritt die Variante **Abbild von lokaler Festplatte oder Netzlaufwerk kopieren** ausgewählt haben, klicken Sie auf **Durchsuchen**. Nachdem Sie den Pfad zur Datei angegeben haben, klicken Sie auf **Weiter**. Im Assistentenfenster wird angezeigt, wie das Kopieren des Disc-Abbilds verläuft.

Wenn Sie beim vorherigen Schritt die Variante **Abbild von Kaspersky-Lab-Server herunterladen** ausgewählt haben, wird sofort der Download des Disc-Abbilds angezeigt.

Nach Abschluss des Kopiervorgangs oder des Ladens des Disc-Abbilds wechselt der Assistent automatisch zum nächsten Schritt.

Schritt 4. Abbild-Datei aktualisieren

Der Vorgang zur Aktualisierung der Abbild-Datei umfasst folgende Aktionen:

- Update der Programm-Datenbanken
- Aktualisierung der Konfigurationsdateien

Die Konfigurationsdateien definieren die Möglichkeit zum Hochfahren des Computers von einem Wechseldatenträger (beispielsweise von einer CD / DVD oder einem USB-Gerät mit der Notfall-CD), der mit dem Assistenten erstellt wurde.

Für die Aktualisierung der Programm-Datenbanken werden die beim letzten Update von Kaspersky PURE heruntergeladenen Datenbanken verwendet. Wenn die Datenbanken veraltet sind, wird empfohlen, die Updateaufgabe auszuführen und den Notfall-CD-Assistenten erneut zu starten.

Klicken Sie auf die Schaltfläche **Weiter**, um die Aktualisierung der Datei zu starten. Im Assistentenfenster wird angezeigt, wie die Aktualisierung verläuft.

Schritt 5. Disc-Abbild auf Datenträger schreiben

In diesem Fenster informiert der Assistent darüber, dass das Notfall-CD-Abbild erfolgreich erstellt wurde, und bietet Ihnen an, das Disc-Abbild auf einen Datenträger zu schreiben.

Geben Sie den Datenträger an, auf den die Notfall-CD geschrieben werden soll:

- Wählen Sie die Variante **Auf CD/DVD brennen** und geben Sie das Laufwerk an, auf das das Abbild geschrieben werden soll, um das Abbild auf eine CD / DVD zu brennen.

- Wählen Sie die Variante **Auf USB-Gerät schreiben** und geben Sie das Gerät an, auf das das Abbild geschrieben werden soll, um das Abbild auf ein USB-Gerät zu schreiben.

Kaspersky Lab rät davon ab, Disc-Abbilder auf Geräten zu speichern, die nicht ausschließlich für die Datenspeicherung konzipiert sind, wie z. B. Smartphones, Mobiltelefone, PDAs und MP3-Player. Solche Geräte können bei Verwendung für die Speicherung von Datenträgerabbildern in ihrer Funktion beeinträchtigt werden.

- Wählen Sie die Variante **Abbild in einer Datei auf lokaler Festplatte oder Netzlaufwerk speichern**, um das Abbild auf die Festplatte Ihres Computers oder auf einem anderen Computer zu schreiben, auf den Sie über das Netzwerk zugreifen können. Legen Sie dann den Ordner fest, in den das Disc-Abbild geschrieben werden soll, und geben Sie einen Namen für die Datei im ISO-Format an.

Schritt 6. Assistent abschließen

Klicken Sie auf **Beenden**, um die Arbeit des Assistenten abzuschließen. Sie können die erstellte Notfall-CD zum Booten des Computers (s. S. 75) verwenden, wenn es aufgrund von Viren- und Malware-Aktivitäten nicht mehr im normalen Modus möglich ist, den Computer hochzufahren und Kaspersky PURE zu starten.

HOCHFAHREN EINES COMPUTERS MITHILFE DER NOTFALL-CD

Wenn sich das Betriebssystem aufgrund eines Virenangriffs nicht mehr hochfahren lässt, können Sie die Notfall-CD einsetzen.

Um das Betriebssystem zu booten, ist eine CD / DVD oder ein USB-Gerät erforderlich, auf der/dem das Programm Notfall-CD gespeichert ist (s. Abschnitt "Notfall-CD erstellen" auf S. 73).

Das Booten des Computers von einem Wechseldatenträger ist nicht immer möglich. Dies wird beispielsweise von einigen älteren Computermodellen nicht unterstützt. Klären Sie zuerst, ob diese Option möglich ist, bevor Sie den Computer herunterfahren, um ihn anschließend von einem Wechseldatenträger zu booten.

➔ Gehen Sie folgendermaßen vor, um den Computer mit einer Notfall-CD zu booten:

1. Aktivieren Sie in den BIOS-Einstellungen das Booten von CD / DVD oder USB-Gerät (Weitere Informationen finden Sie in der Dokumentation zum Motherboard Ihres Computers).
2. Legen Sie die CD / DVD mit dem Programm Notfall-CD in das Laufwerk des infizierten Computers ein oder schließen Sie das USB-Gerät mit dem Programm Notfall-CD an den Computer an.
3. Starten Sie den Computer neu.

Ausführliche Informationen über die Verwendung der Notfall-CD bietet das Benutzerhandbuch zur Kaspersky Notfall-CD, das Sie als PDF-Datei auf der Programm-CD oder unter www.kaspersky.de/downloads finden.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Dieser Abschnitt beschreibt, wie Sie technische Unterstützung erhalten können und nennt die Voraussetzungen, die dafür erfüllt sein müssen.

IN DIESEM ABSCHNITT

Wie Sie technischen Kundendienst erhalten	76
Technischer Support am Telefon	76
Technischen Support erhalten über Mein Kaspersky Account.....	77
Bericht über den Systemstatus erstellen und AVZ-Skript verwenden	78

WIE SIE TECHNISCHEN KUNDENDIENST ERHALTEN

Wenn Sie in der Programmdokumentation und in den Informationsquellen zum Programm (s. Abschnitt "Informationsquellen zum Programm" auf S. [9](#)) 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.
- Aus Mein Kaspersky Account auf der Support-Webseite eine Anfrage senden. Sie können sich über ein Webformular an die Support-Experten wenden.

Der Technische Support steht nur den Benutzern zur Verfügung, die eine kommerzielle Lizenz für die Programmnutzung gekauft haben. Testlizenzen berechtigen nicht zur Nutzung des technischen Kundendienstes.

TECHNISCHER SUPPORT AM TELEFON

Bei dringenden Problemen können Sie den lokalen oder internationalen Technischen Support anrufen (<http://support.kaspersky.com/de/support/international>).

Beachten Sie die Support-Richtlinien (<http://support.kaspersky.com/de/support/details>), bevor Sie sich an den Technischen Support wenden. Dadurch können unsere Spezialisten Ihnen möglichst schnell helfen.

TECHNISCHEN SUPPORT ERHALTEN ÜBER MEIN KASPERSKY ACCOUNT

Mein Kaspersky Account ist Ihr persönlicher Bereich (<https://my.kaspersky.com/de/>) auf der Seite des Technischen Supports.

Sie müssen sich auf der Login-Seite anmelden (<https://my.kaspersky.com/de/>). Geben Sie Ihre E-Mail-Adresse und das Kennwort für den Zugriff auf Ihren Kaspersky Account an.

In Mein Kaspersky Account können Sie folgende Aktionen ausführen:

- Anfragen an den Technischen Support und an das Virenlabor senden.
- mit dem Technischen Support kommunizieren, ohne E-Mails zu verwenden.
- Status Ihrer Anfragen in Echtzeit verfolgen.
- vollständigen Verlauf Ihrer Anfragen an den Technischen Support ansehen.
- Kopie einer Schlüsseldatei erhalten, falls die Schlüsseldatei verloren gegangen ist oder gelöscht wurde.

E-Mail-Anfrage an den Technischen Support

Anfragen an den Technischen Support können per E-Mail auf Deutsch, Englisch, Französisch, Spanisch oder Russisch gestellt werden.

Füllen Sie folgende Felder des elektronischen Formulars aus:

- Typ der Anfrage.
- Name und Versionsnummer des Programms.
- Anfragetext.
- Kundennummer und Kennwort.
- E-Mail-Adresse.

Die Support-Spezialisten richten ihre Antwort an My Kaspersky Account und an die E-Mail-Adresse, die in der Anfrage angegeben wurde.

Elektronische Anfrage an das Virenlabor

Beachten Sie, dass für die Bearbeitung bestimmter Anfragen nicht der Technische Support, sondern das Virenlabor verantwortlich ist.

Sie können folgende Anfragetypen an das Virenlabor richten:

- *Unbekanntes Schadprogramm* – Sie haben den Verdacht, dass eine Datei einen Virus enthält, obwohl Kaspersky PURE sie nicht als infiziert einstuft.

Die Experten des Virenlabors analysieren den eingeschickten Schadcode. Wird ein bisher unbekannter Virus gefunden, so wird seine Beschreibung einer Datenbank hinzugefügt, die bei der nächsten Aktualisierung der Antiviren-Programme verfügbar gemacht wird.

- *Viren-Fehlalarm* – Kaspersky PURE stuft eine Datei als infiziert ein, obwohl Sie sicher sind, dass die Datei virenfrei ist.
- *Anfrage für eine Beschreibung eines Schadprogramms* – Sie möchten auf Basis des Virusnamens die Beschreibung eines Virus erhalten, den Kaspersky PURE gefunden hat.

Anfragen an das Virenlabor können Sie auf der Seite (<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de>) stellen. Dazu ist keine Anmeldung bei Mein Kaspersky Account notwendig. In diesem Fall ist die Angabe eines Aktivierungscode notwendig.

BERICHT ÜBER DEN SYSTEMSTATUS ERSTELLEN UND AVZ-SKRIPT VERWENDEN

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. Die Support-Experten können Sie auch darum bitten, eine Datei mit technischen Informationen über die Systemausführung zu erstellen. Diese Datei 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. Mit Hilfe von AVZ-Skripten können die laufenden Prozesse auf schädlichen Code analysiert, das System auf schädlichen Code untersucht, infizierte Dateien desinfiziert / gelöscht, und ein Bericht über die Ergebnisse der Systemuntersuchung erstellt werden.

IN DIESEM ABSCHNITT

Bericht über den Systemzustand erstellen.....	78
Technische Informationen über die Arbeit des Programms sammeln.....	79
Dateien mit Daten senden.....	79
Skript ausführen.....	80

BERICHT ÜBER DEN SYSTEMZUSTAND ERSTELLEN

➤ *Gehen Sie folgendermaßen vor, um einen Bericht über den Systemzustand zu erstellen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Support**, um das Fenster **Support** zu öffnen.
Klicken Sie auf **Support Tools**.
3. Klicken Sie im folgenden Fenster **Support Tools** auf **Systembericht erstellen**.

Der Bericht über den Systemzustand wird in den Formaten html und xml erstellt und im Archiv sysinfo.zip gespeichert. Nachdem das Sammeln von Daten über das System abgeschlossen wurde, können Sie einen Bericht ansehen.

➤ *Gehen Sie folgendermaßen vor, um einen Bericht anzuzeigen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Support**, um das Fenster **Support** zu öffnen.
Klicken Sie auf **Support Tools**.
3. Klicken Sie im folgenden Fenster **Support Tools** auf **Bericht anzeigen**.
4. Öffnen Sie das Archiv sysinfo.zip, das die Protokolldateien enthält.

TECHNISCHE INFORMATIONEN ÜBER DIE ARBEIT DES PROGRAMMS SAMMELN

Um technische Informationen über das Programm und das Betriebssystem zu sammeln, können Sie die Ereignisprotokollierung verwenden. Mithilfe des Berichts über protokollierte Ereignisse können die Spezialisten vom Technischen Support das Problem auswerten, das bei der Ausführung des Programms aufgetreten ist.

➤ *Gehen Sie folgendermaßen vor, um Informationen über ein Problem in der Programmausführung zu sammeln und zu protokollieren:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Hauptfenster unten auf den Link **Support**, um das Fenster **Support** zu öffnen.
3. Klicken Sie im Fenster **Support** auf **Problemüberwachung**.
4. Wählen Sie im Abschnitt **Problemüberwachung** in der Dropdown-Liste **Ereignisse protokollieren** eine Prioritätsstufe für die Ereignisse aus.

Sie können folgende Prioritätsstufen für im Bericht protokollierte Ereignisse auswählen:

- Wichtig. Kaspersky PURE speichert im Bericht jene Ereignisse, die für die Computersicherheit potenziell wichtig sind (beispielsweise Fund eines möglicherweise infizierten Objekts oder einer verdächtigen Aktivität im System).
 - Empfohlen Kaspersky PURE protokolliert Informationen über wichtige Ereignisse und über Ereignisse, die keine vorrangige Relevanz für die Computersicherheit besitzen.
 - Alle. Kaspersky PURE erstellt einen ausführlichen Bericht über alle Ereignisse, die zur Diagnose des Programms dienen können.
5. Klicken Sie auf **Protokollierung aktivieren**, um die Ereignisprotokollierung zu starten.
 6. Schließen Sie das Fenster **Support** und wiederholen Sie die Aktionenabfolge, bei der ein Problem bei der Arbeit mit dem Programm auftritt.
 7. Nach dem Wiederholen der Aktionen gehen Sie zum Abschnitt **Problemüberwachung** im Fenster **Support** und klicken Sie auf die Schaltfläche **Protokollierung deaktivieren**.

Kaspersky PURE beendet die Protokollierung von technischen Informationen über die Programmarbeit und über das gesamte Betriebssystem.

Nach dem Sammeln von Dienstinformationen über die Programmarbeit können Sie diese Daten an den Technischen Support von Kaspersky Lab senden.

DATEIEN MIT DATEN SENDEN

Nachdem die technischen Informationen über das Programm gesammelt und der Bericht über den Systemzustand erstellt wurden, müssen diese an den Technischen Support von Kaspersky Lab geschickt werden.

Um die Dateien mit den Daten auf den Server des Technischen Supports hochzuladen, benötigen Sie eine Anfragenummer. Diese Nummer erhalten Sie in Ihrem Kaspersky Account auf der Webseite des Technischen Supports, wenn eine aktive Anfrage vorliegt.

➤ *Gehen Sie folgendermaßen vor, um die Dateien mit den Daten auf den Server des Technischen Supports hochzuladen:*

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Support** im unteren Fensterbereich das Fenster **Support**.

3. Klicken Sie im folgenden Fenster auf **Problemüberwachung**.

Das Fenster **Problemüberwachung** wird geöffnet.

4. Klicken Sie im folgenden Fenster auf **Daten an den Technischen Support senden**.

Das Fenster **Bericht senden** wird geöffnet.

5. Aktivieren Sie die Kontrollkästchen für die Daten, die Sie an den Technischen Support schicken möchten, und klicken Sie dann auf **Senden**.

Das Fenster **Geben Sie die Nummer der Anfrage ein** wird geöffnet.

6. Geben Sie die Nummer an, die Ihre Anfrage in Mein Kaspersky Account vom Technischen Support erhalten hat, und klicken Sie auf **OK**.

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

Falls kein Kontakt mit dem Technischen Support möglich ist, können Sie diese Dateien auf Ihrem Computer speichern und sie später aus Mein Kaspersky Account absenden.

➤ *Gehen Sie folgendermaßen vor, um die Dateien mit Daten auf der Festplatte zu speichern:*

1. Öffnen Sie das Programmhauptfenster.

2. Öffnen Sie mit dem Link **Support** im unteren Fensterbereich das Fenster **Support**.

3. Klicken Sie im folgenden Fenster auf **Problemüberwachung**.

4. Das Fenster **Problemüberwachung** wird geöffnet.

5. Klicken Sie im folgenden Fenster auf **Daten an den Technischen Support senden**.

Das Fenster **Bericht senden** wird geöffnet.

6. Aktivieren Sie die Kontrollkästchen für die Daten, die Sie an den Technischen Support schicken möchten, und klicken Sie dann auf **Senden**.

Das Fenster **Geben Sie die Nummer der Anfrage ein** wird geöffnet.

7. Klicken Sie auf **Abbrechen** und bestätigen Sie im folgenden Fenster mit **Ja**, dass die Dateien auf der Festplatte gespeichert werden.

Ein Fenster zum Speichern des Archivs wird geöffnet.

8. Geben Sie einen Namen für das Archiv an und bestätigen Sie das Speichern.

Das fertige Archiv können Sie über Mein Kaspersky Account an den Technischen Support senden.

SKRIPT AUSFÜHREN

Es wird davor gewarnt, den Text eines Skripts, das Ihnen von den Support-Spezialisten geschickt wurde, zu verändern. Sollten bei der Skript-Ausführung Probleme auftreten, dann wenden Sie sich an den technischen Support (s. Abschnitt "Wie Sie technischen Kundendienst erhalten" auf S. [76](#)).

➡ *Gehen Sie folgendermaßen vor, um ein AVZ-Skript auszuführen:*

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Support** im unteren Fensterbereich das Fenster **Support**.
3. Klicken Sie im folgenden Fenster auf **Problemüberwachung**.

Das Fenster **Problemüberwachung** wird geöffnet.

4. Klicken Sie im folgenden Fenster auf **Skript ausführen**.

Das Fenster **Skript ausführen** wird geöffnet.

5. Kopieren Sie den Text des Skripts, das Sie vom Technischen Support erhalten haben, fügen Sie den Text im folgenden Fenster ins Eingabefeld ein und klicken Sie auf **Weiter**.

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.

GLOSSAR

A

ANSTÖßIGE NACHRICHT

Nachricht, die anstößige Ausdrücke enthält.

AUFGABE

Funktionen, die das Kaspersky-Lab-Programm ausführen kann und die als Aufgaben realisiert sind. Beispiele: Echtzeitschutz für Dateien, Vollständige Untersuchung des Computers, Datenbank-Update.

AUFGABENEINSTELLUNGEN

Parameter für die Arbeit des Programms, die für jeden Aufgabentyp individuell sind.

AUTOSTART-OBJEKTE

Programme, die für den Start und die korrekte Funktionsweise des Betriebssystems und der Software auf Ihrem Computer erforderlich sind. Diese Objekte werden jedes Mal beim Hochfahren des Betriebssystems gestartet. Es gibt Viren, die speziell Autostart-Objekte infizieren können. Dadurch kann beispielsweise das Hochfahren des Betriebssystems blockiert werden.

B

BACKUP-SPEICHER

Speicherplatz oder Speichermedien, die im Rahmen von Backup-Aufgaben für das Erstellen von Sicherungskopien für Dateien vorgesehen sind.

BEDROHUNGSSTUFE

Index für die Wahrscheinlichkeit, mit der ein Computerprogramm eine Bedrohung für das Betriebssystem darstellt. Die Bedrohungsstufe wird durch eine heuristische Analyse ermittelt, die auf zweierlei Kriterien beruht:

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

Die Bedrohungsstufe erlaubt es, ein für Schadprogramme typisches Verhalten zu identifizieren. Je niedriger die Bedrohungsstufe, desto mehr Aktionen werden einem Programm im System erlaubt.

BOOTSEKTOR

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 Boot-Programm, das für den Start des Betriebssystems verantwortlich ist.

Laufwerksbootsektoren können von sogenannten Bootviren infiziert werden. Die Kaspersky-Lab-Anwendung erlaubt es, Bootsektoren auf Viren zu untersuchen und infizierte Sektoren zu desinfizieren.

C

CONTAINER

Verschlüsseltes Objekt, das für die Speicherung vertraulicher Informationen vorgesehen ist. Ein Container ist ein kennwortgeschützter virtueller Wechseldatenträger, auf dem Dateien und Ordner gespeichert werden.

Kaspersky PURE muss auf dem Computer installiert sein, um mit Containern arbeiten zu können.

D**DATEIMASKE**

Darstellung eines Dateinamens durch Platzhalter. Die wichtigsten Zeichen, die in Dateimasken verwendet werden, sind * und ? (wobei * - eine beliebige Anzahl von beliebigen Zeichen und ? – ein beliebiges Zeichen).

DATENBANK FÜR PHISHING-WEBADRESSEN

Eine Liste der Webressourcen, die von den Kaspersky-Lab-Spezialisten als Phishing-Adressen eingestuft wurden. Die Datenbank wird regelmäßig aktualisiert und gehört zum Lieferumfang des Kaspersky-Lab-Programms.

DATENBANK FÜR SCHÄDLICHE WEBADRESSEN

Eine Liste der Webressourcen, deren Inhalt als gefährlich eingestuft werden kann. Die Liste ist von den Kaspersky-Lab-Spezialisten angelegt, wird regelmäßig aktualisiert und gehört zum Lieferumfang des Programms.

DATENBANKEN

Datenbanken mit Informationen über Computer-Bedrohungen, die Kaspersky Lab beim Erscheinen der Datenbanken bekannt sind. Mithilfe der Einträge in den Datenbanken wird in den Untersuchungsobjekten schädlicher Code identifiziert. Die Datenbanken werden durch die Fachleute von Kaspersky Lab erstellt und stündlich aktualisiert.

DESINFEKTION VON OBJEKTEN

Verarbeitungsmethode für infizierte Objekte, bei der Daten vollständig oder teilweise wiederhergestellt werden. Nicht alle infizierten Objekte können desinfiziert werden.

DESINFEKTION VON OBJEKTEN BEIM NEUSTART

Methode zur Verarbeitung von infizierten Objekten, die im Augenblick der Desinfektion von anderen Programmen verwendet werden. Dabei wird eine Kopie des infizierten Objekts angelegt. Beim folgenden Neustart wird die Kopie desinfiziert und das infizierte Originalobjekt wird durch die desinfizierte Kopie ersetzt.

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 digitalen Signatur benötigt der Autor eines Dokuments oder Programms ein digitales Zertifikat, das die Identität des Autors bestätigt.

Mit einer digitalen Signatur können Quelle und Integrität von Daten überprüft werden. Dies bietet Schutz vor Fälschungen.

DOMAIN NAME SERVICE (DNS)

Verbreitetes System zur Umformung von Hostnamen (Computer oder anderes Netzwerkgerät) in eine IP-Adresse. DNS funktioniert in TCP/IP-Netzwerken. Im Einzelfall kann DNS auch umgekehrte Anfragen und Definitionen von Hostnamen nach dessen IP (PTR-Eintrag) speichern und verarbeiten. Die Auflösung von DNS-Namen erfolgt gewöhnlich durch Netzwerkprogramme und nicht durch die Benutzer.

DRINGENDES UPDATE

Kritisches Update für die Module des Kaspersky-Lab-Programms.

E**ECHTZEITSCHUTZ**

Funktionsmodus des Programms, in dem Objekte im Echtzeitmodus auf schädlichen Code untersucht werden.

Das Programm fängt jeden Versuch zum Öffnen, Schreiben und Ausführen eines Objekts ab, und durchsucht das Objekt nach Bedrohungen. Nicht infizierte Objekte werden an den Benutzer weitergeleitet, infizierte oder möglicherweise infizierte Objekte werden gemäß den Aufgabeneinstellungen verarbeitet (desinfiziert, gelöscht).

F**FEHLALARM**

Situation, in der ein virenfrees 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 System 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).

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 der 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 PURE verwaltet werden kann.

INTERNETPROTOKOLL (IP)

Basisprotokoll für das Internet, das seit seiner Entwicklung im Jahre 1974 unverändert verwendet wird. Es führt die Grundoperationen bei der Datenübertragung von einem Computer auf einen anderen aus und dient als Basis für alle Protokolle höherer Ebenen wie TCP und UDP. Es kontrolliert die Verbindung und die Fehlerbehandlung. Technologien wie NAT und Masquerading ermöglichen es, umfangreiche Netzwerke hinter einer relativ geringen Anzahl von IP-Adressen zu verbergen (oder sogar hinter einer Adresse). Dadurch wird erlaubt, die Ansprüche des ständig expandierenden Internets unter Verwendung eines relativ begrenzten IPv4-Adressraums zu befriedigen.

K

KASPERSKY SECURITY NETWORK (KSN)

Eine Infrastruktur von Online-Diensten und -Services, die Zugriff auf eine aktuelle Wissensdatenbank von Kaspersky Lab bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Verwendung von Daten aus dem Kaspersky Security Network wird die Reaktion von Kaspersky Internet Security auf unbekannte Bedrohungen beschleunigt und die Leistungsfähigkeit für bestimmte Komponenten erhöht. Außerdem verringert sich das Risiko von Fehlalarmen.

KASPERSKY-LAB-UPDATESERVER

HTTP-Server von Kaspersky Lab, von denen das Kaspersky-Lab-Programm die Updates für Datenbanken und Programm-Module herunterlädt.

KEYLOGGER

Subkomponente des Programms, die für die Untersuchung bestimmter Typen von E-Mails verantwortlich ist. Die Auswahl der zu installierenden Interceptoren ist davon abhängig, in welcher Rolle oder Rollenkombination das Programm eingesetzt werden soll.

KOPFZEILE (HEADER)

Informationen, die am Anfang einer Datei oder E-Mail stehen und Basisdaten über Status und Verarbeitung der Datei (E-Mail) enthalten. Die Kopfzeile einer E-Mail enthält z. B. Angaben über Absender, Empfänger und Datum.

M

MASTER-KENNWORT

Übergeordnetes Kennwort, das dem Schutz der Datenbanken des Password Managers dient und den Zugriff auf die Daten gewährleistet.

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.

N

NACHRICHT LÖSCHEN

Verarbeitungsmethode für eine E-Mail, bei der die Nachricht physikalisch gelöscht wird. Diese Methode wird für E-Mails empfohlen, die eindeutig Spam oder ein schädliches Objekt enthalten. Vor dem Löschen einer Nachricht wird eine Kopie in der Quarantäne gespeichert (falls diese Funktion nicht deaktiviert wurde).

O

OBJEKT BLOCKIEREN

Der Zugriff externer Programme auf ein Objekt wird verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt, verändert oder gelöscht werden.

OBJEKT LÖSCHEN

Methode zur Objektbearbeitung, bei der das Objekt physikalisch von dem Ort gelöscht wird, an dem es vom Programm gefunden wurde (Festplatte, Ordner, Netzwerkressource). Diese Bearbeitungsmethode wird für gefährliche Objekte empfohlen, deren Desinfektion aus bestimmten Gründen nicht möglich ist.

ONLINE-SPEICHER

Methode zur Speicherung von Informationen auf Remote-Servern, die häufig dezentral organisiert sind. Die Verwendung eines Online-Speichers vereinfacht die Datensynchronisierung auf unterschiedlichen Computern und mobilen Geräten. Für den Einsatz eines Online-Speichers ist Internetzugriff notwendig.

P

PHISHING

Eine Art des Internetbetrugs, bei der E-Mails verschickt werden, um vertrauliche Informationen (i. d. R. finanziellen Charakters) zu stehlen.

PRIORITÄTSSTUFE FÜR EIN EREIGNIS

Merkmale eines Ereignisses, das bei der Arbeit der Kaspersky-Lab-Anwendung eingetreten ist. Es gibt vier Prioritätsstufen:

- Kritisches Ereignis.
- Funktionsstörung
- Warnung
- Informative Meldung

Ereignisse des gleichen Typs können unterschiedliche Prioritätsstufen besitzen. Entscheidend ist die Situation, in der ein Ereignis eintritt.

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 Kaspersky-Lab-Programms gehören und für die Realisierung der wichtigsten Aufgaben zuständig sind. Jeder Art von Aufgaben, die das Programm realisiert (Echtzeitschutz, Virensuche, Update), entspricht ein eigenes ausführbares Modul. Wenn die vollständige Untersuchung Ihres Computers aus dem Hauptfenster gestartet wird, initiieren Sie den Start des Moduls für diese Aufgabe.

PROGRAMMEINSTELLUNGEN

Einstellungen für das Programm, die für alle Aufgabentypen gleich sind und sich auf das gesamte Programm beziehen. Beispiele: (z. B. Leistungseinstellungen für das Programm, Einstellungen für Berichte, Backup-Einstellungen).

PROTOKOLL

Genau definierte und standardisierte Kombination von Regeln, die das Verhältnis zwischen Client und Server regulieren. Bekannte Protokolle und die entsprechenden Dienste sind beispielsweise: z. B. HTTP, FTP und NNTP.

PROXYSERVER

Dienst in Computernetzwerken, mit dem Clients indirekte Anfragen an andere Netzwerkdienste richten können. Zunächst baut der Client eine Verbindung zu einem Proxyserver auf und fragt nach einer bestimmten Ressource (zum Beispiel nach einer Datei), die auf einem anderen Server liegt. Dann stellt der Proxyserver mit dem angegebenen Server eine Verbindung her und nimmt von ihm die Ressource entgegen oder schreibt die Ressource in seinen eigenen Cache (falls der Proxy einen Cache besitzt). In einigen Fällen kann die Client-Anfrage oder Server-Antwort vom Proxyserver zu bestimmten Zwecken geändert werden.

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**

Ein Programm oder ein Programmbausatz, dessen Ziel ist, die Spuren des Eindringlings zu verbergen oder die Anwesenheit der Malware im System zu verschleiern.

Im Kontext von Windows-Systemen bedeutet Rootkit ein Programm, das sich im System 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 System effektiv zu verbergen. Außerdem kann ein Rootkit im System gewöhnlich die Existenz aller in seiner Konfiguration beschriebenen Prozesse, Verzeichnisse und Dateien auf dem Laufwerk und Schlüssel in der Registrierung verbergen. Viele Rootkits installieren eigene Treiber und Dienste ins System (die ebenfalls "unsichtbar" sind).

S**SCHUTZ-CENTER**

Dieses Programm-Modul bietet einen komplexen Computerschutz vor unterschiedlichen Bedrohungsarten. Das Schutz-Center schützt den Computer vor Viren sowie vor Spam und Netzwerkangriffen. Das Modul umfasst die Komponenten Update, Aktivitätsmonitor für Programme und Quarantäne.

SCHUTZSTATUS

Aktueller Schutzstatus, der das Sicherheitsniveau des Computers charakterisiert.

SICHERER BROWSER

Browser, der im Modus Sicherer Zahlungsverkehr läuft. Der sichere Browser wird gestartet, wenn auf eine Online-Banking-Seite zugegriffen wird. Dadurch kann das Programm die Benutzerdaten vor Diebstahl schützen. Dabei erscheint im normalen Browser, in dem versucht wurde, auf die Webseite zuzugreifen, eine Meldung über den Start des sicheren Browsers.

SICHERER ZAHLUNGSVERKEHR

Dieses Programm-Modul hat folgende Funktionen: Schutz vertraulicher Daten, die der Nutzer auf Webseiten von Banken und Zahlungssystemen eingibt, und Verhinderung des Diebstahls von Zahlungsmitteln bei Online-Zahlungsvorgängen.

SICHERHEITSTUFE

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für die Arbeit einer Programmkomponente verstanden.

SKRIPT

Ein kleines Computerprogramm oder ein unabhängiger Programmteil (Funktion), das/der in der Regel dazu dient, eine konkrete Aufgabe auszuführen. Meistens werden sie bei Programmen, die in Hypertext integriert sind, verwendet. Skripte werden beispielsweise gestartet, wenn Sie bestimmte Websites öffnen.

Wenn der Echtzeitschutz aktiviert ist, überwacht die Anwendung den Start von Skripten, fängt sie ab und untersucht diese auf Viren. Abhängig von den Untersuchungsergebnissen können Sie die Ausführung eines Skripts verbieten oder erlauben.

SPAM

Unerwünschte massenhafte Versendung von E-Mails, die meistens Werbung enthalten.

SUBNETZMASKE

Die Subnetzmaske (auch Netzwerkmaske genannt) und die Netzwerkadresse definieren die Adressen der Computer, die zu einem Netzwerk gehören.

U

UNBEKANNTER VIRUS

Neuer Virus, über den noch keine Informationen in den Datenbanken vorhanden sind. In der Regel werden unbekannte Viren vom Programm in den Objekten mithilfe der heuristischen Analyse erkannt. Diesen Objekten wird der Status möglicherweise infiziert zugewiesen.

UNTERSUCHUNG DES DATENVERKEHRS

Untersuchung von Objekten, die mit beliebigen Protokollen übertragen werden (beispielsweise HTTP und FTP). Die Untersuchung erfolgt im Echtzeitmodus unter Verwendung der aktuellen (letzten) Datenbankversion.

UPDATE

Vorgang, bei dem vorhandene Dateien (Datenbanken oder Programm-Module) durch neue Dateien ersetzt bzw. neue Dateien hinzugefügt werden. Die neuen Dateien werden von den Kaspersky-Lab-Updateservern heruntergeladen.

UPDATE DER DATENBANKEN

Funktion des Kaspersky-Lab-Programms, die den Computerschutz auf dem neusten Stand hält. Bei der Aktualisierung kopiert das Programm die Updates für die Datenbanken und Programm-Module von den Kaspersky-Lab-Updateservern auf den Computer, und installiert und übernimmt die Updates automatisch.

UPDATEPAKET

Dateipaket für die Aktualisierung der Programm-Module. Das Kaspersky-Lab-Programm kopiert ein Updatepaket von den Kaspersky-Lab-Updateservern, um das Paket anschließend automatisch zu installieren und zu übernehmen.

V

VERFÜGBARES UPDATE

Updatepaket für die Module eines Kaspersky-Lab-Programms, das dringende Updates, die über einen bestimmten Zeitraum gesammelt wurden, sowie Änderungen der Programmarchitektur enthält.

VIRENANGRIFF

Eine Reihe zielgerichteter Versuche, einen Computer mit einem Virus zu infizieren.

W

WIEDERHERSTELLUNG

Verschieben eines Originalobjekts aus der Quarantäne oder aus dem Backup. Das Objekt wird entweder an dem ursprünglichen Ort, an dem es vor dem Verschieben, der Desinfektion oder dem Löschen gespeichert war, oder in einen benutzerdefinierten Ordner wiederhergestellt.

KASPERSKY LAB

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen, die Computer vor Viren und anderer Malware, Spam, Netzwerk- und Hackerangriffen schützen.

Seit 2008 gehört Kaspersky Lab international zu den vier führenden Unternehmen im Bereich der IT-Sicherheit für Endbenutzer (Rating des "IDC Worldwide Endpoint Security Revenue by Vendor"). Nach einer Studie des Marktforschungsinstituts COMCON TGI-Russia war Kaspersky Lab 2009 in Russland der beliebteste Hersteller von Schutzsystemen für Heimanwender.

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern mit Hauptsitz in Moskau und verfügt über fünf regionale Niederlassungen, die in Russland, West- und Osteuropa, im Nahen Osten, in Afrika, Nord- und Südamerika, Japan, China und anderen Ländern aktiv sind. Das Unternehmen beschäftigt über 2.000 hoch spezialisierte Mitarbeiter.

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

Die Palette der Heimanwender-Produkte umfasst Antiviren-Anwendungen für Desktops, Laptops, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Programme und Services für den Schutz von Workstations, Datei- und Webservern, Mail-Gateways und Firewalls. In Verbindung mit Administrationstools ermöglichen es diese Lösungen, netzwerkweit einen effektiven automatisierten Schutz vor Computerbedrohungen aufzubauen. Die Produkte von Kaspersky Lab sind durch namhafte Testlabore zertifiziert, mit den Programmen der meisten Softwarehersteller kompatibel und für die Arbeit mit unterschiedlichen Hardwareplattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Sie finden und analysieren jeden Tag Hunderte neuer Computerbedrohungen. Mit diesem Wissen entwickeln sie Mittel, um Gefahren zu erkennen und zu desinfizieren. Diese Informationen fließen in die Datenbanken ein, auf die Kaspersky-Programme zurückgreifen. *Die Antiviren-Datenbanken von Kaspersky Lab werden stündlich aktualisiert, die Anti-Spam-Datenbanken im 5-Minuten-Takt.*

Technologien. Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Softwarehersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (Großbritannien), CommuniGate Systems (USA), Critical Path (Irland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (Frankreich), NETGEAR (USA), Parallels (Russland), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

Auszeichnungen. Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So wurde Kaspersky Anti-Virus 2010 in Tests des anerkannten österreichischen Antiviren-Labors AV-Comparatives mehrfach mit dem Premium-Award Advanced+ ausgezeichnet. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 300 Millionen Anwender. Über 200.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Webseite von Kaspersky Lab:

<http://www.kaspersky.de>

Viren-Enzyklopädie:

<http://www.securelist.com/de/>

Antiviren-Labor:

newvirus@kaspersky.com (nur zum Einsenden von möglicherweise infizierten Dateien, die zuvor archiviert wurden)

<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de>

(für Fragen an die Virenanalysiker)

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.

Google Chrome ist eine Marke von Google, Inc.

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

Microsoft, Windows, Windows Vista und Internet Explorer sind in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragene Marken der Microsoft Corporation.

Mozilla und Firefox sind Marken der Mozilla Foundation.

SACHREGISTER

A

Aktivierungscode	27
Anti-Spam	
Tipps	39
Aufgabe starten	
Schwachstellensuche	35
Untersuchung	33
Update	32
Aufgaben	
Backup	62

B

Backup	62
Benutzerkonto	51
Berichte	69

C

Computer	
verwaltete	41

D

Daten	
Verschlüsselung	54
Datenbanken	
Manuelles Update	32

E

Einstellungen importieren / exportieren	72
Ereignisbericht	69

F

Fernverwaltung des Programms	41
------------------------------------	----

H

Hardwarevoraussetzungen	15
-------------------------------	----

K

Kaspersky Lab	89
Kindersicherung	
Funktion der Komponente	67
Kontrolle des Zugriffs auf das Programm	
Kennwortschutz	65

L

Lizenz	25
Aktivierungscode	27
Lizenzvertrag	25
Lizenzvertrag	25

N

Notfall-CD	73
------------------	----

P

Password Manager	
Benutzerkonto	51
Programm aktivieren	
Aktivierungscode	27
Lizenz	25
Programm installieren	17

Q

Quarantäne	
Objekt wiederherstellen	35

S

Schlüssel.....	25
Schutzstatus.....	31
Schutzstatus für Netzwerk.....	41
Softwarevoraussetzungen.....	15
Speicher	
Backup.....	62
Quarantäne.....	35
Standardmäßige Einstellungen	70
Standardparameter wiederherstellen	70
Statistik.....	69

U

Untersuchung	
Aufgabe starten	33
Schwachstellensuche	35
Update.....	32

V

Verschlüsselung	
Datenverschlüsselung	54

W

Wiederherstellung nach Infektion	37
--	----