

KASPERSKY LAB

Kaspersky Mobile Security 7.0
Enterprise Edition

BENUTZERHANDBUCH

KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE
EDITION

Benutzerhandbuch

© Kaspersky Lab

www.kaspersky.de

Inhalt

KAPITEL 1. KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION	5
1.1. Hardware- und Softwarevoraussetzungen.....	6
1.2. Installation von Kaspersky Mobile Security	6
1.2.1. Installation per Computer	6
1.2.2. Installation per SMS.....	7
1.3. Programmaktivierung	8
KAPITEL 2. KASPERSKY MOBILE SECURITY FOR SYMBIAN OS	9
2.1. Programmfunktionen.....	9
2.1.1. Start des Programms	9
2.1.2. Grafische Oberfläche.....	10
2.1.3. Allgemeine Parameter.....	11
2.1.4. Antiviren-Untersuchung und Schutz	12
2.1.5. Isolieren in Quarantäne	18
2.1.6. Anti-Spam	20
2.1.7. Anti-Theft.....	25
2.1.8. Update der Programm-Datenbanken	28
2.1.9. Update der Parameter für die Programmfunktionen	32
2.1.10. Firewall-Modul	33
2.1.11. Berichte im Programmablauf	34
2.2. Deinstallation der Anwendung	34
KAPITEL 3. KASPERSKY MOBILE SECURITY FOR MICROSOFT WINDOWS MOBILE	37
3.1. Überblick	37
3.1.1. Start des Programms	37
3.1.2. Grafische Oberfläche.....	38
3.2. Antiviren-Untersuchung und Echtzeitschutz.....	40
3.2.1. Scan auf Befehl	40
3.2.2. Echtzeitschutz.....	43
3.2.3. Untersuchung nach Zeitplan	43
3.3. Isolieren in Quarantäne	44

3.4. Anti-Spam- und Anti-Theft-Modul	46
3.4.1. Anti-Spam	46
3.4.2. Anti-Theft.....	50
3.5. Update der Programm-Datenbanken	54
3.6. Update der Parameter für die Programmfunktionen	56
3.7. Firewall.....	56
3.8. Berichte.....	58
3.9. Deinstallation der Anwendung	59
ANHANG A. KASPERSKY LAB.....	63
ANHANG B. CRYPTOEX LTD.....	65
ANHANG C. KASPERSKY LAB ENDNUTZERVERTRAG.....	66

KAPITEL 1. KASPERSKY

MOBILE SECURITY 7.0

ENTERPRISE EDITION

Kaspersky Mobile Security 7.0 Enterprise Edition dient zum Schutz von Smartphones und PDAs mit den Betriebssystemen Symbian OS und Microsoft Windows Mobile vor schädlichen Programmen und unerwünschten Nachrichten und übernimmt die folgenden Funktionen:

- **Echtzeitschutz** für das Dateisystem des Gerätes – Abfangen und Untersuchen aller:
 - eingehenden Objekte, die über drahtlose Verbindungen empfangen werden (Infrarot-Port, Bluetooth), EMS-Nachrichten, Daten bei der Synchronisierung mit dem Personalcomputer und beim Aufrufen von Dateien über den Browser
 - Dateien, die sich auf dem mobilen Gerät öffnen lassen
 - Programme, die sich auf dem Gerät installieren lassen
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden, auf Befehl des Benutzers und nach einem Zeitplan
- **Zuverlässiges Isolieren von infizierten Objekten** in eine Quarantäne
- **Update der Datenbanken von Kaspersky Mobile Security**, die zur Suche nach schädlichen Programmen und zum Löschen von gefährlichen Objekten eingesetzt werden
- **Sperren von unerwünschten SMS-Nachrichten**
- **Sperren des Zugriffs oder Löschen von Benutzerdaten** bei nicht autorisierten Aktionen am Gerät, zum Beispiel Diebstahl
- **Schutz des Smartphones auf Netzwerkebene**

Dem Benutzer wird die Möglichkeit eingeräumt, die Einstellungen von Kaspersky Mobile Security flexibel zu verwalten, den aktuellen Status des Antivirenschutzes anzuzeigen und ein Ereignisjournal zu führen, in dem die Aktionen des Programms stehen.

Im Programm wird ein Menüsystem umgesetzt und eine einfach zu bedienende Benutzeroberfläche bereitgestellt.

Hinweis

Sollte Kaspersky Mobile Security ein schädliches Programm erkennen, kann das infizierte Objekt desinfiziert (wenn eine Desinfektion möglich ist), gelöscht oder in die Quarantäne verschoben werden. Eine Kopie wird vom zu löschenden Objekt nicht angelegt.

1.1. Hardware- und Softwarevoraussetzungen

Kaspersky Mobile Security wird auf mobilen Geräten installiert, die mit den folgenden Betriebssystemen arbeiten:

- Symbian OS 9.1, 9.2 Series 60 UI
- Microsoft Windows Mobile 5.0
- Microsoft Windows Mobile 6,0

1.2. Installation von Kaspersky Mobile Security

Achtung!

Die installierte Version von Kaspersky Mobile Security sieht keine Möglichkeit zum Sicherungskopieren und zur späteren Wiederherstellung vor.

Das Programm wird zentral über das Kaspersky Administration Kit installiert. Der Administrator des Netzwerkes kann unter den beiden Installationsmethoden für das Programm wählen:

- Installation per Computer des Benutzers
- Installation per SMS

Nähere Informationen zur Remote-Installation einer Anwendung finden Sie im Administratorhandbuch von Kaspersky Mobile Security 7.0 Enterprise Edition.

1.2.1. Installation per Computer

Wenn ein mobiles Gerät an den Computer angeschlossen wird, der zu einem logischen Netzwerk des Administrationssservers gehört, öffnet sich das Fenster

des Utilities *kmlisten.exe* (s. Abb. 1). Dieses Utility installiert Kaspersky Mobile Security 7.0 Enterprise Edition auf dem mobilen Gerät.

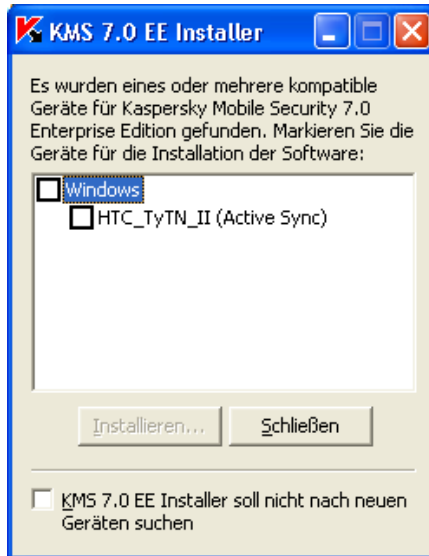


Abbildung 1. Utility **kmlisten**

Um Kaspersky Mobile Security zu installieren, machen Sie Folgendes:

Im Fenster des Utilities *kmlisten.exe* setzen Sie das Häkchen neben dem Namen des Gerätes, auf das das Programm installiert werden soll, und klicken Sie auf die Schaltfläche **Installieren**. Die Installationsdateien werden auf das mobile Gerät kopiert und gestartet.

1.2.2. Installation per SMS

Zur Installation des Programms kann der Netzwerkadministrator den Installer-Service mit einer SMS nutzen (Nähere Informationen finden Sie im Administratorhandbuch für Kaspersky Mobile Security 7.0 Enterprise Edition). Hier wird eine SMS an das mobile Gerät geschickt, in der die URL eines Servers steht, auf dem sich das Installationspaket für das Programm befindet.

Um das Programm mit einer SMS zu installieren, machen Sie Folgendes:

1. Öffnen Sie die SMS, die die URL des Servers enthält, von dem das Installationspaket für Kaspersky Mobile Security geladen werden soll.

2. Klicken Sie auf den Link im Text der Nachricht, um das Installationspaket für das Programm auf das Gerät zu laden.
3. Speichern Sie das Installationspaket der Anwendung.

Daraufhin wird automatisch der Installationsvorgang für das Programm gestartet.

1.3. Programmaktivierung

Achtung!

Das Programm muss aktiviert werden. Ohne Aktivierung können die Programmfunktionen nicht genutzt werden.

Die Aktivierung von Kaspersky Mobile Security 7.0 Enterprise Edition erfolgt bei der Synchronisierung mit dem Administrationsserver. Bei der Synchronisierung wird auf das Gerät die Schlüsseldatei kopiert, die beim Erstellen der Richtlinie für mobile Geräte eingegeben wurde (Näheres über Richtlinien von Kaspersky Administration Kit für mobile Geräte finden Sie im Administratorhandbuch für Kaspersky Mobile Security 7.0 Enterprise Edition).

Der Synchronisierungsvorgang mit dem Administrationsserver wird automatisch in einem Intervall gestartet, das in der Richtlinie für mobile Geräte vorgegeben wurde. Außerdem können Sie die Synchronisierung von Hand starten (s. Pkt. 2.1.9 auf S. 32 oder Pkt. 3.6 auf S. 56).

Achtung!

Ein Ändern der Schlüsseldatei für mobile Geräte sollte während des Erstellens einer Richtlinie unterbunden werden. Sonst wird bei der Synchronisierung mit dem Administrationsserver das Gerät nicht aktiviert.

KAPITEL 2. KASPERSKY

MOBILE SECURITY FOR

SYMBIAN OS

In diesem Kapitel wird die Funktionsweise von Kaspersky Mobile Security 7.0 für Geräte beschrieben, die mit dem Betriebssystem Symbian 9.1, 9.2 oder Series 60 UI laufen.

2.1. Programmfunktionen

In diesem Abschnitt erfahren Sie Näheres zum Einstellen der Parameter für den Scan auf Befehl und den Echtzeitschutz, für das Filtern von SMS-Nachrichten, für den Antiviren-Schutz des Gerätes, für das Updaten der Datenbanken und Programmparameter, für den Schutz des Gerätes auf Netzwerkebene u.ä.

2.1.1. Start des Programms

Um Kaspersky Mobile Security zu starten, machen Sie Folgendes:

1. Öffnen Sie das Hauptmenü des Gerätes.
2. Gehen Sie auf das Symbol **KMS 7.0 EE** und starten Sie das Programm, indem Sie den Punkt **Registerkarte öffnen** im Menü **Optionen** auswählen.

Nach dem Einschalten des Gerätes erscheint auf dem Display das Fenster für den Status der Basiskomponenten von Kaspersky Mobile Security (s. Abb. 2).

- **Echtzeitschutz** – Status des Echtzeitschutzes (s. Pkt. 2.1.4 auf S. 12)
- **Letzte Untersuchung** – Datum für die letzte Antiviren-Untersuchung des Gerätes
- **Datenbanken vom** – Datum für die Erstellung der vom Programm verwendeten Antiviren-Datenbanken
- **Anti-Spam** – Funktionsmodus für Anti-Spam (s. Pkt. 2.1.6 auf S. 20)
- **Firewall** – Schutzstufe des Gerätes auf Netzwerkebene (s. Pkt. 2.1.9 auf S. 32)



Abbildung 2. Fenster **Status der Programmkomponenten**

Um zur Programmoberfläche zu wechseln, klicken Sie auf **OK**.

2.1.2. Grafische Oberfläche

Die grafische Oberfläche des Programms besteht aus sechs Registerkarten:

- Auf der Registerkarte **Untersuchung** können die Antiviren-Untersuchung des Gerätes eingestellt, die Parameter für die Antiviren-Untersuchung, der Echtzeitschutz und die Quarantäne bearbeitet und ein Zeitplan für den Start einer automatischen Untersuchung konfiguriert werden.
- Auf der Registerkarte **Update** können das Update der Antiviren-Datenbanken eingestellt, die Parameter für das Update bearbeitet und ein Zeitplan für das Update konfiguriert werden.
- Die Registerkarte **Firewall** kontrolliert die Netzwerkaktivität und den Schutz des Gerätes auf Netzwerkebene.
- Auf der Registerkarte **Anti-Theft** können das Gerät gesperrt und bei Diebstahl oder Verlust des Gerätes Daten gelöscht werden (Anti-Theft-Modul).
- Auf der Registerkarte **Anti-Spam** können Sie das Filtern von eingehenden SMS-Nachrichten einstellen (Anti-Spam-Modul).
- Auf der Registerkarte **Informationen** können das Ereignisjournal für die Programmkomponenten, allgemeine Informationen zum Programm und

der verwendeten Datenbanken angezeigt sowie die allgemeinen Parameter für die Programmfunktionen bearbeitet werden.

Zum Navigieren zwischen den Registerkarten verwenden Sie die Pfeiltasten Ihres Gerätes, oder gehen Sie im Menü **Optionen** auf den Punkt **Registerkarte öffnen** (s. Abb. 3).



Abbildung 3. Menü **Optionen**

Um zum Fenster **Status der Programmkomponenten** zurückzukehren, gehen Sie auf den Punkt **Aktueller Status** im Menü **Optionen**.

2.1.3. Allgemeine Parameter

Die auf der Registerkarte **Informationen** im Punkt **Einstellungen** (s. Abb. 4) befindlichen Parameter sorgen für die folgenden Programmfunktionen:

- **Statusfenster zeigen** legt fest, ob der aktuelle Status beim Programmstart angezeigt werden soll.
- **Protokollgröße** bestimmt die höchstens zulässige Größe des Protokolls. Wird der untere eingegebene Wert erreicht, werden alte Protokollmeldungen bis zum eingegebenen oberen Wert gelöscht.
- **Hintergrundbeleuchtung** bestimmt, ob die Hintergrundbeleuchtung bei der Virenuntersuchung eingeschaltet bleiben soll. Als Standard ist die Hintergrundbeleuchtung deaktiviert.
- **Sound** bestimmt die Sound-Benachrichtigung bei Eintreten von bestimmten Ereignissen (Erkennen eines infizierten Objektes, Meldungen zum Programmstatus usw.). Standardmäßig hängt das

Sound-Signal beim Erkennen eines Virus vom Geräteprofil ab (Wert **Nach Profil**). Wählen Sie **Aktiv** aus, wenn Sie den Sound unabhängig vom aktivierten Geräteprofil hören wollen.

- **Lautstärke** reguliert die Lautstärke der Soundwiedergabe beim Erkennen eines infizierten Objektes.
- **Vibration** bestimmt, ob das Gerät beim Erkennen eines infizierten Objektes vibrieren soll. In der Grundeinstellung ist die Vibration aktiviert.



Abbildung 4. Menü **Einstellungen**

Zum Bearbeiten der Werte verwenden Sie die Pfeiltasten Ihres Gerätes, oder gehen Sie im Menü **Optionen** auf den Punkt **Ändern**.

2.1.4. Antiviren-Untersuchung und Schutz

Auf der Registerkarte **Untersuchung** können Sie die Antiviren-Untersuchung des gesamten Dateisystems und Gerätespeichers oder einzelner Verzeichnisse bzw. Dateien einstellen. Außerdem können Sie die Parameter für die Antiviren-Untersuchung und den Echtzeitschutz ändern, den Bericht über die Untersuchungsergebnisse anzeigen und einen Zeitplan für den automatischen Start einer Untersuchung einrichten.

2.1.4.1. Echtzeitschutz und Scan auf Befehl

Der Echtzeitschutz ist ein Modus, bei dem ein Teil von Kaspersky Mobile Security dauerhaft im Arbeitsspeicher des Gerätes liegt und alle Daten wie den Posteingang (von außen zum Gerät gelangende Nachrichten) kontrolliert.

Der Echtzeitschutz ist mit dem Einschalten des Gerätes in Betrieb und funktioniert bis zum Ausschalten (wenn dieser Modus nicht in den Schutzeinstellungen deaktiviert wurde).

Außerdem kann Kaspersky Mobile Security das Dateisystem des Gerätes komplett untersuchen und dabei Objekte analysieren, die sich auf eingesteckten Speichererweiterungskarten befinden.

Die Ergebnisse des Echtzeitschutzes und des Scans auf Befehl werden in einen Bericht eingetragen. Zum Anzeigen des Berichtes müssen Sie auf der Registerkarte **Untersuchung** den Eintrag **Protokoll** wählen.

Um den Echtzeitschutz zu starten, machen Sie Folgendes:

1. Auf der Registerkarte **Untersuchung** gehen Sie auf **Einstellungen**.
2. Gehen Sie im Abschnitt **Einstellungen** auf den Punkt **Echtzeitschutz**.
3. Aktivieren / Deaktivieren Sie den Echtzeitschutz, indem Sie den entsprechenden Wert bei **Echtzeitschutz** setzen.

Um die Parameter für den Echtzeitschutz zu ändern, machen Sie Folgendes:

1. Auf der Registerkarte **Untersuchung** gehen Sie auf **Einstellungen**.
2. Gehen Sie im Abschnitt **Einstellungen** auf den Punkt **Echtzeitschutz**.
3. Geben Sie im Block **Dateityp** den Untersuchungsbereich ein, indem Sie die Dateitypen markieren, die untersucht werden sollen:
 - **Alle Dateien** – Es werden alle Dateien untersucht.
 - **Ausführbare** – Untersucht werden nur ausführbare Programmdateien (zum Beispiel *.exe, *.sis, *.mdl, *.app).
4. Wählen Sie die Aktion beim Erkennen eines infizierten Objektes (Parameter **Aktion**).

Standardmäßig werden gefundene schädliche Objekte in die Quarantäne verschoben (Wert **Quarantäne**).

Um Daten von einem gefundenen infizierten Objekt in den Programmbericht einzutragen, markieren Sie den Wert **Im Bericht erfassen**.

Damit das Programm gefundene schädliche Objekte ohne Benachrichtigung des Benutzers löscht, setzen Sie den Wert auf **Löschen**.

5. Aktivieren / Deaktivieren Sie den Modus **Untersuchung einer neuen Karte** (Parameter **Neue Karte untersuchen**).

Standardmäßig benachrichtigt beim Einlegen einer Speicherkarte das Programm, dass die Karte untersucht werden muss.

Um die Untersuchung von Flash-Karten zu aktivieren, die in das Gerät eingelegt werden, setzen Sie den Wert auf **Untersuchung**. Um die automatische Untersuchung von Flash-Karten zu deaktivieren, gehen Sie auf **Inaktiv**.

6. Aktivieren / Deaktivieren Sie die Darstellung des Schutzsymbols (Parameter **Schutz-Symbol**).

Damit bei aktiviertem Echtzeitschutz das Programmsymbol auf dem Display des Gerätes angezeigt wird, setzen Sie den Wert im entsprechenden Menüpunkt auf **Immer**. Damit das Symbol nur im Menü des Gerätes angezeigt wird, setzen Sie den Wert auf **Nur im Menü**. Damit das Symbol nicht angezeigt wird, setzen Sie den Wert auf **Nie**.

Um die Parameter für den Scan auf Befehl zu ändern, machen Sie Folgendes:

1. Auf der Registerkarte **Untersuchung** gehen Sie auf **Einstellungen**.
2. Gehen Sie im Abschnitt **Einstellungen** auf den Punkt **Untersuchung**.
3. Geben Sie im Block **Dateityp** den Untersuchungsbereich ein, indem Sie die Dateitypen markieren, die untersucht werden sollen:
 - **Alle Dateien** – Es werden alle Dateien untersucht.
 - **Ausführbare** – Untersucht werden nur ausführbare Programmdateien (zum Beispiel *.exe, *.sis, *.mdl, *.app).
4. Wählen Sie die Aktion beim Erkennen eines infizierten Objektes (Parameter **Aktion**).

Standardmäßig versucht das Programm, gefundene schädliche Objekte zu reparieren (Wert **Reparaturversuch**).

Damit gefundene schädliche Objekte in die Quarantäne verschoben werden, setzen Sie den Wert auf **Quarantäne**.

Um Daten von einem gefundenen infizierten Objekt in den Programmbericht einzutragen, markieren Sie **Im Bericht erfassen**.

Damit das Programm gefundene schädliche Objekte ohne Benachrichtigung des Benutzers löscht, setzen Sie den Wert auf **Löschen**.

Damit beim Erkennen eines infizierten Objektes eine eine Aktion erfragt wird, setzen Sie den Wert auf **Anfrage**.

5. Definieren Sie die Aktion bei unmöglicher Reparatur des infizierten Objektes (Parameter **Desinfektion nicht mögl.**).

Standardmäßig werden gefundene schädliche Objekte in die Quarantäne verschoben (Wert **Quarantäne**).

Um Daten von einem gefundenen infizierten Objekt in den Programmbericht einzutragen, markieren Sie **Im Bericht erfassen**.

Damit das Programm gefundene schädliche Objekte ohne Benachrichtigung des Benutzers löscht, setzen Sie den Wert auf **Löschen**.

Damit beim Erkennen eines infizierten Objektes eine Benachrichtigung eine Aktion erfragt, setzen Sie den Wert auf **Anfrage**.

6. Aktivieren / Deaktivieren Sie die Untersuchung des ROM-Speichers für das Gerät (Parameter **ROM-Untersuchung**).

Unter bestimmten Umständen kann der ROM-Speicher für schädliche Programme anfällig sein. Damit der ROM-Speicher untersucht wird, setzen Sie den Wert auf **Ja**.

7. Aktivieren / Deaktivieren Sie das Entpacken von SIS- und ZIP-Archiven (Parameter **Entpacken von Archiven**).

Damit das Programm bei einer Untersuchung SIS- und ZIP-Archive entpackt, setzen Sie den Wert auf **Ja**. Wenn ein Entpacken von Archiven nicht gebraucht wird, gehen sie auf **Nein**.

Hinweis.

Zum Bearbeiten des Wertes verwenden Sie die Pfeiltasten Ihres Gerätes, oder gehen Sie im Menü **Optionen** auf den Punkt **Ändern**.

Das Programm arbeitet als Standard mit Werten, die von den Kaspersky-Lab-Experten empfohlen werden. Wenn Sie im Laufe der Arbeit mit dem Programm zu den empfohlenen Werten zurückkehren wollen, öffnen Sie die Registerkarte **Untersuchung** und gehen im Menü **Optionen** auf den Punkt **Wiederherstellen**.

Um die Virenuntersuchung zu starten, machen Sie Folgendes:

1. Starten Sie Kaspersky Mobile Security (s. Pkt. 2.1.1 auf S. 9).
2. Auf der Registerkarte **Untersuchung** (s. Abb. 5) wählen Sie den Punkt **Alles untersuch.**, wenn Sie das gesamte Dateisystem des Gerätes untersuchen wollen, oder **Ordner scannen**, wenn Sie einen einzelnen Ordner untersuchen wollen.



Abbildung 5. Registerkarte **Untersuchung**

Sollten Sie sich für den Punkt **Ordner scannen** entschieden haben, öffnet sich ein Fenster, das das Dateisystem des Gerätes darstellt. Zur Navigation im Dateisystem verwenden Sie die Pfeiltasten. Um die Untersuchung eines Ordners zu starten, selektieren Sie einen Ordner und gehen auf den Punkt **Untersuchen** im Menü **Optionen**.

Nachdem die Untersuchung begonnen hat, öffnet sich das Untersuchungsfenster, in dem der aktuelle Status angezeigt wird: Anzahl der untersuchten Objekte, Pfad zu dem Objekt, das gerade untersucht wird, und Fortschrittsanzeige in Prozent (s. Abb. 6).



Abbildung 6. Fenster des Untersuchungsprozesses

Wenn ein infiziertes Objekt erkannt wird, wird die Aktion ausgeführt, die in den entsprechenden Parameter im Abschnitt **Einstellungen**→**Untersuchung** eingegeben wurden.



Abbildung 7. Meldung eines erkannten Virus

Nach der Untersuchung erscheint eine allgemeine Statistik über gefundene und gelöschte schädliche Objekte.

Um die Hintergrundbeleuchtung bei der Untersuchung nicht auszuschalten, machen Sie Folgendes:

Wechseln Sie zur Registerkarte **Informationen**, öffnen Sie das Menü **Einstellungen** und setzen Sie den Wert **Ja** für den Parameter **Hintergrundbeleuchtung**.

Standardmäßig wird die Hintergrundbeleuchtung automatisch ausgeschaltet, um Batterieladung zu sparen.

2.1.4.2. Untersuchung nach Zeitplan

Mit Kaspersky Mobile Security kann der Benutzer einen Zeitplan für das automatische Untersuchen des Gerätes erstellen. Die Untersuchung erfolgt im Hintergrund. Wenn ein infiziertes Objekt erkannt wird, wird die Aktion ausgeführt, die in den Untersuchungsparametern vorgegeben wurde (s. Pkt. 2.1.4.1 auf S. 12).

Die Untersuchung nach Zeitplan ist standardmäßig deaktiviert.



Abbildung 8. Menü **Zeitplan**

Um einen Zeitplan für den Untersuchungsstart zu erstellen, machen Sie Folgendes:

Auf der Registerkarte **Untersuchung** gehen Sie auf den Punkt **Zeitplan** und wählen einen der folgenden **AutoScan**-Parameter (s. Abb. 8):

- **Täglich** – Untersuchung erfolgt jeden Tag. Im Eingabefeld geben Sie die **Untersuchungszeit** ein.
- **Wöchentlich** – Untersuchung erfolgt einmal pro Woche. Geben Sie den **Untersuchungstag** und die **Untersuchungszeit** ein.

2.1.5. Isolieren in Quarantäne

Infizierte Objekte, die in die Quarantäne verschoben wurden, bedrohen nicht mehr die Sicherheit des Gerätes und können später gelöscht oder wiederhergestellt werden.

Als infiziert erkannte Objekte können von einer Anwendung entweder automatisch oder nach Ihrer Bestätigung in die Quarantäne verschoben werden.

Damit das Programm gefundene schädliche Objekte ohne Nachfrage in die Quarantäne verschiebt, machen Sie Folgendes:

1. Öffnen Sie Registerkarte **Untersuchung**.
2. Gehen Sie auf den Punkt **Einstellungen**.
3. Gehen Sie auf den Punkt **Untersuchung** oder **Echtzeitschutz**.
4. Markieren Sie **Quarantäne**.

Wenn Sie als Aktion **Anfrage** angegeben haben, schlägt Ihnen Kaspersky Mobile Security beim Erkennen eines infizierten Objektes vor, das Objekt zu löschen oder es in die Quarantäne zu verschieben.

Um die Liste mit den Quarantäne-Objekten anzusehen, machen Sie Folgendes:

Öffnen Sie die Registerkarte **Untersuchung** und gehen Sie auf den Punkt **Quarantäne** (s. Abb. 9).



Abbildung 9. Infizierte Objekte in der Quarantäne

Im Menü **Optionen**, das im Fenster **Anzeige der Quarantäne** angeboten wird, können Sie Folgendes machen:

- Detaillierte Informationen zu jedem Objekt anzeigen, das in der Quarantäne gespeichert wird (**Hinweise**)
- Markiertes Objekt löschen (**Löschen**)
- Quarantäne leeren, indem der gesamte Inhalt mit den Objekten gelöscht wird (**Alle löschen**)
- Markiertes Objekt aus Quarantäne im ursprünglichen Verzeichnis wiederherstellen (**Wiederherstellen**)
- Hilfe aufrufen (**Hilfe**)

Um die Quarantäne-Parameter einzugeben, machen Sie Folgendes:

1. Öffnen Sie Registerkarte **Untersuchung**.
2. Gehen Sie auf den Punkt **Einstellungen**.
3. Gehen Sie auf den Punkt **Quarantäne** (s. Abb. 10).



Abbildung 10. Quarantäne-Parameter

Der Parameter **Quarantäne-Größe** bestimmt die maximale Anzahl von infizierten Objekten, die in der Quarantäne gespeichert werden können. Sie können als mögliche Werte **20**, **50** oder **100** Dateien eingeben.

Der Parameter **Speichern** bestimmt die Dauer, die die infizierten Objekte in der Quarantäne gespeichert bleiben können. Nach Ablauf der eingegebenen Frist werden die infizierten Objekte automatisch gelöscht.

Hinweis.

Um die Werte der Quarantäne wiederherzustellen, die die Kaspersky-Lab-Experten empfehlen, gehen Sie im Menü **Optionen** auf den Punkt **Wiederherstellen**.

2.1.6. Anti-Spam

Das Anti-Spam-Modul schützt das Gerät vor unerwünschten SMS-Nachrichten.

Das Filter-Prinzip für Nachrichten beruht auf der Verwendung einer „schwarzen“ und einer „weißen“ Liste. Diese Listen enthalten Telefonnummern und Phrasen-Muster, die erwünschte und unerwünschte Nachrichten charakterisieren. Die Analyse der Nachricht erfolgt in dieser Reihenfolge:

- Untersuchung der Sendernummer auf Zugehörigkeit zur "schwarzen" Liste
- Untersuchung der Sendernummer auf Zugehörigkeit zur "weißen" Liste

- Untersuchung des Nachrichtentextes auf Übereinstimmung mit Phrasen aus der "schwarzen" Liste
- Untersuchung des Nachrichtentextes auf Übereinstimmung mit Phrasen aus der "weißen" Liste.

Wird wenigstens eine Übereinstimmung festgestellt, erfolgt keine weitere Untersuchung. Die Nachricht, die einem Element aus der "schwarzen" Liste entspricht, wird gesperrt. Die Nachricht, die einem Element aus der "weißen" Liste entspricht, wird übersprungen.

2.1.6.1. Modus für Anti-Spam

Anti-Spam filtert Nachrichten in den folgenden Modi:

- **Aktiviert.** In diesem Modus filtert Anti-Spam eingehende Nachrichten anhand der „schwarzen“ und „weißen“ Liste. Geht eine Nachricht von einer Telefonnummer ein, die in keiner Liste steht, benachrichtigt Anti-Spam den Benutzer und schlägt das Sperren oder Zulassen des Nachrichtenempfangs vor und empfiehlt außerdem die Übernahme der Telefonnummer in die „weiße“ oder „schwarze“ Liste.
- **Schwarze Liste.** In diesem Modus sperrt Anti-Spam den Empfang von Nachrichten, die auf der "schwarzen" Liste stehen. Die übrigen Nachrichten werden durchgelassen.
- **Weißer Liste.** In diesem Modus lässt Anti-Spam Nachrichten durch, die auf der "weißen" Liste stehen. Die übrigen Nachrichten werden gesperrt.
- **Deaktiviert.** In diesem Modus ist Anti-Spam deaktiviert. Eingehende Nachrichten werden nicht gefiltert.

Um einen Modus für Anti-Spam zu wählen, machen Sie Folgendes:

1. Öffnen Sie die Registerkarte **Anti-Spam**.
2. Gehen Sie auf den Punkt **Einstellungen**.
3. Geben Sie einen Funktionsmodus für Anti-Spam mit dem Parameter **Anti-Spam** ein.

2.1.6.2. „Schwarze“ und „Weiße“ Liste bearbeiten

Die „schwarze Liste“ und die „weiße Liste“ enthalten Einträge mit Telefonnummern, von denen der Empfang von SMS-Nachrichten durch Anti-Spam gesperrt oder freigegeben ist. Die Daten zu gesperrten und gelöschten Nachrichten stehen im Abschnitt **Protokoll**.

Um die Einträge in der "schwarzen" oder "weißen" Liste zu ändern, machen Sie Folgendes:

Öffnen Sie die Registerkarte **Anti-Spam** (s. Abb. 11) und gehen Sie auf den entsprechenden Punkt.

Zur Bearbeitung der Liste gehen Sie auf das Menü **Optionen**:

- **Eintrag hinzufügen** – Es wird ein neuer Eintrag in der Liste erzeugt.
- **Eintrag bearbeiten** – Der aktuelle Eintrag wird bearbeitet.
- **Eintrag löschen** – Der aktuelle Eintrag wird gelöscht.
- **Alle Einträge löschen** – Die Liste wird geleert, indem alle Einträge gelöscht werden.
- **Hilfe** – Aufruf der Hilfefunktion



Abbildung 11. Registerkarte **Anti-Spam**

Entscheiden Sie sich für den Punkt **Eintrag hinzufügen** oder **Eintrag bearbeiten**, werden Ihnen die folgenden Parameter für den Eintrag vorgeschlagen (s. Abb. 12):

- **Nummer.** Geben Sie die Telefonnummer an, für die der Nachrichtenempfang gesperrt oder zugelassen ist. Die Nummer kann mit einer Ziffer oder dem Zeichen „+“ beginnen und darf nur Ziffern enthalten. Außerdem dürfen beim Anlegen der Nummer die Ersatzzeichen "?" und "*" verwendet werden ("?" steht für eine einzelne Ziffer, "*" für eine beliebig lange Ziffernfolge).

- **Text.** Geben Sie einen Text ein, bei dessen Erkennung in der eingegangenen Nachricht die Nachricht gesperrt oder durchgelassen wird.

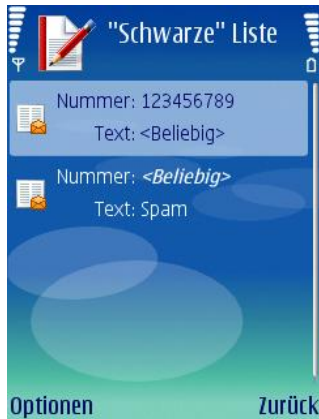


Abbildung 12. „Schwarze“ Liste

2.1.6.3. Parameter für Anti-Spam

Um die Parameter für Anti-Spam einzugeben, machen Sie Folgendes:

Öffnen Sie die Registerkarte **Anti-Spam** und gehen Sie auf den Punkt **Einstellungen** (s. Abb. 13).

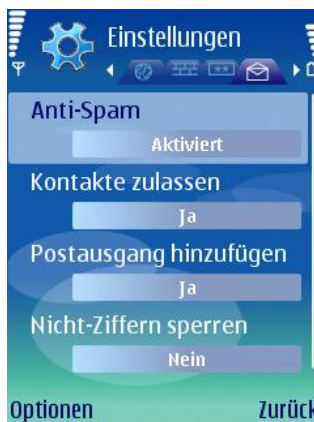


Abbildung 13. Parameter für Anti-Spam

Im Menü **Einstellungen** lassen sich die folgenden Parameter für Anti-Spam bearbeiten:

- **Anti-Spam.** Der Parameter regelt den Modus für Anti-Spam (s. Pkt. 2.1.6.1 auf S. 21).
- **Kontakte zulassen:** Besitzt dieser Parameter den Wert **Ja**, sperrt Anti-Spam den Nachrichteneingang nicht von Nummern, die in Ihrem Telefonbuch gespeichert sind. Ist diese Option deaktiviert (Wert steht auf **Nein**), richtet sich Anti-Spam beim Filtern danach, ob die Telefonnummer in der „schwarzen“ oder „weißen“ Liste steht.
- **Postausgang zulassen.** Wenn der Parameter den Wert **Ja** hat, werden alle Telefonnummern, denen Sie eine SMS-Nachricht senden, automatisch in die „weiße“ Liste gespeichert. Zum Deaktivieren dieser Option wählen Sie **Nein** aus.
- **Nicht-Ziffern sperren.** Wählen Sie **Ja**, sperrt Anti-Spam den Nachrichteneingang von Nummern, die nicht nur Ziffern enthalten. Bei **Nein** sind auch Nicht-Ziffer-Nummern als Absender zugelassen.

Hinweis.

Dieser Parameter beeinflusst nur Einträge, die Anti-Spam in einer der folgenden Situationen erstellt hat:

- Erfassen von ausgehenden Nummern in der „weißen“ Liste (Parameter **Postausgang hinzufügen** aktiviert)
- Erfassen von neuen Telefonnummern in einer Liste, von denen eine Nachricht eingegangen ist (s. Pkt. 2.1.6.4 auf S. 24).

Zum Bearbeiten des Wertes verwenden Sie die Pfeiltasten Ihres Gerätes, oder gehen Sie im Menü **Funktionen** auf den Punkt **Ändern**.

2.1.6.4. Aktionen für Nachrichten

Geht eine SMS-Nachricht von einer Telefonnummer ein, die nicht in der „schwarzen“ oder „weißen“ Liste steht, fängt sie Anti-Spam ab und meldet auf dem Display des Gerätes den Vorgang (s. Abb. 14).

Über das Menü **Optionen** können Sie eine der folgenden Aktionen für eine Nachricht wählen:

- **In „weiße“ Liste** – Empfang der Nachricht wird zugelassen und Telefonnummer des Absenders wird in die „weiße“ Liste gespeichert

- **In „schwarze“ Liste** – Empfang der Nachricht wird gesperrt und Telefonnummer des Absenders wird in die „schwarze“ Liste gespeichert
- **Überspringen** – Empfang der Nachrichten zulassen. Die Telefonnummer des Absenders wird in keine Liste gespeichert.

Die Daten über gesperrte Nachrichten werden in das Anwendungsprotokoll eingetragen. Zum Anzeigen des Berichtes müssen Sie auf der Registerkarte **Informationen** den Eintrag **Protokoll** wählen.



Abbildung 14. Anti-Spam warnt

2.1.7. Anti-Theft

Das Anti-Theft-Modul schützt Daten, die auf dem mobilen Gerät gespeichert sind, vor dem unautorisierten Zugriff, falls das Gerät gestohlen wird oder verloren geht.

Beim erstmaligen Aufrufen der Modul-Parameter muss ein Geheimcode eingegeben werden. Der Code wird später gebraucht, um auf die Parameter des Moduls und die Verwaltung der Funktion zuzugreifen. Die Funktion **SMS-Block** sperrt das Gerät auf Wunsch des Benutzers. Es lässt sich erst nach Eingabe des Geheimcodes entsperren, der für den Zugriff auf das Anti-Theft-Modul verwendet wird. Um das Gerät mit der Funktion SMS-Block zu sperren, schicken Sie auf Ihr Gerät eine SMS mit dem Text: "block:Code". Standardmäßig ist SMS-Block deaktiviert. Um diese Option zu aktivieren, gehen Sie auf **Akt.**

Die Funktion **SMS-Clean** löscht persönliche Benutzerdaten (Kontakte, Nachrichten, Speicherkartendaten, Netzwerkeinstellungen). Um die Funktion SMS-Clean einzuschalten, schicken Sie auf Ihr Gerät eine SMS mit dem Text:

"clean:Code". Standardmäßig ist SMS-Clean deaktiviert. Um diese Option zu aktivieren, gehen Sie auf **Akt.**

SIM Watch kann an eingegebene Nummern die neue Telefonnummer senden und das Gerät sperren, wenn die SIM-Karte im gestohlenen Gerät gewechselt wird. Um diese Option zu aktivieren, gehen Sie auf **Akt.**

Um den Geheimcode für das Anti-Theft-Modul zu ändern, gehen Sie auf den Punkt **Code ändern**. Geben Sie den neuen Code und dessen Bestätigung ein und klicken Sie auf **OK**.

Bei jedem Zugriff auf die Parameter des Anti-Theft-Moduls (s. Abb. 15) muss der vorgegebene Geheimcode eingegeben werden.



Abbildung 15. Registerkarte **Anti-Theft**

Alle Vorgänge werden in das Anwendungsprotokoll eingetragen. Zum Anzeigen des Berichtes gehen Sie auf der Registerkarte **Anti-Theft** auf den Punkt **Protokoll**.

2.1.7.1. Parameter von SMS-Clean

Um Parameter für die Funktion SMS-Clean einzugeben, machen Sie Folgendes:

1. Öffnen Sie die Registerkarte **Anti-Theft** und geben Sie den Geheimcode ein (s. Pkt. 2.1.7 auf S. 25).
2. Gehen Sie auf den Punkt **Einstellungen**.
3. Gehen Sie auf den Punkt **SMS-Clean**.

Der Abschnitt **SMS-Clean** enthält eine Liste von Daten, die für den Fall gelöscht werden, wenn das Gerät verloren geht (s. Abb. 16).

Abbildung 16. Registerkarte **SMS-Clean**

Wenn Sie wollen, dass bei einem Verlust des mobilen Gerätes oder dessen Diebstahl das Telefonbuch gelöscht werden kann, gehen Sie auf den Punkt **Kontakte löschen** und setzen Sie den Wert auf **Ja**.

Hinweis

Die Kontakte werden aus dem Telefonbuch gelöscht, das auf dem Gerät gespeichert ist. Das Telefonbuch auf der SIM-Karte wird nicht gelöscht.

Zum Löschen von Post und SMS-Nachrichten (Ordner Inbox und Mailbox) gehen Sie auf den Punkt **Nachrichten löschen** und setzen Sie den Wert auf **Ja**.

Der Punkt **Dateien löschen** löscht persönliche Daten (Daten aus Ordner `!:\Data`). Standardmäßig ist das Löschen von persönlichen Daten nicht vorgesehen. Wenn Sie wollen, dass bei einem Diebstahl oder Verlust des Gerätes die persönlichen Daten gelöscht werden können, gehen Sie auf diesen Punkt und setzen Sie den Wert auf **Ja**.

Gehen Sie auf den Punkt **Alle Kartendaten löschen**, um die Daten auf der Speicherkarte eines gestohlenen Gerätes zu löschen. Standardmäßig ist diese Option aus. Um das Löschen der Daten auf der Speicherkarte zu ermöglichen, gehen Sie auf den Punkt **Alle Kartendaten löschen** und wählen **Ja** aus.

Um die Option zum Löschen der Netzwerkverbindungen anzuschalten, gehen Sie auf den Punkt **Netzwerkein. lösch.** und geben Sie den Wert **Ja** ein.

Klicken Sie auf **Ja**, um die Änderungen zu übernehmen.

2.1.7.2. Parameter von SIM Watch

Um die Parameter von SIM Watch einzurichten, wechseln Sie auf die Registerkarte **Anti-Theft**. Geben Sie den Geheimcode (s. Pkt. 2.1.7 auf S. 25) ein und gehen Sie im nächsten Fenster auf den Punkt **SIM Watch**.

Der Abschnitt **SIM Watch** überwacht den Wechsel der SIM-Karte auf dem Gerät (s. Abb. 17).



Abbildung 17. Registerkarte **SIM Watch**

In den Feldern **Telefonnummer 1** und **Telefonnummer 2** geben Sie diejenigen Telefonnummern ein, an die Sie die neue Telefonnummer erhalten wollen, falls die SIM-Karte auf Ihrem Gerät gewechselt wird. Die Nummern können mit einer Ziffer oder dem Zeichen „+“ beginnen und dürfen nur Ziffern enthalten.

Zusätzlich können Sie eine Sperre des Gerätes beim Wechsel der SIM-Karte aufrufen. Gehen Sie dazu auf den Punkt **Sperren** und setzen Sie den Wert auf **Ja**. Das Gerät wird mit Eingabe des Geheimcodes entsperrt, der für den Zugriff auf das Anti-Theft-Modul angegeben wurde. Standardmäßig ist das Sperren des Gerätes nicht vorgesehen.

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

2.1.8. Update der Programm-Datenbanken

Nach schädlichen Programmen wird mithilfe von Einträgen in einer Programm-Datenbank gesucht, in der eine Beschreibung aller bekannten und zurzeit als schädlich eingestuft Programme steht. Es ist absolut wichtig, dass die Datenbanken auf dem neuesten Stand sind.

Die Datenbanken können entweder manuell oder nach Zeitplan aktualisiert werden. Das Update erfolgt über das Internet von den Kaspersky-Lab-Servern.

Sie können die automatische Antiviren-Untersuchung des Gerätes nach jedem Update der Antiviren-Datenbanken von Kaspersky Mobile Security aktivieren. Wechseln Sie dazu auf die Registerkarte **Update**, gehen auf den Punkt **Einstellungen** und setzen bei **Scan nach Update** den Wert auf **Akt.**

Der Wert **Quarantäne nach Update** bestimmt, ob die Objekte in der Quarantäne jedes Mal nach dem Update der Programm-Datenbanken untersucht werden sollen oder nicht. Standardmäßig erfolgt diese Untersuchung. Um eine Untersuchung zu unterbinden, wählen Sie **Inaktiv** aus.

Wenn der aktive Access Point geändert werden muss, verwenden Sie den Parameter **Access Point**. Sie müssen dann den gewünschten Parameterwert in der Liste auswählen. Standardmäßig ist der Access Point der Default-Wert des Gerätes.

Der Parameter **Update-Server** bestimmt die Quelle für das Update der Programm-Datenbanken: Update-Server von Kaspersky Lab (Wert **Standard**) oder vom Benutzer angegebener Server (Wert **Eingeben**). Bei Auswahl des Wertes **Eingeben** tragen Sie im nächsten Fenster die URL für Updates ein. Bei Bedarf kann ein alternativer Update-Server eingegeben werden.

Detaillierte Informationen zu den gerade verwendeten Datenbanken finden Sie unter dem Punkt **Datenbank-Info**, der sich auf der Registerkarte **Informationen** befindet.

Der Update-Vorgang der Datenbanken wird in das Protokoll eingetragen. Um das Protokoll anzuzeigen, gehen Sie auf der Registerkarte **Update** auf den Punkt **Protokoll**.

2.1.8.1. Update-Parameter

Um die Parameter für das Update der Programm-Datenbanken einzugeben, machen Sie Folgendes:

1. Starten Sie Kaspersky Mobile Security (s. Pkt. 2.1.1 auf S. 9).
2. Auf der Registerkarte **Update** gehen Sie auf den Punkt **Einstellungen** (s. Abb. 18).

Abbildung 18. Registerkarte **Update**

3. Gehen Sie auf den Access Point (Parameter **Access Point**) (s. Abb. 19).

Hinweis

Der Access Point wird mit Parametern eingerichtet, die der Mobilfunkbetreiber vorschreibt.

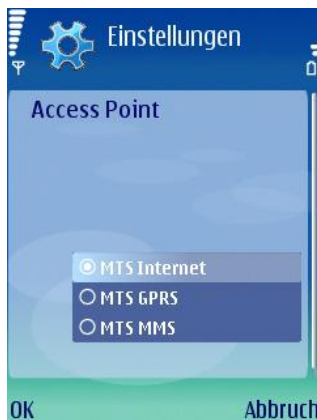


Abbildung 19. Access Point auswählen

4. Geben Sie die Adresse des Update-Servers (wenn nötig) ein. Gehen Sie dazu auf den Punkt **Update-Server** und setzen Sie den Wert auf

Eingeben. Im nächsten Fenster geben Sie die URL für Updates ein (s. Abb. 20).

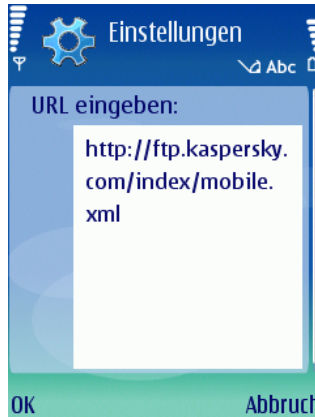


Abbildung 20. Adresse des Update-Servers

Standardmäßig erfolgen Updates vom Kaspersky-Lab-Server: <http://ftp.kaspersky.com/index/mobile.xml>.

Achtung!

Unabhängig davon, ob zuvor eine Internetverbindung geöffnet wurde, wird sie nach dem Update-Vorgang geschlossen.

2.1.8.2. Manuelles Update

Um das Update der Datenbanken von Hand zu starten, machen Sie Folgendes:

1. Starten Sie Kaspersky Mobile Security (s. Pkt. 2.1.1 auf S. 9).
2. Auf der Registerkarte **Update** gehen Sie auf den Punkt **Update** (s. Abb. 18).

2.1.8.3. Update nach Zeitplan

Um einen Zeitplan für den Start des Updates der Programm-Datenbanken zu erstellen, machen Sie Folgendes:

1. Starten Sie Kaspersky Mobile Security (s. Pkt. 2.1.1 auf S. 9).
2. Auf der Registerkarte **Update** gehen Sie auf den Punkt **Zeitplan** und geben die Parameter **AutoUpdate** ein:

- **Inakt.** – kein Update nach Zeitplan durchführen
- **Täglich** – Update erfolgt jeden Tag. Geben Sie die Update-Uhrzeit in das entsprechende Feld ein.
- **Wöchentlich** – Update erfolgt einmal pro Woche. Geben Sie den Update-Tag und die Update-Uhrzeit in die entsprechenden Felder ein.

2.1.9. Update der Parameter für die Programmfunktionen

Hinweis

Nähere Informationen über das Zusammenspiel von Kaspersky Mobile Security Enterprise Edition und Kaspersky Administration Kit finden Sie im Administratorhandbuch von Kaspersky Mobile Security Enterprise Edition.

Wenn Kaspersky Mobile Security Enterprise Edition zusammen mit Kaspersky Administration Kit eingesetzt wird, werden die Parameter für die Programmfunktionen durch die Richtlinie für die Gruppe der mobilen Geräte vorgegeben. Die Aktivierung des Programms und die Übernahme der Richtlinienparameter, die nicht geändert werden dürfen, erfolgen beim Hinzufügen des Gerätes in die Administrationsgruppe.

Im Anschluss wird automatisch die Synchronisierung mit dem Administrationsserver mit einem Intervall gestartet, der in den Parametern der Richtlinie vorgegeben wurde.

Um die Synchronisierung des Programms mit dem Administrationsserver von Hand zu starten, machen Sie Folgendes:

1. Starten Sie Kaspersky Mobile Security (s. Pkt. 2.1.1 auf S. 9).
2. Öffnen Sie die Registerkarte **Update**.
3. Gehen Sie auf den Punkt **Synchronisierung**.

Bei der Synchronisierung mit dem Administrationsserver werden die Parameter für die Programmfunktionen geladen und vom Gerät Berichte über die Arbeit des Programms auf den Administrationsserver geschickt. Wenn die Parameter für die Programmfunktionen seit der letzten Synchronisierung nicht geändert wurden, werden die Richtlinienparameter nicht übernommen.

2.1.10. Firewall-Modul

Die Firewall kontrolliert die Netzwerkaktivität und den Schutz des Gerätes auf Netzwerkebene (s. Abb. 21).

Um eine Überwachungsstufe für den ein- und ausgehenden Traffic festzulegen, können Sie eine Schutzstufe (Parameter **Firewall**) unter den vorgeschlagenen Varianten auswählen:

- **Hoch** – Jede Netzwerkaktivität wird unterbunden, außer dem Update der Datenbanken und der Verbindung mit dem Kaspersky Administration Kit.
- **Mittel** – Es werden alle eingehenden Verbindungen gesperrt. Die ausgehenden Verbindungen können nur über die Ports SSH, HTTP, HTTPS, IMAP, SMTP hergestellt werden.
- **Niedrig** – Es werden nur eingehende Verbindungen gesperrt.
- **Deaktiviert** – Der Netzwerkaktivität wird zugelassen.

Mit dem Parameter **Benachrichtigung** können Sie die Benachrichtigung über den versuchten Aufbau einer Verbindung aktivieren/deaktivieren, der in der ausgewählten Firewall-Sicherheitsstufe unterbunden wurde. Um keine Benachrichtigungen zu erhalten, wählen Sie **Deakt.** aus.



Abbildung 21. Registerkarte **Firewall**

Die Daten über das Firewall-Modul werden in das Anwendungsprotokoll eingetragen. Zum Anzeigen des Berichtes wählen Sie auf der Registerkarte **Firewall** den Eintrag **Protokoll**.

2.1.11. Berichte im Programmablauf

Auf der Registerkarte **Informationen** können Sie das chronologische Ereignisprotokoll für Kaspersky Mobile Security anzeigen lassen. Wechseln Sie dazu auf die Registerkarte und gehen Sie auf den Punkt **Protokoll** (s. Abb. 22).



Abbildung 22. Berichte über Programmablauf

2.2. Deinstallation der Anwendung

Um Kaspersky Mobile Security vom mobilen Gerät zu deinstallieren, machen Sie Folgendes:

1. Beenden Sie Kaspersky Mobile Security. Gehen Sie wie folgt vor:
 - a) Halten Sie die Schaltfläche **Menü**.
 - b) In der Liste der gestarteten Programme gehen Sie auf **KMS 7.0 EE** und klicken auf die Schaltfläche **Optionen**.
 - c) Gehen Sie auf den Menüpunkt **Beenden** (s. Abb. 23).



Abbildung 23. Programm beenden

2. Deinstallieren Sie Kaspersky Mobile Security:

- a) Klicken Sie auf die Schaltfläche **Menü** und gehen Sie auf den Menüpunkt **Progr.-Man.** (s. Abb. 24).

Abbildung 24. **Taskmanager** starten

- b) In der Programmliste gehen Sie auf **KMS7 EE** und klicken auf die Schaltfläche **Optionen** (s. Abb. 25).

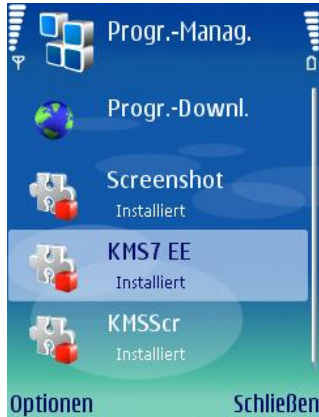


Abbildung 25. Programm auswählen

- c) Gehen Sie auf den Menüpunkt **Entfernen** (s. Abb. 26).



Abbildung 26. Deinstallation der Anwendung

- d) Beim Bestätigen der Programm-Deinstallation klicken Sie auf die Schaltfläche **Ja**.

KAPITEL 3. KASPERSKY MOBILE SECURITY FOR MICROSOFT WINDOWS MOBILE

In diesem Kapitel wird die Funktionsweise von Kaspersky Mobile Security für mobile Geräte beschrieben, die mit einem der folgenden Betriebssysteme laufen:

- Microsoft Windows Mobile 5.0
- Microsoft Windows Mobile 6.0

3.1. Überblick

In diesem Abschnitt stehen Informationen darüber, wie das Programm gestartet wird. Außerdem erfahren Sie die Grundprinzipien für die Organisation der grafischen Benutzeroberfläche.

3.1.1. Start des Programms


Um Kaspersky Mobile Security zu starten, machen Sie Folgendes:

1. Öffnen Sie auf dem mobilen Gerät das Menü **Programme**.
2. Gehen Sie auf den Punkt **KMS 7.0 EE**, um das Programm zu starten.

Nach dem Start des Programms erscheint auf dem Display des mobilen Gerätes das Fenster für den Status der Basiskomponenten von Kaspersky Mobile Security (s. Abb. 27):

- **Echtzeitschutz** – Status des Echtzeitschutz-Moduls
- **Letzter Scan** – Datum für die letzte Antiviren-Untersuchung des mobilen Gerätes
- **Ausgabedatum** – Datum für die Erstellung der von Kaspersky Mobile Security verwendeten Antiviren-Datenbanken

Achtung!

Wenn das mobile Gerät nicht auf Viren untersucht wurde oder seit dem letzten Update der Antiviren-Datenbanken zwei Wochen vergangen sind, verändert das Symbol neben dem jeweiligen Punkt sein Aussehen in . Das gleiche Symbol erscheint, wenn der Echtzeitschutz und / oder das Anti-Spam-Modul deaktiviert werden.

- **Firewall** – Schutzstufe des Gerätes auf Netzwerkebene
- **Anti-Spam** – Status des Anti-Spam-Moduls zum Filtern von SMS-Nachrichten

Achtung!

Auf PDAs gibt es kein Anti-Spam!



Abbildung 27. Status-Fenster der Programmkomponenten

3.1.2. Grafische Oberfläche

Die grafische Programmoberfläche besteht aus sechs Registerkarten, auf die Sie über **Menü** zugreifen können (s. Abb. 28):

- Im Abschnitt **Untersuchung** können Sie die Antiviren-Untersuchung des mobilen Gerätes aufrufen, die Parameter für die Antiviren-Untersuchung, den Echtzeitschutz und die Quarantäne bearbeiten und

einen Zeitplan für den automatischen Start der Untersuchung konfigurieren (s. Pkt. 3.2 auf S. 40).

- Der Abschnitt **Firewall** kontrolliert die Netzwerkaktivität und den Schutz des Gerätes auf Netzwerkebene (s. Pkt. 3.7 auf S. 56).
- Im Abschnitt **Update** kann das Update der Antiviren-Datenbanken ausgeführt, die Parameter für das Update bearbeitet und ein Zeitplan für das Update konfiguriert werden (s. Pkt. 3.5 auf S. 54).
- Der Abschnitt **Anti-Spam** richtet das Filtern von eingehenden SMS-Nachrichten ein (Anti-Spam-Modul, s. Pkt. 3.4.1 auf S. 46).
- Der Abschnitt **Anti-Theft** sperrt das Gerät und löscht darauf befindliche Daten bei Diebstahl oder Verlust des Gerätes (Anti-Theft-Modul, s. Pkt. 3.4.2 auf S. 50).
- Der Abschnitt **Informationen** zeigt das Ereignisjournal für die Programmkomponenten, allgemeine Informationen zum Programm und der verwendeten Datenbanken an und stellt die allgemeinen Parameter für die Programmfunktionen bereit (s. Pkt. 3.8 auf S. 58).



Abbildung 28. Menü **Programme**

Um zum Status-Fenster der Programmkomponenten zurückzukehren, gehen Sie auf den Punkt **Aktueller Status**.

Um allgemeine Informationen über das Programm anzuzeigen, gehen Sie auf den Punkt **Programminfo**.

Um das Programm zu beenden, gehen Sie auf **Beenden**.

3.2. Antiviren-Untersuchung und Echtzeitschutz

Im Abschnitt **Untersuchung** können Sie die Antiviren-Untersuchung des gesamten Dateisystems und des Speichers für das mobile Gerät oder einzelner Verzeichnisse bzw. Dateien einstellen. Außerdem können Sie die Parameter für die Antiviren-Untersuchung und den Echtzeitschutz ändern, den Bericht über die Untersuchungsergebnisse anzeigen und einen Zeitplan für den automatischen Start einer Untersuchung einrichten.

3.2.1. Scan auf Befehl

Um die Parameter für den Scan auf Befehl zu ändern, machen Sie Folgendes:

1. Gehen Sie im Abschnitt **Untersuchung** auf den Punkt **Scan-Einstellungen**.
2. Geben Sie im Block **Dateitypen** den Untersuchungsbereich ein, indem Sie die Dateitypen markieren, die untersucht werden sollen:
 - **Archive** – Auch Dateien untersuchen, die als Archiv gepackt sind
 - **Nur exe-Dateien** – Untersucht werden nur ausführbare Programmdateien.
3. Wählen Sie im Block **Bei Viruserkennung** die Aktion aus, die das Programm bei Entdecken eines infizierten Objektes ausführt. Soll das Objekt nicht desinfiziert werden, wählen Sie für den Parameter **Basis-Aktionen** einen der folgenden Werte aus:
 - **In Quarantäne** – Die erkannten infizierten Objekte werden in die Quarantäne verschoben.
 - **Aktion erfragen** – Meldung über erkannten Virus machen und vorschlagen, das infizierte Objekt zu löschen, es in die Quarantäne zu verschieben oder zu überspringen.
 - **Löschen** – Erkannte infizierte Objekte werden gelöscht.
 - **Überspringen** – An infizierten Objekten keine Aktion ausführen.

Damit das Programm versucht, ein erkanntes infiziertes Objekt zu desinfizieren, setzen Sie das Häkchen bei **Reparaturversuch**. Definieren Sie im Block **Wenn Reparatur nicht geht** die Aktion, die das

Programm ausführt, wenn das infizierte Objekt nicht repariert werden kann.

Um die Vireuntersuchung zu starten, machen Sie Folgendes:

1. Starten Sie Kaspersky Mobile Security (s. Pkt. 3.1.1 auf S. 37).
2. Im Abschnitt **Untersuchung** (s. Abb. 29) wählen Sie den Punkt **Voll Scan**, wenn Sie das gesamte Dateisystem des mobilen Gerätes untersuchen wollen, oder **Ordner-Scan**, wenn Sie einen einzelnen Ordner untersuchen wollen.



Abbildung 29. Abschnitt **Scan**

Sollten Sie sich für den Punkt **Ordner-Scan** entschieden haben, öffnet sich ein Fenster, das das Dateisystem des Gerätes anzeigt. Um die Untersuchung eines Ordners zu starten, setzen Sie den Cursor auf den Ordner und gehen auf **Scan**.

Nachdem die Untersuchung begonnen hat, öffnet sich das Untersuchungsfenster, in dem der aktuelle Status angezeigt wird: Die Anzahl der untersuchten Objekte und der Pfad zum Objekt, das gerade untersucht wird (s. Abb. 30).



Abbildung 30. Fenster des Untersuchungsprozesses



Abbildung 31. Meldung eines erkannten Virus

Nach der Untersuchung erscheint eine allgemeine Statistik über gefundene und gelöschte schädliche Objekte.

3.2.2. Echtzeitschutz

Der Echtzeitschutz ist ein Modus, bei dem ein residenter Teil von Kaspersky Mobile Security dauerhaft im Arbeitsspeicher des mobilen Gerätes verbleibt und ausführbare Programmdateien und Dateien untersucht, die der Benutzer öffnet.

Der Echtzeitschutz ist mit dem Einschalten des Gerätes in Betrieb und funktioniert bis zum Ausschalten (wenn der Modus nicht in den Schutzeinstellungen deaktiviert wird).

Außerdem kann Kaspersky Mobile Security das Dateisystem des mobilen Gerätes komplett untersuchen.

Die Ergebnisse des Echtzeitschutzes und eines Scans auf Befehl werden in einen Bericht eingetragen. Zum Anzeigen des Berichtes wählen Sie den Eintrag **Scan-Bericht**. Außerdem erreichen Sie den Bericht im Abschnitt **Informationen** (s. Pkt. 3.8 auf S. 58).

Um den Echtzeitschutz einzuschalten, machen Sie Folgendes:

1. Gehen Sie im Abschnitt **Scan** auf den Punkt **Schutzeinstellungen**.
2. Setzen Sie das Häkchen bei **Aktiviert**.

Um die Parameter für den Echtzeitschutz zu ändern, machen Sie Folgendes:

1. Gehen Sie im Abschnitt **Scan** auf den Punkt **Schutzeinstellungen**.
2. Setzen Sie das Häkchen bei **Nur exe-Dateien** im Block **Dateitypen**, damit der Echtzeitschutz nur ausführbare Programmdateien untersucht. Entfernen Sie das Häkchen, damit der Echtzeitschutz ausführbare Programmdateien und Dateien untersucht, die der Benutzer öffnet.
3. Wählen Sie im Block **Bei Viruserkennung** die Aktion aus, die das Programm bei Entdecken eines infizierten Objektes ausführt. Sie können eine der folgenden Varianten wählen:
 - **In Quarantäne** – Die erkannten infizierten Objekte werden in die Quarantäne verschoben.
 - **Löschen** – Erkannte infizierte Objekte werden gelöscht.
 - **Überspringen** – An infizierten Objekten keine Aktion ausführen.

3.2.3. Untersuchung nach Zeitplan

Mit Kaspersky Mobile Security kann der Benutzer einen Zeitplan für die automatische Antiviren-Untersuchung des mobilen Gerätes erstellen. Die Untersuchung erfolgt im Hintergrund. Wird ein infiziertes Objekt erkannt, wird die

Aktion ausgeführt, die in den Untersuchungsparametern vorgegeben wurde (Punkt **Scan-Einstellungen**).

Die Untersuchung nach Zeitplan ist standardmäßig deaktiviert.

Um einen Zeitplan für den Start der Untersuchung des Geräte-Dateisystems zu erstellen, machen Sie Folgendes:

Im Abschnitt **Scan** gehen Sie auf den Punkt **Zeitplan** und erstellen einen Zeitplan für den Untersuchungsstart (s. Abb. 32):

- **Täglich** – Untersuchung erfolgt jeden Tag. Die Untersuchungszeit wird mit dem Parameter **Zeit** angegeben.
- **Wöchentlich** – Untersuchung erfolgt einmal pro Woche. Der Tag und die Uhrzeit für die Untersuchung werden mit den Parametern **Wochentag** und **Zeit** bestimmt.
- **Deaktivieren** – Der Benutzer ruft die Untersuchung manuell auf.



Abbildung 32. Menü **Zeitplan**

3.3. Isolieren in Quarantäne

Infizierte Objekte, die in die Quarantäne verschoben wurden, bedrohen nicht mehr die Sicherheit des mobilen Gerätes und können später gelöscht oder wiederhergestellt werden.

Als infiziert erkannte Objekte können von einer Anwendung automatisch in die Quarantäne verschoben werden oder nach Ihrer Bestätigung.

Um das automatische Verschieben von infizierten Objekten in die Quarantäne einzuschalten, machen Sie Folgendes:

1. Öffnen Sie den Abschnitt **Scan**.
2. Gehen Sie auf den Punkt **Scan-Einstellungen**.
3. Im Block **Bei Viruserkennung** geben Sie als Aktion bei Entdecken eines schädlichen Objektes die Aktion **In Quarantäne** vor.

Wenn Sie als Aktion **Aktion erfragen** angegeben haben, öffnet sich bei Erkennen des infizierten Objektes das Benachrichtigungsfenster, in dem ein Löschen des Objektes oder dessen Verschieben in die Quarantäne vorgeschlagen wird.

Um den Quarantäne-Inhalt anzuzeigen, machen Sie Folgendes:

Öffnen Sie den Abschnitt **Scan** und gehen Sie auf den Punkt **Quarantäne** (s. Abb. 33).



Abbildung 33. Quarantäne

Im **Menü**, das im Fenster Anzeige der Quarantäne angeboten wird, können Sie Folgendes machen:

- Detaillierte Informationen zu einem markierten Objekt anzeigen, das in der Quarantäne gespeichert wird (Punkt **Meldungen**)

- Aktuelles Objekt löschen (Punkt **Löschen**)
- Aktuelles Objekt aus der Quarantäne in das ursprüngliche Verzeichnis wiederherstellen (Punkt **Wiederherstellen**)
- Quarantäne leeren, indem der gesamte Inhalt mit den Objekten gelöscht wird (Punkt **Alle löschen**)

3.4. Anti-Spam- und Anti-Theft-Modul

Das Anti-Spam-Modul schützt das Gerät vor unerwünschten SMS-Nachrichten.

Das Filter-Prinzip für Nachrichten beruht auf der Verwendung einer „schwarzen“ und einer „weißen“ Liste. Diese Listen enthalten Telefonnummern und Phrasen-Muster, die erwünschte und unerwünschte Nachrichten charakterisieren. Die Analyse der Nachricht erfolgt in dieser Reihenfolge:

- Untersuchung der Sendernummer auf Zugehörigkeit zur "schwarzen" Liste
- Untersuchung der Sendernummer auf Zugehörigkeit zur "weißen" Liste
- Untersuchung des Nachrichtentextes auf Übereinstimmung mit Phrasen aus der "schwarzen" Liste
- Untersuchung des Nachrichtentextes auf Übereinstimmung mit Phrasen aus der "weißen" Liste.

Wird wenigstens eine Übereinstimmung festgestellt, erfolgt keine weitere Untersuchung. Nachrichten, die einem Element aus der "schwarzen" Liste entsprechen, werden gesperrt. Nachrichten, die einem Element aus der "weißen" Liste entsprechen, werden durchgelassen.

3.4.1. Anti-Spam

Das Modul Anti-Spam schützt das mobile Gerät vor unerwünschten SMS-Nachrichten.

Achtung!

Auf PDAs gibt es kein Anti-Spam!

Das Filter-Prinzip für Nachrichten beruht auf der Verwendung einer „schwarzen“ und einer „weißen“ Liste. Diese Listen enthalten Telefonnummern und Phrasen-Muster, die erwünschte und unerwünschte Nachrichten charakterisieren. Die Analyse der Nachricht erfolgt in dieser Reihenfolge:

- Untersuchung der Sendernummer auf Zugehörigkeit zur "schwarzen" Liste
- Untersuchung der Sendernummer auf Zugehörigkeit zur "weißen" Liste
- Untersuchung des Nachrichtentextes auf Übereinstimmung mit Phrasen aus der "schwarzen" Liste
- Untersuchung des Nachrichtentextes auf Übereinstimmung mit Phrasen aus der "weißen" Liste.

Wird wenigstens eine Übereinstimmung festgestellt, erfolgt keine weitere Untersuchung. Die Nachricht, die einem Element aus der "schwarzen" Liste entspricht, wird gesperrt. Die Nachricht, die einem Element aus der "weißen" Liste entspricht, wird durchgelassen.

Um die Parameter für Anti-Spam zu ändern, machen Sie Folgendes:

1. Im Abschnitt **Anti-Spam** gehen Sie auf **Einstellungen**.
2. Wählen Sie für das Modul **Anti-Spam** den gewünschten Modus:
 - **Aktiviert.** In diesem Modus filtert Anti-Spam eingehende Nachrichten anhand der „schwarzen“ und „weißen“ Liste. Geht eine Nachricht von einer Telefonnummer ein, die in keiner Liste steht, benachrichtigt Anti-Spam den Benutzer und schlägt das Sperren oder Zulassen des Nachrichtenempfangs vor und empfiehlt außerdem die Übernahme der Telefonnummer in die „weiße“ oder „schwarze“ Liste.
 - **Nur „schwarze“ Liste.** In diesem Modus sperrt Anti-Spam den Empfang von Nachrichten, die auf der "schwarzen" Liste stehen. Die übrigen Nachrichten werden durchgelassen.
 - **Nur „weiße“ Liste.** In diesem Modus lässt Anti-Spam Nachrichten durch, die auf der "weißen" Liste stehen. Die übrigen Nachrichten werden gesperrt.
 - **Deaktiviert.** In diesem Modus ist Anti-Spam deaktiviert. Eingehende Nachrichten werden nicht gefiltert.
3. Setzen Sie das Häkchen bei **Kontakte zulassen**, damit Anti-Spam den Nachrichtenempfang von Nummern aus der Kontaktliste nicht sperrt.
4. Setzen Sie das Häkchen bei **Nicht-Ziffern sperren**, damit Anti-Spam den Nachrichtenempfang von Nummern, die nicht ausschließlich aus Ziffern bestehen, sperrt.

3.4.1.1. „Schwarze“ und „Weiße“ Liste bearbeiten

Die „schwarze“ Liste enthält Einträge, bei deren Übereinstimmung die Nachrichten durch Anti-Spam gesperrt werden.

Die „weiße“ Liste enthält Einträge, bei deren Übereinstimmung die Nachrichten durch Anti-Spam durchgelassen werden.

Um die "schwarze" oder "weiße" Liste zu bearbeiten, machen Sie Folgendes:

Öffnen Sie den Abschnitt **Anti-Spam** (s. Abb. 34) und gehen Sie auf die entsprechende Liste.

Zur Bearbeitung der Liste gehen Sie auf **Menü**:

- **Eintrag hinzufügen** – Es wird ein neuer Eintrag in der Liste erzeugt.
- **Eintrag löschen** – Der aktuelle Eintrag wird gelöscht.
- **Eintrag bearbeiten** – In der Liste wird der aktuelle Eintrag bearbeitet.

Nachdem Sie den Punkt **Eintrag hinzufügen** ausgewählt haben, geben Sie die Telefonnummer ein (Feld **Geben Sie die Nummer ein**), die Sie in die Liste aufnehmen wollen. Die Nummer kann mit einer Ziffer oder dem Zeichen „+“ beginnen. Außerdem dürfen beim Anlegen der Nummer die Ersatzzeichen "?" und "*" verwendet werden ("?" steht dabei für ein einzelnes Zeichen, "*" für eine beliebig lange Zeichenfolge).

Zusätzlich können Sie einen Text eintragen (Feld **Geben Sie den Text ein**), bei dessen Erkennen durch das Programm in der eingegangenen Nachricht die folgenden Aktionen ausgeführt werden:

- Die Nachricht, in der Text gefunden wird, der in der "weißen" Liste steht, wird durchgelassen.
- Die Nachricht, in der Text gefunden wird, der in der "schwarzen" Liste steht, wird gesperrt.

Abbildung 34. Abschnitt **Anti-Spam**

Nachdem Sie die Liste bearbeitet haben, klicken Sie auf **OK**, um zum Abschnitt **Anti-Spam** zurückzukehren.

3.4.1.2. Aktionen für Nachrichten

Geht eine Nachricht von einer Telefonnummer ein, die nicht in der „schwarzen“ oder „weißen“ Liste steht –vorausgesetzt, in den Anti-Spam-Parametern ist der Nachrichten-Empfang von unbekanntem Nummern zugelassen (s. Abb. 3.4.1 auf S. 46) –, erscheint im Display des mobilen Gerätes eine Warnmeldung (s. Abb. 35).

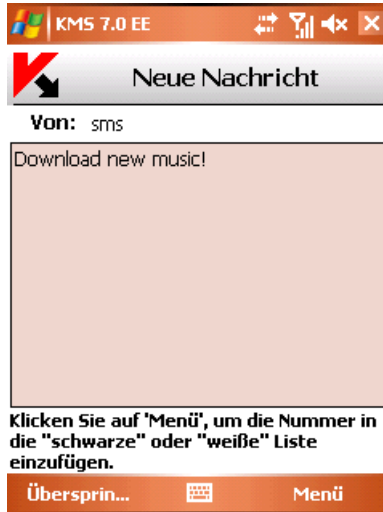


Abbildung 35. Anti-Spam warnt

Über **Menü** können Sie eine der folgenden Aktionen für eine Nachricht wählen:

- In **„weiße“ Liste** – Empfang der Nachricht wird zugelassen und Telefonnummer des Absenders wird in die „weiße“ Liste gespeichert
- In **„schwarze“ Liste** – Empfang der Nachricht wird gesperrt und Telefonnummer des Absenders wird in die „schwarze“ Liste gespeichert

Klicken Sie auf die Schaltfläche **Überspringen**, um den Empfang der Nachricht zuzulassen. Die Telefonnummer des Absenders wird in keine Liste gespeichert.

Die Daten über gesperrte Nachrichten werden in das Anwendungsprotokoll eingetragen.

Um das Journal anzuzeigen, gehen Sie im Abschnitt **Anti-Spam** auf den Punkt **Anti-Spam-Bericht**. Außerdem erreichen Sie den Bericht im Abschnitt **Informationen** (s. Pkt. 3.8 auf S. 58).

3.4.2. Anti-Theft

Das Anti-Theft-Modul (Abschnitt **Anti-Theft**, s. Abb. 36) schützt Daten, die auf dem mobilen Gerät gespeichert sind, vor dem unautorisierten Zugriff, falls das Gerät gestohlen wird oder verloren geht.

Beim erstmaligen Aufrufen der Modul-Parameter muss ein Geheimcode eingegeben werden. Mit dessen Hilfe kann künftig auf die Modul-Parameter

zugegriffen und die Modul-Funktionen aktiviert werden. Der Geheimcode wird gebraucht, damit die Parameter nicht unautorisiert geändert werden können und damit der Benutzer Daten sperren und löschen kann, die auf dem Gerät bei Diebstahl oder Verlust gespeichert waren.

Die Funktion **SMS-Block** sperrt das Gerät auf Wunsch des Benutzers. Es lässt sich erst nach Eingabe des Geheimcodes entsperren, der für den Zugriff auf das Anti-Theft-Modul verwendet wird. Die Funktion tritt in Kraft, wenn der Benutzer an das verloren gegangene Gerät eine SMS mit dem folgenden Inhalt schickt: «*block:Code*».

Die Funktion **SMS-Clean** löscht persönliche Benutzerdaten (Kontakte, Posteingang, persönliche Dateien, Parameter der Netzwerkverbindungen). Die Funktion tritt in Kraft, wenn der Benutzer an das verloren gegangene Gerät eine SMS mit dem folgenden Inhalt schickt: «*clean:Code*».

Die Funktion **SIM Watch** schickt bei einem Verlust des Gerätes die neue Telefonnummer an die eingegebenen Nummern und sperrt es. Das Gerät wird mit Eingabe des Geheimcodes entsperrt, der für den Zugriff auf das Anti-Theft-Modul angegeben wurde.

Um den Geheimcode für das Anti-Theft-Modul zu ändern, gehen Sie auf den Punkt **Code austauschen**. Geben Sie den neuen Code und dessen Bestätigung ein und klicken Sie auf **OK**.

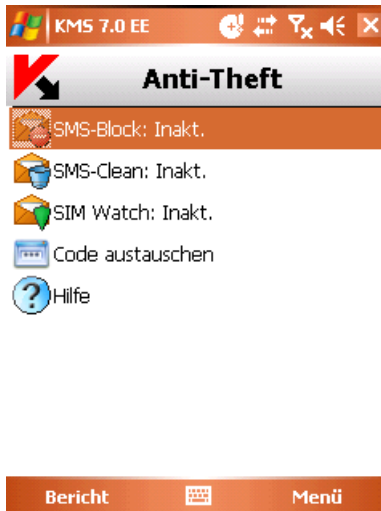


Abbildung 36. Abschnitt **Anti-Theft**

Die Daten über das Anti-Theft-Modul werden in das Anwendungsprotokoll eingetragen. Um das Protokoll anzuzeigen, gehen Sie auf den Punkt **Bericht** im

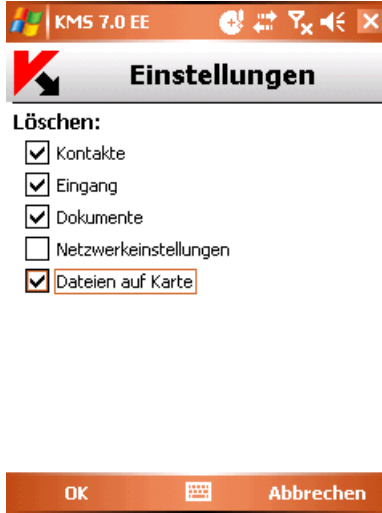
Abschnitt **Anti-Theft**. Außerdem erreichen Sie den Bericht im Abschnitt **Informationen** (s. Pkt. 3.8 auf S. 58).

3.4.2.1. Parameter von SMS-Clean

Die Funktion **SMS-Clean** löscht auf dem verloren gegangenen Gerät Daten (s. Abb. 37).

Um die Parameter für SMS-Clean zu ändern, machen Sie Folgendes:

1. Öffnen Sie den Abschnitt **Anti-Theft**
2. Geben Sie den Geheimcode ein und gehen Sie im nächsten Fenster auf den Punkt **SMS-Clean**.
3. Setzen Sie das Häkchen bei **Kontakte**, wenn Sie wollen, dass bei einem Verlust oder Diebstahl des mobilen Gerätes das Telefonbuch gelöscht werden kann.
4. Setzen Sie das Häkchen bei **Eingang**, wenn Sie wollen, dass die Post sowie die SMS-Nachrichten gelöscht werden können.
5. Setzen Sie das Häkchen bei **Dokumente**, damit die persönlichen Dateien des Benutzers gelöscht werden können.
6. Setzen Sie das Häkchen bei **Netzwerkeinstellungen**, damit die Parameter der Netzwerkverbindungen gelöscht werden können.
7. Setzen Sie das Häkchen bei **Dateien auf Karte**, damit Dateien auf Speicherkarten des Gerätes gelöscht werden können.
8. Klicken Sie auf **OK**, um die vorgenommenen Änderungen zu speichern.

Abbildung 37. Parameter von **SMS-Clean**

3.4.2.2. Parameter von SIM Watch

Die Funktion **SIM Watch** überwacht den Wechsel der SIM-Karte auf dem Gerät (s. Abb. 38).

Um die Parameter für SIM Watch zu ändern, machen Sie Folgendes:

1. Öffnen Sie den Abschnitt **Anti-Theft**
2. Geben Sie den Geheimcode ein und gehen Sie im nächsten Fenster auf den Punkt **SIM Watch**.
3. In den Feldern **1)** und **2)** geben Sie diejenigen Telefonnummern ein, an die Sie die neue Telefonnummer erhalten wollen, falls die SIM-Karte auf Ihrem Gerät gewechselt wird. Die Nummern können mit einer Ziffer oder dem Zeichen „+“ beginnen und dürfen nur Ziffern enthalten.
4. Setzen Sie das Häkchen bei **Sperren**, um das Gerät beim Wechsel der SIM-Karte zu sperren.
5. Klicken Sie auf **OK**, um die eingegebenen Daten zu speichern.



KMS 7.0 EE

Telefonnummern

1) 123456789

2) +71112233

Sperrern

OK Abbrechen

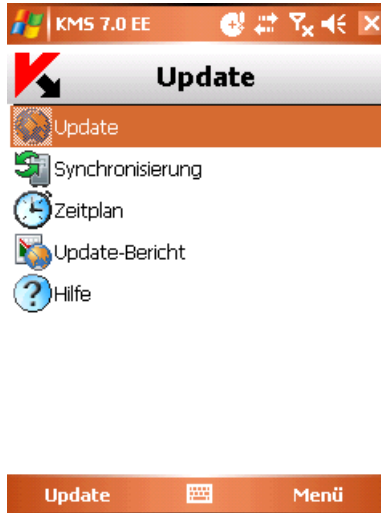
Abbildung 38. Parameter von **SIM Watch**

3.5. Update der Programm-Datenbanken

Nach schädlichen Programmen wird mithilfe von Einträgen in der Datenbank von Kaspersky Mobile Security gesucht, in der eine Beschreibung aller bekannten und zurzeit als schädlich eingestuft Programme steht. Es ist absolut wichtig, dass die Datenbanken auf dem neuesten Stand sind.

Die Datenbanken können entweder manuell oder nach Zeitplan aktualisiert werden. Zum Einrichten der Parameter und Starten eines Updates dient der Abschnitt **Update** (s. Abb. 39). Das Update erfolgt über das Internet von den Kaspersky-Lab-Servern.

Der Update-Vorgang der Datenbanken wird in das Protokoll eingetragen. Um das Journal anzuzeigen, gehen Sie im Abschnitt **Update** auf den Punkt **Update-Bericht**. Außerdem erreichen Sie den Bericht auf der Registerkarte **Informationen** (s. Pkt. 3.8 auf S. 58).

Abbildung 39. Abschnitt **Update**

Um das **Update** für die Programm-Datenbanken von Hand zu starten, machen Sie Folgendes:

1. Starten Sie Kaspersky Mobile Security (s. Pkt. 3.1.1 auf S. 37) und wechseln Sie in den Abschnitt **Update**.
2. Gehen Sie auf **Update**, um den Update-Download zu starten.

Um einen **Zeitplan** für den Start des **Updates** der Programm-Datenbanken zu erstellen, machen Sie Folgendes:

1. Starten Sie Kaspersky Mobile Security (s. Pkt. 3.1.1 auf S. 37) und wechseln Sie in den Abschnitt **Update**.
2. Gehen Sie auf den Punkt **Zeitplan**.
3. Geben Sie das Update-Intervall im Block **AutoUpdate** ein:
 - **Täglich** – Update startet jeden Tag. Geben Sie zusätzlich die **Uhrzeit** des Updates vor.
 - **Wöchentlich** – Update startet einmal pro Woche. Geben Sie zusätzlich den **Wochentag** und die **Zeit** des Updates ein.
 - **Deaktivieren** – Der Benutzer ruft das Update manuell auf.

Im Abschnitt **Informationen** können Sie das Erstellungsdatum der Programm-Datenbanken und die enthaltenen Virussignaturen erfahren. Gehen Sie dazu auf der Registerkarte auf den Punkt **Datenbank-Info**.

3.6. Update der Parameter für die Programmfunktionen

Anmerkung

Nähere Informationen über das Zusammenspiel von Kaspersky Mobile Security Enterprise Edition und dem Kaspersky Administration Kit finden Sie im Administratorhandbuch von Kaspersky Mobile Security Enterprise Edition.

Wenn Kaspersky Mobile Security Enterprise Edition zusammen mit Kaspersky Administration Kit eingesetzt wird, werden die Parameter für die Programmfunktionen durch die Richtlinie für die Gruppe der mobilen Geräte vorgegeben. Die Aktivierung des Programms und die Übernahme der Richtlinienparameter, die nicht geändert werden dürfen, erfolgen beim Hinzufügen des Gerätes in die Administrationsgruppe.

Im Anschluss wird automatisch die Synchronisierung mit dem Administrationsserver mit einem Intervall gestartet, der in den Parametern der Richtlinie vorgegeben wurde.

Um die Synchronisierung des Programms mit dem Administrationsserver von Hand zu starten, machen Sie Folgendes:

1. Starten Sie Kaspersky Mobile Security (s. Pkt. 2.1.1 auf S. 9).
2. Öffnen Sie den Abschnitt **Update**.
3. Gehen Sie auf den Punkt **Synchronisierung**.

Bei der Synchronisierung mit dem Administrationsserver werden die Parameter für die Programmfunktionen geladen und vom Gerät Berichte über die Arbeit des Programms auf den Administrationsserver geschickt. Wenn die Parameter für die Programmfunktionen seit der letzten Synchronisierung nicht geändert wurden, werden die Richtlinienparameter nicht übernommen.

3.7. Firewall

Das Modul **Firewall** kontrolliert die Netzwerkaktivität und den Schutz des mobilen Gerätes auf Netzwerkebene (s. Abb. 40).

Um die Parameter für die Firewall zu ändern, machen Sie Folgendes:

1. Starten Sie Kaspersky Mobile Security (s. Pkt. 3.1.1 auf S. 37) und wechseln Sie in den Abschnitt **Firewall**.

2. Gehen Sie auf den Punkt **Firewall-Einstellungen**. Im nächsten Fenster können Sie die Schutzstufe einrichten, um eine Überwachungsstufe für den ein- und ausgehenden Traffic festzulegen. Es gibt die folgenden Varianten:
- **Hohe Stufe** – Jede Netzwerkaktivität ist unterbunden, außer dem Update der Datenbanken und der Verbindung mit Kaspersky Administration Kit.
 - **Mittlere Stufe** – Es werden alle eingehenden Verbindungen gesperrt. Die ausgehenden Verbindungen können nur über die Ports SSH, HTTP, HTTPS, IMAP, SMTP hergestellt werden.
 - **Niedrige Stufe** – Es werden nur eingehende Verbindungen gesperrt.
 - **Deaktiviert** – Jede Netzwerkaktivität wird zugelassen.

Die Daten über das Modul Firewall werden in das Protokoll eingetragen. Um das Journal anzuzeigen, gehen Sie im Abschnitt **Firewall** auf den Punkt **Firewall-Bericht**.

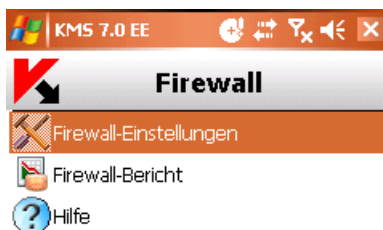


Abbildung 40. Abschnitt **Firewall**

3.8. Berichte

Berichte werden auf der Registerkarte **Informationen** im Punkt **Berichte** gesammelt. Sie können einen Bericht für eine beliebige Aufgabe anzeigen, die Kaspersky Mobile Security ausgeführt hat:

- Antiviren-Untersuchung
- Update der Programm-Datenbanken
- Funktion der Firewall
- Funktion von Anti-Spam
- Funktion von Anti-Theft

Um einen Bericht für eine Programmkomponente einzusehen, machen Sie Folgendes:

1. Starten Sie Kaspersky Mobile Security (s. Pkt. 3.1.1 auf S. 37).
2. Im Abschnitt **Informationen** gehen Sie auf den Punkt **Berichte** (s. Abb. 41).
3. Im nächsten Fenster markieren Sie den Bericht der gewünschten Komponente.



Abbildung 41. Abschnitt **Berichte**

3.9. Deinstallation der Anwendung

Um Kaspersky Mobile Security zu deinstallieren, machen Sie Folgendes:

1. Deaktivieren Sie den Echtzeitschutz (Details s. Pkt. 3.2 auf S. 40).



Abbildung 42. Echtzeitschutz deaktivieren

2. Beenden Sie Kaspersky Mobile Security. Gehen Sie dazu im Programmmenü auf den Punkt **Beenden** (s. Abb. 43).

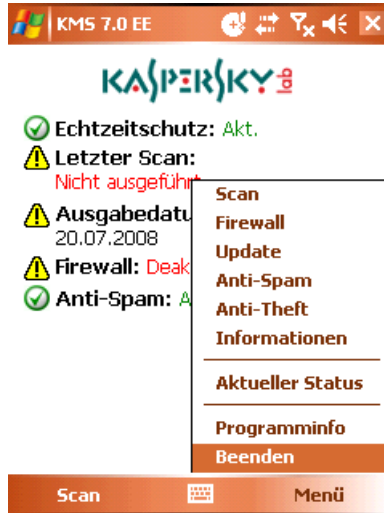


Abbildung 43. Programm beenden

3. Deinstallieren Sie die Anwendung. Gehen Sie wie folgt vor:
 - a) Klicken Sie auf die Schaltfläche **Start**, gehen Sie auf das Menü **Einstellungen**, öffnen Sie die Registerkarte **System** und gehen Sie dann auf **Programm entfernen** (s. Abb. 44):

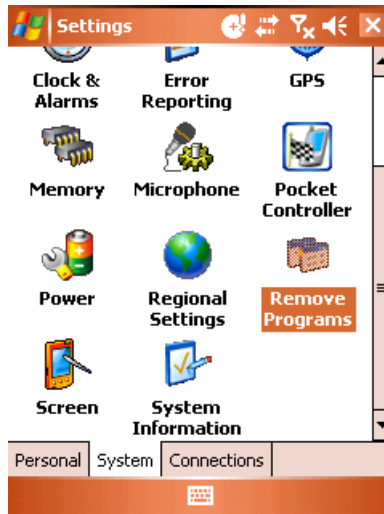


Abbildung 44. Programm-Deinstallation aufrufen

- b) In der Liste der installierten Programme gehen Sie auf **Kaspersky Mobile Security** und klicken auf die Schaltfläche **Deinstallieren** (s. Abb. 45).

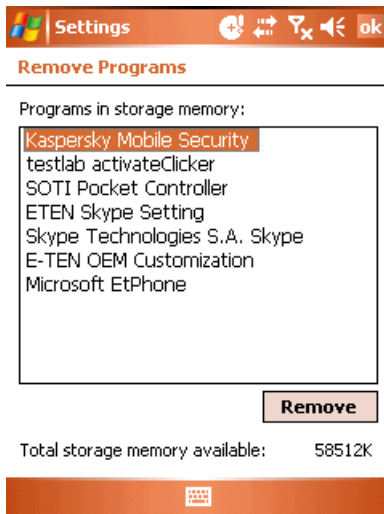


Abbildung 45. Programm auswählen

- c) Bei der Bestätigungsabfrage für die Programm-Deinstallation klicken Sie auf die Schaltfläche **Ja** (s. Abb. 46). Es öffnet sich daraufhin die Meldung zum Löschen der Datei mit den Parametern für die Programmfunktionen. Klicken Sie auf die Schaltfläche **Nein**, damit das Programm komplett deinstalliert wird. Beim Klick auf die Schaltfläche **Ja** wird auf dem Gerät die Datei mit den Parametern der Programmfunktionen gespeichert.

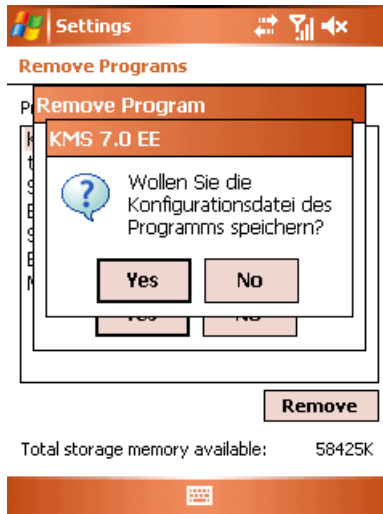


Abbildung 46. Speichern der Parameter mit den Programmfunktionen

ANHANG A. KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Die Firma ist heute das bekannteste Unternehmen für Datenschutz-Software in Russland und bietet eine breite Palette an IT-Sicherheitslösungen zum Schutz vor Viren, Spam und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Der Stammsitz befindet sich in Russland. Das Unternehmen unterhält Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Beneluxstaaten, in China, Polen, Rumänien und in den USA. In Frankreich wurde eine neue Filiale gegründet, das Europäische Zentrum für Antivirenforschung. Unser Partnernetzwerk verbindet weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das ist heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome, sechzehn einen Dokortitel haben. Die führenden Virusanalytiker von Kaspersky Lab gehören zur prestigeträchtigen Computer Anti-virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens besteht in dem einzigartigen Wissen und in der Erfahrung, die von den Mitarbeitern im Laufe des mehr als vierzehnjährigen kontinuierlichen Kampfes gegen Viren gesammelt wurden. Dank der permanenten Analyse von Virenaktivitäten sind wir in der Lage, Tendenzen in der Malware-Entwicklung zu prognostizieren und unseren Benutzern rechtzeitig zuverlässigen Schutz vor neuen Angriffen zu gewährleisten. Dieser Vorteil manifestiert sich in den Erzeugnissen und Leistungen von Kaspersky Lab. Wir sind unseren Konkurrenten stets einen Schritt voraus und bieten unseren Kunden Schutz von höchster Güte.

Aufgrund der jahrelangen Tätigkeit ist das Unternehmen jetzt ein führender Entwickler im Bereich der Virenschutztechnologien. Kaspersky Lab hat als erstes Unternehmen viele moderne Standards für Antiviren-Software gesetzt. Die Basisprodukt des Unternehmens heißt Kaspersky Anti-Virus®. Es bietet für alle Arten von Objekten zuverlässigen Schutz vor Virenangriffen: Arbeitsstationen, Dateiserver, Mailsysteme, Firewalls und Internet-Gateways, Handhelds. Bequeme Steuerelemente erlauben es dem Benutzer, den Antivirenschutz von Computern und Firmennetzwerken möglichst weitgehend zu automatisieren. Viele von Welt-Entwicklern verwenden in ihrer Software den Kern vom Kaspersky Anti-Virus®. Zu ihnen gehören u.a.: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die das störungsfreie Funktionieren der Erzeugnisse und die genaue Kompatibilität mit speziellen Business-Vorgaben garantieren. Wir planen, realisieren und begleiten komplexe Antivirenlösungen für Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Rund um die Uhr steht

unseren Benutzern ein technischer Kundendienst in mehreren Sprachen zur Verfügung.

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

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

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

Kontakt: <http://www.kaspersky.de/kontakt>

Technischer Support: <http://support.kaspersky.de>

Feedback zu unseren Benutzerhandbüchern: docfeedback@kaspersky.de

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

Webforum von Kaspersky Lab: <http://forum.kaspersky.com>

ANHANG B. CRYPTOEX LTD.

Für die Erstellung und Überprüfung elektronischer digitaler Signaturen wird in Kaspersky Anti-Virus die Krypto-Bibliothek (Programmbibliothek zum Informationsschutz - PBSI) "Crypto-Si" verwendet, die von CryptoEx Ltd. entwickelt wurde.

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

Die Rechte an der Krypto-Bibliothek sind exklusives Eigentum der CryptoEx Ltd.

ANHANG C. KASPERSKY LAB

ENDNUTZERVERTRAG

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE BITTE DEN FOLGENDEN VERTRAG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

DURCH ANKLICKEN DER SCHALTFLÄCHE „ANNEHMEN“ IM LIZENZVERTRAG ODER DURCH DIE EINGABE EINES ENTSPRECHENDEN ZEICHENS BZW. ENTSPRECHENDER ZEICHEN ERKLÄREN SIE SICH DAMIT EINVERSTANDEN, DASS SIE AN DIE BEDINGUNGEN DIESES VERTRAGES GEBUNDEN SIND. **DURCH EINE DERARTIGE HANDLUNG, DIE GLEICHBEDEUTEND IST MIT IHRER UNTERSCHRIFT, ERKLÄREN SIE SICH DAMIT EINVERSTANDEN, AN DIESEN VERTRAG GEBUNDEN ZU SEIN UND PARTEI DES VERTRAGES ZU WERDEN. SIE SIND AUSSERDEM DAMIT EINVERSTANDEN, DASS DIESER VERTRAG WIE JEDER SCHRIFTLICHE, VON IHNEN UNTERZEICHNETE VERTRAG DURCHSETZBAR IST. FALLS SIE NICHT MIT ALLEN BEDINGUNGEN DIESES VERTRAGES EINVERSTANDEN SIND, BRECHEN SIE BITTE DIE INSTALLATION DER SOFTWARE AB UND INSTALLIEREN SIE DIE SOFTWARE NICHT.**

NACH DEM ANKLICKEN DER SCHALTFLÄCHE „ANNEHMEN“ IM LIZENZVERTRAG BZW. NACH DER EINGABE EINES ENTSPRECHENDEN ZEICHENS / ENTSPRECHENDER ZEICHEN SIND SIE BERECHTIGT, DIE SOFTWARE GEMÄSS DEN BEDINGUNGEN DIESES VERTRAGES ZU NUTZEN.

1. **Begriffsbestimmungen**

- 1.1 **Software** bedeutet Software einschließlich aller Updates und zugehöriger Materialien.
- 1.2 **Rechteinhaber** (Inhaber aller ausschließlichen oder sonstigen Rechte an der Software) ist Kaspersky Lab ZAO, ein nach dem Recht der Russischen Föderation errichtetes Unternehmen.
- 1.3 **Computer** bedeutet Hardware wie Personal Computer, Laptops, Workstations, PDAs, Smartphones, Handhelds und andere elektronische Geräte, für die die Software entwickelt wurde und auf denen die Software installiert und/oder verwendet wird.
- 1.4 **Endnutzer (Sie)** sind Personen, die die Software im eigenen Namen installieren bzw. nutzen oder eine Kopie der Software rechtmäßig nutzen. Wurde die Software im Namen einer Organisation, etwa eines

Unternehmens, heruntergeladen oder installiert, bezieht sich „Sie“ außerdem auf die Organisation, für die die Software heruntergeladen oder installiert wurde. Es wird zugesichert, dass diejenige Person, die dem Vertrag zugestimmt hat, von der betreffenden Organisation hierzu bevollmächtigt ist. Der Ausdruck

„*Organisation*“ im Sinne dieses Vertrages umfasst insbesondere Partnerschaften, Gesellschaften mit beschränkter Haftung, Körperschaften, Aktiengesellschaften, Trusts, Joint Ventures, Arbeitnehmerorganisationen, Personengesellschaften oder staatliche Behörden.

- 1.5 **Partner** sind Organisationen oder Personen, denen der Rechteinhaber vertraglich gestattet hat, die Software zu vertreiben.
- 1.6 **Updates** sind Verbesserungen, Überarbeitungen, Korrekturen, Erweiterungen, Reparaturen, Modifizierungen, Reproduktionen, Ergänzungen oder Wartungspakete etc.
- 1.7 **Benutzerhandbuch** bezieht sich auf die Bedienungsanleitung, die Administrator-Anleitung, ein Nachschlagewerk und ähnliche erläuternde oder sonstige Materialien.

Lizenzerteilung

- 2.1 Der Rechteinhaber gewährt Ihnen hiermit die nicht ausschließliche Lizenz, die Software auf einer bestimmten Anzahl von Computern zu speichern, zu laden, zu installieren, auszuführen und anzuzeigen (zu „nutzen“), um dadurch Ihren Computer, auf dem die Software installiert wurde, vor den im Benutzerhandbuch beschriebenen Gefahren gemäß den technischen, im Benutzerhandbuch beschriebenen Anforderungen sowie gemäß den Bedingungen dieses Vertrages (der „Lizenz“) zu schützen. Sie nehmen diese Lizenz an.

Testversion. Falls Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert und damit eine Testlizenz für die Software erworben haben, können Sie sie nur zu Testzwecken sowie, falls nicht anderweitig angegeben, ausschließlich während des Testzeitraums ab dem Zeitpunkt der erstmaligen Installation nutzen. Eine Nutzung der Software zu anderen Zwecken oder über den Testzeitraum hinaus ist streng verboten.

Software für Mehrfachumgebungen; mehrsprachige Software; Dual-Media-Software; Mehrfachexemplare; Pakete. Falls Sie verschiedene Versionen oder verschiedensprachige Ausgaben der Software nutzen, die Software auf mehreren Medien oder sonst mehrere Exemplare der Software bzw. die Software im Paket mit anderer Software erhalten haben, entspricht die zulässige Gesamtzahl der Computer, auf denen

sämtliche Versionen der Software installiert sind, der Anzahl der Lizenzen, die Sie vom Rechteinhaber erworben haben. Dabei gibt Ihnen – vorbehaltlich abweichender Lizenzbestimmungen – jede erworbene Lizenz das Recht, die Software auf der in Ziff. 2.2 und 2.3 festgelegten Anzahl von Computern zu installieren und zu nutzen.

- 2.2 Wurde die Software auf einem Datenträger erworben, sind Sie berechtigt, die Software zum Schutz der auf der Software-Verpackung angegebenen Anzahl von Computern zu nutzen.
- 2.3 Wurde die Software über das Internet bezogen, sind Sie berechtigt, die Software zum Schutz der beim Erwerb der Software festgelegten Anzahl von Computern zu nutzen.
- 2.4 Sie dürfen die Software ausschließlich zu Sicherungszwecken als Ersatz für das rechtmäßig in Ihrem Besitz befindliche Exemplar für den Fall kopieren, dass dieses Exemplar verloren geht bzw. zerstört oder unbrauchbar wird. Für andere Zwecke darf die Sicherungskopie nicht verwendet werden. Sie ist zu zerstören, sobald Sie das Recht zur Nutzung der Software verlieren bzw. wenn Ihre Lizenz abläuft oder aus sonstigen Gründen nach den im Land Ihres Hauptwohnsitzes oder im Land der Softwarenutzung geltenden Gesetzen beendet wird.
- 2.5 Sie können die nicht ausschließliche Lizenz zur Nutzung der Software im Rahmen des Ihnen vom Rechteinhaber gewährten Umfangs auf andere natürliche oder juristische Personen übertragen. Der Erwerber muss anerkennen, dass er an alle Bedingungen dieses Vertrages gebunden ist und Ihnen als Inhaber der vom Rechteinhaber gewährten Lizenz in vollem Umfang nachfolgt. Falls Sie die vom Rechteinhaber gewährten Rechte zur Nutzung der Software in vollem Umfang übertragen, sind Sie verpflichtet, sämtliche Exemplare der Software einschließlich der Sicherungskopie zu zerstören. Als Erwerber einer übertragenen Lizenz müssen Sie sich verpflichten, alle Bedingungen dieses Vertrages einzuhalten. Falls Sie nicht anerkennen, dass Sie an alle Bedingungen dieses Vertrages gebunden sind, dürfen Sie die Software weder installieren noch nutzen. Als Erwerber einer übertragenen Lizenz erkennen Sie außerdem an, dass Sie keine weitergehenden oder besseren Rechte haben als der ursprüngliche Endnutzer, der die Software vom Rechteinhaber erworben hat.
- 2.6 Sobald die Software aktiviert bzw. die Lizenzschlüsseldatei installiert wurde (gilt nicht für eine Testversion der Software), sind Sie berechtigt, während des auf der Software-Verpackung angegebenen Zeitraums (beim Erwerb der Software auf einem Datenträger) bzw. des beim Erwerb festgelegten Zeitraums (falls die Software über das Internet bezogen wurde) die folgenden Leistungen in Anspruch zu nehmen:
 - Aktualisierungen der Software (Updates) über das Internet, sobald der Rechteinhaber sie auf seiner Website oder durch andere Online-Dienste herausgibt. Die von Ihnen bezogenen

- Updates werden Teil der Software. Die Bedingungen dieses Vertrages gelten auch für die Updates;
- Technischer Support über das Internet und technische Support-Hotline per Telefon.

3. Aktivierung und Laufzeit

- 3.1 Wenn Sie Ihren Computer modifizieren oder die darauf installierte Software anderer Anbieter verändern, kann es aufgrund von Vorgaben des Rechteinhabers erforderlich werden, die Aktivierung der Software bzw. die Installierung der Lizenzschlüsseldatei zu wiederholen. Der Rechteinhaber behält sich das Recht vor, die Gültigkeit der Lizenz und/oder die Rechtmäßigkeit einer Kopie der auf Ihrem Computer installierten bzw. genutzten Software mit allen zur Verfügung stehenden Mitteln und Nachweisverfahren zu überprüfen.
- 3.2 Wurde die Software auf einem Datenträger erworben, kann sie nach Ihrer Zustimmung zu diesem Vertrag während des auf der Verpackung angegebenen Zeitraums, beginnend mit dem Zeitpunkt der Vertragsannahme, genutzt werden.
- 3.3 Wurde die Software über das Internet bezogen, kann sie nach Ihrer Zustimmung zu diesem Vertrag während des beim Erwerb festgelegten Zeitraums genutzt werden.
- 3.4 Sie sind berechtigt, ab dem Zeitpunkt der Software-Aktivierung gemäß diesem Vertrag für einen einmaligen Testzeitraum von 30 Tagen eine Testversion der Software gemäß Ziff. 2.1 zu nutzen. Die Testversion berechtigt Sie nicht zum Bezug von Updates sowie zur Inanspruchnahme von technischem Support über das Internet bzw. über die technische Support-Hotline per Telefon.
- 3.5 Ihre Lizenz zur Nutzung der Software ist auf den in Ziff. 3.2 bzw. 3.3 angegebenen Zeitraum begrenzt. Die verbleibende Vertragslaufzeit kann auf die im Benutzerhandbuch beschriebene Weise abgefragt werden.
- 3.6 Haben Sie die Software zur Nutzung auf mehr als einem Computer erworben, beginnt der Zeitraum, auf den Ihre Lizenz zur Nutzung der Software begrenzt ist, am Tag der Aktivierung der Software bzw. der Installation der Lizenzschlüsseldatei auf dem ersten Computer.
- 3.7 Falls Sie eine Bestimmung dieses Vertrages verletzen, ist der Rechteinhaber unbeschadet sonstiger ihm nach Gesetz oder Billigkeit zustehender Rechtsmittel jederzeit berechtigt, diese Lizenz zur Nutzung der Software ohne vorherige Ankündigung fristlos zu kündigen. Eine Rückerstattung des Kaufpreises - ganz oder teilweise - ist in diesem Fall ausgeschlossen.
- 3.8 Bei der Nutzung der Software sowie bei der Verwendung von aus der Nutzung der Software herrührenden Informationen oder Daten verpflichten Sie sich zur Einhaltung aller einschlägigen internationalen,

nationalen, bundesstaatlichen, regionalen und lokalen Vorschriften. Hierzu zählen insbesondere Datenschutz-, Urheberrechts- und Ausfuhrüberwachungsgesetze sowie gegen Obszönität gerichtete Gesetze.

- 3.9 Falls nicht ausdrücklich anderweitig bestimmt, dürfen Sie die Ihnen nach diesem Vertrag gewährten Rechte bzw. die sich hieraus ergebenden Pflichten nicht übertragen oder abtreten.

4. Technischer Support

Den in Ziff. 2.6 dieses Vertrages dargestellten technischen Support können Sie in Anspruch nehmen, wenn das neueste Update der Software installiert ist (gilt nicht für eine Testversion der Software).

Technischer Support: <http://support.kaspersky.com>

5. Einschränkungen

- 5.1 Sie dürfen die Software nicht emulieren, klonen, vermieten, verleihen, verleasen, verkaufen, verändern, dekompileieren oder zurückentwickeln. Ebenso wenig dürfen Sie auf der Software basierende, abgeleitete Werke disassemblieren oder erstellen, es sei denn, Sie sind hierzu durch eine gesetzliche Regelung unabdingbar berechtigt. Sie dürfen auch auf andere Weise keinen Teil der Software auf eine für den Menschen lesbare Form reduzieren oder die lizenzierte Software ganz oder teilweise übertragen bzw. Dritten die Übertragung gestatten, es sei denn, die Möglichkeit dieses Verbots wird durch einschlägige Gesetze ausdrücklich ausgeschlossen. Weder der Binärcode der Software noch der Quellcode darf dazu genutzt werden, den proprietären Programmalgorithmus nachzubilden. Alle nicht durch diesen Vertrag ausdrücklich gewährten Rechte bleiben dem Rechteinhaber und/oder dessen Lieferanten vorbehalten. Eine unbefugte Nutzung der Software hat die unverzügliche, automatische Beendigung des Vertrages und der darin erteilten Lizenz zur Folge. Außerdem müssen Sie mit strafrechtlicher und/oder zivilrechtlicher Verfolgung rechnen.
- 5.2 Sie dürfen die Rechte zur Nutzung der Software nur im Rahmen der in Ziff. 2.5 dieses Vertrages enthaltenen Bestimmungen auf Dritte übertragen.
- 5.3 Sie dürfen weder den Aktivierungscode noch die Lizenzschlüsseldatei an Dritte weitergeben oder Dritten Zugang zum Aktivierungscode und/oder der Lizenzschlüsseldatei gestatten. Diese gelten als vertrauliche Daten des Rechteinhabers. Können Sie den Aktivierungscode und/oder die Lizenzschlüsseldatei gemäß den in Ziff. 2.5 dieses Vertrages enthaltenen Bestimmungen auf Dritte übertragen,

- haben Sie die zum Schutz der Vertraulichkeit des Aktivierungscode bzw. der Lizenzschlüsseldatei angemessene Sorgfalt aufzuwenden.
- 5.4 Sie dürfen die Software an Dritte weder vermieten noch verleasen oder verleihen.
- 5.5 Es ist Ihnen nicht gestattet, die Software zur eigenen Erstellung von Daten bzw. von Software zur Entdeckung, Blockierung oder Bearbeitung der im Benutzerhandbuch beschriebenen Gefahren nutzen.
- 5.6 Falls Sie eine Bestimmung dieses Vertrages verletzen, ist der Rechteinhaber befugt, die Schlüsseldatei ohne Anspruch auf Rückerstattung zu blockieren oder Ihre Lizenz zu kündigen.
- 5.7 Wenn Sie die Testversion der Software nutzen, haben Sie keinen Anspruch auf den in Ziff. 4 dieses Vertrages dargestellten technischen Support. Außerdem sind Sie nicht berechtigt, die Lizenz bzw. die Rechte zur Nutzung der Software auf Dritte zu übertragen.

6. Eingeschränkte Gewährleistung und Haftungsausschluss

- 6.1 Der Rechteinhaber steht dafür ein, dass die Software im Wesentlichen gemäß den im Benutzerhandbuch niedergelegten Angaben und Beschreibungen funktioniert. Diese eingeschränkte Gewährleistung gilt allerdings nicht, falls einer der folgenden Fälle vorliegt: (w) Mängel an Ihrem Computer und ähnliche Unregelmäßigkeiten, für die der Rechteinhaber ausdrücklich keine Gewähr übernimmt; (x) Fehlfunktionen, Mängel oder Defekte aufgrund fehlerhafter Anwendung; Missbrauch; Störfälle; Nachlässigkeit; unsachgemäße Installation, Handhabung oder Wartung; Diebstahl; Vandalismus; höhere Gewalt; terroristische Aktionen; Stromausfälle oder Überspannungen; Unfälle; Änderungen, nicht gestattete Modifizierungen oder Instandsetzungen durch andere als den Rechteinhaber; durch Sie vorgenommene Handlungen oder Handlungen Dritter; Umstände, die der Rechteinhaber nicht zu vertreten hat; (y) Mängel, die Sie dem Rechteinhaber nicht so schnell wie möglich nach dem erstmaligen Auftreten angezeigt haben; (z) Inkompatibilitäten, die von auf Ihrem Computer installierten Hardware- und/oder Softwarekomponenten verursacht wurden.
- 6.2 Sie erkennen an, akzeptieren und bestätigen, dass keine Software frei von Fehlern ist. Es wird empfohlen, den Computer mit der für Ihre Zwecke angemessenen Häufigkeit und Zuverlässigkeit zu sichern.
- 6.3 Bei Verletzungen der im Benutzerhandbuch bzw. in diesem Vertrag enthaltenen Bestimmungen gewährt der Rechteinhaber keine Garantie dafür, dass die Software korrekt funktioniert.
- 6.4 Wenn Sie die in Ziff. 2.6 des Vertrages geregelten Updates nicht regelmäßig herunterladen, übernimmt der Rechteinhaber keine Garantie dafür, dass die Software korrekt funktioniert.

- 6.5 Nach Ablauf des in den Ziff. 3.2 bzw. 3.3 dieses Vertrages geregelten Zeitraums sowie nach einer Beendigung der Lizenz zur Nutzung der Software aus anderen Gründen garantiert der Rechteinhaber keinen Schutz vor den im Benutzerhandbuch beschriebenen Gefahren.
- 6.6 DIE SOFTWARE WIRD GELIEFERT WIE BESEHEN. DER RECHTEINHABER GIBT HINSICHTLICH IHRER NUTZUNG ODER FUNKTION KEINE ZUSICHERUNG AB UND LEISTET KEINE GEWÄHR. GARANTIEEN SOWIE ENTSPRECHENDE BEDINGUNGEN, ZUSICHERUNGEN ODER BESTIMMUNGEN WERDEN DURCH DEN RECHTEINHABER UND SEINE PARTNER AUSGESCHLOSSEN BZW. BESCHRÄNKT, SOWEIT DIES GESETZLICH MÖGLICH IST; SIE WERDEN WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND BZW. DURCH GESETZ, GEWOHNHEITSRECHT, (HANDELS-)BRAUCH ODER AUF ANDERE WEISE ABGEGEBEN. DIES GILT INSBESONDERE FÜR DIE BEACHTUNG VON RECHTEN DRITTER, DIE VERKEHRSFÄHIGKEIT, EINE ZUFRIEDENSTELLENDENDE QUALITÄT, DIE INTEGRATIONSFÄHIGKEIT SOWIE DIE VERWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK. NEBEN DER GEFAHR VON MÄNGELN TRAGEN SIE DAS GESAMTE RISIKO IM HINBLICK AUF DIE FUNKTION DER SOFTWARE. AUSSERDEM SIND SIE VERANTWORTLICH FÜR DIE AUSWAHL DER SOFTWARE IM HINBLICK AUF DIE GEEIGNETHEIT ZUR ERREICHUNG IHRER ZWECKE SOWIE FÜR DIE INSTALLATION, DIE NUTZUNG UND DIE AUS DER SOFTWARE ERZIELTEN ERGEBNISSE. UNBESCHADET DER VORANGEGANGENEN BESTIMMUNGEN GIBT DER RECHTEINHABER KEINE ZUSICHERUNG AB UND LEISTET KEINE GEWÄHR DAFÜR, DASS DIE SOFTWARE FEHLER- UND UNTERBRECHUNGSFREI ARBEITET UND SONST FREI VON MÄNGELN IST ODER DASS DIE SOFTWARE IHRE ANFORDERUNGEN GANZ ODER TEILWEISE ERFÜLLT, SEIEN SIE DEM RECHTEINHABER BEKANNTGEGEBEN ODER NICHT.

7. Ausschluss und Beschränkung der Haftung

SOWEIT GESETZLICH ZULÄSSIG, LEISTEN DER RECHTEINHABER UND SEINE PARTNER KEINEN ERSATZ FÜR KONKRETE SCHÄDEN, EVENTUALSCHÄDEN, STRAFSCHADENSERSATZBETRÄGE, MITTELBARE SCHÄDEN ODER FOLGESCHÄDEN ALLER ART (INSBESONDERE FÜR ENTGANGENEN GEWINN SOWIE FÜR DEN VERLUST VERTRAULICHER ODER SONSTIGER DATEN, FÜR GESCHÄFTSUNTERBRECHUNGEN, FÜR DIE VERLETZUNG DER PRIVATSPHÄRE, FÜR DIE VERFÄLSCHUNG, BESCHÄDIGUNG UND DEN VERLUST VON DATEN ODER PROGRAMMEN, FÜR DIE NICHTERFÜLLUNG VON PFLICHTEN WIE ETWA GESETZLICHER VERPFLICHTUNGEN, TREUEPFLICHTEN ODER SORGFALTSPFLICHTEN, FÜR FAHRLÄSSIGKEIT, FÜR WIRTSCHAFTLICHE VERLUSTE SOWIE FÜR

ANDERE MATERIELLE ODER SONSTIGE VERLUSTE ALLER ART), DIE IM ZUSAMMENHANG MIT ODER AUFGRUND EINES DER FOLGENDEN UMSTÄNDE ENTSTEHEN: VERWENDUNG ODER UNMÖGLICHKEIT DER VERWENDUNG DER SOFTWARE, GEWÄHRUNG ODER VERSAGUNG VON SUPPORT- UND SONSTIGEN LEISTUNGEN, BEREITSTELLUNG VON DATEN SOWIE VON SOFTWARE- UND ÄHNLICHEN INHALTEN DURCH DIE SOFTWARE ODER ANLÄSSLICH IHRER NUTZUNG SOWIE SONST IM ZUSAMMENHANG MIT DER DURCHFÜHRUNG DIESES VERTRAGES, VERTRAGSVERLETZUNG ODER UNERLAUBTE HANDLUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT, ARGLIST UND VERSCHULDENSUNABHÄNGIGER HAFTUNG), VERLETZUNG GESETZLICHER PFLICHTEN ODER GEWÄHRLEISTUNGSVERLETZUNG DURCH DEN RECHTEINHABER ODER SEINE PARTNER; UND ZWAR AUCH DANN NICHT, WENN DER RECHTEINHABER ODER SEINE PARTNER AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDEN.

SIE ERKLÄREN SICH DAMIT EINVERSTANDEN, DASS BEI ANSPRÜCHEN GEGEN DEN RECHTEINHABER UND/ODER SEINE PARTNER DIE HAFTUNG DES RECHTEINHABERS UND/ODER SEINER PARTNER AUF DEN BETRAG DER FÜR DIE SOFTWARE AUFGEWANDTEN KOSTEN BEGRENZT IST. IN KEINEM FALL ÜBERSTEIGT DIE HAFTUNG DES RECHTEINHABERS UND/ODER SEINER PARTNER DIE FÜR DIE SOFTWARE AN DEN RECHTEINHABER BZW. AN SEINE PARTNER GEZAHLTEN GEBÜHREN.

ANSPRÜCHE AUFGRUND DER TÖTUNG ODER VERLETZUNG EINER PERSON WERDEN DURCH DIESEN VERTRAG WEDER AUSGESCHLOSSEN NOCH EINGESCHRÄNKT. IST EIN AUSSCHLUSS ODER EINE BESCHRÄNKUNG DER HAFTUNG DURCH DIESEN VERTRAG NACH DEN JEWEILS GELTENDEN GESETZEN IM EINZELFALL NICHT ZULÄSSIG, GILT DER AUSSCHLUSS ODER DIE BESCHRÄNKUNG DER HAFTUNG NUR FÜR DIESEN FALL NICHT. DIE ÜBRIGEN HAFTUNGSAUSSCHLÜSSE UND - BESCHRÄNKUNGEN GELTEN WEITERHIN.

8. GNU und sonstige Lizenzen Dritter

Die Software kann Software-Programme enthalten, für die der Nutzer eine (Unter-) Lizenz gemäß der GNU General Public License (GPL) bzw. ähnliche kostenlose Software-Lizenzen erhalten hat, die den Nutzer unter anderem dazu berechtigen, bestimmte Programme oder Teile davon zu kopieren, zu ändern und weiterzugeben und die den Zugang zum Quellcode gestatten („Open Source Software“). Sofern diese Lizenzen erfordern, dass der Quellcode für eine in einem ausführbaren, binären Format weitergegebene Software dem Nutzer ebenfalls zugänglich gemacht wird, wird der Quellcode nach einer entsprechenden Anforderung an source@kaspersky.com zur Verfügung gestellt bzw. mit der Software geliefert. Erfordern Lizenzen für Open Source Software,

dass der Rechteinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms gewährt, die weiter gehen als die in diesem Vertrag gewährten Rechte, haben jene Rechte Vorrang vor den in diesem Vertrag enthaltenen Rechten und Beschränkungen.

9. Geistiges Eigentum

- 9.1 Sie erkennen an, dass die Software, die Urheberschaft, Systeme, Ideen, Handhabungsmethoden, Dokumentationen und sonstige in der Software enthaltene Daten geistiges Eigentum und/oder wertvolle Geschäftsgeheimnisse des Rechteinhabers oder seiner Partner sind und der Rechteinhaber bzw. seine Partner durch Zivil- und Strafgesetze sowie durch internationale Verträge ebenso geschützt werden wie durch die Gesetze der Russischen Föderation, der Europäischen Union, der Vereinigten Staaten und anderer Länder über Urheberrechte, Geschäftsgeheimnisse, Warenzeichen und Patente. Dieser Vertrag verleiht Ihnen keine Rechte an geistigem Eigentum einschließlich der Waren- und Dienstleistungszeichen des Rechteinhabers und/oder seiner Partner („Warenzeichen“). Sie dürfen die Warenzeichen nur zur Kennzeichnung von durch die Software erstellten Ausdrucken gemäß anerkannter Warenzeichenpraxis nutzen. Hierzu zählt auch die Kennzeichnung mit dem Namen des Warenzeicheninhabers. Die derartige Nutzung eines Warenzeichens gewährt Ihnen kein Eigentumsrecht an diesem Warenzeichen. Der Rechteinhaber und/oder seine Partner besitzen und behalten alle Rechte, Ansprüche und Anteile an der Software, insbesondere in Bezug auf Fehlerbehebung, Verbesserungen, Updates und sonstige Änderungen der Software durch den Rechteinhaber oder Dritte sowie sämtliche Urheberrechte, Patente, Geschäftsgeheimnisse, Warenzeichen und sonstige geistigen Eigentumsrechte nach diesem Vertrag. Durch Besitz, Installierung und Nutzung der Software haben Sie keinen Anspruch auf das geistige Eigentum an der Software. Sie erwerben nur die in diesem Vertrag ausdrücklich festgelegten Rechte an der Software. Alle gemäß diesem Vertrag gefertigten Kopien der Software müssen Eigentumsangaben enthalten, die den auf und in der Software erkennbaren Angaben entsprechen. Dieser Vertrag gewährt Ihnen keine anderen als die vertraglich genannten geistigen Eigentumsrechte an der Software. Sie erkennen an, dass Ihnen die vertraglich erteilte Lizenz, wie unten näher erläutert, lediglich ein begrenztes Nutzungsrecht gemäß den Bedingungen dieses Vertrages verleiht. Rechte, die Ihnen nicht ausdrücklich durch diesen Vertrag verliehen werden, behält sich der Rechteinhaber vor.
- 9.2 Sie erkennen an, dass der Quellcode, der Aktivierungscode und/oder die Lizenzschlüsseldatei Eigentum des Rechteinhabers sind und Geschäftsgeheimnisse des Rechteinhabers darstellen. Sie verpflichten

sich, den Quellcode der Software keinesfalls zu verändern, anzupassen, zurückzuentwickeln, zu dekompileieren, zu disassemblieren oder auf sonstige Weise seine Entschlüsselung zu versuchen.

- 9.3 Sie verpflichten sich, die Software selbst in keiner Weise zu modifizieren oder zu ändern. Auf Kopien der Software angebrachte Urheberrechts- und sonstige Eigentumsangaben dürfen Sie nicht entfernen oder verändern.

10. Anwendbares Recht; Schiedsgerichtsbarkeit

Der vorliegende Vertrag unterliegt dem Recht der Russischen Föderation und ist nach diesem Recht auszulegen. Das Kollisionsrecht bleibt unberücksichtigt. Der Vertrag unterliegt nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf, dessen Geltung ausdrücklich ausgeschlossen wird. Für die Entscheidung von aus der Auslegung bzw. Anwendung von Bestimmungen dieses Vertrages oder deren Verletzung entstehenden Streitigkeiten, die nicht durch direkte Verhandlungen beigelegt werden können, ist das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation (Tribunal of International Commercial Arbitration at the Russian Federation Chamber of Commerce and Industry) in Moskau zuständig. Ein Schiedsspruch des Schiedsgerichts ist endgültig und für die Parteien bindend. Das Schiedsgerichtsurteil kann vor dem zuständigen Gericht durchgesetzt werden. Unbeschadet der Vorschriften dieses Abschnitts ist es jeder Partei gestattet, bei einem zuständigen Gericht vor, während oder nach dem Schiedsverfahren einen Rechtsbehelf aus Billigkeitsgründen einzulegen.

11. Frist für gerichtliche Geltendmachung

Ansprüche, die sich aus der Durchführung dieses Vertrages ergeben, sind spätestens ein (1) Jahr nach ihrer Entstehung bzw. Feststellung gerichtlich geltend zu machen. Für Klagen wegen einer Verletzung geistigen Eigentums gilt jedoch die gesetzliche Höchstfrist.

12. Vollständigkeit der Vereinbarung; salvatorische Klausel; Abdingbarkeit

Dieser Vertrag stellt die gesamte Vereinbarung zwischen Ihnen und dem Rechteinhaber dar. Er ersetzt alle früheren mündlichen oder schriftlichen Vereinbarungen, Angebote, Mitteilungen oder Anzeigen in Bezug auf die Software bzw. den Vertragsgegenstand.

Sie erklären, dass Sie den Vertrag gelesen haben, ihn verstehen und sich an seine Bestimmungen gebunden halten. Falls ein zuständiges Gericht eine

Bestimmung dieses Vertrages aus irgendeinem Grund ganz oder teilweise für ungültig, nichtig oder nicht durchsetzbar erachtet, ist der betreffenden Bestimmung durch engere Auslegung zu Rechtsgültigkeit und Durchsetzbarkeit zu verhelfen. Der Vertrag insgesamt wird hierdurch nicht gefährdet; vielmehr bleibt der Rest des Vertrages in vollem Umfang wirksam, soweit nach Gesetz oder Billigkeit zulässig. Der ursprüngliche Vertragszweck ist so weit wie möglich beizubehalten. Eine Bestimmung bzw. Klausel dieses Vertrages kann nur in schriftlicher Form durch ein von Ihnen und einem bevollmächtigten Vertreter des Rechteinhabers unterzeichnetes Dokument abbedungen werden. Sieht eine Partei davon ab, sich auf die Verletzung einer Bestimmung dieses Vertrags zu berufen, stellt dies keinen Verzicht auf die Geltendmachung früherer, gleichzeitiger oder späterer Vertragsverletzungen dar. Unterlässt es der Rechteinhaber, auf der strikten Durchführung einer Bestimmung dieses Vertrages oder auf der Durchsetzung eines Rechts zu bestehen, so gilt dies nicht als Verzicht auf die Geltendmachung der Bestimmung bzw. des Rechts.

13. Kontaktdaten

Haben Sie Fragen zu diesem Vertrag oder möchten Sie mit dem Rechteinhaber aus anderen Gründen in Kontakt treten, wenden Sie sich bitte an unsere Kundendienstabteilung:

Kaspersky Lab ZAO, 1 Volokolamsky Proezd, d. 10, str. 1
Moskau, 123060
Russische Föderation
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-Mail: info@kaspersky.com
Website: www.kaspersky.com

© 1997-2009 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Die Software ist mit der gesamten Begleitdokumentation durch Urheberrechtsgesetze und internationale Urheberrechtsverträge sowie andere Gesetze und Verträge zum Schutz geistigen Eigentums urheberrechtlich geschützt.