

Kaspersky Endpoint Security 8 für Smartphones

für Microsoft® Windows® Mobile

KASPERSKY

Benutzerhandbuch

PROGRAMMVERSION: 8.0

Sehr geehrte Benutzerinnen und Benutzer!

Vielen Dank, dass Sie sich für unser Produkt entschieden haben. Wir hoffen, dass Ihnen diese Dokumentation bei der Arbeit behilflich sein und auf die mit dem Produkt verbundenen Fragen antworten wird.

Wichtiger Hinweis: Die Rechte an diesem Dokument liegen bei Kaspersky Lab und sind durch die Urhebergesetze der Russischen Föderation und durch internationale Abkommen 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.

Die Materialien dürfen nur mit schriftlicher Einwilligung von Kaspersky Lab auf elektronische, mechanische oder sonstige Weise kopiert, verbreitet oder übersetzt werden.

Das Dokument und die darin enthaltenen Bilder sind ausschließlich für informative, nicht gewerbliche und persönliche Zwecke bestimmt.

Das Dokument kann zukünftig ohne besondere Ankündigung geändert werden. Die aktuelle Version des Dokuments steht auf der Seite von Kaspersky Lab unter der Adresse <http://www.kaspersky.com/de/docs> zur Verfügung.

Kaspersky Lab übernimmt keine Haftung für Inhalt, Qualität, Aktualität und Richtigkeit von in diesem Dokument verwendeten Materialien, deren Rechte bei anderen Eigentümern liegen, sowie für möglichen Schaden, der mit der Verwendung dieser Materialien verbunden ist.

In diesem Dokument werden registrierte oder nicht registrierte Markenzeichen verwendet, die Eigentum der rechtmäßigen Besitzer sind. ActiveSync, Microsoft und Windows sind Markenzeichen der Microsoft Corporation und sind in den USA und in weiteren Ländern registriert.

Redaktionsdatum: 27.05.2011

© 1997-2011 Kaspersky Lab ZAO. Alle Rechte vorbehalten.

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

INHALT

ÜBER DIESES HANDBUCH.....	6
ZUSÄTZLICHE INFORMATIONSMQUELLEN.....	7
Informationsquellen zur selbstständigen Recherche	7
Diskussion über die Programme von Kaspersky Lab im Webforum	8
Kontakt zur Abteilung für Handbücher und Hilfesysteme	8
KASPERSKY ENDPOINT SECURITY 8 FÜR SMARTPHONES	9
Neuerungen in Kaspersky Endpoint Security 8 für Smartphones	10
Hard- und Softwarevoraussetzungen	10
KASPERSKY ENDPOINT SECURITY 8 FÜR SMARTPHONES INSTALLIEREN.....	11
Automatische Programminstallation	11
Über die Programminstallation über eine Workstation.....	12
Programminstallation über eine Workstation	12
Über die Programminstallation nach dem Empfang einer E-Mail-Nachricht	13
Programminstallation nach dem Empfang einer E-Mail-Nachricht.....	14
PROGRAMM DEINSTALLIEREN	16
Manuelle Deinstallation des Programms	16
Automatische Deinstallation des Programms	17
PROGRAMMEINSTELLUNGEN VERWALTEN.....	19
LIZENZVERWALTUNG.....	20
Über Lizenzen für Kaspersky Endpoint Security 8 für Smartphones	20
Lizenz installieren	21
Lizenz-Info anzeigen	21
SYNCHRONISIERUNG MIT DEM REMOTE-MANAGEMENT-SYSTEM	22
Synchronisierung manuell starten	22
Synchronisierungseinstellungen ändern	23
ERSTE SCHRITTE	25
Programm starten.....	25
Geheimcode eingeben	25
Update der Programm-Datenbanken.....	26
Gerät auf Viren untersuchen.....	26
Programm-Infos anzeigen	27
PROGRAMMOBERFLÄCHE	28
Fenster für den Schutzstatus.....	28
Programm-Menü.....	29
SCHUTZ FÜR DAS DATEISYSTEM.....	31
Schutz.....	31
Schutz aktivieren / deaktivieren	31
Aktion für schädliche Objekte auswählen	33
UNTERSUCHUNG DES GERÄTS.....	35
Über Scan auf Befehl	35
Untersuchung manuell starten.....	36

Untersuchung nach Zeitplan starten	37
Typ der Untersuchungsobjekte wählen	38
Archiv-Untersuchung anpassen.....	39
Aktion für gefundene Objekte wählen.....	40
QUARANTÄNE FÜR SCHÄDLICHE OBJEKTE	42
Über die Quarantäne	42
Quarantäneobjekte anzeigen.....	42
Quarantäneobjekte wiederherstellen	43
Quarantäneobjekte löschen.....	43
EINGEHENDE ANRUFEN UND SMS FILTERN	45
Über Anti-Spam	45
Über die Modi für Anti-Spam	46
Anti-Spam-Modus ändern.....	46
Schwarze Liste anlegen.....	47
Eintrag zur Schwarzen Liste hinzufügen.....	47
Eintrag der Schwarzen Liste ändern	48
Eintrag aus Schwarzer Liste löschen	49
Weiße Liste anlegen.....	50
Eintrag zur Weißen Liste hinzufügen	50
Eintrag der Weißen Liste ändern	51
Eintrag aus Weißer Liste löschen	52
Reaktion auf SMS und Anrufe von Nummern, die nicht zu den Kontakten zählen.	53
Reaktion auf SMS von Nicht-Ziffern-Nummern.....	54
Aktion für eingehende SMS wählen.....	54
Aktion für eingehende Anrufe wählen.....	55
DATENSCHUTZ BEI VERLUST ODER DIEBSTAHL DES GERÄTS	57
Über den Diebstahlschutz.....	57
Gerät blockieren	58
Persönliche Daten löschen	60
Liste der zu löschenden Ordner erstellen	62
Wechsel der SIM-Karte auf dem Gerät überwachen	63
Geografische Koordinaten des Geräts ermitteln.....	64
Diebstahlschutz-Funktionen ferngesteuert starten	67
VERBERGEN SENSIBLER DATEN	69
Über die Privatsphäre.....	69
Über die Modi der Privatsphäre.....	69
Privatsphäre aktivieren / deaktivieren.....	70
Funktion zum Verbergen von sensiblen Daten automatisch aktivieren	71
Funktion zum Verbergen von sensiblen Daten ferngesteuert aktivieren.....	72
Liste der vertraulichen Nummern erstellen	74
Hinzufügen einer Nummer zur Liste der vertraulichen Nummern	75
Bearbeiten einer Nummer der Liste der vertraulichen Nummern	76
Löschen einer Nummer aus der Liste der vertraulichen Nummern	76
Auswahl der zu verbergenden Informationen: Privatsphäre	77
NETZWERKAKTIVITÄT FILTERN. FIREWALL	79
Firewall	79
Über die Modi der Firewall.....	79

Firewall-Modus auswählen	79
Meldungen über blockierte Verbindungen	80
PERSÖNLICHE DATEN VERSCHLÜSSELN	82
Verschlüsselung	82
Daten verschlüsseln	82
Daten entschlüsseln	85
Zugriff auf verschlüsselte Daten verbieten.....	86
UPDATE DER PROGRAMM-DATENBANKEN.....	88
Über das Update der Programm-Datenbanken	88
Datenbankinfos anzeigen	89
Manuelles Update.....	89
Update nach Zeitplan starten.....	90
Update im Roaming.....	91
PROGRAMMBERICHTE.....	93
Berichte	93
Berichtseinträge anzeigen	93
Einträge aus Bericht löschen	94
ERWEITERTE EINSTELLUNGEN ANPASSEN	95
Geheimcode ändern	95
Tooltips anzeigen	95
Audiosignale verwalten.....	96
GLOSSAR.....	98
KASPERSKY LAB.....	101
INFORMATIONEN ZUM PROGRAMMCODE VON DRITHTHERSTELLERN	102
SACHREGISTER.....	103

ÜBER DIESES HANDBUCH

Dieses Handbuch informiert über Installation, Konfiguration und Verwendung des Programms Kaspersky Endpoint Security 8 für Smartphones. Das Dokument ist für gewöhnliche Anwender gedacht.

Das Dokument soll:

- dem Anwender helfen, das Programm selbst auf einem mobilen Gerät zu installieren, es zu aktivieren und unter Berücksichtigung individueller Aufgaben optimal anzupassen.
- Fragen, die sich auf das Programm beziehen, schnell beantworten.
- auf alternative Informationsquellen über das Programm und auf Möglichkeiten des technischen Supports hinweisen.

ZUSÄTZLICHE INFORMATIONSQUELLEN

Zu Fragen über Installation oder Verwendung von Kaspersky Endpoint Security 8 für Smartphones stehen unterschiedliche Informationsquellen zur Verfügung. Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage eine passende Quelle wählen.

IN DIESEM ABSCHNITT

Informationsquellen zur selbstständigen Recherche	7
Diskussion über die Programme von Kaspersky Lab im Webforum	8
Kontakt zur Abteilung für Handbücher und Hilfesysteme	8

INFORMATIONSQUELLEN ZUR SELBSTSTÄNDIGEN RECHERCHE

Bei Fragen über die Anwendung stehen folgende Informationsquellen zur Verfügung:

- Seite über das Programm auf der Webseite von Kaspersky Lab
- Seite über das Programm auf der Webseite des Technischen Supports (in der Wissensdatenbank)
- elektronisches Hilfesystem
- Dokumentationen

Seite auf der Webseite von Kaspersky Lab

<http://www.kaspersky.com/de/kaspersky-work-space-security>

Auf dieser Seite finden Sie allgemeine Informationen über Kaspersky Endpoint Security 8 für Smartphones, seine Funktionen und Besonderheiten.

Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

<http://support.kaspersky.com/de/kes8m>

Auf dieser Seite finden Sie Artikel, die von Spezialisten des Technischen Supports veröffentlicht wurden.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen zu Kauf, Installation und Verwendung von Kaspersky Endpoint Security 8 für Smartphones. Sie sind nach Themen wie "Arbeit mit Schlüsseldateien", "Datenbank-Update" oder "Beheben von Störungen bei der Arbeit" angeordnet. Die Artikel können außerdem Fragen behandeln, die nicht nur Kaspersky Endpoint Security 8 für Smartphones, sondern auch andere Produkte von Kaspersky Lab betreffen. Außerdem können Sie Neuigkeiten über den Technischen Support enthalten.

Elektronisches Hilfesystem

Bei Fragen zu einem speziellen Fenster oder zu einer Registerkarte von Kaspersky Endpoint Security 8 für Smartphones hilft Ihnen die Kontexthilfe.

Um die Kontexthilfe zu öffnen, öffnen Sie das entsprechende Programmfenster und klicken Sie auf **Hilfe** oder wählen Sie **Menü** → **Hilfe**.

Dokumentation

Zum Lieferumfang von Kaspersky Endpoint Security 8 für Smartphones gehört das Dokument **Benutzerhandbuch** (im PDF-Format). Dieses Dokument beschreibt Installation und Deinstallation des Programms, Konfiguration der Programmeinstellungen, erste Schritte bei der Arbeit mit dem Programm und Konfiguration der Programmkomponenten. 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 nicht dringend ist, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse <http://forum.kaspersky.com> diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben, neue Themen eröffnen und die Hilfefunktion verwenden.

KONTAKT ZUR ABTEILUNG FÜR HANDBÜCHER UND HILFESYSTEME

Wenn Sie Fragen zu dieser Dokumentation haben, einen Fehler darin gefunden haben oder Ihre Meinung über unsere Dokumentationen schreiben möchten, richten Sie sich bitte direkt an unsere Abteilung für Handbücher und Hilfesysteme. Zur Kontaktaufnahme mit der Dokumentationsgruppe senden Sie eine Nachricht an docfeedback@kaspersky.de. Geben Sie folgenden Betreff an: "Kaspersky Help Feedback: Kaspersky Endpoint Security 8 für Smartphones".

KASPERSKY ENDPOINT SECURITY 8 FÜR SMARTPHONES

Kaspersky Endpoint Security 8 für Smartphones schützt mobile Geräte, die mit dem Betriebssystem Microsoft® Windows® Mobile arbeiten. Das Programm kann die Informationen auf dem Gerät vor einer Infektion durch bekannte Bedrohungen schützen, den Empfang unerwünschter SMS und Anrufe verhindern, eine Netzwerkverbindung auf dem Gerät kontrollieren, Informationen verschlüsseln, Informationen für vertrauliche Kontakte verbergen und die Informationen bei Diebstahl oder Verlust des Geräts schützen. Jeder Bedrohungstyp wird von bestimmten Programmkomponenten verarbeitet. Dadurch wird erlaubt, die Programmeinstellungen flexibel an die Erfordernisse eines konkreten Benutzers anzupassen. Programminstallation und Konfiguration werden vom Administrator mit Hilfe von Remote-Management-Systemen ausgeführt.

Kaspersky Endpoint Security 8 für Smartphones umfasst folgende Schutzkomponenten:

- **Anti-Virus.** Schützt das Dateisystem des mobilen Geräts vor Viren und anderen Schadprogrammen. Anti-Virus bietet folgende Optionen: Objekte erkennen und neutralisieren; Antiviren-Datenbanken des Programms aktualisieren.
- **Anti-Spam.** Prüft alle eingehenden SMS und Anrufe auf Spam. Diese Komponente erlaubt es, das Blockieren von SMS und Anrufe, die als unerwünscht gelten, flexibel anzupassen.
- **Diebstahlschutz.** Schützt die Informationen auf dem Gerät vor unbefugtem Zugriff, wenn es verloren geht oder gestohlen wird, und hilft bei der Suche nach dem Gerät. Außerdem kann der Diebstahlschutz Ihr Gerät durch einen SMS-Befehl von einem anderen Gerät aus ferngesteuert blockieren, auf dem Gerät gespeicherte Daten löschen und das Gerät orten (falls Ihr Gerät einen GPS-Empfänger besitzt). Außerdem kann der Diebstahlschutz das Gerät blockieren, falls die SIM-Karte gewechselt oder das Gerät ohne SIM-Karte eingeschaltet wird.
- **Privatsphäre.** Verbirgt Informationen, die mit vertraulichen Nummern aus der erstellten Kontaktliste zusammenhängen. Für diese Nummern verbirgt die Privatsphäre Einträge in den Kontakten, SMS-Korrespondenz, Einträge in der Anrufliste, neu empfangene SMS und eingehende Anrufe.
- **Firewall.** Kontrolliert die Netzwerkverbindungen auf Ihrem mobilen Gerät. Mit der Firewall können die Verbindungen festgelegt werden, die erlaubt oder verboten werden sollen.
- **Verschlüsselung.** Speichert Informationen in verschlüsselter Form. Die Komponente Verschlüsselung erlaubt es, eine beliebige Anzahl von Ordnern zu verschlüsseln. Die Ordner können sich im Gerätespeicher oder auf Speicherkarten befinden. Ein Zugriff auf die Dateien aus verschlüsselten Ordnern ist erst nach der Eingabe des Geheimcodes für das Programm möglich.

Das Programm bietet außerdem eine Reihe von Servicefunktionen. Diese Funktionen erlauben es, das Programm auf dem neuesten Stand zu halten, die Einsatzmöglichkeiten des Programms zu erweitern und den Benutzer bei der Arbeit zu unterstützen:

- **Schutzstatus.** Auf dem Display werden die Status der Programmkomponenten angezeigt. Auf Basis der angezeigten Informationen können Sie den aktuellen Schutzstatus für die Informationen auf Ihrem Gerät einschätzen.
- **Update der Antiviren-Datenbanken des Programms.** Diese Funktion hält die Antiviren-Datenbanken von Kaspersky Endpoint Security 8 für Smartphones aktuell.
- **Ereignisbericht.** Das Programm führt für jede Komponente einen separaten Ereignisbericht, der die Arbeit der Komponente dokumentiert (z. B. Untersuchungsbericht, Bericht über das Update der Antiviren-Datenbanken, Informationen über eine blockierte Datei). Die Berichte über die Arbeit der Komponenten werden an das Remote-Management-System weitergeleitet und dort gespeichert.

Kaspersky Endpoint Security 8 für Smartphones führt keine Sicherung und Wiederherstellung von Informationen aus.

IN DIESEM ABSCHNITT

Neuerungen in Kaspersky Endpoint Security 8 für Smartphones.....	10
Hard- und Softwarevoraussetzungen.....	10

NEUERUNGEN IN KASPERSKY ENDPOINT SECURITY 8 FÜR SMARTPHONES

Details zu den Neuerungen in Kaspersky Endpoint Security 8 für Smartphones

Neuerungen im Schutz:

- Der Zugriff auf das Programm wird durch einen Geheimcode geschützt.
- Die Liste der ausführbaren Dateien, die von den Komponenten Schutz und Scan untersucht werden, wenn die zu untersuchenden Dateitypen eingeschränkt sind, wurde erweitert. Es werden ausführbare Programmdateien der folgenden Formate untersucht: EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS. Außerdem wurde die Liste der untersuchten Archive erweitert. Das Programm entpackt und untersucht Archive der folgenden Formate: ZIP, JAR, JAD, SIS und SISX.
- Die Komponente Privatsphäre erlaubt es, die folgenden Informationen für vertrauliche Kontakte zu verbergen: Einträge in den Kontakten, SMS-Korrespondenz, Anrufliste sowie neu eingegangene SMS und eingehende Anrufe. Vertrauliche Informationen können angezeigt werden, wenn das Verbergen deaktiviert ist.
- Die Komponente Verschlüsselung erlaubt es, Ordner zu verschlüsseln, die sich im Gerätespeicher oder auf einer Speicherkarte befinden. Die Komponente speichert vertrauliche Daten in verschlüsselter Form und erlaubt den Zugriff auf verschlüsselte Informationen erst nach Eingabe des Geheimcodes für das Programm.
- Die aktuelle Version des Diebstahlschutzes enthält eine neue Funktion von GPS-Find. Bei Verlust oder Diebstahl des Geräts können mit dieser Funktion die geografischen Koordinaten an eine Telefonnummer und an eine bestimmte E-Mail-Adresse gesendet werden. Außerdem wurde im Diebstahlschutz die Funktion SMS-Clean aktualisiert. Mit dieser Funktion können nicht nur persönliche Benutzerinformationen per Fernsteuerung gelöscht werden, die sich im Telefonspeicher oder auf einer Speicherkarte befinden, sondern auch Dateien aus einer dafür vorgesehenen Liste.
- Um den Netzwerkverkehr zu reduzieren, besteht die Möglichkeit, das automatische Update der Programm-Datenbanken zu deaktivieren, wenn sich das mobile Endgerät im Roaming befindet.
- Es wurde eine neue Service-Funktion für die Anzeige von Tooltips hinzugefügt: Kaspersky Endpoint Security 8 für Smartphones zeigt eine kurze Beschreibung für die Komponente an, wenn diese angepasst werden soll.

HARD- UND SOFTWAREVORAUSSETZUNGEN

Kaspersky Endpoint Security 8 für Smartphones kann auf mobilen Geräten installiert werden, die mit den folgenden Betriebssystemen arbeiten:

- Microsoft Windows Mobile 5.0;
- Microsoft Windows Mobile 6.0, 6.1, 6.5

Für bestimmte Remote-Management-Systeme wird die Arbeit mit Geräten nicht unterstützt, die mit dem Betriebssystem Microsoft Windows Mobile 5.0 arbeiten. Fragen Sie Ihren Administrator nach Einzelheiten über die unterstützten Betriebssysteme.

KASPERSKY ENDPOINT SECURITY 8 FÜR SMARTPHONES INSTALLIEREN

Für die Installation von Kaspersky Endpoint Security 8 für Smartphones verwendet der Administrator Remote-Management-Tools. Abhängig davon, welches Management-Tool der Administrator verwendet, kann die Installation automatisch erfolgen oder eine Mitwirkung des Benutzers erfordern.

Falls für die Programminstallation eine Mitwirkung des Benutzers erforderlich ist, folgt die Installation einem der folgenden Schemata:

- Auf Ihrer Workstation wird das gleichnamige Installationstool für Kaspersky Endpoint Security 8 für Smartphones installiert. Mit diesem Tool können Sie Kaspersky Endpoint Security 8 für Smartphones auf Ihrem mobilen Gerät installieren.
- Sie erhalten per E-Mail eine Nachricht von Ihrem Administrator, die eine Programmdistribution oder einen Link für deren Download enthält. Mithilfe dieser Informationen installieren Sie Kaspersky Endpoint Security 8 für Smartphones auf dem mobilen Gerät.

Dieser Abschnitt erläutert die Vorbereitungen für die Installation von Kaspersky Endpoint Security 8 für Smartphones. Außerdem werden Varianten für die Programminstallation auf einem mobilen Gerät und die entsprechenden Benutzeraktionen beschrieben.

IN DIESEM ABSCHNITT

Automatische Programminstallation	11
Über die Programminstallation über eine Workstation	12
Programminstallation über eine Workstation	12
Über die Programminstallation nach dem Empfang einer E-Mail-Nachricht	13
Programminstallation nach dem Empfang einer E-Mail-Nachricht	14

AUTOMATISCHE PROGRAMMINSTALLATION

Der Administrator verwendet Remote-Management-Tools, um die Programminstallation auf dem Gerät zu starten.

Dabei erhält das mobile Gerät eine Distribution von Kaspersky Endpoint Security 8 für Smartphones und die Programminstallation wird automatisch gestartet.

Für den Installationsvorgang bestehen folgende Varianten:

- Das Programm wird ohne Mitwirkung des Benutzers automatisch auf dem Gerät installiert. Der Status der Programminstallation wird nicht angezeigt.
- Das Programm zeigt den Installationsstatus an. Beim Abschluss der Installation wird auf dem Display des Geräts eine Meldung über die erfolgreiche Programminstallation angezeigt.

Der automatische Installationsvorgang ist vom Remote-Management-Tool abhängig, dass der Administrator für die Ferninstallation des Programms verwendet.

Falls bei der Programminstallation Fehler auftreten sollten, wenden Sie sich an den Administrator.

ÜBER DIE PROGRAMMINSTALLATION ÜBER EINE WORKSTATION

Wenn der Administrator das Übertragungstool für Kaspersky Endpoint Security 8 für Smartphones auf Ihrer Workstation installiert hat, können Sie Kaspersky Endpoint Security 8 für Smartphones auf den mobilen Geräten installieren, die an diesen Computer angeschlossen werden. Das Übertragungstool für Kaspersky Endpoint Security 8 für Smartphones enthält eine Programmdistribution und sendet diese an das mobile Gerät. Das Tool wird nach der Installation auf einer Workstation automatisch gestartet und überwacht die Verbindung von mobilen Geräten mit dem Computer. Jedes Mal, wenn ein mobiles Gerät mit der Workstation verbunden wird, prüft das Tool, ob das Gerät die Systemvoraussetzungen für Kaspersky Endpoint Security 8 für Smartphones erfüllt, und bietet anschließend an, das Programm darauf zu installieren.

Eine Installation ist nur möglich, wenn das Programm Microsoft ActiveSync® auf der Workstation installiert ist.

PROGRAMMINSTALLATION ÜBER EINE WORKSTATION

Wenn das Übertragungstool für Kaspersky Endpoint Security 8 für Smartphones auf Ihrer Workstation installiert ist, wird Ihnen bei jeder Verbindung mit mobilen Geräten, die die Systemanforderungen erfüllen, vorgeschlagen, Kaspersky Endpoint Security 8 für Smartphones darauf zu installieren.

Sie können verbieten, dass Kaspersky Endpoint Security 8 für Smartphones bei künftigen Verbindungen von Geräten mit dem Computer installiert wird.

➔ Gehen Sie folgendermaßen vor, um das Programm auf einem mobilen Gerät zu installieren:

1. Um das mobile Gerät mit der Workstation zu verbinden, verwenden Sie das Programm Microsoft ActiveSync.

Erfüllt das Gerät die Systemanforderungen für die Installation der Anwendung, so öffnet das Fenster **KES 8** mit Informationen über das Tool (s. Abb. unten).

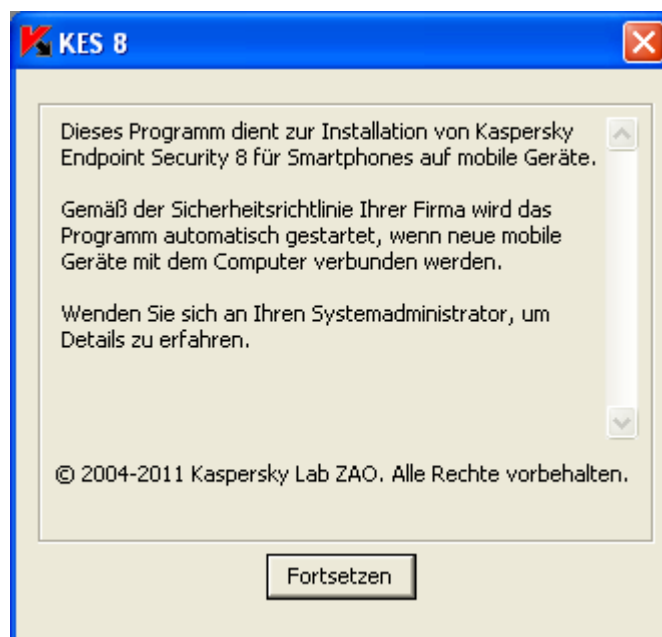


Abbildung 1: Installationsprogramm für Kaspersky Endpoint Security 8 für Smartphones

2. Klicken Sie auf die Schaltfläche **Weiter**.

Es öffnet sich das Fenster **KES 8** mit einer Liste der gefundenen angeschlossenen Geräte.

Wenn mehrere Geräte, die die Systemvoraussetzungen erfüllen, an die Workstation angeschlossen sind, werden diese im folgenden Fenster **KES 8** in einer Liste der gefundenen verbundenen Geräte angezeigt.

3. Wählen Sie ein oder mehrere Geräte aus der Liste der gefundenen verbundenen Geräte aus, auf denen das Programm installiert werden soll. Aktivieren Sie dazu die Kontrollkästchen für die Gerätenamen (s. Abb. unten).

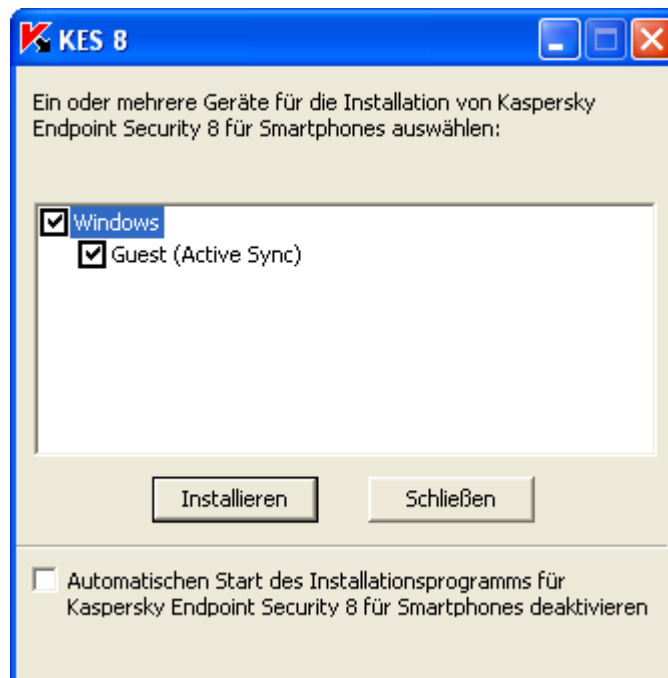


Abbildung 2: Auswahl der Geräte für die Installation von Kaspersky Endpoint Security 8 für Smartphones

4. Klicken Sie auf **Installieren**.

Das Tool verteilt die Programmdistribution an die ausgewählten Geräte. Der Status der Übertragung der Programmdistribution auf das Gerät wird auf der Workstation im Fenster **KES 8** dargestellt.

Nachdem die Distribution auf die ausgewählten mobilen Geräte kopiert wurde, startet automatisch die Programminstallation.

Falls bei der Programminstallation Fehler auftreten sollten, wenden Sie sich an den Administrator.

- ➔ Um zu verbieten, dass Kaspersky Endpoint Security 8 für Smartphones bei künftigen Verbindungen von Geräten mit dem Computer installiert wird:

aktivieren Sie im Fenster **KES 8** das Kontrollkästchen **Automatischen Start des Installationsprogramms für Kaspersky Endpoint Security 8 für Smartphones deaktivieren**.

ÜBER DIE PROGRAMMINSTALLATION NACH DEM EMPFANG EINER E-MAIL-NACHRICHT

Sie erhalten per E-Mail eine Nachricht von Ihrem Administrator. Die Nachricht enthält eine Programmdistribution oder einen Link für deren Download.

Die Nachricht enthält folgende Informationen:

- Anhang mit der Programmdistribution oder Link zum Download der Distribution
- Informationen über die Einstellungen für eine Verbindung des Programms mit dem Remote-Management-System

Bewahren Sie diese Nachricht auf, bis die Installation von Kaspersky Endpoint Security 8 für Smartphones auf dem Gerät abgeschlossen wurde.

PROGRAMMINSTALLATION NACH DEM EMPFANG EINER E-MAIL-NACHRICHT

➔ *Zur Installation von Kaspersky Endpoint Security 8 für Smartphones:*

1. Öffnen Sie auf dem mobilen Gerät oder auf der Workstation die Nachricht des Administrators, die die Einstellungen für die Programminstallation enthält.
2. Führen Sie eine der folgende Aktionen aus:
 - Wenn die Nachricht einen Link enthält, folgen Sie dem Link und laden Sie die Programmdistribution herunter.
 - Wenn die Distribution an die Nachricht angehängt ist, laden Sie die Programmdistribution herunter.

Wenn Sie die Programmdistribution auf ein mobiles Gerät herunterladen, wird diese auf dem Gerät standardmäßig im Ordner **Eigene Dateien** gespeichert.

3. Führen Sie eine der folgende Aktionen aus:
 - Wenn Sie die Programmdistribution auf das mobile Gerät heruntergeladen haben, öffnen Sie sie.
 - Wenn Sie die Programmdistribution auf die Workstation heruntergeladen haben, verbinden Sie das Gerät über Microsoft ActiveSync mit der Workstation, kopieren Sie die Distribution auf das Gerät und öffnen Sie sie.

Die Programminstallation startet automatisch und das Programm wird auf dem Gerät installiert.

4. Öffnen Sie das Programm (s. Abschnitt "Programm starten" auf S. [25](#)). Wählen Sie dazu **Start** → **Programme** → **KES 8** und starten Sie das Programm. Verwenden Sie dazu den Stylus oder die mittlere Joystick-Taste.
5. Legen Sie einen Geheimcode für das Programm fest (s. Abschnitt "Geheimcode eingeben" auf S. [25](#)). Füllen Sie dazu die Felder **Neuen Code eingeben** und **Code bestätigen** aus, und klicken Sie auf **OK**.

Das Fenster **Synchr.-Einstellungen** wird geöffnet (s. Abb. unten).

Server

test.company.com

Port

13292

Gruppe

KES8

Ihre E-Mail-Adresse

user@company.com

Beenden Weiter

Abbildung 3: Synchronisierungseinstellungen

6. Passen Sie die Einstellungen für eine Verbindung mit dem Remote-Management-System an, wenn die entsprechenden Werte in der Nachricht des Administrators enthalten waren. Legen Sie Werte für folgende Einstellungen fest:

- **Server**
- **Port**
- **Gruppe**

Falls es überflüssig ist, die Einstellungen für eine Verbindung mit dem Remote-Management-System anzupassen, wird dieser Schritt übersprungen.

7. Geben Sie im Feld **Ihre E-Mail-Adresse** Ihre geschäftliche E-Mail-Adresse ein und klicken Sie auf **Weiter**.

Achten Sie darauf, dass die E-Mail-Adresse richtig eingegeben wird, da diese bei der Anmeldung des Geräts im Remote-Management-System verwendet wird.

Falls bei der Programminstallation Fehler auftreten sollten, wenden Sie sich an den Administrator.

PROGRAMM DEINSTALLIEREN

Es bestehen folgende Möglichkeiten, um das Programm von einem Gerät zu entfernen:

- manuell durch den Benutzer (s. Abschnitt "Manuelle Deinstallation des Programms" auf S. [16](#))
- ferngesteuert durch den Administrator, mithilfe eines Remote-Management-Systems

Beim Löschen werden automatisch folgende Aktionen ausgeführt:

- Das Verbergen sensibler Daten wird deaktiviert.
- Daten, die auf dem Gerät mit Kaspersky Endpoint Security 8 für Smartphones verschlüsselt worden sind, werden entschlüsselt.

Bei der automatischen Deinstallation (s. Abschnitt "Automatische Deinstallation des Programms" auf S. [17](#)), kann eine Mitwirkung des Benutzer erforderlich sein, falls für das Programm ein Geheimcode festgelegt wurde:

Wenn das Programm nicht gestartet und kein Geheimcode festgelegt wurde, verläuft die automatische Deinstallation ohne Mitwirkung des Benutzers.

IN DIESEM ABSCHNITT

Manuelle Deinstallation des Programms	16
Automatische Deinstallation des Programms	17

MANUELLE DEINSTALLATION DES PROGRAMMS

➔ *Gehen Sie folgendermaßen vor, um das Programm manuell zu entfernen:*

1. Beenden Sie Kaspersky Endpoint Security 8 für Smartphones. Gehen Sie dazu auf **Menü** → **Beenden**.
2. Entfernen Sie Kaspersky Endpoint Security 8 für Smartphones. Gehen Sie dazu folgendermaßen vor:
 - a. Klicken Sie auf **Start** → **Einstellungen**.
 - b. Wählen Sie auf der Registerkarte **System** den Punkt **Programme entfernen** (s. Abb. unten).

Abbildung 4: Registerkarte **System**

- c. Wählen Sie in der Liste der installierten Programme **KES 8** aus und klicken Sie auf **Entfernen**.
- d. Bestätigen Sie die Deinstallation im folgenden Fenster mit **Ja**.
- e. Geben Sie den Geheimcode ein und klicken Sie auf **OK**.
- f. Legen Sie fest, ob Programmeinstellungen und Quarantäneobjekte gespeichert werden sollen:
 - Wenn Sie Programmeinstellungen und Quarantäneobjekte speichern möchten, klicken Sie auf **Speichern**.
 - Um das Programm vollständig zu entfernen, klicken Sie auf **Löschen**.

Die Deinstallation des Programms beginnt.

Wenn auf Ihrem Gerät das Verbergen sensibler Daten aktiviert ist und / oder wenigstens ein Ordner mit Kaspersky Endpoint Security 8 für Smartphones verschlüsselt wurde, deaktiviert das Programm automatisch das Verbergen sensibler Daten und / oder entschlüsselt alle Ordner.

3. Starten Sie das Gerät neu, um die Deinstallation des Programms abzuschließen.

AUTOMATISCHE DEINSTALLATION DES PROGRAMMS

Wenn die Programmdeinstallation vom Administrator über das Remote-Management-System ausgeführt wird und Sie keinen Geheimcode für das Programm festgelegt haben, wird automatisch das Fenster von Kaspersky Endpoint Security 8 für Smartphones geöffnet, in dem Sie zu den Aktionen aufgefordert werden, die zur Programmdeinstallation erforderlich sind.

➔ *Geben Sie den Geheimcode ein*

und klicken Sie im Fenster **Kaspersky Endpoint Security 8 für Smartphones** auf **OK**, um das Programm zu entfernen.

Es erscheint ein Fenster zur Bestätigung der Programmdeinstallation. Bestätigen Sie die Deinstallation des Programms mit **Ja**.

Wenn auf Ihrem Gerät das Verbergen sensibler Daten aktiviert ist und / oder wenigstens ein Ordner mit Kaspersky Endpoint Security 8 für Smartphones verschlüsselt wurde, deaktiviert das Programm automatisch das Verbergen sensibler Daten und / oder entschlüsselt alle Ordner.

Das Programm wird vom Gerät entfernt und auf dem Bildschirm wird eine Meldung über die erfolgreiche Deinstallation angezeigt.

Wenn Sie ablehnen, wird die Deinstallation abgebrochen. In diesem Fall erfolgt ein erneuter Deinstallationsversuch bei der nächsten Synchronisierung mit dem Remote-Management-System. Danach wird Ihnen erneut vorgeschlagen, das Programm zu entfernen.

PROGRAMMEINSTELLUNGEN VERWALTEN

Alle Einstellungen für die Arbeit von Kaspersky Endpoint Security 8 für Smartphones, einschließlich der Lizenz, werden vom Administrator über ein Remote-Management-System angepasst. Dabei kann der Administrator dem Benutzer erlauben oder verbieten, diese Einstellungen zu ändern.

Sie können die Funktionseinstellungen für das Programm auf dem mobilen Gerät ändern, falls der Administrator dies nicht untersagt hat.

Der Administrator kann entweder alle oder nur bestimmte Einstellungen einer Komponente für Änderungen sperren. Wenn im oberen Bereich des Konfigurationsfensters einer Komponente ein Schlosssymbol und eine Warnmeldung vorhanden sind, können die Einstellungen der Komponente auf dem mobilen Gerät nicht geändert werden.

Wenn der Administrator die Programmeinstellungen geändert hat, werden sie über das Remote-Management-System an das Gerät übertragen. Dabei werden auf dem Gerät die Werte der Programmeinstellungen geändert, die vom Administrator gesperrt wurden. Einstellungen, die vom Administrator nicht gesperrt wurden, bleiben unverändert und behalten die zuvor eingestellten Werte bei.

Wenn das Gerät keine Programmeinstellungen empfangen hat oder Sie die vom Administrator festgelegten Einstellungen wiederherstellen möchten, verwenden Sie die Funktion zur Synchronisierung des Geräts mit dem Remote-Management-System (s. Abschnitt "Synchronisierung manuell starten" auf S. [22](#)).

Verwenden Sie die Synchronisierungsfunktion nur unter Anleitung des Administrators.

LIZENZVERWALTUNG

Dieser Abschnitt informiert über die Programmlizenz, die Lizenzaktivierung und die Anzeige von Lizenzinformationen.

IN DIESEM ABSCHNITT

Über Lizenzen für Kaspersky Endpoint Security 8 für Smartphones.....	20
Lizenz installieren.....	21
Lizenz-Info anzeigen	21

ÜBER LIZENZEN FÜR KASPERSKY ENDPOINT SECURITY 8 FÜR SMARTPHONES

Die *Lizenz* verleiht das Recht zur Nutzung von Kaspersky Endpoint Security 8 für Smartphones und der zum Programm gehörenden Zusatzleistungen, die von Kaspersky Lab und seinen Partnern angeboten werden.

Um das Programm nutzen zu können, muss eine Lizenz installiert sein.

Jede Lizenz wird durch Gültigkeitsdauer und Typ charakterisiert.

Die *Gültigkeitsdauer einer Lizenz* ist die Zeitspanne, für die Ihnen die Zusatzleistungen zur Verfügung stehen.

- Technischer Support;
- Update der Antiviren-Datenbanken des Programms

Der Umfang der angebotenen Leistungen ist vom Lizenztyp abhängig.

Es sind folgende Lizenztypen vorgesehen:

- *Test* – Kostenlose Lizenz mit begrenzter Gültigkeitsdauer (z. B. 30 Tage) zum Kennenlernen von Kaspersky Endpoint Security 8 für Smartphones.

Während der Gültigkeitsdauer der Testlizenz sind alle Programmfunktionen verfügbar. Nach Ablauf der Gültigkeitsdauer einer Testlizenz stellt Kaspersky Endpoint Security 8 für Smartphones alle Funktionen ein. In diesem Fall sind nur folgende Aktionen möglich:

- Deaktivieren der Komponenten Verschlüsselung und Privatsphäre
- Der Benutzer kann die Ordner entschlüsseln, die er zur Verschlüsselung ausgewählt hat.
- Verbergen von sensiblen Daten deaktivieren
- Hilfesystem für das Programm anzeigen
- Synchronisierung mit dem Remote-Management-System.
- *Kommerziell* – Gekaufte Lizenz, die eine begrenzte Gültigkeitsdauer (z. B. 1 Jahr) besitzt und beim Kauf von Kaspersky Endpoint Security 8 für Smartphones zur Verfügung gestellt wird.

Während der Laufzeit einer kommerziellen Lizenz sind alle Programmfunktionen und zusätzliche Services verfügbar.

Nach Ablauf der Gültigkeitsdauer einer kommerziellen Lizenz kommt es zu einer Einschränkung des Funktionsumfangs von Kaspersky Endpoint Security 8 für Smartphones. Sie können weiterhin die Komponenten Anti-Spam und Firewall verwenden, Ihr mobiles Gerät auf Viren untersuchen und die Schutzkomponenten nutzen, jedoch nur mit den Antiviren-Datenbanken, die bei Ablauf der Lizenz aktuell waren. Für die übrigen Programmkomponenten sind nur folgende Aktionen verfügbar:

- Deaktivieren der Komponenten Verschlüsselung, Diebstahlschutz und Privatsphäre
- Entschlüsselung der Ordner, die vom Benutzer für die Verschlüsselung gewählt wurden
- Verbergen von sensiblen Daten deaktivieren
- Hilfesystem für das Programm anzeigen
- Synchronisierung mit dem Remote-Management-System.

LIZENZ INSTALLIEREN

Die Lizenz wird vom Administrator über das Remote-Management-System installiert.

Ohne Lizenz funktioniert Kaspersky Endpoint Security 8 für Smartphones innerhalb von drei Tagen nach der Programminstallation in vollem Funktionsumfang. Innerhalb dieser Frist installiert der Administrator über das Remote-Management-System eine Lizenz und das Programm wird aktiviert.

Wenn innerhalb von drei Tagen keine Lizenz installiert wurde, wird die Funktionalität des Programms eingeschränkt. In diesem Modus sind folgende Aktionen möglich:

- Alle Komponenten deaktivieren
- Einen oder mehrere Ordner verschlüsseln
- Verbergen von sensiblen Daten deaktivieren
- Hilfesystem für das Programm anzeigen

Wenn innerhalb von drei Tagen nach der Installation keine Lizenz installiert wurde, verwenden Sie zur Lizenzinstallation die Funktion zur Synchronisierung des Geräts mit dem Remote-Management-System (s. Abschnitt "Synchronisierung manuell starten" auf S. [22](#)).

LIZENZ-INFO ANZEIGEN

Sie können folgende Informationen zur Lizenz lesen: Nummer und Typ der Lizenz, Aktivierungsdatum, Ablaufdatum, verbleibende Gültigkeitsdauer und Seriennummer des Geräts.

➡ *Gehen Sie folgendermaßen vor, um Informationen zur Lizenz anzuzeigen:*

1. Gehen Sie auf **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie **Lizenz-Info**.

SYNCHRONISIERUNG MIT DEM REMOTE-MANAGEMENT-SYSTEM

Bei der Synchronisierung werden die vom Administrator festgelegten Programmeinstellungen auf das Gerät übertragen. Vom Gerät werden Berichte über die Arbeit der Programmkomponenten an das Remote-Management-System übertragen.

Die Synchronisierung des Geräts mit dem Remote-Management-System erfolgt automatisch.

Falls die Synchronisierung nicht automatisch ausgeführt wird, können Sie sie manuell starten.

Eine manuelle Synchronisierung ist erforderlich, wenn innerhalb von drei Tagen nach der Programminstallation keine Lizenz installiert wurde.

Abhängig vom Remote-Management-System, das der Administrator zur Programmverwaltung einsetzt, kann der Benutzer bei der Programminstallation aufgefordert werden, die Einstellungen für eine Verbindung zu dem Remote-Management-System einzugeben. In diesem Fall können die Werte, die der Benutzer manuell festgelegt hat, vom Programm aus geändert werden (s. Abschnitt "Synchronisierungseinstellungen ändern" auf S. [23](#)).

Ändern Sie die Einstellungen für eine Verbindung zu dem Remote-Management-System nur unter Anleitung des Administrators.

IN DIESEM ABSCHNITT

Synchronisierung manuell starten	22
Synchronisierungseinstellungen ändern.....	23

SYNCHRONISIERUNG MANUELL STARTEN

➤ Gehen Sie folgendermaßen vor, um das Gerät manuell mit dem Remote-Management-System zu synchronisieren:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie den Punkt **Synchronisierung starten** (s. Abb. unten) aus.



Abbildung 5: Synchronisierung manuell starten

Wenn der Benutzer bei der Programminstallation nicht aufgefordert wurde, die Einstellungen für eine Verbindung zum Remote-Management-System einzugeben, so erscheint ein Fenster zur Bestätigung der Internetverbindung. Erlauben Sie die Verbindung mit **Ja**. Es wird eine Verbindung mit dem Remote-Management-System hergestellt.

Wenn der Benutzer bei der Programminstallation aufgefordert wurde, die Einstellungen für eine Verbindung zum Remote-Management-System anzugeben, so heißt in diesem Fall der Menüpunkt **Synchronisierung** und das Fenster **Synchronisierung** wird geöffnet. Wählen Sie den Punkt **Synchronisierung starten** aus. Erlauben Sie die Internetverbindung mit **Ja**. Es wird eine Verbindung mit dem Remote-Management-System hergestellt.

SYNCHRONISIERUNGSEINSTELLUNGEN ÄNDERN

Ändern Sie die Einstellungen für eine Verbindung zu dem Remote-Management-System nur auf Anweisung des Administrators.

➤ Gehen Sie folgendermaßen vor, um die Einstellungen für eine Verbindung mit dem Remote-Management-System zu ändern:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Synchronisierung**.

Das Fenster **Synchronisierung** wird geöffnet.

3. Gehen Sie auf **Synchronisierungseinstellungen** (s. Abb. unten).



Abbildung 6: Synchronisierungseinstellungen ändern

4. Ändern Sie die Werte für folgende Einstellungen:
 - **Server**
 - **Port**
 - **Gruppe**
5. Klicken Sie auf **OK**.

ERSTE SCHRITTE

Dieser Abschnitt informiert über die ersten Schritte bei der Arbeit mit Kaspersky Endpoint Security 8 für Smartphones: Geheimcode für das Programm festlegen, Programm starten, Antiviren-Datenbanken aktualisieren und Gerät auf Viren untersuchen.

IN DIESEM ABSCHNITT

Programm starten	25
Geheimcode eingeben	25
Update der Programm-Datenbanken	26
Gerät auf Viren untersuchen	26
Programm-Infos anzeigen	27

PROGRAMM STARTEN

➤ *Gehen Sie folgendermaßen vor, um Kaspersky Endpoint Security 8 für Smartphones zu starten:*

1. Wählen Sie **Start** → **Programme**.
2. Wählen Sie **KES 8** und starten Sie das Programm. Verwenden Sie dazu den Stylus oder die mittlere Joystick-Taste.
3. Gehen Sie zur Eingabe des Geheimcodes des Programms (s. Abschnitt "Geheimcode eingeben" auf S. [25](#)).

GEHEIMCODE EINGEBEN

Nachdem das Programm gestartet wurde, werden Sie aufgefordert, den Geheimcode des Programms einzugeben. Der *Geheimcode des Programms* verhindert einen unautorisierten Zugriff auf die Programmeinstellungen. Der aktuelle Geheimcode des Programms kann später geändert werden.

Kaspersky Endpoint Security 8 für Smartphones fragt in folgenden Fällen nach dem Geheimcode:

- für den Zugriff auf das Programm
- für den Zugriff auf verschlüsselte Ordner
- wenn von einem anderen mobilen Gerät aus ein SMS-Befehl gesendet wird, um folgende Funktionen ferngesteuert zu starten: SMS-Block, SMS-Clean, SIM-Watch, GPS-Find, Privatsphäre.
- bei der Deinstallation des Programms

Merken Sie sich den Geheimcode des Programms, Ohne Geheimcode können die Funktionen von Kaspersky Endpoint Security 8 für Smartphones nicht mehr ausgeführt werden und es ist es nicht mehr möglich, auf verschlüsselte Dateien zuzugreifen und das Programm zu entfernen.

Der Geheimcode des Programms besteht aus Ziffern. Er muss aus mindestens vier Zeichen bestehen.

➤ *Gehen Sie folgendermaßen vor, um den Geheimcode für das Programm einzugeben:*

1. Nach dem ersten Start des Programms geben Sie im Feld **Neuen Code eingeben** Ihren Geheimcode ein.
2. Wiederholen Sie die Eingabe im Feld **Code bestätigen**.

Ein eingegebener Code wird automatisch auf seine Sicherheit geprüft.

3. Ergibt die Prüfung, dass ein Code unsicher ist, so erscheint auf dem Bildschirm eine Warnung und das Programm erfragt eine Bestätigung. Um das Fenster zu schließen, klicken Sie auf **OK**. Klicken Sie auf **Nein**, um einen neuen Code festzulegen.
4. Klicken Sie zum Abschluss auf **OK**.

UPDATE DER PROGRAMM-DATENBANKEN

Bei der Suche nach Bedrohungen verwendet Kaspersky Endpoint Security 8 für Smartphones die Antiviren-Datenbanken des Programms, die eine Beschreibung aller derzeit bekannten schädlichen Programme und entsprechende Desinfektionsmethoden sowie eine Beschreibung sonstiger unerwünschter Objekte enthalten. Die Antiviren-Datenbanken, die zum Lieferumfang von Kaspersky Endpoint Security 8 für Smartphones gehören, können zum Zeitpunkt der Programminstallation bereits veraltet sein.

Es wird empfohlen, die Antiviren-Datenbanken des Programms sofort nach der Programminstallation zu aktualisieren.

Um die Antiviren-Datenbanken des Programms zu aktualisieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

➤ *Gehen Sie folgendermaßen vor, um das Update der Antiviren-Datenbanken des Programms zu starten:*

1. Wählen Sie **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Update**.

Das Fenster **Update** wird geöffnet.

3. Gehen Sie auf **Update**.

Das Programm startet das Update der Datenbanken von dem Server, der vom Administrator festgelegt wurde. Informationen über den Updatevorgang werden auf dem Bildschirm angezeigt.

GERÄT AUF VIREN UNTERSUCHEN

Es wird empfohlen, Ihr mobiles Gerät nach der Programminstallation vollständig auf schädliche Objekte zu untersuchen.

Sie können eine Untersuchung mit den aktuellen Einstellungen starten oder die Einstellungen vorher anpassen (s. Abschnitt "Untersuchung des Geräts" auf S. [35](#)).

➤ *Gehen Sie folgendermaßen vor, um eine vollständige Untersuchung des Geräts zu starten:*

1. Wählen Sie **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Scan**.

Das Fenster **Scan** wird geöffnet.

3. Wählen Sie **Alles scannen**.

PROGRAMM-INFOS ANZEIGEN

Sie können allgemeine Informationen über das Programm Kaspersky Endpoint Security 8 für Smartphones und seine Version anzeigen.

➔ *Gehen Sie folgendermaßen vor, um Informationen über das Programm anzuzeigen:*

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf den Punkt **Programm-Infos** (s. Abb. unten).



Abbildung 7: Programm-Infos

PROGRAMMOBERFLÄCHE

Dieser Abschnitt informiert über die wichtigsten Elemente der Benutzeroberfläche von Kaspersky Endpoint Security 8 für Smartphones.

IN DIESEM ABSCHNITT

Fenster für den Schutzstatus	28
Programm-Menü	29

FENSTER FÜR DEN SCHUTZSTATUS

Der Status der wichtigsten Programmkomponenten wird im Fenster für den Schutzstatus angezeigt.

Es gibt drei Statusvarianten. Jeder Status wird durch eine Farbe signalisiert. Die Farben entsprechen den Signalen einer Ampel. Grün bedeutet, dass der Schutz Ihres Geräts dem erforderlichen Niveau entspricht. Gelb und Rot signalisieren, dass bestimmte Sicherheitsrisiken vorliegen. Als Bedrohung gelten nicht nur veraltete Datenbanken, sondern auch deaktivierte Schutzkomponenten und Auswahl einer niedrigen Sicherheitsstufe.

Das Fenster für den Schutzstatus ist sofort nach dem Programmstart verfügbar und bietet folgende Informationen:

- **Schutz** – Status des Echtzeitschutzes (s. Abschnitt "Schutz für das Dateisystem " auf S. [31](#)).

Grün bedeutet, dass der Schutz aktiviert ist und dem erforderlichen Niveau entspricht. Die Antiviren-Datenbanken des Programms sind aktuell.

Gelb zeigt an, dass die Datenbanken seit mehreren Tagen nicht aktualisiert wurden.

Rot signalisiert Probleme, die zu Datenverlust oder zur Infektion des Geräts führen können. Beispiele: Der Schutz wurde deaktiviert, oder das Programm wurde seit über zwei Wochen nicht aktualisiert.

- **Firewall** – Stufe für den Schutz des Geräts vor unerwünschter Netzwerkaktivität (s. Abschnitt "Filterung der Netzwerkaktivität. Firewall" auf S. [79](#)).

Das grüne Statussymbol bedeutet, dass die Komponente aktiviert ist. Der Firewall-Modus wurde ausgewählt.

Rot zeigt an, dass die Firewall deaktiviert wurde.

- **Diebstahlschutz** – Status des Datenschutzes für den Fall eines Diebstahls oder Verlusts des Geräts (s. Abschnitt "Datenschutz bei Verlust oder Diebstahl des Geräts" auf S. [57](#)).

Das grüne Statussymbol bedeutet, dass die Diebstahlschutz-Funktionen, die unter dem Status der Komponente angezeigt werden, aktiviert sind.

Rot zeigt an, dass alle Funktionen des Diebstahlschutzes deaktiviert sind.

- **Privatsphäre** – Status für das Verbergen sensibler Daten (s. Abschnitt "Verbergen sensibler Daten" auf S. [69](#)).

Grün bedeutet, dass das Verbergen sensibler Daten aktiviert ist. Vertrauliche Informationen werden verborgen.

Das gelbe Symbol warnt davor, dass das Verbergen sensibler Daten deaktiviert wurde. Vertrauliche Informationen werden angezeigt und können angezeigt werden.

- **Lizenz** – Gültigkeitsdauer der Lizenz (s. Abschnitt "Lizenzverwaltung" auf S. [20](#)).

Das grüne Statussymbol bedeutet, dass die Lizenz noch mehr als 14 Tage gültig ist.

Gelb warnt davor, dass die Lizenz weniger als 14 Tage gültig ist.

Rot signalisiert, dass die Gültigkeit der Lizenz abgelaufen ist oder keine Lizenz installiert wurde.



Abbildung 8: Fenster für den Schutzstatus

Sie können auch in das Fenster für den Schutzstatus wechseln. Wählen Sie dazu **Menü** → **Schutzstatus**.

PROGRAMM-MENÜ

Die Programmkomponenten sind logisch angeordnet und stehen im Programm-Menü zur Verfügung. Die einzelnen Menüpunkte erlauben es, die Einstellungen einer ausgewählten Komponente zu öffnen oder Schutzaufgaben zu wählen (s. Abb. unten).



Abbildung 9: Programm-Menü

Das Menü von Kaspersky Endpoint Security 8 für Smartphones enthält folgende Punkte:

- **Anti-Virus** – Virenschutz für das Dateisystem, Untersuchung und Update der Antiviren-Datenbanken des Programms.
- **Diebstahlschutz** – Schutz für die Informationen auf dem Gerät bei Diebstahl oder Verlust.
- **Privatsphäre** – Verbergen von vertraulichen Informationen auf dem Gerät.
- **Verschlüsselung** – Verschlüsselung von Daten auf dem Gerät.
- **Anti-Spam** – Filterung von unerwünschten eingehenden Anrufen und SMS.
- **Firewall** – Kontrolle der Netzwerkaktivität.
- **Erweitert** – allgemeine Programmeinstellungen, Start der Synchronisierung des Geräts mit dem Remote-Management-System, Informationen zum Programm und zur Lizenz.
- **Schutzstatus** – Informationen zum Status der wichtigsten Programmkomponenten.
- **Beenden** – Anpassen der Programmeinstellungen beenden.

➤ *Um das Programm-Menü zu öffnen,*
gehen Sie auf **Menü**.

Verwenden Sie zur Navigation innerhalb des Programm-Menüs den Joystick des Geräts oder den Stylus.

➤ *Gehen Sie folgendermaßen vor, um zum Statusfenster für die Programmkomponenten zurückzukehren:*
gehen Sie auf **Menü** → **Schutzstatus**.

➤ *Gehen Sie folgendermaßen vor, um das Programm zu beenden:*
gehen Sie auf **Menü** → **Beenden**.

SCHUTZ FÜR DAS DATEISYSTEM

Dieser Abschnitt informiert über die Komponente Schutz, die das Dateisystem Ihres Geräts vor Infektionen schützt. Außerdem wird hier beschrieben, wie der Schutz aktiviert / angehalten wird und wie die Schutzeinstellungen angepasst werden.

IN DIESEM ABSCHNITT

Schutz	31
Schutz aktivieren / deaktivieren.....	31
Aktion für schädliche Objekte auswählen.....	33

SCHUTZ

Der Schutz startet beim Hochfahren des Betriebssystems und befindet sich permanent im Arbeitsspeicher des Geräts. Schutz überwacht im Hintergrundmodus alle Veränderungen, die im Dateisystem erfolgen, und untersucht das Dateisystem auf schädliche Objekte. Der Untersuchungsvorgang für eine Datei wird nach folgendem Algorithmus ausgeführt:

1. Der Schutz untersucht jede Datei, auf die Sie zugreifen.
2. Der Schutz analysiert eine Datei auf schädliche Objekte. Schädliche Objekte werden auf Basis der Antiviren-Datenbanken des Programms erkannt. Die Antiviren-Datenbanken des Programms enthalten eine Beschreibung aller momentan bekannten schädlichen Objekte und entsprechende Desinfektionsmethoden.
3. Aufgrund der Analyseergebnisse sind folgende Varianten für das Verhalten des Schutzes möglich:
 - Wenn in einer Datei Schadcode gefunden wird, sperrt der Schutz die Datei und führt die festgelegte Aktion aus.
 - Wenn in einer Datei kein schädlicher Code gefunden wird, erhält der Benutzer sofort Zugriff auf die Datei.

Informationen über die Arbeit des Schutzes werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [93](#)).

SCHUTZ AKTIVIEREN / DEAKTIVIEREN

Wenn der Schutz aktiviert ist, werden alle Aktionen in Ihrem System permanent kontrolliert.

Der Schutz vor Viren und anderen Bedrohungen beansprucht die Ressourcen des Geräts. Wenn mehrere Aufgaben ausgeführt werden, kann der Schutz vorübergehend beendet werden, um die Auslastung des Geräts zu senken.

Die Kaspersky-Lab-Spezialisten warnen davor, den Schutz zu deaktivieren, weil dies zur Infektion Ihres Computers und zu Datenverlust führen kann.

Das Deaktivieren des Schutzes beeinflusst die Ausführung von Aufgaben zum Scan auf Befehl und zum Update der Antiviren-Datenbanken des Programms nicht.

Der aktuelle Schutzstatus wird im Fenster **Anti-Virus** neben dem Menüpunkt **Schutz** angezeigt.

Der Schutz kann folgendermaßen aktiviert / deaktiviert werden:

- aus dem Menü für die Einstellungen der Komponente
- aus dem Menü **Anti-Virus**

Verwenden Sie die Joystick-Tasten des Geräts, um die Parameterwerte zu ändern.

➔ *Gehen Sie folgendermaßen vor, um den Schutz zu aktivieren:*

1. Wählen Sie **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Schutz**.

Das Fenster **Schutz** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Schutz aktivieren** (s. Abb. unten).

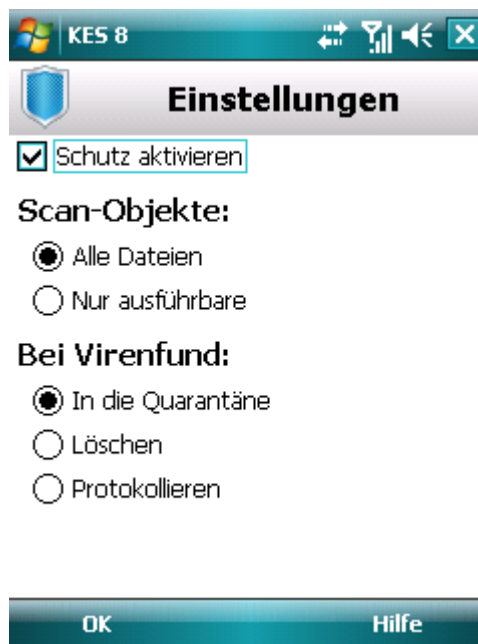


Abbildung 10: Schutz aktivieren

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

➔ *Gehen Sie folgendermaßen vor, um den Schutz zu deaktivieren:*

1. Wählen Sie **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Schutz**.

Das Fenster **Schutz** wird geöffnet.

3. Deaktivieren Sie das Kontrollkästchen **Schutz aktivieren**.

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

➤ Gehen Sie folgendermaßen vor, um den Schutz schnell zu aktivieren / deaktivieren:

1. Gehen Sie auf **Menü** → **Anti-Virus**.
2. Das Fenster **Anti-Virus** wird geöffnet.
3. Klicken Sie auf **Aktivieren** / **Deaktivieren**. Die Beschriftung des Menüpunkts ändert sich abhängig vom aktuellen Schutzstatus in das jeweilige Gegenteil.

AKTION FÜR SCHÄDLICHE OBJEKTE AUSWÄHLEN

Sie können eine Aktion auswählen, die Kaspersky Endpoint Security 8 für Smartphones mit gefundenen schädlichen Objekten ausführen soll.

Verwenden Sie die Joystick-Tasten des Geräts, um die Parameterwerte zu ändern.

Um die Schutzeinstellungen zu ändern, vergewissern Sie sich, dass der Schutz aktiviert ist.

➤ Gehen Sie folgendermaßen vor, um eine Aktion für ein gefundenes schädliches Objekt festzulegen:

1. Wählen Sie **Menü** → **Anti-Virus**.
Das Fenster **Anti-Virus** wird geöffnet.
2. Gehen Sie auf **Schutz**.
Das Fenster **Schutz** wird geöffnet.
3. Legen Sie eine Aktion fest, die das Programm mit einem schädlichen Objekt ausführen soll. Wählen Sie dazu einen Wert für **Bei Virenfund** (s. Abb. unten):
 - **Nach Quarantäne** – Objekte in die Quarantäne verschieben.
 - **Löschen** – schädliche Objekte löschen, ohne den Benutzer zu benachrichtigen.
 - **Protokollieren** – schädliche Objekte überspringen und Fund in den Programmbericht eintragen. Zugriffsversuche auf ein Objekt (z. B. Objekt kopieren oder öffnen) blockieren.

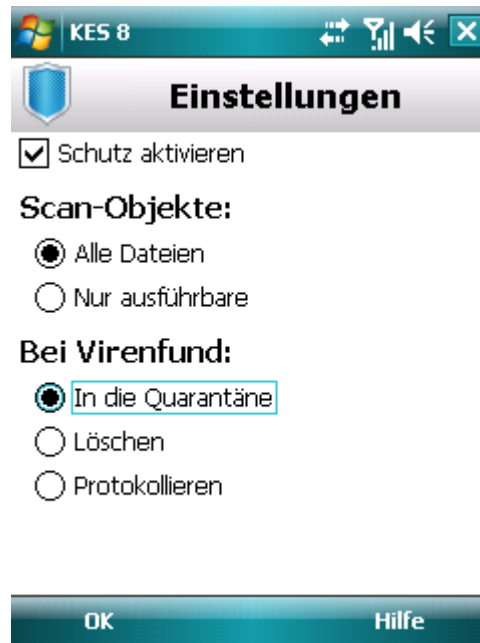


Abbildung 11: Aktion für gefundene Bedrohung wählen

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

UNTERSUCHUNG DES GERÄTS

Dieser Abschnitt informiert über die auf Befehl gestartete Untersuchung des Geräts, mit der Bedrohungen auf Ihrem Gerät erkannt und beseitigt werden können. Außerdem werden hier folgende Vorgänge beschrieben: Untersuchung des Geräts starten, Zeitplan für die automatische Untersuchung des Dateisystems erstellen, Untersuchungsobjekte auswählen, Aktion des Programms für gefundene Schadobjekte festlegen.

IN DIESEM ABSCHNITT

Über Scan auf Befehl	35
Untersuchung manuell starten	36
Untersuchung nach Zeitplan starten	37
Typ der Untersuchungsobjekte wählen	38
Archiv-Untersuchung anpassen	39
Aktion für gefundene Objekte wählen	40

ÜBER SCAN AUF BEFEHL

Mit der auf Befehl gestarteten Untersuchung lassen sich schädliche Objekte erkennen und neutralisieren. Mit Kaspersky Endpoint Security 8 kann der Inhalt des Geräts vollständig oder teilweise untersucht werden, d.h., die Untersuchung lässt sich auf den Inhalt des internen Gerätespeichers oder eines bestimmten Ordners (auch eines Ordners auf einer Speicherkarte) beschränken.

Die Untersuchung des Geräts wird nach folgendem Algorithmus ausgeführt:

1. Kaspersky Endpoint Security 8 für Smartphones untersucht die Dateien, die in den Untersuchungseinstellungen festgelegt wurden (s. Abschnitt "Typ der Untersuchungsobjekte auswählen" auf S. [38](#)).
2. Bei der Untersuchung analysiert das Programm eine Datei auf schädliche Objekte. Schädliche Objekte werden auf Basis der Antiviren-Datenbanken des Programms erkannt. Die Antiviren-Datenbanken des Programms enthalten eine Beschreibung aller momentan bekannten schädlichen Objekte und entsprechende Desinfektionsmethoden.
3. Aufgrund der Analyseergebnisse bestehen folgende Varianten für das Verhalten von Kaspersky Endpoint Security 8 für Smartphones:
 - Wenn in einer Datei schädlicher Code gefunden wird, sperrt Kaspersky Endpoint Security 8 für Smartphones die Datei und führt die in den Einstellungen festgelegte Aktion aus (s. Abschnitt "Aktion für gefundene Objekte wählen" auf S. [40](#)).
 - Wenn kein schädlicher Code gefunden wird, wird die Datei sofort zum Zugriff freigegeben.

Eine Untersuchung kann manuell oder automatisch nach einem erstellten Zeitplan (s. Abschnitt "Untersuchung nach Zeitplan starten" auf S. [37](#)) gestartet werden.

Informationen über die Ergebnisse des Scan auf Befehl werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [93](#)).

UNTERSUCHUNG MANUELL STARTEN

Sie können eine vollständige oder partielle Untersuchung manuell starten, wenn der Prozessor des Geräts nicht mit anderen Aufgaben beschäftigt ist.

➔ Gehen Sie folgendermaßen vor, um die Untersuchung zu starten:

1. Wählen Sie **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Scan**.

Das Fenster **Scan** wird geöffnet.

3. Wählen Sie einen Untersuchungsbereich für das Gerät (s. Abb. unten):

- **Alles scannen** – das gesamte Dateisystem des Geräts untersuchen. Das Programm untersucht standardmäßig die Dateien, die sich im Gerätespeicher oder auf Speicherkarten befinden.
- **Speicher scannen** – im Systemspeicher laufende Prozesse und die dazu gehörenden Dateien untersuchen.
- **Ordner scannen** – Das ausgewählte Objekt im Dateisystem des Geräts oder auf einer Speicherkarte untersuchen. Bei Auswahl dieses Punkts wird ein Fenster geöffnet, das die Dateisystemstruktur des Geräts enthält. Hier kann ein zu untersuchender Ordner ausgewählt werden. Verwenden Sie zur Navigation im Dateisystem die Joystick-Tasten oder den Stylus. Um die Untersuchung eines Ordners zu starten, markieren Sie den entsprechenden Ordner und klicken Sie auf **Scannen**.



Abbildung 12: Untersuchungsbereich wählen

Nach dem Start der Untersuchung öffnet sich das Untersuchungsfenster, in dem der aktuelle Status angezeigt wird: Anzahl der untersuchten Dateien und Pfad der momentan untersuchten Datei.

Wenn Kaspersky Endpoint Security 8 für Smartphones ein infiziertes Objekt erkennt, führt das Programm die Aktion aus, die in den Untersuchungseinstellungen festgelegt wurde (s. Abschnitt "Aktion für gefundene Objekte auswählen" auf S. 40).

Beim Abschluss einer Untersuchung erscheinen folgende Informationen auf dem Bildschirm:

- Anzahl der untersuchten Dateien
 - Anzahl der gefundenen, unter Quarantäne gestellten und gelöschten schädlichen Objekte
 - Anzahl der übersprungenen Dateien (Beispiele: Datei wird vom Betriebssystem verwendet oder Keine ausführbare Datei, wenn nur ausführbare Dateien untersucht werden)
 - Zeitpunkt der Untersuchung
4. Klicken Sie zum Abschluss auf **OK**.

UNTERSUCHUNG NACH ZEITPLAN STARTEN

Kaspersky Endpoint Security 8 für Smartphones erlaubt es, einen Zeitplan für den automatischen Start einer Untersuchung des Dateisystems anzupassen. Die geplante Untersuchung erfolgt im Hintergrund. Wenn ein infiziertes Objekt gefunden wird, führt das Programm die Aktion aus, die in den Untersuchungseinstellungen festgelegt wurde (s. Abschnitt "Aktion für gefundene Objekte wählen" auf S. [40](#)).

Damit eine geplante Untersuchung ausgeführt wird, muss das Gerät zum entsprechenden Zeitpunkt eingeschaltet sein.

➤ *Gehen Sie folgendermaßen vor, um den automatischen Start der Untersuchung anzupassen und einen Startzeitplan zu erstellen:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Scan**.

Das Fenster **Scan** wird geöffnet.

3. Gehen Sie auf **Scan-Zeitplan**.

Das Fenster **Zeitplan** wird geöffnet.

4. Aktivieren Sie das Kontrollkästchen **Scan nach Zeitplan** (s. Abb. unten).

5. Wählen Sie ein Intervall für den Start der Untersuchung aus. Wählen Sie dazu einen Wert für **Frequenz** aus:

- **Täglich:** Die Untersuchung erfolgt jeden Tag. Geben Sie im Feld **Zeit** einen Startzeitpunkt an.
- **Wöchentlich:** Die Untersuchung erfolgt einmal pro Woche. Legen Sie einen Zeitpunkt und einen Tag für den Untersuchungsstart fest. Geben Sie dazu Werte für die Einstellungen **Zeit** und **Wochentag** an.



Abbildung 13: Einstellungen für den automatischen Start einer geplanten vollständigen Untersuchung

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

TYP DER UNTERSUCHUNGSOBJEKTE WÄHLEN

Sie können den Typ der Dateien festlegen, die das Programm bei einer Untersuchung analysieren soll.

Verwenden Sie die Joystick-Tasten des Geräts, um die Parameterwerte zu ändern.

➤ Gehen Sie folgendermaßen vor, um einen Typ für die zu untersuchenden Dateien auszuwählen:

1. Wählen Sie **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Scan**.

Das Fenster **Scan** wird geöffnet.

3. Gehen Sie auf **Objekte/Aktionen**.

Das Fenster **Objekte/Aktionen** wird geöffnet.

4. Wählen Sie den Typ der zu untersuchenden Dateien im Block **Untersuchungsobjekte** aus (s. Abb. unten):

- **Alle Dateien** – alle Dateitypen untersuchen.
- **Nur ausführbare** – Es werden nur ausführbare Programmdateien der folgenden Formate untersucht: EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.

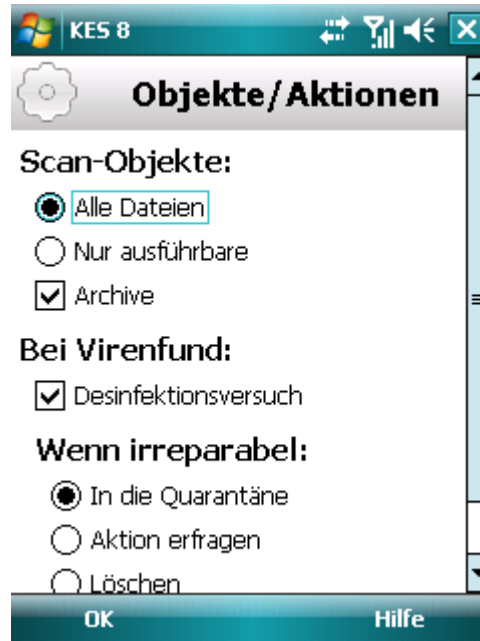


Abbildung 14: Typ der Untersuchungsobjekte wählen

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

ARCHIV-UNTERSUCHUNG ANPASSEN

Viren werden häufig in Archiven versteckt. Das Programm erlaubt eine Untersuchung von Archiven der folgenden Formate: ZIP, JAR, JAD und CAB. Archive werden bei der Untersuchung entpackt, wodurch die Geschwindigkeit des Scan auf Befehl wesentlich sinken kann.

Die Untersuchung von Archiven auf schädlichen Code, die während eines Scan auf Befehl ausgeführt wird, kann aktiviert / deaktiviert werden.

Verwenden Sie die Joystick-Tasten des Geräts, um die Parameterwerte zu ändern.

➤ Gehen Sie folgendermaßen vor, um die Untersuchung von Archiven zu aktivieren:

1. Gehen Sie auf **Menü** → **Anti-Virus**.
Das Fenster **Anti-Virus** wird geöffnet.
2. Gehen Sie auf **Scan**.
Das Fenster **Scan** wird geöffnet.
3. Gehen Sie auf **Objekte/Aktionen**.
Das Fenster **Objekte/Aktionen** wird geöffnet.
4. Aktivieren Sie im Block **Untersuchungsobjekte** das Kontrollkästchen **Archive**.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

AKTION FÜR GEFUNDENE OBJEKTE WÄHLEN

Wenn in einer Datei schädlicher Code gefunden wird, sperrt Kaspersky Endpoint Security 8 für Smartphones die Datei und führt die in den Einstellungen festgelegte Aktion aus.

Sie können die Aktion ändern, die das Programm mit einem gefundenen schädlichen Objekt ausführen soll.

Verwenden Sie die Joystick-Tasten des Geräts, um die Parameterwerte zu ändern.

➤ *Gehen Sie folgendermaßen vor, um die Aktion für ein gefundenes schädliches Objekt zu ändern:*

1. Wählen Sie **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Scan**.

Das Fenster **Scan** wird geöffnet.

3. Gehen Sie auf **Objekte/Aktionen**.

Das Fenster **Objekte/Aktionen** wird geöffnet.

4. Damit das Programm versucht, infizierte Objekte zu desinfizieren, aktivieren Sie für **Bei Virenfund** das Kontrollkästchen **Desinfektionsversuch** (s. Abb. unten).

5. Legen Sie eine Aktion für gefundene schädliche Objekte fest. Wählen Sie dazu einen Wert für **Aktion ausführen**:

Wenn das Kontrollkästchen **Desinfektionsversuch** aktiviert ist, heißt dieser Parameter **Wenn irreparabel**. Dieser Parameter legt fest, welche Aktion das Programm ausführen soll, wenn sich ein Objekt nicht desinfizieren lässt.

- **Nach Quarantäne** – Objekte in die Quarantäne verschieben.
- **Aktion erfragen** – beim Fund von schädlichen Objekten den Benutzer nach einer Aktion fragen.
- **Löschen** – schädliche Objekte löschen, ohne den Benutzer zu benachrichtigen.
- **Protokollieren** – schädliche Objekte überspringen und Fund in den Programmbericht eintragen.

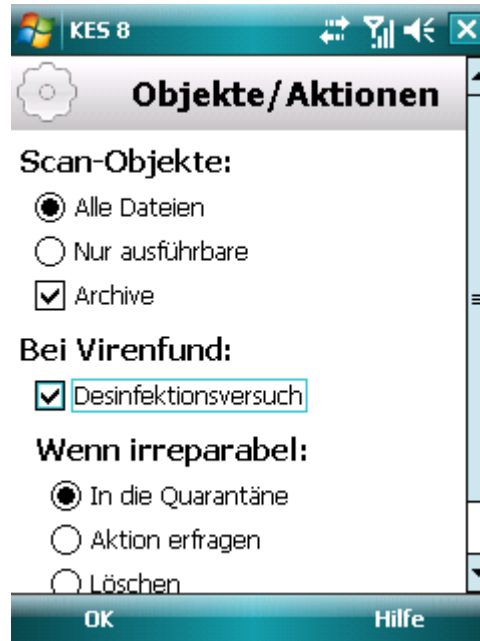


Abbildung 15: Aktion für gefundene Bedrohung wählen

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

QUARANTÄNE FÜR SCHÄDLICHE OBJEKTE

Dieser Abschnitt informiert über den speziellen Speicher *Quarantäne*, in den potentiell gefährliche Objekte verschoben werden. Außerdem wird hier beschrieben, wie schädliche Objekte, die in diesem Ordner gespeichert sind, angezeigt, wiederhergestellt oder gelöscht werden können.

IN DIESEM ABSCHNITT

Über die Quarantäne.....	42
Quarantäneobjekte anzeigen	42
Quarantäneobjekte wiederherstellen.....	43
Quarantäneobjekte löschen	43

ÜBER DIE QUARANTÄNE

Während einer Untersuchung des Geräts oder im Rahmen des Schutzes verschiebt das Programm die gefundenen Schadobjekte in die *Quarantäne* (spezieller Isolationsordner). Schädliche Objekte werden in der Quarantäne in gepackter Form gespeichert, sodass deren Aktivierung ausgeschlossen ist und von ihnen keine Gefahr mehr für das Gerät ausgeht.

Sie können Dateien, die sich in der Quarantäne befinden, anzeigen, löschen oder wiederherstellen.

QUARANTÄNEOBJEKTE ANZEIGEN

Sie können eine Liste der schädlichen Objekte, die vom Programm in die Quarantäne verschoben wurden, anzeigen lassen. Für jedes Objekt in der Liste werden der vollständige Name und das Funddatum angezeigt.

Sie können sich auch zusätzliche Informationen über das ausgewählte schädliche Objekt anzeigen lassen: Pfad des Objekts auf dem Gerät, bevor es in die Quarantäne verschoben wurde, sowie Name der Bedrohung.

➡ *Gehen Sie folgendermaßen vor, um eine Liste der Quarantäneobjekte anzuzeigen:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Quarantäne**.

Das Fenster **Quarantäne** wird geöffnet. Es enthält eine Liste der in die Quarantäne verschobenen Objekte (s. Abb. unten).



Abbildung 16: Liste der in die Quarantäne verschobenen Dateien

- Um Informationen über ein infiziertes Objekt anzuzeigen,

klicken Sie auf **Details**.

Im Fenster **Details** werden folgende Informationen über das Objekt angezeigt: Dateipfad, unter dem das Programm das Objekt auf dem Gerät gefunden hat, und Name des Virus.

Das Fenster **Details** wird geöffnet.

QUARANTÄNEOBJEKTE WIEDERHERSTELLEN

Wenn Sie sicher sind, dass ein gefundenes Objekt keine Gefahr für das Gerät darstellt, können Sie es aus der Quarantäne wiederherstellen. Ein wiederhergestelltes Objekt wird in den ursprünglichen Ordner verschoben.

- Gehen Sie folgendermaßen vor, um ein Objekt aus der Quarantäne wiederherzustellen:

1. Wählen Sie **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Quarantäne**.

Das Fenster **Quarantäne** wird geöffnet.

3. Wählen Sie ein Objekt, das wiederhergestellt werden soll, und gehen Sie dann auf **Menü** → **Wiederherstellen**.

Das markierte Objekt wird aus der Quarantäne im ursprünglichen Ordner wiederhergestellt.

QUARANTÄNEOBJEKTE LÖSCHEN

Sie können entweder ein einzelnes Objekt oder alle Objekte aus der Quarantäne löschen.

➤ *Gehen Sie folgendermaßen vor, um ein Objekt aus der Quarantäne zu löschen:*

1. Wählen Sie **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Quarantäne**.

Das Fenster **Quarantäne** wird geöffnet.

3. Wählen Sie ein zu löschendes Objekt und klicken Sie dann auf **Menü** → **Löschen**.

Das markierte Objekt wird aus der Quarantäne gelöscht.

➤ *Gehen Sie folgendermaßen vor, um alle Quarantäneobjekte zu löschen:*

1. Wählen Sie **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Quarantäne**.

Das Fenster **Quarantäne** wird geöffnet.

3. Klicken Sie auf **Menü** → **Alle löschen**.

Alle Quarantäneobjekte werden gelöscht.

EINGEHENDE ANRUFEN UND SMS FILTERN

Dieser Abschnitt informiert über Anti-Spam. Diese Komponente verhindert die Zustellung von unerwünschten Anrufen und SMS, und verwendet dazu eine benutzerdefinierte Schwarze und Weiße Liste. Außerdem wird in diesem Abschnitt beschrieben, wie ein Modus ausgewählt wird, nach dem Anti-Spam eingehende Anrufe und SMS untersuchen soll, wie erweiterte Einstellungen für die Filterung von eingehenden SMS und Anrufen vorgenommen werden, und wie eine Schwarze und eine Weiße Liste erstellt werden.

IN DIESEM ABSCHNITT

Über Anti-Spam.....	45
Über die Modi für Anti-Spam	46
Anti-Spam-Modus ändern	46
Schwarze Liste anlegen	47
Weißer Liste anlegen	50
Reaktion auf SMS und Anrufe von Nummern, die nicht zu den Kontakten zählen	53
Reaktion auf SMS von Nicht-Ziffern-Nummern	54
Aktion für eingehende SMS wählen	54
Aktion für eingehende Anrufe wählen	55

ÜBER ANTI-SPAM

Anti-Spam verhindert die Zustellung von unerwünschten Anrufen und SMS und verwendet dazu eine benutzerdefinierte Schwarze und Weiße Liste.

Die Listen bestehen aus Einträgen. Jeder Listeneintrag enthält folgende Informationen:

- Telefonnummer, von der Anti-Spam für die Schwarze Liste Informationen blockieren und für die Weiße Liste zustellen soll.
- Typ der Ereignisse, die Anti-Spam für die Schwarze Liste blockieren und für die Weiße Liste erlauben soll. Folgende Informationstypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- Schlüsselphrase, nach der Anti-Spam erwünschte und unerwünschte SMS unterscheidet. Für die Schwarze Liste blockiert Anti-Spam die SMS, die diese Phrase enthalten, und stellt die SMS zu, in denen diese Schlüsselphrase nicht enthalten ist. Für die Weiße Liste stellt Anti-Spam die SMS zu, die diese Phrase enthalten, und blockiert die SMS, in denen diese Schlüsselphrase nicht enthalten ist.

Anti-Spam richtet sich bei der Filterung von eingehenden SMS und Anrufen nach dem ausgewählten Modus (s. Abschnitt "Über die Modi für Anti-Spam" auf S. [46](#)). Nach diesem Modus untersucht Anti-Spam alle eingehenden Anrufe und Nachrichten und stuft sie als erwünscht oder unerwünscht (Spam) ein. Sobald Anti-Spam einen Anruf oder eine SMS als erwünscht oder unerwünscht einstuft, wird die Untersuchung abgeschlossen.

Informationen über blockierte SMS und Anrufe werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. [93](#)).

ÜBER DIE MODI FÜR ANTI-SPAM

Der Modus bestimmt die Regeln, nach denen Anti-Spam die eingehenden Anrufe und SMS filtert.

Es sind folgende Modi für Anti-Spam vorgesehen:

- **Aus** – Alle eingehenden SMS-Nachrichten und Anrufe werden zugestellt.
- **Weißer Liste erlauben:** Anrufe und SMS-Nachrichten werden nur von Nummern aus der Weißen Liste zugestellt.
- **Schwarze Liste blockieren:** Anrufe und SMS-Nachrichten werden von allen Nummern unter Ausnahme der Schwarzen Liste zugestellt.
- **Beide Listen** – Eingehende Anrufe und SMS-Nachrichten werden von Nummern aus der Weißen Liste zugestellt und von Nummern aus der Schwarzen Liste blockiert. Nach einem Gespräch oder dem Empfang einer SMS von einer Nummer, die auf keiner Liste steht, schlägt Anti-Spam vor, die Nummer in eine der Listen aufzunehmen.

Sie können den Modus für Anti-Spam ändern (s. Abschnitt "Anti-Spam-Modus ändern" auf S. [46](#)). Der aktuelle Modus von Anti-Spam wird im Fenster **Anti-Spam** neben dem Menüpunkt **Modus** angezeigt.

ANTI-SPAM-MODUS ÄNDERN

➔ Gehen Sie folgendermaßen vor, um einen Modus für Anti-Spam zu wählen:

1. Wählen Sie **Menü** → **Anti-Spam**.

Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Modus**.

Das Fenster **Modus** wird geöffnet.

3. Wählen Sie dazu einen Wert für **Anti-Spam-Modus** (s. Abb. unten).

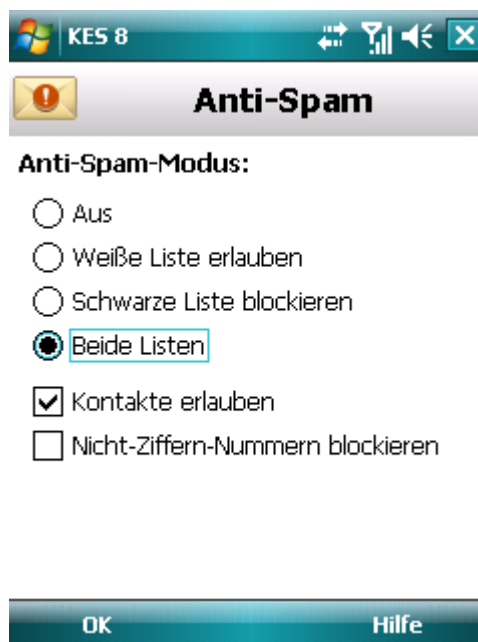


Abbildung 17: Anti-Spam-Modus ändern

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

SCHWARZE LISTE ANLEGEN

Die Schwarze Liste enthält Einträge über verbotene Nummern, d.h. jene Nummern, von denen Anrufe und SMS durch Anti-Spam blockiert werden. Jeder Eintrag enthält folgende Informationen:

- Telefonnummer, von der Anti-Spam Anrufe und / oder SMS blockieren soll.
- Typ der Ereignisse, die Anti-Spam von dieser Nummer blockieren soll. Folgende Ereignistypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- Schlüsselphrase, nach der Anti-Spam eine SMS als unerwünscht (Spam) einstufen soll. Anti-Spam blockiert nur die SMS, die diese Schlüsselphrase enthalten. Die übrigen SMS werden von Anti-Spam zugestellt.

Anti-Spam blockiert die Anrufe und SMS, die alle Kriterien eines Eintrags aus der Schwarzen Liste erfüllen. Anrufe und SMS, die auch nur ein Kriterium eines Eintrags aus der Schwarzen Liste nicht erfüllen, werden von Anti-Spam zugestellt.

Eine Telefonnummer mit identischen Filterkriterien kann nicht gleichzeitig zur Schwarzen und Weißen Liste hinzugefügt werden.

Informationen über blockierte SMS und Anrufe werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. [93](#)).

IN DIESEM ABSCHNITT

Eintrag zur Schwarzen Liste hinzufügen	47
Eintrag der Schwarzen Liste ändern	48
Eintrag aus Schwarzer Liste löschen	49

EINTRAG ZUR SCHWARZEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer mit identischen Filterkriterien nicht gleichzeitig auf der Schwarzen und Weißen Liste der Telefonnummern für Anti-Spam stehen kann. Wenn eine Nummer mit identischen Filterkriterien bereits in einer der Listen vorhanden ist, zeigt Kaspersky Endpoint Security 8 für Smartphones eine entsprechende Meldung an.

➔ Zum Hinzufügen eines Eintrags zur Schwarzen Liste für Anti-Spam:

1. Gehen Sie auf **Menü** → **Anti-Spam**.
Das Fenster **Anti-Spam** wird geöffnet.
2. Gehen Sie auf **Schwarze Liste**.
Das Fenster **Schwarze Liste** wird geöffnet.
3. Gehen Sie auf **Menü** → **Hinzufügen**.
Das Fenster **Neuer Eintrag** wird geöffnet.
4. Nehmen Sie folgende Einstellungen vor (s. Abb. unten):

- **Eingehende verbieten** – Typ von Ereignissen einer Telefonnummer, die von Anti-Spam für Nummern aus der Schwarzen Liste blockiert werden:
 - **Anrufe und SMS** – eingehende SMS und Anrufe blockieren.
 - **Nur Anrufe** – nur eingehende Anrufe blockieren.
 - **Nur SMS** - nur eingehende SMS blockieren.
- **Telefonnummer** – Telefonnummer, für die Anti-Spam eingehende Informationen blockieren soll. Die Nummer kann mit einer Ziffer, einem Buchstaben oder dem Zeichen "+" beginnen und darf Ziffern und / oder Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer *1234? aus der Schwarzen Liste. Anti-Spam blockiert Anrufe und SMS von einer Nummer, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.
- **Mit Text** – Schlüsselphrase, die darauf hinweist, dass eine empfangene SMS unerwünscht (Spam) ist. Anti-Spam blockiert nur die SMS, die eine Schlüsselphrase enthalten. Die übrigen SMS werden zugestellt.

Wenn alle SMS von einer beliebigen Nummer aus der Schwarzen Liste blockiert werden sollen, lassen Sie das Feld **Mit Text** für diesen Eintrag leer.

Abbildung 18: Einstellungen für einen Eintrag der Schwarzen Liste

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG DER SCHWARZEN LISTE ÄNDERN

Alle Einstellungen für Einträge aus der Schwarzen Liste können geändert werden.

➔ *Zum Ändern eines Eintrags in der Schwarzen Liste für Anti-Spam:*

1. Gehen Sie auf **Menü** → **Anti-Spam**.
Das Fenster **Anti-Spam** wird geöffnet.
2. Gehen Sie auf **Schwarze Liste**.

Das Fenster **Schwarze Liste** wird geöffnet.

3. Wählen Sie aus der Liste ein Element, das geändert werden soll, und gehen Sie dann auf **Menü** → **Ändern**.

Das Fenster **Eintrag ändern** wird geöffnet.

4. Ändern Sie die erforderlichen Parameter:

- **Eingehende verbieten** – Typ von Ereignissen einer Telefonnummer, die von Anti-Spam für Nummern aus der Schwarzen Liste blockiert werden:
 - **Anrufe und SMS** – eingehende SMS und Anrufe blockieren.
 - **Nur Anrufe** – nur eingehende Anrufe blockieren.
 - **Nur SMS** - nur eingehende SMS blockieren.
- **Telefonnummer** – Telefonnummer, für die Anti-Spam eingehende Informationen blockieren soll. Die Nummer kann mit einer Ziffer, einem Buchstaben oder dem Zeichen "+" beginnen und darf Ziffern und / oder Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer *1234? aus der Schwarzen Liste. Anti-Spam blockiert Anrufe und SMS von einer Nummer, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.
- **Mit Text** – Schlüsselphrase, die darauf hinweist, dass eine empfangene SMS unerwünscht (Spam) ist. Anti-Spam blockiert nur die SMS, die eine Schlüsselphrase enthalten. Die übrigen SMS werden zugestellt.

Wenn alle SMS von einer beliebigen Nummer aus der Schwarzen Liste blockiert werden sollen, lassen Sie das Feld **Mit Text** für diesen Eintrag leer.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG AUS SCHWARZER LISTE LÖSCHEN

Eine Nummer kann aus der Schwarzen Liste gelöscht werden. Außerdem können Sie die Schwarze Liste von Anti-Spam leeren, d.h. alle Einträge daraus löschen.

➤ *Zum Löschen eines Eintrags aus der Schwarzen Liste von Anti-Spam:*

1. Gehen Sie auf **Menü** → **Anti-Spam**.

Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Schwarze Liste**.

Das Fenster **Schwarze Liste** wird geöffnet.

3. Markieren Sie den zu löschenden Eintrag in der Liste und gehen Sie dann auf **Menü** → **Löschen**.

4. Bestätigen Sie das Löschen des Eintrags. Klicken Sie dazu auf **Ja**.

➤ *Zum Leeren der Schwarzen Liste für Anti-Spam:*

1. Gehen Sie auf **Menü** → **Anti-Spam**.

Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Schwarze Liste**.

Das Fenster **Schwarze Liste** wird geöffnet.

3. Gehen Sie auf **Menü** → **Alle löschen**.

Die Liste wird geleert.

WEIßE LISTE ANLEGEN

Die Weiße Liste enthält Einträge über erlaubte Nummern, d.h. jene Nummern, von denen Anrufe und SMS durch Anti-Spam erlaubt werden. Jeder Eintrag enthält folgende Informationen:

- Telefonnummer, von der Anti-Spam Anrufe und / oder SMS zustellen soll.
- Typ der Ereignisse, die Anti-Spam von dieser Nummer zustellen soll. Folgende Ereignistypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- Schlüsselphrase, nach der Anti-Spam eine SMS als erwünscht (kein Spam) einstufen soll. Anti-Spam stellt nur SMS zu, die diese Schlüsselphrase enthalten. Die übrigen SMS werden von Anti-Spam blockiert.

Anti-Spam stellt nur die Anrufe und SMS zu, die alle Kriterien eines Eintrags aus der Weißen Liste erfüllen. Anrufe und SMS, die auch nur ein Kriterium eines Eintrags aus der Weißen Liste nicht erfüllen, werden von Anti-Spam blockiert.

IN DIESEM ABSCHNITT

Eintrag zur Weißen Liste hinzufügen	50
Eintrag der Weißen Liste ändern.....	51
Eintrag aus Weißer Liste löschen.....	52

EINTRAG ZUR WEIßEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer mit identischen Filterkriterien nicht gleichzeitig auf der Schwarzen und Weißen Liste der Telefonnummern für Anti-Spam stehen kann. Wenn eine Nummer mit identischen Filterkriterien bereits in einer der Listen vorhanden ist, zeigt Kaspersky Endpoint Security 8 für Smartphones eine entsprechende Meldung an.

➔ *Zum Hinzufügen eines Eintrags zur Weißen Liste für Anti-Spam:*

1. Gehen Sie auf **Menü** → **Anti-Spam**.
Das Fenster **Anti-Spam** wird geöffnet.
2. Gehen Sie auf **Weißer Liste**.
Das Fenster **Weißer Liste** wird geöffnet.
3. Gehen Sie auf **Menü** → **Hinzufügen**.
Das Fenster **Neuer Eintrag** wird geöffnet.
4. Nehmen Sie folgende Einstellungen vor (s. Abb. unten):
 - **Eingehende erlauben** – Typ von Ereignissen von einer Telefonnummer, die von Anti-Spam für Nummern aus der Weißen Liste erlaubt werden:
 - **Anrufe und SMS** – eingehende Anrufe und SMS erlauben.
 - **Nur Anrufe** – nur eingehende Anrufe erlauben.

- **Nur SMS** - nur eingehende SMS erlauben.
- **Telefonnummer** – Telefonnummer, für die Anti-Spam eingehende Informationen zustellen soll. Die Nummer kann mit einer Ziffer, einem Buchstaben oder dem Zeichen "+" beginnen und darf Ziffern und / oder Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer *1234? aus der Weißen Liste. Anti-Spam erlaubt Anrufe und SMS von einer Nummer, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.
- **Mit Text** – Schlüsselphrase, die darauf hinweist, dass eine empfangene SMS erwünscht ist. Für Nummern aus der Weißen Liste stellt Anti-Spam nur die SMS zu, die die Schlüsselphrase enthalten. Alle übrigen SMS von dieser Nummer werden blockiert.

Wenn alle SMS von einer beliebigen Nummer aus der Weißen Liste zugestellt werden sollen, lassen Sie das Feld **Mit Text** für diesen Eintrag leer.

Abbildung 19: Einstellungen für einen Eintrag der Weißen Liste

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG DER WEIßEN LISTE ÄNDERN

Alle Einstellungen für Einträge aus der Weißen Liste können geändert werden.

➤ *Zum Ändern eines Eintrags in der Weißen Liste für Anti-Spam:*

1. Gehen Sie auf **Menü** → **Anti-Spam**.
Das Fenster **Anti-Spam** wird geöffnet.
2. Gehen Sie auf **Weißer Liste**.
Das Fenster **Weißer Liste** wird geöffnet.
3. Wählen Sie aus der Liste ein Element, das geändert werden soll, und gehen Sie dann auf **Menü** → **Ändern**.
Das Fenster **Ändern** wird geöffnet.

4. Ändern Sie die erforderlichen Parameter:

- **Eingehende erlauben** – Typ von Ereignissen von einer Telefonnummer, die von Anti-Spam für Nummern aus der Weißen Liste erlaubt werden:
 - **Anrufe und SMS** – eingehende Anrufe und SMS erlauben.
 - **Nur Anrufe** – nur eingehende Anrufe erlauben.
 - **Nur SMS** - nur eingehende SMS erlauben.
- **Telefonnummer** – Telefonnummer, für die Anti-Spam eingehende Informationen zustellen soll. Die Nummer kann mit einer Ziffer, einem Buchstaben oder dem Zeichen "+" beginnen und darf Ziffern und / oder Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer *1234? aus der Weißen Liste. Anti-Spam erlaubt Anrufe und SMS von einer Nummer, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.
- **Mit Text** – Schlüsselphrase, die darauf hinweist, dass eine empfangene SMS erwünscht ist. Für Nummern aus der Weißen Liste stellt Anti-Spam nur die SMS zu, die die Schlüsselphrase enthalten. Alle übrigen SMS von dieser Nummer werden blockiert.

Wenn alle SMS von einer beliebigen Nummer aus der Weißen Liste zugestellt werden sollen, lassen Sie das Feld **Mit Text** für diesen Eintrag leer.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG AUS WEIßER LISTE LÖSCHEN

Sie können einen Eintrag aus der Weißen Liste löschen oder die Liste vollständig leeren.

➤ *Zum Löschen eines Eintrags aus der Weißen Liste für Anti-Spam:*

1. Gehen Sie auf **Menü** → **Anti-Spam**.
Das Fenster **Anti-Spam** wird geöffnet.
2. Gehen Sie auf **Weißer Liste**.
Das Fenster **Weißer Liste** wird geöffnet.
3. Markieren Sie den zu löschenden Eintrag in der Liste und gehen Sie dann auf **Menü** → **Löschen**.
4. Bestätigen Sie das Löschen des Eintrags. Klicken Sie dazu auf **Ja**.

➤ *Zum Leeren der Weißen Liste für Anti-Spam:*

1. Gehen Sie auf **Menü** → **Anti-Spam**.
Das Fenster **Anti-Spam** wird geöffnet.
2. Gehen Sie auf **Weißer Liste**.
Das Fenster **Weißer Liste** wird geöffnet.
3. Gehen Sie auf **Menü** → **Alle löschen**.

Die Liste wird geleert.

REAKTION AUF SMS UND ANRUF VON NUMMERN, DIE NICHT ZU DEN KONTAKTEN ZÄHLEN.

Im Modus **Beide Listen** oder **Weißer Liste** (s. Abschnitt "Über die Modi für Anti-Spam" auf S. 46) können Sie die Weiße Liste erweitern. In diesem Fall behandelt Anti-Spam die Anrufe und SMS, die von Nummern aus den Kontakten stammen, als würden diese Nummern auf der Weißen Liste stehen.

Verwenden Sie die Joystick-Tasten des Geräts, um die Parameterwerte zu ändern.

➔ *Zum Erweitern der Weißen Liste durch Aufnahme der Nummern aus den Kontakten:*

1. Gehen Sie auf **Menü** → **Anti-Spam**.

Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Modus**.

3. Das Fenster **Modus** wird geöffnet.

4. Wählen Sie einen Wert für **Kontakte erlauben** (s. Abb. unten):

- Damit Anti-Spam die Nummern aus den Kontakten als zusätzliche Weiße Liste betrachtet und SMS und Anrufe von Nummern blockiert, die nicht in den Kontakten stehen, aktivieren Sie das Kontrollkästchen **Kontakte erlauben**.
- Damit Anti-Spam SMS und Anrufe nur nach dem festgelegten Anti-Spam-Modus filtert, deaktivieren Sie das Kontrollkästchen **Kontakte erlauben**.

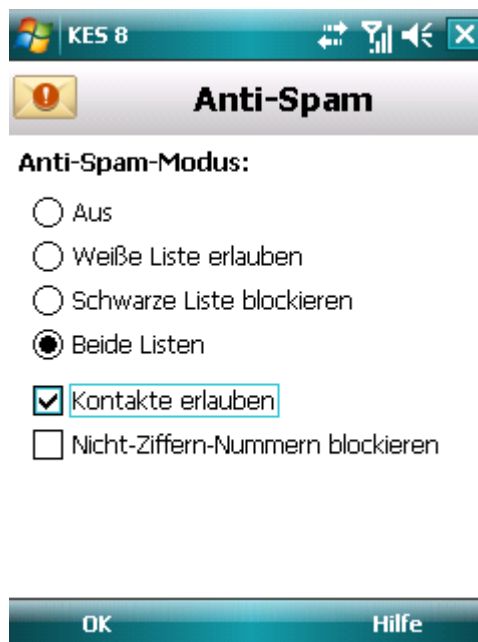


Abbildung 20: Reaktion von Anti-Spam auf Nummern, die nicht zu den Kontakten gehören

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

REAKTION AUF SMS VON NICHT-ZIFFERN-NUMMERN

Im Modus **Beide Listen** oder **Schwarze Liste** (s. Abschnitt "**Anti-Spam-Modus ändern**" auf S. 46) können Sie die Schwarze Liste durch Aufnahme aller Nicht-Ziffern-Nummern (Nummern, die Buchstaben enthalten) erweitern. In diesem Fall behandelt Anti-Spam die Anrufe und SMS, die von Nicht-Ziffern-Nummern stammen, als würden diese Nummern auf der Schwarzen Liste stehen.

Verwenden Sie die Joystick-Tasten des Geräts, um die Parameterwerte zu ändern.

➤ *Zum Erweitern der Schwarzen Liste durch Aufnahme aller Nicht-Ziffern-Nummern:*

1. Gehen Sie auf **Menü** → **Anti-Spam**.

Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Modus**.

Das Fenster **Modus** wird geöffnet.

3. Wählen Sie einen Wert für den Parameter **Nicht-Ziffern-Nummern blockieren** (s. Abb. unten):

- Damit Anti-Spam SMS von Nicht-Ziffern-Nummern blockiert, aktivieren Sie das Kontrollkästchen **Nicht-Ziffern-Nummern blockieren**.
- Damit Anti-Spam SMS von Nicht-Ziffern-Nummern auf Basis des gewählten Anti-Spam-Modus filtert, deaktivieren Sie das Kontrollkästchen **Nicht-Ziffern-Nummern blockieren**.

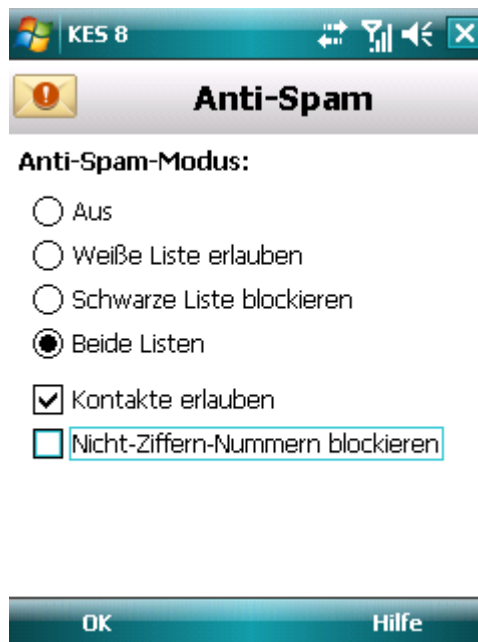


Abbildung 21: Auswahl einer Anti-Spam-Aktion für eingehende SMS-Nachrichten von Nicht-Ziffern-Nummern

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

AKTION FÜR EINGEHENDE SMS WÄHLEN

Im Modus **Beide Listen** (s. Abschnitt "**Über die Modi für Anti-Spam**" auf S. 46) untersucht Anti-Spam die eingehenden SMS unter Verwendung der Schwarzen und Weißen Liste.

Nach dem Empfang einer SMS von einer Nummer, die auf keiner Liste steht, schlägt Anti-Spam vor, die Nummer in eine der Listen aufzunehmen (s. Abb. unten).

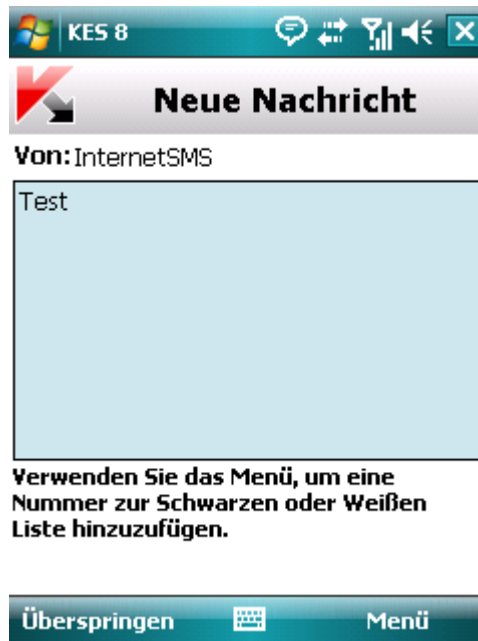


Abbildung 22: Meldung von Anti-Spam über den Empfang einer Nachricht

Sie können eine der folgenden Aktionen für eine SMS wählen:

- Um eine SMS zu blockieren und die Telefonnummer des Absenders in die Schwarze Liste aufzunehmen, wählen Sie **Menü → Zur Schwarzen Liste**.
- Um eine SMS zu erlauben und die Telefonnummer des Absenders in die Weiße Liste aufzunehmen, wählen Sie **Menü → Zur Weißen Liste**.
- Klicken Sie auf **Überspringen**, damit die SMS zugestellt und die Telefonnummer des Absenders nicht in eine Liste eingetragen wird.

Informationen über blockierte SMS werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [93](#)).

AKTION FÜR EINGEHENDE ANRUF WÄHLEN

Im Modus **Beide Listen** (s. Abschnitt "[Über die Modi für Anti-Spam](#)" auf S. [46](#)) untersucht Anti-Spam die eingehenden Anrufe unter Verwendung der Schwarzen und Weißen Liste. Nach einem Anruf von einer Nummer, die auf keiner Liste steht, schlägt Anti-Spam vor, die Nummer in eine der Listen aufzunehmen (s. Abb. unten).

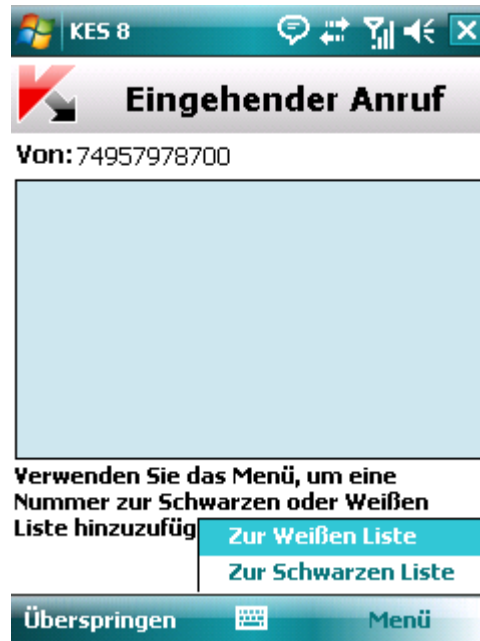


Abbildung 23: Meldung von Anti-Spam über einen angenommenen Anruf

Für eine Nummer, von der ein Anruf erfolgte, können Sie eine der folgenden Aktionen wählen:

- Um die Telefonnummer des Anrufers in die Schwarze Liste aufzunehmen, wählen Sie **Menü** → **Zur Schwarzen Liste**.
- Um die Telefonnummer des Anrufers in die Weiße Liste aufzunehmen, wählen Sie **Menü** → **Zur Weißen Liste**.
- Klicken Sie auf **Überspringen**, damit die Telefonnummer des Anrufers nicht in eine Liste eingetragen wird.

Informationen über blockierte Anrufe werden im Programmbericht erfasst.

DATENSCHUTZ BEI VERLUST ODER DIEBSTAHL DES GERÄTS

Dieser Abschnitt informiert über die Komponente Diebstahlschutz, die bei Diebstahl oder Verlust des Geräts die auf dem Gerät gespeicherten Informationen vor unbefugtem Zugriff schützt und das Auffinden des Geräts erleichtert.

Außerdem werden hier folgende Vorgänge beschrieben: Diebstahlschutz-Funktionen aktivieren / deaktivieren, Diebstahlschutz anpassen, Diebstahlschutz-Funktionen von einem anderen Gerät aus ferngesteuert starten.

IN DIESEM ABSCHNITT

Über den Diebstahlschutz	57
Gerät blockieren	58
Persönliche Daten löschen.....	60
Liste der zu löschenden Ordner erstellen.....	62
Wechsel der SIM-Karte auf dem Gerät überwachen.....	63
Geografische Koordinaten des Geräts ermitteln	64
Diebstahlschutz-Funktionen ferngesteuert starten.....	67

ÜBER DEN DIEBSTAHLSCHEUTZ

Der Diebstahlschutz schützt die Informationen, die auf Ihrem mobilen Gerät gespeichert sind, vor unbefugtem Zugriff.

Der Diebstahlschutz umfasst folgende Funktionen:

- **SMS-Block** erlaubt es, das Gerät ferngesteuert zu blockieren und einen Text festzulegen, der auf dem Display des blockierten Geräts angezeigt wird.
- **SMS-Clean** erlaubt es, die persönlichen Benutzerdaten (Einträge in den Kontakten, Nachrichten, Bilder, Kalender, Berichte, Internet-Einstellungen) sowie Daten auf Speicherkarten und von Dateien aus der Löschl-Liste per Fernsteuerung vom Gerät zu löschen.
- **SIM-Watch** erlaubt es, die aktuelle Telefonnummer zu ermitteln, wenn die SIM-Karte gewechselt wurde. Außerdem kann das Gerät automatisch blockiert werden, wenn die SIM-Karte gewechselt oder das Gerät ohne SIM eingeschaltet wird. Informationen über die neue Telefonnummer werden als Nachricht an die von Ihnen angegebene Telefonnummer und / oder E-Mail-Adresse geschickt.
- Mit **GPS-Find** kann ein Gerät geortet werden. Die geografischen Koordinaten des Geräts werden als Nachricht an die Telefonnummer, von der der spezielle SMS-Befehl stammte, und an eine E-Mail-Adresse geschickt.

Die Diebstahlschutz-Funktionen von Kaspersky Endpoint Security 8 für Smartphones lassen sich durch einen SMS-Befehl von einem anderen Gerät aus starten (s. Abschnitt "Diebstahlschutz-Funktionen ferngesteuert starten" auf S. [67](#)).

Um die Diebstahlschutz-Funktionen ferngesteuert zu starten, ist der Geheimcode des Programms erforderlich, der beim ersten Start von Kaspersky Endpoint Security 8 für Smartphones auf Ihrem Gerät festgelegt wird.

Der aktuelle Status der einzelnen Funktionen wird im Fenster **Diebstahlschutz** neben der jeweiligen Funktion angezeigt.

Informationen über die Arbeit einer Komponente werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 93).

GERÄT BLOCKIEREN

Nach Empfang eines speziellen SMS-Befehls kann die Funktion SMS-Block per Fernsteuerung den Zugriff auf das Gerät und die darauf gespeicherten Daten sperren. Das Gerät kann nur durch Eingabe des Geheimcodes entsperrt werden.

Diese Funktion blockiert das Gerät nicht, sondern aktiviert eine Option für das ferngesteuerte Blockieren.

➔ Gehen Sie folgendermaßen vor, um die Funktion SMS-Block zu aktivieren:

1. Wählen Sie **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

2. Gehen Sie auf **SMS-Block**.

Das Fenster **SMS-Block** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **SMS-Block aktivieren**.

4. Ändern Sie im Feld **Text beim Blockieren** den Text, der auf dem Display des blockierten Geräts angezeigt werden soll (s. Abb. unten). In der Grundeinstellung wird für die Meldung ein Standardtext verwendet, dem Sie die Nummer des Telefonbesitzers hinzufügen können.



Abbildung 24: Einstellungen der Funktion SMS-Block

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Ein anderes Gerät, auf dem die Funktion SMS-Block aktiviert ist, kann auf folgende Weise gesperrt werden:

- Erstellen Sie auf einem anderen mobilen Gerät in einem Programm für mobile Endgeräte (z. B. in Kaspersky Endpoint Security 8 für Smartphones) einen speziellen SMS-Befehl und senden Sie diesen an Ihr Gerät. Um einen speziellen SMS-Befehl zu erstellen, verwenden Sie bitte die Funktion **Befehl senden**. Dadurch erhält Ihr Gerät unbemerkt eine SMS und das Gerät wird blockiert.

- Erstellen Sie auf einem anderen mobilen Gerät eine SMS mit einem speziellen Text und dem Geheimcode des Geräts, an das die SMS geht, und senden Sie diese.

Für das Senden einer SMS fallen für das sendende Gerät die tarifgemäßen Gebühren an.

Um ein Gerät per Fernzugriff zu blockieren, wird die sichere Methode mit der Funktion **Befehl senden** empfohlen. In diesem Fall wird der Geheimcode für das Programm in verschlüsselter Form gesendet.

➔ Gehen Sie folgendermaßen vor, um den SMS-Befehl mithilfe der Funktion **Befehl senden** an das andere Gerät zu senden:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Befehl senden**.

Das Fenster **Befehl senden** wird geöffnet.

3. Setzen Sie den Parameter **SMS-Befehl auswählen** auf **Gerät blockieren** (s. Abb. unten).

4. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.

5. Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode des Geräts ein, an das der SMS-Befehl gerichtet ist.



Abbildung 25: Ferngesteuerter Start der Funktion SMS-Block

6. Klicken Sie auf **Senden**.

➔ Um mithilfe der Standardfunktionen eines Telefons eine SMS zu erstellen,

schicken Sie an das andere Gerät eine SMS mit dem Text `block:<Code>` (wobei `<Code>` der Geheimcode des anderen Geräts ist). Groß- und Kleinschreibung von Buchstaben sowie Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

PERSÖNLICHE DATEN LÖSCHEN

Nach Erhalt des speziellen SMS-Befehls ermöglicht es die Funktion SMS-Clean, die folgenden, auf dem Gerät gespeicherten Informationen zu löschen:

- persönliche Benutzerdaten (Einträge in den Kontakten und auf der SIM- Karte, SMS, Bilder, Kalender, Internet-Einstellungen)
- Informationen auf einer Speicherkarte
- Die Dateien aus dem Ordner **Eigene Dateien** und aus anderen Ordnern der Liste **Zu löschende Ordner**.

Diese Funktion löscht die auf dem Gerät gespeicherten Daten nicht, sondern aktiviert die Möglichkeit, diese nach Empfang eines speziellen SMS-Befehls zu löschen.

➔ *Gehen Sie folgendermaßen vor, um die Funktion SMS-Clean zu aktivieren:*

1. Gehen Sie auf **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

2. Gehen Sie auf **SMS-Clean**.

Das Fenster **SMS-Clean** wird geöffnet.

3. Gehen Sie auf **Modus**.

Das Fenster **SMS-Clean** wird geöffnet.

4. Aktivieren Sie das Kontrollkästchen **SMS-Clean aktivieren**.

5. Wählen Sie die Informationen aus, die nach Empfang eines speziellen SMS-Befehls gelöscht werden sollen. Aktivieren Sie dazu im Block **Löschen** die entsprechenden Kontrollkästchen (s. Abb. unten):

- Aktivieren Sie das Kontrollkästchen **Persönliche Daten**, damit persönliche Daten gelöscht werden.
- Aktivieren Sie das Kontrollkästchen **Zu löschende Ordner**, damit die Dateien aus dem Ordner **Eigene Dateien** und aus der Liste **Zu löschende Ordner** gelöscht werden.



Abbildung 26: Zu löschende Informationen wählen

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.
7. Wechseln Sie zur Erstellung der Liste **Zu löschende Ordner** (s. Abschnitt "**Liste der zu löschenden Ordner erstellen**" auf S. 62).

Wenn die Funktion aktiviert ist, können persönliche Daten auf folgende Weise vom Gerät gelöscht werden:

- Erstellen Sie auf einem anderen mobilen Gerät in einem Programm für mobile Endgeräte (z. B. in Kaspersky Endpoint Security 8 für Smartphones) einen speziellen SMS-Befehl und senden Sie diesen an Ihr Gerät. Dadurch erhält Ihr Gerät unbemerkt eine SMS und die Informationen werden gelöscht. Um einen speziellen SMS-Befehl zu erstellen, verwenden Sie bitte die Funktion Befehl senden.
- Erstellen Sie auf einem anderen mobilen Gerät eine SMS mit einem speziellen Text und dem Geheimcode des Geräts, an das die SMS geht, und senden Sie diese. Dadurch erhält Ihr Gerät unbemerkt eine SMS und die Informationen werden gelöscht.

Für das Senden einer SMS fallen für das sendende Gerät die tarifgemäßen Gebühren an.

Um per Fernsteuerung Daten vom Gerät zu löschen, wird die sichere Methode mit der Funktion Befehl senden empfohlen. In diesem Fall wird der Geheimcode für das Programm in verschlüsselter Form gesendet.

➤ Gehen Sie folgendermaßen vor, um den SMS-Befehl mithilfe der Funktion Befehl senden an das andere Gerät zu senden:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Befehl senden**.

Das Fenster **Befehl senden** wird geöffnet.

3. Setzen Sie den Parameter **SMS-Befehl auswählen** auf **Daten löschen** (s. Abb. unten).

4. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.

- Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode des Geräts ein, an das der SMS-Befehl gerichtet ist.



Abbildung 27: Ferngesteuerter Start der Funktion SMS-Clean

- Klicken Sie auf **Senden**.

➤ Um mithilfe der Standardfunktionen eines Telefons eine SMS zu erstellen,

schicken Sie an das andere Gerät eine SMS mit dem Text `wipe:<Code>` (wobei `<Code>` der Geheimcode des anderen Geräts ist). Groß- und Kleinschreibung von Buchstaben sowie Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

LISTE DER ZU LÖSCHENDEN ORDNER ERSTELLEN

Die Funktion SMS-Clean erlaubt es, eine Liste mit Ordnern anzulegen, die nach dem Empfang eines speziellen SMS-Befehls gelöscht werden sollen.

Damit der Diebstahlschutz die Ordner aus dieser Liste nach Empfang eines speziellen SMS-Befehls löscht, stellen Sie sicher, dass im Menüpunkt **Modus** das Kontrollkästchen **Zu löschende Ordner** aktiviert ist.

Die Liste der zu löschenden Ordner kann Ordner enthalten, die vom Administrator hinzugefügt wurden. Solche Ordner können nicht aus der Liste entfernt werden.

➤ Gehen Sie folgendermaßen vor, um einen Ordner zur Liste der zu löschenden Ordner hinzuzufügen:

- Gehen Sie auf **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

- Gehen Sie auf **SMS-Clean**.

Das Fenster **SMS-Clean** wird geöffnet.

- Gehen Sie auf **Zu löschende Ordner**.

Das Fenster **Zu löschende Ordner** wird geöffnet.

4. Gehen Sie auf **Menü** → **Hinzufügen** (s. Abb. unten).



Abbildung 28: Liste der zu löschenden Ordner erstellen

5. Wählen Sie den entsprechenden Ordner aus der Ordnerstruktur aus und gehen Sie auf **Auswählen**.

Der Ordner wird zur Liste hinzugefügt.

➔ Gehen Sie folgendermaßen vor, um einen Ordner aus der Liste zu löschen:

1. Gehen Sie auf **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

2. Gehen Sie auf **SMS-Clean**.

Das Fenster **SMS-Clean** wird geöffnet.

3. Gehen Sie auf **Zu löschende Ordner**.

Das Fenster **Zu löschende Ordner** wird geöffnet.

4. Wählen Sie einen Ordner aus der Liste und gehen Sie auf **Menü** → **Löschen**.

WECHSEL DER SIM-KARTE AUF DEM GERÄT ÜBERWACHEN

Wenn die SIM-Karte ausgetauscht wird, kann SIM-Watch die neue Telefonnummer an eine vorgegebene Telefonnummer und / oder E-Mail-Adresse schicken und das Gerät blockieren.

➔ Gehen Sie folgendermaßen vor, um die Funktion SIM-Watch zu aktivieren und den Wechsel der SIM-Karte auf dem Gerät zu überwachen:

1. Wählen Sie **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

2. Gehen Sie auf **SIM-Watch**.

Das Fenster **SIM-Watch** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **SIM-Watch aktivieren**.

4. Passen Sie folgende Parameter an, um den Wechsel der SIM-Karte auf dem Gerät zu kontrollieren (s. Abb. unten):

- Um automatisch eine SMS mit der neuen Nummer Ihres Telefons zu erhalten, geben Sie unter **Bei Wechsel der SIM-Karte** im Feld **SMS an Telefonnummer** die Telefonnummer ein, die per SMS benachrichtigt werden soll.

Die Nummer kann mit einer Ziffer oder dem Zeichen "+" beginnen und darf nur Ziffern enthalten.

- Wenn Sie per E-Mail über die neue Nummer Ihres Telefons informiert werden möchten, tragen Sie unter **Beim Wechsel der SIM-Karte neue Nummer senden** im Feld **Nachricht an E-Mail-Adresse** die entsprechende E-Mail-Adresse ein.
- Aktivieren Sie unter **Erweitert** das Kontrollkästchen **Gerät blockieren**, damit das Gerät blockiert wird, wenn die SIM-Karte ausgetauscht oder das Gerät ohne SIM eingeschaltet wird. Das Gerät kann durch Eingabe des Geheimcodes für das Programm entsperrt werden.
- Damit auf dem Display des blockierten Geräts eine Nachricht angezeigt wird, füllen Sie das Feld **Text beim Blockieren** aus. In der Grundeinstellung wird für die Meldung ein Standardtext verwendet, dem Sie die Nummer des Besitzers hinzufügen können.



Abbildung 29: Einstellungen die Funktion SIM-Watch

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

GEOGRAFISCHE KOORDINATEN DES GERÄTS ERMITTELN

Nach Empfang eines speziellen SMS-Befehls kann die Funktion GPS-Find die geografischen Koordinaten des Geräts ermitteln und diese mit einer SMS oder E-Mail an das anfragende Gerät und an eine E-Mail-Adresse schicken.

Für das Senden einer SMS fallen die tarifüblichen Gebühren an.

- Diese Funktion eignet sich nur für Geräte mit integriertem GPS-Empfänger. Der Empfänger wird automatisch aktiviert, nachdem das Gerät einen speziellen SMS-Befehl erhalten hat. Wenn sich das Gerät im Empfangsbereich von Satelliten befindet, empfängt die Funktion GPS-Find die Gerätekoordinaten und leitet sie weiter. Besteht im Augenblick der Anfrage kein Satellitenempfang, dann versucht GPS-Find in regelmäßigen Abständen, das Gerät zu orten und die Suchergebnisse zu übermitteln. Gehen Sie folgendermaßen vor, um GPS-Find zu aktivieren:

1. Gehen Sie auf **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

2. Gehen Sie auf **GPS-Find**.

Das Fenster **GPS-Find** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **GPS-Find aktivieren**.

Kaspersky Endpoint Security 8 für Smartphones schickt die Gerätekoordinaten mit einer Antwort-SMS.

4. Um die Koordinaten des Geräts auch per E-Mail zu erhalten, geben Sie bitte im Block **Gerätekoordinaten senden** für den Parameter **Nachricht an E-Mail-Adresse** die entsprechende E-Mail-Adresse ein (s. Abb. unten).



Abbildung 30: Einstellungen der Funktion GPS-Find

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Wenn GPS-Find aktiviert ist, können die Koordinaten des Geräts auf folgende Weise ermittelt werden:

- Erstellen Sie auf einem anderen mobilen Gerät in einem Programm für mobile Endgeräte (z. B. in Kaspersky Endpoint Security 8 für Smartphones) einen speziellen SMS-Befehl und senden Sie diesen an Ihr Gerät. Dadurch erhält Ihr Gerät eine SMS und das Programm sendet die Gerätekoordinaten. Um einen speziellen SMS-Befehl zu erstellen, verwenden Sie bitte die Funktion Befehl senden.
- Erstellen Sie auf einem anderen mobilen Gerät eine SMS mit einem speziellen Text und dem Geheimcode des Geräts, an das die SMS geht, und senden Sie diese. Dadurch erhält Ihr Gerät eine SMS und das Programm sendet die Gerätekoordinaten.

Für das Senden einer SMS fallen für das sendende Gerät die tarifgemäßen Gebühren an.

Um die Gerätekoordinaten zu erhalten, wird die sichere Methode mit der Funktion **Befehl senden** empfohlen. In diesem Fall wird der Geheimcode in verschlüsselter Form gesendet.

➤ Gehen Sie folgendermaßen vor, um den Befehl mithilfe der Funktion **Befehl senden** an das andere Gerät zu senden:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Befehl senden**.

Das Fenster **Befehl senden** wird geöffnet.

3. Setzen Sie den Parameter **SMS-Befehl auswählen** auf **GPS-Find** (s. Abb. unten).

4. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.

5. Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode des Geräts ein, an das der SMS-Befehl gerichtet ist.



Abbildung 31: Ferngesteuerter Start der Funktion GPS-Find

6. Klicken Sie auf **Senden**.

➤ Um mithilfe der Standardfunktionen eines Telefons eine SMS zu erstellen,

schicken Sie an das andere Gerät eine SMS mit dem Text `find:<Code>`, wobei `<Code>` der Geheimcode ist, der auf dem anderen Gerät hinterlegt ist. Groß- und Kleinschreibung von Buchstaben sowie Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

Eine SMS mit den Gerätekoordinaten wird an die Telefonnummer gesendet, von dem der SMS-Befehl stammte, sowie an eine E-Mail-Adresse, sofern eine solche in den Einstellungen für GPS-Find hinterlegt wurde.

DIEBSTAHLSCHUTZ-FUNKTIONEN FERNGESTEUERT

STARTEN

Das Programm ermöglicht den Versand eines speziellen SMS-Befehls, um auf einem anderen Gerät, auf dem Kaspersky Endpoint Security 8 für Smartphones installiert ist, die Diebstahlschutz-Funktionen ferngesteuert zu starten. Der SMS-Befehl wird in Form einer verschlüsselten SMS gesendet und erhält den Geheimcode für das Programm, das auf dem anderen Geräts installiert ist. Der Empfang des SMS-Befehls bleibt auf dem anderen Gerät unbemerkt.

Für die SMS fallen die tarifgemäßen Gebühren an.

➤ Gehen Sie folgendermaßen vor, um einen SMS-Befehl an das andere Gerät zu senden:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Befehl senden**.

Das Fenster **Befehl senden** wird geöffnet.

3. Wählen Sie eine Funktion aus, die per Fernsteuerung gestartet werden soll: Wählen Sie dazu einen der folgenden Werte für **SMS-Befehl auswählen** (s. Abb. unten):

- SMS-Block
- SMS-Clean
- GPS-Find
- Privatsphäre (s. Abschnitt "Verbergen sensibler Daten" auf S. [69](#)).

4. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.

5. Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode des Geräts ein, an das der SMS-Befehl gerichtet ist.



Abbildung 32: Ferngesteuerter Start der Diebstahlschutz-Funktionen

6. Klicken Sie auf **Senden**.

VERBERGEN SENSIBLER DATEN

Dieser Abschnitt informiert über die Komponente Privatsphäre, mit der vertrauliche Benutzerinformationen verborgen werden können.

IN DIESEM ABSCHNITT

Über die Privatsphäre.....	69
Über die Modi der Privatsphäre.....	69
Privatsphäre aktivieren / deaktivieren	70
Funktion zum Verbergen von sensiblen Daten automatisch aktivieren	71
Funktion zum Verbergen von sensiblen Daten ferngesteuert aktivieren	72
Liste der vertraulichen Nummern erstellen.....	74
Auswahl der zu verbergenden Informationen: Privatsphäre.....	77

ÜBER DIE PRIVATSPHÄRE

Die Privatsphäre verbirgt vertrauliche Informationen. Dazu dient eine festgelegte Kontaktliste, die vertrauliche Nummern enthält. Für vertrauliche Nummern verbirgt die Privatsphäre Einträge in den Kontakten, Eingehende, Entwürfe, weitergeleitete SMS sowie Einträge der Anrufliste. Die Privatsphäre blockiert das Signal, das über den Empfang einer neuen SMS-Nachricht informiert und verbirgt die SMS im Eingangsordner. Die Privatsphäre blockiert einen von einer vertraulichen Nummer eingehenden Anruf und zeigt auf dem Display keine Informationen über den Anruf an. Der Anrufer hört in diesem Fall das "Besetzt"-Zeichen. Um die Anrufe und SMS-Nachrichten anzuzeigen, die eingegangen sind, während das Verbergen sensibler Daten aktiviert war, deaktivieren Sie diese Funktion. Wenn das Verbergen wieder aktiviert wird, werden die Informationen verborgen.

Sie können die Funktion zum Verbergen sensibler Daten in Kaspersky Endpoint Security 8 für Smartphones oder ferngesteuert von einem anderen mobilen Gerät aus aktivieren. Das Deaktivieren der Funktion zum Verbergen sensibler Daten ist nur vom Programm aus möglich.

Informationen über die Arbeit der Privatsphäre werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. [93](#)).

ÜBER DIE MODI DER PRIVATSPHÄRE

Sie können den Privatsphären-Modus steuern. Dieser Modus legt fest, ob das Verbergen vertraulicher Informationen aktiviert oder deaktiviert ist.

Es sind die folgenden Privatsphären-Modi vorgesehen:

- **Anzeigen** – vertrauliche Informationen werden angezeigt. Die Einstellungen der Privatsphäre können geändert werden.
- **Verbergen** – vertrauliche Informationen werden verborgen. Die Einstellungen der Privatsphäre können nicht geändert werden.

Sie können entweder eine automatische Aktivierung des Verbergens sensibler Daten (auf S. 71) oder eine ferngesteuerte Aktivierung dieser Funktion von einem anderen Gerät aus einrichten (s. Abschnitt "Funktion zum Verbergen von sensiblen Daten ferngesteuert aktivieren" auf S. 72).

Der aktuelle Status des Verbergens sensibler Daten wird auf dem Bildschirm **Privatsphäre** neben dem Menüpunkt **Modus** angezeigt.

Es kann eine gewisse Zeit beanspruchen, bis eine Modusänderung der Privatsphäre wirksam wird.

PRIVATSPHÄRE AKTIVIEREN / DEAKTIVIEREN

Der Privatsphären-Modus kann folgendermaßen geändert werden:

- aus dem Menü mit den Einstellungen für die Privatsphäre
- aus dem Menü für **Privatsphäre**

➔ *Gehen Sie folgendermaßen vor, um den Privatsphären-Modus zu ändern:*

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Modus**.

Das Fenster **Modus** wird geöffnet.

3. Wählen Sie einen Wert für **Privatsphären -Modus**. (s. Abb. unten).

4. Klicken Sie auf **OK**.

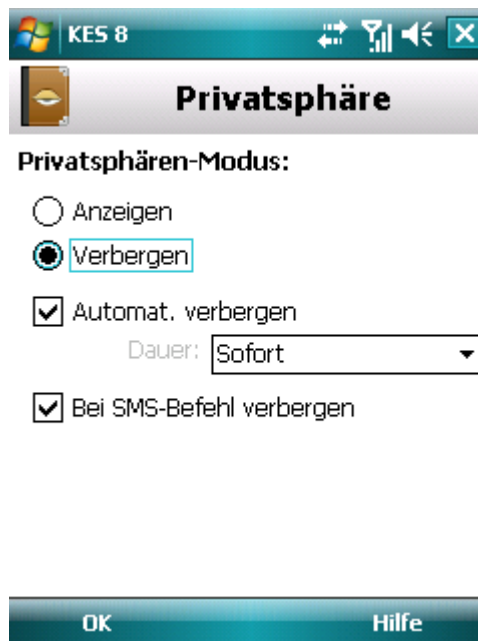


Abbildung 33: Privatsphären-Modus ändern

5. Bestätigen Sie, dass der Privatsphären-Modus geändert werden soll. Klicken Sie dazu auf **Ja**.

➤ *Gehen Sie folgendermaßen vor, um den Privatsphären-Modus schnell zu ändern:*

1. Gehen Sie auf **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Klicken Sie auf **Verbergen / Anzeigen**. Die Beschriftung dieses Punkts ändert sich abhängig vom aktuellen Modus der Privatsphäre in das jeweilige Gegenteil.
3. Bestätigen Sie, dass der Privatsphären-Modus geändert werden soll. Klicken Sie dazu auf **Ja**.

FUNKTION ZUM VERBERGEN VON SENSIBLEN DATEN AUTOMATISCH AKTIVIEREN

Sie können eine automatische Aktivierung des Verbergens vertraulicher Informationen nach Ablauf einer bestimmten Zeit einrichten. Diese Funktion wird aktiviert, nachdem das Gerät in den Energiesparmodus wechselt.

Deaktivieren Sie die Funktion zum Verbergen von sensiblen Daten, bevor die Einstellungen der Privatsphäre geändert werden sollen.

➤ *Gehen Sie folgendermaßen vor, um festzulegen, dass das Verbergen sensibler Daten nach Ablauf eines bestimmten Zeitraums automatisch aktiviert wird:*

1. Gehen Sie auf **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Modus**.
3. Das Fenster **Modus** wird geöffnet.
4. Aktivieren Sie das Kontrollkästchen **Automatisch verbergen** (s. Abb. unten).
5. Legen Sie einen Zeitraum fest, nach dem das Verbergen sensibler Daten automatisch aktiviert werden soll. Wählen Sie dazu einen der folgenden Werte für **Zeit**:
 - **Sofort**
 - **In 1 Minute**
 - **In 5 Minuten**
 - **In 15 Minuten**
 - **In 1 Stunde**

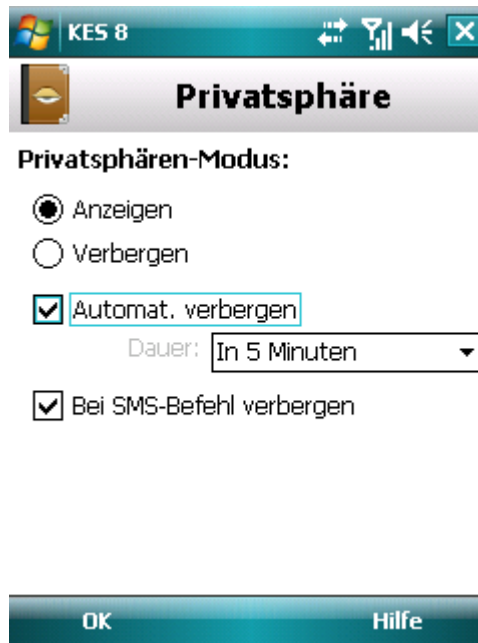


Abbildung 34: Einstellungen für das automatische Verbergen von sensiblen Daten

6. Klicken Sie auf **OK**.

FUNKTION ZUM VERBERGEN VON SENSIBLEN DATEN FERNGESTEUERT AKTIVIEREN

Kaspersky Endpoint Security 8 für Smartphones erlaubt es, das Verbergen sensibler Daten ferngesteuert von einem anderen mobilen Gerät aus zu aktivieren. Dazu muss zuvor auf Ihrem Gerät die Funktion **Bei SMS-Befehl verbergen** aktiviert werden.

➤ *Um eine ferngesteuerte Aktivierung des Verbergens vertraulicher Informationen zu ermöglichen, gehen Sie wie folgt vor:*

1. Gehen Sie auf **Menü** → **Privatsphäre**.
Das Fenster **Privatsphäre** wird geöffnet.
2. Gehen Sie auf **Modus**.
Das Fenster **Modus** wird geöffnet.
3. Aktivieren Sie das Kontrollkästchen **Bei SMS verbergen** (s. Abb. unten).

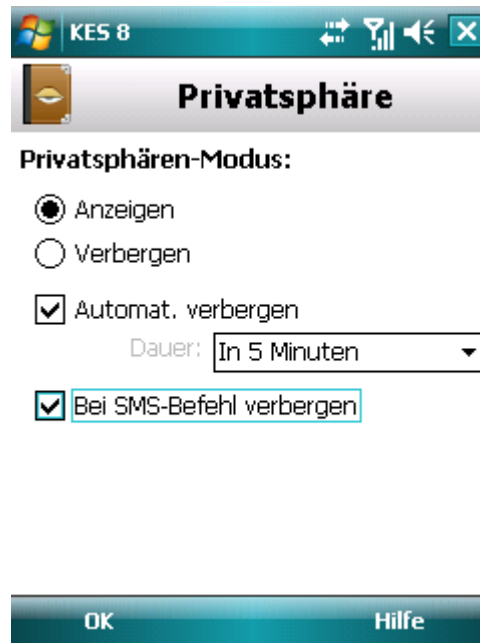


Abbildung 35: Einstellungen für das ferngesteuerte Verbergen von sensiblen Daten

4. Klicken Sie auf **OK**.

Für die ferngesteuerte Aktivierung des Verbergens vertraulicher Informationen stehen Ihnen folgende Methoden zur Verfügung:

- Erstellen Sie auf einem anderen mobilen Gerät in einem Programm für mobile Endgeräte (z. B. in Kaspersky Endpoint Security 8 für Smartphones) einen speziellen SMS-Befehl und senden Sie diesen an Ihr Gerät. Dadurch erhält Ihr Gerät unbemerkt eine SMS und die vertraulichen Daten werden verborgen. Um einen speziellen SMS-Befehl zu erstellen, verwenden Sie bitte die Funktion Befehl senden.
- Erstellen Sie auf einem anderen mobilen Gerät eine SMS mit einem speziellen Text und dem Geheimcode des Programms auf Ihrem Gerät, an das die SMS geht, und senden Sie diese. Dadurch erhält Ihr Gerät eine SMS und die vertraulichen Daten werden verborgen.

Für das Senden einer SMS fallen auf dem Telefon, von dem der SMS-Befehl gesendet wird, die tarifgemäßen Gebühren an.

➔ Um das Verbergen vertraulicher Informationen mithilfe eines speziellen SMS-Befehls von einem anderen Gerät aus ferngesteuert zu aktivieren, gehen Sie wie folgt vor:

1. Gehen Sie auf **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Befehl senden**.

Das Fenster **Befehl senden** wird geöffnet.

3. Setzen Sie den Parameter **SMS-Befehl auswählen** auf **Privatsphäre** (s. Abb. unten).

4. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.

5. Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode für das Programm ein, der für das Gerät gilt, an das der SMS-Befehl gerichtet ist.



Abbildung 36: Funktion zum Verbergen von sensiblen Daten ferngesteuert aktivieren

6. Klicken Sie auf **Senden**.

Wenn das Gerät den SMS-Befehl empfängt, wird das Verbergen sensibler Daten automatisch aktiviert.

➔ Um das Verbergen sensibler Daten mithilfe der Standard-SMS-Funktionen des Telefons ferngesteuert zu aktivieren:

schicken Sie an das andere Gerät eine SMS mit dem Text `hide:<Code>`, wobei `<Code>` der Geheimcode für das Programm ist, der auf dem anderen Gerät festgelegt wurde. Die Groß- und Kleinschreibung von Buchstaben und die Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

LISTE DER VERTRAULICHEN NUMMERN ERSTELLEN.

Die Kontaktliste enthält vertrauliche Nummern, für die die Privatsphäre Informationen verbirgt. Eine neue Nummer kann entweder manuell zur Liste hinzugefügt oder aus den Kontakten oder von der SIM-Karte importiert werden.

Deaktivieren Sie das Verbergen von sensiblen Daten, bevor die Kontaktliste erstellt werden soll.

IN DIESEM ABSCHNITT

Hinzufügen einer Nummer zur Liste der vertraulichen Nummern.....	75
Bearbeiten einer Nummer der Liste der vertraulichen Nummern	76
Löschen einer Nummer aus der Liste der vertraulichen Nummern	76

HINZUFÜGEN EINER NUMMER ZUR LISTE DER VERTRAULICHEN NUMMERN

Sie können der Kontaktliste eine Nummer (z. B. +12345678) manuell hinzufügen, oder sie aus den Kontakten oder von der SIM-Karte importieren.

Deaktivieren Sie das Verbergen von sensiblen Daten, bevor die Kontaktliste erstellt werden soll.

➤ Gehen Sie folgendermaßen vor, um eine Nummer zur Kontaktliste hinzuzufügen:

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Kontaktliste**.

Das Fenster **Kontaktliste** wird geöffnet.

3. Führen Sie im nächsten Fenster eine der folgenden Aktionen aus (s. Abb. unten):

- Um eine Nummer aus den Kontakten hinzuzufügen, gehen Sie auf **Menü** → **Hinzufügen** → **Outlook-Kontakt**. Wählen Sie im folgenden Fenster **Outlook-Kontakt** den entsprechenden Eintrag aus und klicken Sie dann auf **Auswählen**.
- Gehen Sie auf **Menü** → **Hinzufügen** → **Von SIM hinzufügen**, um eine Nummer hinzuzufügen, die auf der SIM-Karte gespeichert ist. Wählen Sie im folgenden Fenster **Kontakt von SIM** den entsprechenden Eintrag aus und klicken Sie auf **Auswählen**.
- Um eine Nummer manuell hinzuzufügen, gehen Sie auf **Menü** → **Hinzufügen** → **Nummer**. Füllen Sie im folgenden Fenster **Hinzufügen** das Feld **Telefonnummer** aus und klicken Sie auf **OK**.



Abbildung 37: Eintrag zur Liste der geschützten Kontakte hinzufügen.

Die Nummer wird zur Kontaktliste hinzugefügt.

BEARBEITEN EINER NUMMER DER LISTE DER VERTRAULICHEN NUMMERN

Deaktivieren Sie das Verbergen von sensiblen Daten, bevor die Kontaktliste erstellt werden soll.

Es können nur Nummern aus der Kontaktliste geändert werden, die manuell hinzugefügt wurden. Nummern, die aus den Kontakten oder aus der SIM-Nummernliste übernommen wurden, können nicht geändert werden.

➤ Gehen Sie folgendermaßen vor, um eine Nummer in der Kontaktliste zu ändern:

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Kontaktliste**.

Das Fenster **Kontaktliste** wird geöffnet.

3. Markieren Sie in der Kontaktliste die Nummer, die Sie ändern möchten, und gehen Sie dann auf das **Menü** → **Ändern**.

Das Fenster **Ändern** wird geöffnet.

4. Ändern Sie die Daten im Feld **Telefonnummer**.

5. Klicken Sie nach Abschluss der Änderungen auf **OK**.

Die Nummer wird geändert.

LÖSCHEN EINER NUMMER AUS DER LISTE DER VERTRAULICHEN NUMMERN

Sie können eine Nummer aus der Liste der vertraulichen Kontakte löschen oder die gesamte Kontaktliste leeren.

Deaktivieren Sie das Verbergen von sensiblen Daten, bevor die Kontaktliste erstellt werden soll.

➤ Gehen Sie folgendermaßen vor, um eine Nummer aus der Kontaktliste zu löschen:

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Kontaktliste**.

Das Fenster **Kontaktliste** wird geöffnet.

3. Wählen Sie eine Nummer aus, die gelöscht werden soll, und gehen Sie dann auf **Menü** → **Löschen**.

4. Bestätigen Sie das Löschen. Klicken Sie dazu auf **Ja**.

➤ Gehen Sie folgendermaßen vor, um die Kontaktliste zu leeren:

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Kontaktliste**.

Das Fenster **Kontaktliste** wird geöffnet.

3. Gehen Sie auf **Menü** → **Alle löschen**.
4. Bestätigen Sie das Löschen. Klicken Sie dazu auf **Ja**.

Die Kontaktliste wird geleert.

AUSWAHL DER ZU VERBERGENDEN INFORMATIONEN: PRIVATSPHÄRE

Die Privatsphäre erlaubt es, für Nummern aus der Kontaktliste die folgenden Informationen zu verbergen: Kontakte, SMS-Korrespondenz, Einträge in den Anruflisten, eingehende SMS und Anrufe. Sie können die Informationen und Ereignisse auswählen, die von der Privatsphäre für vertrauliche Nummern verborgen werden sollen.

Deaktivieren Sie die Funktion zum Verbergen von sensiblen Daten, bevor die Einstellungen der Privatsphäre geändert werden sollen.

➔ Gehen Sie folgendermaßen vor, um die zu verbergenden Informationen und Ereignisse für vertrauliche Nummern auszuwählen:

1. Gehen Sie auf **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Verborgene Objekte**.

Es öffnet sich das Fenster **Zu verbergende Objekte** (s. Abb. unten).

3. Wählen Sie im Block **Einträge verbergen** die Informationen aus, die für vertrauliche Nummern verborgen werden sollen. Folgende Einstellungen sind vorgesehen:

- **Kontakte** – Alle Informationen über vertrauliche Nummern in den Kontakten ausblenden.
- **SMS** – SMS in den Ordnern **Eingehende**, **Weitergeleitete** und **Entwürfe** für vertrauliche Nummern verbergen.
- **Anrufe** – Anrufe von vertraulichen Nummern werden angenommen. Die Nummer des Anrufers wird aber nicht ermittelt und in der Anrufliste werden Infos über vertrauliche Nummern (Angenommen, Gewählt, Unbeantwortet) verborgen.

4. Wählen Sie im Block **Ereignisse verbergen** die Ereignisse aus, die für vertrauliche Nummern verborgen werden sollen. Folgende Einstellungen sind vorgesehen:

- **Eingehende SMS** – Der Empfang eingehender SMS wird verborgen (auf dem Display erscheint kein Signal darüber, dass eine neue SMS von einer vertraulichen Nummer empfangen wurde). Alle SMS, die von vertraulichen Nummern empfangen wurden, können gelesen werden, wenn das Verbergen sensibler Daten deaktiviert wird.
- **Eingehende Anrufe** – Anrufe von vertraulichen Nummern werden blockiert (der Anrufer hört in diesem Fall ein "Besetzt"-Zeichen). Informationen über eingegangene Anrufe werden angezeigt, wenn das Verbergen sensibler Daten deaktiviert wird.

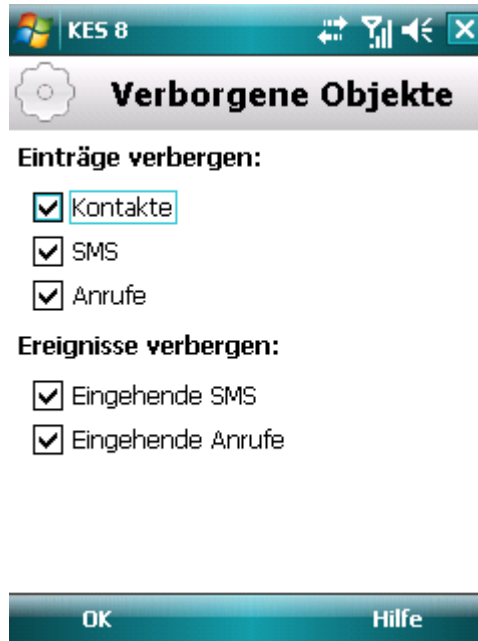


Abbildung 38: Auswahl der zu verbergenden Informationen und Ereignisse

5. Klicken Sie auf **OK**.

NETZWERKAKTIVITÄT FILTERN. FIREWALL

Dieser Abschnitt informiert über die Firewall, die auf Ihrem Gerät die Netzwerkverbindungen überwacht. Außerdem wird hier beschrieben, wie die Firewall aktiviert / deaktiviert wird und wie ein Funktionsmodus ausgewählt wird.

IN DIESEM ABSCHNITT

Firewall.....	79
Über die Modi der Firewall	79
Firewall-Modus auswählen.....	79
Meldungen über blockierte Verbindungen.....	80

FIREWALL

Die Firewall richtet sich bei der Kontrolle von Netzwerkverbindungen auf Ihrem Gerät nach dem ausgewählten Modus. Mit der Firewall lassen sich erlaubte Verbindungen (z. B. für die Synchronisierung mit dem Remote-Management-System) und verbotene Verbindungen (z. B. für Suche im Internet, Datei-Download) festlegen.

Die Firewall erlaubt es, die Meldungen über blockierte Verbindungen anzupassen (s. Abschnitt "Über die Modi der Firewall" auf S. [79](#)).

Informationen über die Arbeit der Firewall werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [93](#)).

ÜBER DIE MODI DER FIREWALL

Sie können einen Modus auswählen, nach dem die Firewall erlaubte und verbotene Verbindungen ermittelt. Es sind die folgenden Firewall-Modi vorgesehen:

- **Aus** – jede Netzwerkaktivität erlauben.
- **Minimaler Schutz** – nur eingehende Verbindungen blockieren. Ausgehende Verbindungen werden erlaubt.
- **Maximaler Schutz** – alle eingehenden Verbindungen blockieren. Prüfen eines E-Mail-Postfachs, Anzeige von Webseiten und Download von Dateien sind erlaubt. Ausgehende Verbindungen können nur über die Ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3 erfolgen.
- **Alle blockieren** – jede Netzwerkaktivität blockieren, außer Update die Antiviren-Datenbanken und Verbindung mit dem Remote-Management-System.

Sie können den Firewall-Modus ändern (s. Abschnitt "Firewall-Modus auswählen" auf S. [79](#)). Der aktuelle Modus wird auf dem Bildschirm **Firewall** neben dem Menüpunkt **Modus** angezeigt.

FIREWALL-MODUS AUSWÄHLEN

Verwenden Sie die Joystick-Tasten des Geräts, um die Parameterwerte zu ändern.

➤ Gehen Sie folgendermaßen vor, um einen Modus für die Firewall auszuwählen:

1. Wählen Sie **Menü** → **Firewall**.

Das Fenster **Firewall** wird geöffnet.

2. Gehen Sie auf **Modus**.

Das Fenster **Firewall** wird geöffnet.

3. Wählen Sie einen Modus für die Firewall aus (s. Abb. unten).

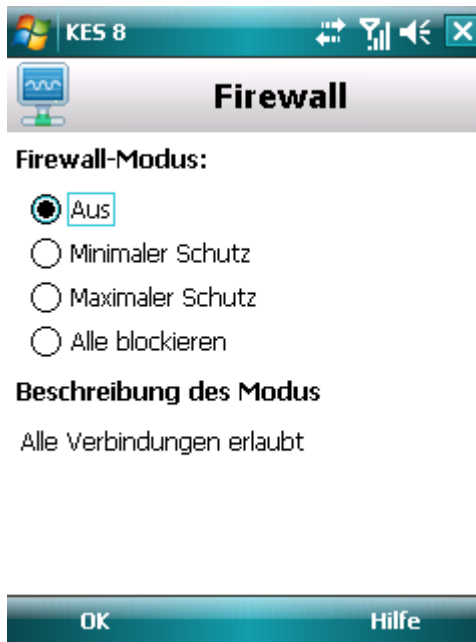


Abbildung 39: Sicherheitsstufe für Firewall wählen

4. Klicken Sie auf **OK**.

MELDUNGEN ÜBER BLOCKIERTE VERBINDUNGEN

Die Firewall erlaubt den Empfang von Meldungen über blockierte Verbindungen. Sie können den Empfang von Firewall-Benachrichtigungen anpassen.

➤ Gehen Sie folgendermaßen vor, um den Versand von Meldungen über Blockierungen zu verwalten:

1. Gehen Sie auf **Menü** → **Firewall**.

Das Fenster **Firewall** wird geöffnet.

2. Gehen Sie auf **Benachrichtigungen**.

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



Abbildung 40: Einrichtung für Meldungen über Blockierungen

3. Wählen Sie im Block **Meldungen über Blockieren** eine der folgenden Aktionen aus:
 - **Anzeigen** – der Versand von Meldungen wird aktiviert. Die Firewall informiert über blockierte Verbindungen.
 - **Verbergen** – Der Versand von Meldungen wird deaktiviert. Die Firewall informiert nicht über blockierte Verbindungen.
4. Klicken Sie auf **OK**.

PERSÖNLICHE DATEN VERSCHLÜSSELN

Dieser Abschnitt informiert über die Komponente Verschlüsselung, mit der die Ordner auf dem Gerät verschlüsselt werden können. Außerdem wird hier beschrieben, wie ausgewählte Ordner verschlüsselt und entschlüsselt werden können.

IN DIESEM ABSCHNITT

Verschlüsselung	82
Daten verschlüsseln	82
Daten entschlüsseln	85
Zugriff auf verschlüsselte Daten verbieten	86

VERSCHLÜSSELUNG

Die Funktion Verschlüsselung chiffriert die Informationen, die sich in den von Ihnen ausgewählten Ordnern befinden. Die Verschlüsselungsfunktion basiert auf einer analogen Funktion, die in das Betriebssystem Ihres Geräts integriert ist. Die Chiffrierfunktion erlaubt es, Ordner eines beliebigen Typs zu verschlüsseln. Eine Ausnahme bilden Systemdateien. Zur Verschlüsselung können Sie Ordner auswählen, die sich im Gerätespeicher oder auf einer Speicherkarte befinden. Um auf verschlüsselte Informationen zuzugreifen, muss der Geheimcode des Programms eingegeben werden, der beim ersten Start des Programms festgelegt wurde.

Um ausführbare exe-Dateien aus einem verschlüsselten Ordner zu starten, müssen diese vorher entschlüsselt werden. Dazu muss der Geheimcode des Programms eingegeben werden.

Um Zugriff auf verschlüsselte Daten zu erhalten, geben Sie den Geheimcode für das Programm ein (s. Abschnitt "Geheimcode eingeben" auf S. [25](#)). Sie können eine Zeitspanne festlegen (s. Abschnitt "Zugriff auf verschlüsselte Daten verbieten" auf S. [86](#)), nach deren Ablauf ein Zugriffsverbot für verschlüsselte Ordner aktiviert wird und die Eingabe des Geheimcodes für das Programm erforderlich ist, um mit den Ordnern zu arbeiten. Diese Funktion wird aktiviert, nachdem das Gerät in den Energiesparmodus wechselt.

Informationen über die Arbeit der Verschlüsselung werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [93](#)).

DATEN VERSCHLÜSSELN

Die Verschlüsselung erlaubt es, eine beliebige Anzahl von Ordnern, die nicht zum System gehören, zu verschlüsseln. Die Ordner können sich im Gerätespeicher oder auf einer Speicherkarte befinden.

Eine Liste aller bisher verschlüsselten und entschlüsselten Ordner befindet sich im Fenster **Verschlüsselung** unter dem Menüpunkt **Ordnerliste**.

Außerdem können Sie einen einzelnen Ordner oder alle Ordner, die in der Ordnerliste stehen, verschlüsseln.

➡ *Gehen Sie folgendermaßen vor, um einen Ordner zur Liste der zu verschlüsselnden Ordner hinzuzufügen und ihn zu verschlüsseln:*

1. Wählen Sie **Menü** → **Verschlüsselung**.

Das Fenster **Verschlüsselung** wird geöffnet.

2. Gehen Sie auf **Ordnerliste**.

Das Fenster **Ordnerliste** wird geöffnet.

3. Klicken Sie auf **Menü** → **Hinzufügen** (s. Abb. unten).



Abbildung 41: Zu verschlüsselnde Ordner auswählen

Ein Fenster mit einer Übersicht des Dateisystems Ihres Geräts wird geöffnet.

4. Wählen Sie den Ordner aus, der verschlüsselt werden soll, und klicken Sie auf **Verschlüsseln**.

Verwenden Sie zur Navigation im Dateisystem den Stylus oder die Joystick-Tasten des Geräts.

Sie werden von Kaspersky Endpoint Security 8 für Smartphones benachrichtigt, wenn der Verschlüsselungsvorgang abgeschlossen wurde. Es erscheint ein Meldungsfenster.

5. Klicken Sie auf **OK**.

Für einen verschlüsselten Ordner ändert sich im **Menü** der Punkt **Verschlüsseln** in **Entschlüsseln**.

Nach der Verschlüsselung werden die Dateien automatisch ent- und verschlüsselt, wenn Sie mit den Dateien in einem verschlüsselten Ordner arbeiten, Dateien aus einem verschlüsselten Ordner entnehmen oder neue Dateien darin speichern.

➤ *Gehen Sie folgendermaßen vor, um alle Ordner der Liste auf einmal zu verschlüsseln:*

1. Wählen Sie **Menü** → **Verschlüsselung**.

Das Fenster **Verschlüsselung** wird geöffnet.

2. Gehen Sie auf **Ordnerliste**.

Das Fenster **Ordnerliste** wird geöffnet.

3. Gehen Sie auf **Menü** → **Zusatzaktionen** → **Alle verschlüsseln**.

Sie werden von Kaspersky Endpoint Security 8 für Smartphones benachrichtigt, wenn der Verschlüsselungsvorgang abgeschlossen wurde. Es erscheint ein Meldungsfenster.

4. Klicken Sie auf **OK**.

DATEN ENTSCHLÜSSELN

Sie können zuvor verschlüsselte Daten entschlüsseln (s. Abschnitt "Datenverschlüsselung" auf S. [82](#)). Sie können einen Ordner oder alle Ordner, die Sie auf dem Gerät chiffriert haben, entschlüsseln.

Ordner, die auf der Verschlüsselungsliste stehen und vom Administrator chiffriert wurden, können nicht entschlüsselt oder von der Liste entfernt werden.

➔ Gehen Sie folgendermaßen vor, um einen zuvor verschlüsselten Ordner zu entschlüsseln:

1. Gehen Sie auf **Menü** → **Verschlüsselung**.

Das Fenster **Verschlüsselung** wird geöffnet.

2. Gehen Sie auf **Ordnerliste**.

Das Fenster **Ordnerliste** wird geöffnet. Es enthält eine Liste aller bisher ver- und entschlüsselten Ordner.

3. Wählen Sie einen verschlüsselten Ordner aus der Liste und klicken Sie auf **Menü** → **Entschlüsseln** (s. Abb. unten).



Abbildung 42: Funktion aktivieren

Sie werden von Kaspersky Endpoint Security 8 für Smartphones über den Abschluss des Entschlüsselungsvorgangs benachrichtigt. Es erscheint ein Meldungsfenster.

4. Klicken Sie auf **OK**.

Für einen entschlüsselten Ordner ändert sich im **Menü** der Punkt **Entschlüsseln** in **Verschlüsseln**. Sie können den Ordner erneut verschlüsseln (s. Abschnitt "Daten verschlüsseln" auf S. [82](#)).

➔ Gehen Sie folgendermaßen vor, um alle Ordner aus der Verschlüsselungsliste auf einmal zu entschlüsseln:

1. Wählen Sie **Menü** → **Verschlüsselung**.

Das Fenster **Verschlüsselung** wird geöffnet.

2. Gehen Sie auf **Ordnerliste**.

Das Fenster **Ordnerliste** wird geöffnet.

3. Gehen Sie auf **Menü** → **Zusatzaktionen** → **Alle entschlüsseln**.

Sie werden von Kaspersky Endpoint Security 8 für Smartphones durch eine Bildschirmmeldung benachrichtigt, wenn der Entschlüsselungsvorgang abgeschlossen wurde.

4. Klicken Sie auf **OK**.

ZUGRIFF AUF VERSCHLÜSSELTE DATEN VERBIETEN

Die Verschlüsselung erlaubt es, eine Zeitspanne festzulegen, nach deren Ablauf das Zugriffsverbot für verschlüsselte Ordner automatisch aktiviert werden soll. Diese Funktion wird aktiviert, nachdem das Gerät in den Energiesparmodus wechselt. Um mit verschlüsselten Informationen zu arbeiten, muss der Geheimcode des Programms eingegeben werden.

- *Gehen Sie folgendermaßen vor, damit der Zugriff auf einen verschlüsselten Ordner nach Ablauf einer bestimmten Zeitspanne verboten wird:*

1. Gehen Sie auf **Menü** → **Verschlüsselung**.

Das Fenster **Verschlüsselung** wird geöffnet.

2. Gehen Sie auf **Zugriff verbieten**.

Das Fenster **Zugriff verbieten** wird geöffnet.

3. Legen Sie fest, nach welcher Zeitspanne das Zugriffsverbot für verschlüsselte Ordner aktiviert werden soll. Wählen Sie dazu für **Zugriff verbieten** einen der folgenden Werte (s. Abb. unten):

- **Sofort**
- **In 1 Minute**
- **In 5 Minuten**
- **In 15 Minuten**

- In 1 Stunde



Abbildung 43: Zugriff auf verschlüsselte Daten blockieren

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

- ➔ Um den Zugriff auf verschlüsselte Ordner zu verbieten, nachdem sie geöffnet wurden,

klicken Sie auf das Symbol von Kaspersky Endpoint Security 8 in der Taskleiste des Geräts und wählen Sie den Punkt **Daten blockieren** aus (s. Abb. unten). Das Zugriffsverbot für verschlüsselte Informationen wird aktiviert.



Abbildung 44: Kontextmenü des Programms in der Taskleiste des Geräts

UPDATE DER PROGRAMM-DATENBANKEN

Dieser Abschnitt informiert über das Update der Antiviren-Datenbanken des Programms. Das Update hält den Schutz Ihres Geräts auf dem neusten Stand. Außerdem werden hier folgende Vorgänge beschrieben: Informationen über die installierten Antiviren-Datenbanken des Programms anzeigen, Updatevorgang manuell starten, automatisches Datenbank-Update nach Zeitplan anpassen.

IN DIESEM ABSCHNITT

Über das Update der Programm-Datenbanken.....	88
Datenbankinfos anzeigen.....	89
Manuelles Update	89
Update nach Zeitplan starten	90
Update im Roaming	91

ÜBER DAS UPDATE DER PROGRAMM-DATENBANKEN

Die Suche erfolgt auf Basis von Antiviren-Datenbanken des Programms, die eine Beschreibung aller momentan bekannten schädlichen Programme und entsprechende Desinfektionsmethoden sowie eine Beschreibung sonstiger unerwünschter Objekte enthalten. Es ist sehr wichtig, die Antiviren-Datenbanken des Programms auf dem neuesten Stand zu halten.

Es wird empfohlen, die Programm-Datenbanken regelmäßig zu aktualisieren. Die Programm-Datenbanken gelten als stark veraltet, wenn seit der letzten Aktualisierung 15 Tage vergangen sind. In diesem Fall sinkt das Schutzniveau.

Kaspersky Endpoint Security 8 für Smartphones lädt die Updates der Programm-Datenbanken von den Updateservern herunter, die vom Administrator festgelegt wurden.

Um die Antiviren-Datenbanken des Programms zu aktualisieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

Die Aktualisierung der Antiviren-Datenbanken des Programms wird nach folgendem Algorithmus ausgeführt:

1. Die Programm-Datenbanken auf Ihrem mobilen Gerät werden mit den Datenbanken verglichen, die sich auf dem festgelegten Updateserver befinden.
2. Kaspersky Endpoint Security 8 für Smartphones führt eine der folgenden Aktionen aus:
 - Wenn aktuelle Programm-Datenbanken installiert sind, wird das Update abgebrochen. Es erscheint eine Meldung auf dem Bildschirm.
 - Wenn sich die installierten Datenbanken von den angebotenen unterscheiden, wird ein neues Updatepaket heruntergeladen und installiert.

Die Verbindung wird nach Abschluss des Updatevorgangs automatisch getrennt. Eine Verbindung, die bereits vor dem Update aufgebaut wurde, bleibt bestehen.

Sie können die Updateaufgabe entweder zu einem beliebigen Zeitpunkt manuell starten, wenn das Gerät nicht für andere Aufgaben benötigt wird, oder einen Zeitplan für das automatische Update erstellen.

Ausführliche Informationen über die verwendeten Datenbanken stehen im Fenster **Update** unter dem Menüpunkt **Datenbank-Infos** zur Verfügung.

Informationen über das Update der Antiviren-Datenbanken werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [93](#)).

DATENBANKINFOS ANZEIGEN

Sie können folgende Informationen über die installierten Antiviren-Datenbanken des Programms anzeigen: Datum des letzten Updates, Erscheinungsdatum der Datenbanken, Größe der Datenbanken und Anzahl der Einträge in den Datenbanken.

➔ *Gehen Sie folgendermaßen vor, um Informationen über die aktuellen Datenbanken anzuzeigen:*

1. Wählen Sie **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Update**.

Das Fenster **Update** wird geöffnet.

3. Wählen Sie **Datenbank-Infos**.

Das folgende Fenster **Datenbank-Infos** informiert über die installierten Antiviren-Datenbanken des Programms (s. Abb. unten).



Abbildung 45: Informationen über die installierten Antiviren-Datenbanken des Programms

MANUELLES UPDATE

Sie können das Update der Antiviren-Datenbanken manuell starten.

➔ *Gehen Sie folgendermaßen vor, um das Update der Antiviren-Datenbanken des Programms manuell zu starten:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Update**.

Das Fenster **Update** wird geöffnet.

3. Gehen Sie auf **Update** (s. Abb. unten).

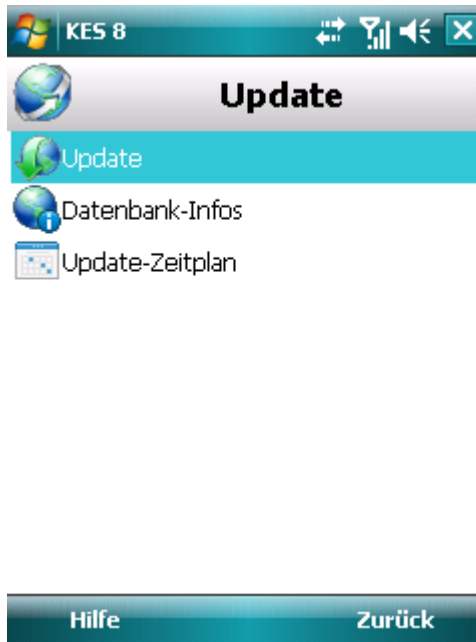


Abbildung 46: Update manuell starten

Das Programm startet das Update der Antiviren-Datenbanken von dem Server, der vom Administrator festgelegt wurde. Informationen über den Updatevorgang werden auf dem Bildschirm angezeigt.

UPDATE NACH ZEITPLAN STARTEN

Eine wichtige Voraussetzung für die Sicherheit des Geräts besteht darin, den Schutz auf dem neusten Stand zu halten. Sie können ein automatisches Update für die Antiviren-Datenbanken festlegen und einen entsprechenden Startzeitplan anlegen.

Damit ein geplantes Update ausgeführt wird, muss das Gerät zum entsprechenden Zeitpunkt eingeschaltet sein.

➤ Gehen Sie folgendermaßen vor, um einen Startzeitplan für das Update anzupassen:

1. Wählen Sie **Menü** → **Anti-Virus**.

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

2. Gehen Sie auf **Update**.

Das Fenster **Update** wird geöffnet.

3. Gehen Sie auf den Punkt **Update-Zeitplan**.

Das Fenster **Zeitplan** wird geöffnet.

4. Aktivieren Sie das Kontrollkästchen **Update nach Zeitplan** (s. Abb. unten).

5. Erstellen Sie einen Zeitplan für das Update. Wählen Sie dazu einen Wert für den Parameter **Frequenz**:
- **Täglich**: Die Programm-Datenbanken werden jeden Tag aktualisiert. Legen Sie einen Wert für **Zeit** fest.
 - **Wöchentlich**: Die Programm-Datenbanken werden ein Mal in der Woche aktualisiert. Legen Sie Werte für **Zeit** und **Wochentag** fest.



Abbildung 47: Einstellungen für den Start eines geplanten Updates

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

UPDATE IM ROAMING

Sie können kontrollieren, ob ein geplantes Update erfolgen soll, wenn sich das Gerät im Roaming befindet. Dies ist sinnvoll, weil der Datenverkehr für eine Internetverbindung nach Roamingtarifen abgerechnet wird.

Wenn ein geplantes Update im Roaming verboten wurde, ist eine manuelle Aktualisierung im gewöhnlichen Modus möglich.

➤ Gehen Sie folgendermaßen vor, um einen geplanten Updatestart im Roaming zu verbieten:

1. Gehen Sie auf **Menü** → **Anti-Virus**.
Das Fenster **Anti-Virus** wird geöffnet.
2. Gehen Sie auf **Update**.
Das Fenster **Update** wird geöffnet.
3. Gehen Sie auf den Punkt **Update-Zeitplan**.
Das Fenster **Zeitplan** wird geöffnet.
4. Deaktivieren Sie im Block **Update im Roaming** das Kontrollkästchen **Update im Roaming**.

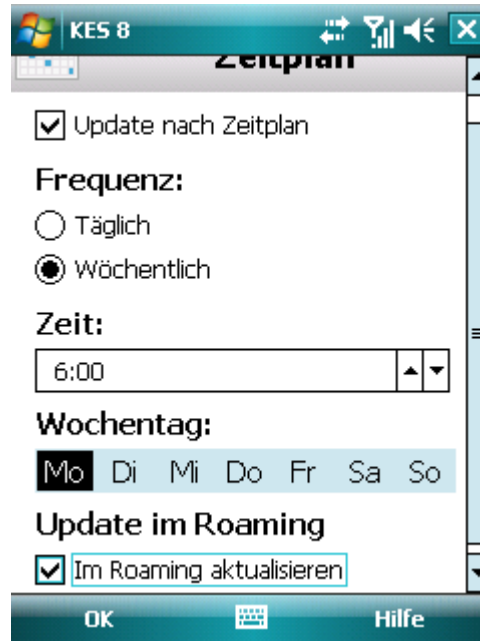


Abbildung 48: Einstellungen für den automatischen Start des Updates im Roaming

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

PROGRAMMBERICHTE

Dieser Abschnitt informiert über die Berichte, in denen die Arbeit der einzelnen Komponenten und die Ausführung aller Aufgaben (z. B. Update der Antiviren-Datenbanken des Programms, Scan auf Befehl) protokolliert werden.

IN DIESEM ABSCHNITT

Berichte	93
Berichtseinträge anzeigen	93
Einträge aus Bericht löschen	94

BERICHTE

In Berichten werden Ereignisse gespeichert, die bei der Arbeit der einzelnen Komponenten von Kaspersky Endpoint Security 8 für Smartphones auftreten. Für jede Komponente wird ein eigener Ereignisbericht geführt. Sie können einen Bericht über die Ereignisse auswählen und ansehen, die bei der Arbeit der Komponente eingetreten sind. Die Einträge werden im Bericht chronologisch in absteigender Reihenfolge angeordnet.

BERICHTSEINTRÄGE ANZEIGEN

➔ *Gehen Sie folgendermaßen vor, um alle Einträge anzuzeigen:*

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie den Punkt **Berichte**.

Das Fenster **Berichte** wird geöffnet.

3. Wählen Sie die Komponente, für die ein Ereignisbericht angezeigt werden soll.

Der Ereignisbericht der gewählten Komponente wird geöffnet (s. Abb. unten).



Abbildung 49: Berichtseinträge anzeigen

- Um ausführliche Informationen über einen Berichtseintrag anzuzeigen,

wählen Sie einen Eintrag aus und klicken Sie auf **Details**.

Im Fenster **Details** werden ausführliche Informationen zu der vom Programm ausgeführten Aktion angezeigt. So wird für die Aktion "Objekt wurde in die Quarantäne verschoben" zum Beispiel der Pfad der infizierten Datei auf dem Gerät angezeigt.

- Um zur Berichtsliste zurückzukehren,

klicken Sie auf **Menü** → **Zurück**.

EINTRÄGE AUS BERICHT LÖSCHEN

Sie können alle Berichte leeren. Dabei werden die Informationen über die Arbeit aller Komponenten von Kaspersky Endpoint Security 8 für Smartphones gelöscht.

- Gehen Sie folgendermaßen vor, um alle Berichte zu leeren:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie den Punkt **Berichte**.

Das Fenster **Bericht** wird geöffnet.

3. Öffnen Sie den Bericht einer beliebigen Komponente.

4. Gehen Sie auf **Menü** → **Alle löschen**.

5. Bestätigen Sie die Deinstallation mit **Ja**.

Es werden alle Einträge im Bericht aller Komponenten gelöscht.

ERWEITERTE EINSTELLUNGEN ANPASSEN

Dieser Abschnitt informiert über zusätzliche Optionen von Kaspersky Endpoint Security 8 für Smartphones: Geheimcode für das Programm ändern, Audiosignale des Programms verwalten, Tooltips aktivieren / deaktivieren (Tooltips anzeigen, wenn eine Komponente angepasst werden soll).

IN DIESEM ABSCHNITT

Geheimcode ändern.....	95
Tooltips anzeigen.....	95
Audiosignale verwalten.....	96

GEHEIMCODE ÄNDERN

Der Geheimcode für das Programm, der nach dem ersten Start des Programms festgelegt wurde, kann geändert werden.

➤ *Gehen Sie folgendermaßen vor, um den Geheimcode des Programms zu ändern:*

1. Gehen Sie auf **Menü** → **Erweitert**.
Das Fenster **Erweitert** wird geöffnet.
2. Gehen Sie auf **Einstellungen**.
Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie den Punkt **Code eingeben**.
4. Geben Sie den aktuellen Geheimcode des Programms im Feld **Code eingeben** ein.
5. Geben Sie in den Feldern **Neuen Code eingeben** und **Code bestätigen** einen neuen Geheimcode für das Programm ein und klicken Sie auf **OK**, um die Änderungen zu speichern.

TOOLTIPS ANZEIGEN

Während Sie die Einstellungen der Komponenten anpassen, zeigt Kaspersky Endpoint Security 8 für Smartphones standardmäßig kurze Tooltips für die jeweilige Funktion an. Sie können die Anzeige von Tooltips für Kaspersky Endpoint Security 8 für Smartphones anpassen.

➤ *Gehen Sie folgendermaßen vor, um die Anzeige von Tooltips anzupassen:*

1. Wählen Sie **Menü** → **Erweitert**.
Das Fenster **Erweitert** wird geöffnet.
2. Gehen Sie auf **Einstellungen**.
Das Fenster **Einstellungen** wird geöffnet.
3. Gehen Sie auf **Tooltips**.

Das Fenster **Tooltips** wird geöffnet.

4. Wählen Sie einen Wert für **Tooltips**:
 - **Anzeigen** – Tooltips anzeigen, bevor eine Funktion angepasst wird.
 - **Verbergen** – keine Tooltips anzeigen.



Abbildung 50: Anzeige von Tooltips anpassen

5. Klicken Sie auf **OK**.

AUDIOSIGNALE VERWALTEN

Bei der Arbeit des Programms treten unterschiedliche Ereignisse auf. Beispiele: Fund eines infizierten Objekts oder eines Virus; Die Lizenz ist abgelaufen. Damit das Programm Sie über solche Ereignisse informiert, können Sie entsprechende Audiosignale aktivieren.

Kaspersky Endpoint Security 8 für Smartphones aktiviert die Tonsignale nur in Übereinstimmung mit dem aktuellen Gerätemodus.

Verwenden Sie die Joystick-Tasten des Geräts, um die Parameterwerte zu ändern.

➤ *Gehen Sie folgendermaßen vor, um die Audiosignale des Programms zu verwalten:*

1. Gehen Sie auf **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Einstellungen**.

Das Fenster **Einstellungen** wird geöffnet.

3. Gehen Sie auf **Ton**.

Das Fenster **Ton** wird geöffnet.

4. Wählen Sie einen Wert für **Audiosignale** (s. Abb. unten):

- **Aktivieren** – unabhängig vom Geräteprofil immer Audiosignale verwenden.
- **Deaktivieren** – keine Audiosignale verwenden.

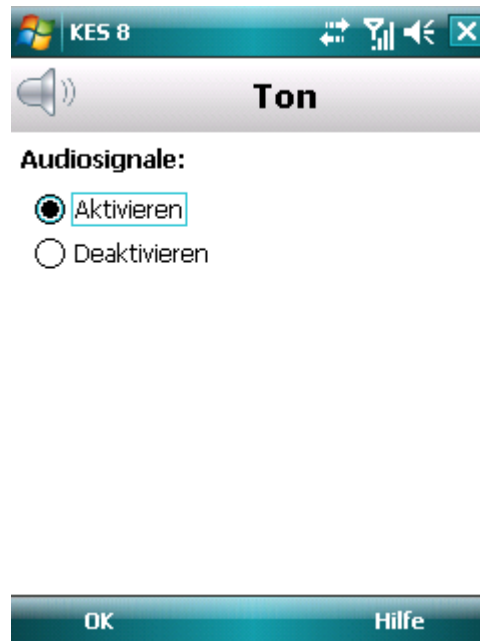


Abbildung 51: Einstellungen für Audiosignale

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

GLOSSAR

A

ANTIVIREN-DATENBANKEN

Die Datenbanken werden von den Kaspersky-Lab-Spezialisten erstellt und enthalten eine detaillierte Beschreibung aller im Moment existierenden Bedrohungen für die Computersicherheit und der dafür notwendigen Erkennungs- und Desinfektionsmethoden. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, wenn neue Bedrohungen auftauchen.

ARCHIV

Datei, die ein oder mehrere Objekte "enthält", die ihrerseits auch Archive sein können.

D

DATENBANK-UPDATE

Eine Funktion, die vom Kaspersky-Lab-Programm ausgeführt wird und die es erlaubt, den aktuellen Zustand des Schutzes aufrecht zu erhalten. Dabei werden die Antiviren-Datenbanken von den Kaspersky-Lab-Updateservern auf das Gerät kopiert und automatisch vom Programm übernommen.

DESINFEKTION VON OBJEKTEN

Verarbeitungsmethode für infizierte Objekte, bei der die Daten vollständig oder teilweise wiederhergestellt werden oder sich ergibt, dass eine Desinfektion unmöglich ist. Objekte werden auf Basis von Datenbank-Einträgen desinfiziert. Beim Desinfektionsvorgang können Daten teilweise verloren gehen.

G

GEHEIMCODE FÜR DAS PROGRAMM

Der Geheimcode des Programms verhindert einen unautorisierten Zugriff auf die Programmeinstellungen und auf die geschützten Informationen auf dem Gerät. Er wird beim ersten Start des Programms vom Benutzer festgelegt und besteht aus mindestens vier Ziffern. Der Geheimcode des Programms wird in folgenden Fällen abgefragt:

- für den Zugriff auf die Programmeinstellungen
- für den Zugriff auf verschlüsselte Ordner
- wenn von einem anderen mobilen Gerät aus ein SMS-Befehl gesendet wird, um folgende Funktionen ferngesteuert zu starten: SMS-Block, SMS-Clean, SIM-Watch, GPS-Find, Privatsphäre.
- bei der Deinstallation des Programms

I

INFIZIERTES OBJEKT

Objekt, das schädlichen Code enthält: Bei der Untersuchung des Objekts wurde erkannt, dass ein Abschnitt des Objektcodes vollständig mit dem Code einer bekannten Bedrohung übereinstimmt. Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Objekten zu arbeiten, weil dies zur Infektion Ihres Geräts führen kann.

L**LÖSCHEN VON SMS**

Verarbeitungsmethode für SMS, die Spam-Merkmale aufweisen. Dabei wird die Nachricht physikalisch gelöscht. Diese Methode wird für SMS empfohlen, die eindeutig als Spam gelten.

M**MASKE FÜR EINE TELEFONNUMMER**

Platzhalter für eine Telefonnummer in der Schwarzen oder Weißen Liste. Die beiden wichtigsten Zeichen in Masken für Telefonnummern sind * und ? (wobei * für eine beliebige Anzahl von beliebigen Zeichen steht und ? für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer *1234? aus der Schwarzen Liste. Anti-Spam blockiert Anrufe und SMS von einer Nummer, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.

N**NICHT-ZIFFERN-NUMMERN**

Eine Nicht-Ziffern-Nummer (auch Buchstabenwahl-, Wortwahlrufnummer oder Vanity-Rufnummer) ist eine Telefonnummer, die teilweise oder vollständig aus Buchstaben besteht.

O**OBJEKT BLOCKIEREN**

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

OBJEKT LÖSCHEN

Verarbeitungsmethode für ein Objekt, bei der das Objekt physikalisch von dem Ort gelöscht wird, an dem es vom Programm gefunden wurde (Festplatte, Ordner, Netzwerkressource). Diese Verarbeitungsmethode wird für gefährliche Objekte empfohlen, deren Desinfektion nicht möglich ist.

P**PROGRAMM AKTIVIEREN**

Freischaltung aller Programmfunktionen. Zur Aktivierung des Programms ist eine installiert Lizenz erforderlich.

Q**QUARANTÄNE**

Die Quarantäne ist ein besonderer Ordner, in den alle möglicherweise infizierten Objekte verschoben werden, die während der Untersuchung des Geräts oder im Laufe des Echtzeitschutzes erkannt werden.

QUARANTÄNE (OBJEKTE IN DIE QUARANTÄNE VERSCHIEBEN)

Verarbeitungsmethode für ein möglicherweise infiziertes Objekt. Dabei wird der Zugriff auf das Objekt gesperrt und das Objekt wird vom ursprünglichen Ort in den Quarantäneordner verschoben. Dort wird es in verschlüsselter Form gespeichert, um eine Infektion auszuschließen.

R

REMOTE-MANAGEMENT-SYSTEM

System, mit dem Geräte ferngesteuert und in Echtzeit verwaltet werden können.

S

SCAN AUF BEFEHL

Funktionsmodus von Kaspersky-Lab-Programmen, der vom Benutzer initiiert wird und der Untersuchung bestimmter Dateien dient.

SCHWARZE LISTE

Die Einträge dieser Liste enthalten folgende Informationen:

- *Telefonnummer*, von der Anti-Spam Anrufe und / oder SMS blockieren soll.
- *Typ der Ereignisse*, die Anti-Spam von dieser Nummer blockieren soll. Folgende Ereignistypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- *Schlüsselphrase*, nach der Anti-Spam eine SMS als unerwünscht (Spam) einstufen soll. Anti-Spam blockiert nur die SMS, die diese Schlüsselphrase enthalten. Die übrigen SMS werden von Anti-Spam zugestellt.

SYNCHRONISIERUNG

Vorgang, bei dem eine Verbindung zwischen dem mobilen Gerät und dem Remote-Management-System hergestellt wird, um Daten zu übertragen. Bei der Synchronisierung werden die vom Administrator festgelegten Programmeinstellungen auf das Gerät übertragen. Vom Gerät werden Berichte über die Arbeit der Programmkomponenten an das Remote-Management-System übertragen.

W

WEIßE LISTE

Die Einträge dieser Liste enthalten folgende Informationen:

- *Telefonnummer*, von der Anti-Spam Anrufe und / oder SMS zustellen soll.
- *Typ der Ereignisse*, die Anti-Spam von dieser Nummer zustellen soll. Folgende Ereignistypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- *Schlüsselphrase*, nach der Anti-Spam eine SMS als erwünscht (kein Spam) einstufen soll. Anti-Spam stellt nur SMS zu, die diese Schlüsselphrase enthalten. Die übrigen SMS werden von Anti-Spam blockiert.

WIEDERHERSTELLUNG

Ein Originalobjekt wird aus der Quarantäne oder aus dem Backup entweder an den ursprünglichen Ort, an dem das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einen benutzerdefinierten Ordner verschoben.

KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Das Unternehmen ist heute der bekannteste Hersteller für Datenschutz-Software in Russland und bietet eine breite Palette von Programmen zum Schutz vor Viren, Spam und Hackerangriffen an.

Kaspersky Lab ist ein international tätiger Konzern. Die Zentrale befindet sich in Russland, es gibt Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, den Benelux-Ländern, China, Polen, Rumänien und den USA (Kalifornien). In Frankreich wurde eine neue Tochtergesellschaft gegründet, das Europäische Zentrum für Antiviren-Forschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das sind heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome und sechzehn einen Dokortitel besitzen. Die führenden Viren-Analytiker von Kaspersky Lab gehören zu der anerkannten Computer Anti-Virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens sind einzigartiges Wissen und Erfahrung, die von den Mitarbeitern im Laufe des über vierzehnjährigen permanenten Kampfes gegen Viren gesammelt wurden. Dank der ständigen Analyse von Virenaktivitäten können wir Tendenzen in der Malware-Entwicklung vorhersagen und unseren Anwendern frühzeitig einen zuverlässigen Schutz vor neuen Angriffen bieten. Dieser Vorsprung bildet die Basis der Produkte und Services von Kaspersky Lab. Wir sind unseren Konkurrenten stets einen Schritt voraus und bieten unseren Kunden den Schutz von höchster Qualität.

Nach vielen Jahren innovativer Entwicklungen zählt Kaspersky Lab heute zu den führenden Herstellern von Sicherheits-Software. Kaspersky Lab ist ein wichtiger Wegbereiter für neue Standards von Antiviren-Programmen. Die Basis-Software des Unternehmens heißt Kaspersky Anti-Virus und sie sorgt für einen zuverlässigen Schutz aller Objekte vor Virenangriffen: Arbeitsstationen, Dateiserver, Mail-Systeme, Firewalls und Internet-Gateways sowie Taschencomputer. Intuitiv bedienbare Verwaltungstools ermöglichen es, den Antivirenschutz von Computern und Firmennetzwerken maximal zu automatisieren. Viele internationale Developer verwenden in ihrer Software den Kernel von Kaspersky Anti-Virus. Zu ihnen zählen Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien) und BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die eine störungsfreie Funktion der Produkte und präzise Kompatibilität mit spezifischen Business-Vorgaben garantieren. Wir planen, realisieren und begleiten komplexe Antiviren-Lösungen für Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Für unsere Benutzer haben wir einen technischen Kundendienst in mehreren Sprachen eingerichtet.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir beraten Sie gerne am Telefon oder per E-Mail. Alle Ihre Fragen werden ausführlich beantwortet.

Webseite von Kaspersky Lab: <http://www.kaspersky.de>

Viren-Enzyklopädie: <http://www.securelist.com/de/>

Antiviren-Labor: newvirus@kaspersky.com
(nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden)
<http://support.kaspersky.de/helpdesk.html>
(für Fragen an die Virenanalytiker)

INFORMATIONEN ZUM PROGRAMMCODE VON DRITHTHERSTELLERN

Bei der Entwicklung des Programms wurde der Code von Drittherstellern verwendet.

Für das Erstellen und die Überprüfung elektronischer digitaler Signaturen wird die Programmbibliothek für den Informationsschutz (PBSI) "Crypto-C" verwendet, die von CryptoEx OOO entwickelt wurde.

Webseite von CryptoEx OOO: <http://www.cryptoex.ru>.

SACHREGISTER

A

Aktionen	
Scan auf Befehl	40
Aktionen für Objekte	33, 40
Aktivieren	
Anti-Spam	46
Firewall	79
Privatsphäre	70
Verschlüsselung	82

Ä

Ändern	
Liste der vertraulichen Kontakte für die Privatsphäre	76
Schwarze Liste für Anti-Spam	48
Weiße Liste für Anti-Spam	51

A

Anti-Spam	45
Modi	46
Aktion für Anruf	55
Aktion für SMS	54
Nicht-Ziffern-Nummern	54
Nummern, die nicht zu den Kontakten zählen	53
Schwarze Liste	47
Weiße Liste	50
Archive	
Scan auf Befehl	38, 39

B

Bildschirm	
Fenster für den Schutzstatus	28

C

Code	
Geheimcode für das Programm	25

D

Daten	
Entschlüsselung	85
ferngesteuertes Löschen	60
Verschlüsselung	82
Zugriff mit Geheimcode	86
DATEN	
VERTRAULICHE INFORMATIONEN	69
Datenbanken	
automatisches Update	90
manuelles Update	89
Deaktivieren	
Anti-Spam	46
Privatsphäre	69, 70
Verschlüsselung	85
Diebstahlschutz	57
GPS-Find	64
SIM-Watch	63

SMS-Block.....	58
SMS-Clean	60, 62
E	
Eintrag	
Schwarze Liste für Anti-Spam	47
Weiße Liste für Anti-Spam.....	50
Ereignisbericht	93
Ereignisberichte	
Einträge anzeigen.....	93
Einträge löschen	94
Erlauben	
eingehende Anrufe	50
eingehende SMS	50
Netzwerkverbindungen	79
F	
FILTERUNG	
EINGEHENDE ANRUFE	45
EINGEHENDE SMS	45
Firewall	
Meldung über Verbindung	80
G	
Geheimcode für das Programm	25, 95
Gerät orten	64
H	
Hardwarevoraussetzungen	10
Hinzufügen	
Liste der vertraulichen Nummern für die Privatsphäre.....	75
Schwarze Liste für Anti-Spam	47
Weiße Liste für Anti-Spam.....	50
K	
KASPERSKY LAB.....	101
L	
Lizenz.....	20
Ablaufdatum	20
Informationen.....	21
Installation	21
Löschen	
Berichtseinträge.....	94
Informationen, die auf dem Gerät gespeichert sind	60
Quarantäneobjekt	43
Schwarze Liste für Anti-Spam	49
Weiße Liste für Anti-Spam.....	52
LÖSCHEN	
PROGRAMM	16
Löschen Liste der vertraulichen Kontakte für die Privatsphäre	76
M	
Modi	
Anti-Spam	46
Privatsphäre	69, 70

O

Objekt wiederherstellen.....	43
------------------------------	----

P

Privatsphäre	
Auswahl der zu verbergenden Informationen und Ereignisse.....	77
automatischer Start	71
ferngesteuerter Start.....	72
Liste der vertraulichen Kontakte	74
Modi.....	69, 70
PRIVATSPHÄRE	69
Programm aktivieren	
Lizenz	20
PROGRAMM INSTALLIEREN	11
Programm-Menü	29
PROGRAMMOBERFLÄCHE	28

Q

Quarantäne	
Objekt löschen.....	43
Objekt wiederherstellen	43
Objekte anzeigen.....	42
QUARANTÄNE	42

S

Scan auf Befehl	
Aktionen für Objekte	40
Archive.....	39
Manuell starten	36
Start nach Zeitplan	37
Untersuchungsobjekte.....	38
Schutzstatus.....	28
Schwarze Liste	
Anti-Spam.....	47
Sicherheitsstufe	
Firewall	79
Sicherheitsstufe der Firewall wählen	79
SMS-Befehl senden	67
SMS-Block	
Eingehende Anrufe.....	47, 50
eingehende SMS	47
Gerät	58
Informationen verschlüsseln	86
Start	
Programm.....	25
Scan auf Befehl	36
Update.....	89

T

Ton.....	96
----------	----

U

Update	
Manuell starten	89
Roaming	91
Start nach Zeitplan	90

V

Verbieten
 Netzwerkverbindungen79

Verschlüsselung
 Daten entschlüsseln85
 Daten verschlüsseln82
 Zugriff automatisch blockieren86

W

Weiße Liste
 Anti-Spam50

Z

Zeitplan
 Scan auf Befehl37
 Update90

Zugriff auf verschlüsselte Daten verbieten86