

KASPERSKY LAB

---

Kaspersky Anti-Virus<sup>®</sup> Mobile 6.0  
Enterprise Edition

**BENUTZERHANDBUCH**

KASPERSKY ANTI-VIRUS® MOBILE 6.0  
ENTERPRISE EDITION

---

# Benutzerhandbuch

© Kaspersky Lab  
Tel., Fax: +7 (495) 797-8700, +7 (495) 645-7939, +7 (495) 956-7000  
<http://www.kaspersky.com/de>

Redaktionsdatum: Oktober 2007

# Inhalt

KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION .....	4
1.1. Hardware- und Softwarevoraussetzungen .....	5
1.2. Lieferumfang .....	5
KAPITEL 2. KASPERSKY ANTI-VIRUS FÜR MICROSOFT WINDOWS MOBILE .....	6
2.1. Kaspersky Anti-Virus installieren .....	6
2.2. Arbeit mit dem Programm .....	10
2.2.1. Programm starten .....	10
2.2.2. Grafische Oberfläche .....	12
2.2.3. Antiviren-Untersuchung und Schutz .....	14
2.2.4. Isolieren in Quarantäne .....	20
2.2.5. Anti-Spam .....	22
2.2.6. Update der Anti-Virus-Datenbanken .....	26
2.2.7. Berichte im Programmablauf .....	28
2.3. Programm deinstallieren .....	29
KAPITEL 3. VERWALTUNG DES PROGRAMMS ÜBER KASPERSKY ADMINISTRATION KIT .....	33
3.1. Richtlinienverwaltung .....	35
3.1.1. Richtlinie erstellen .....	35
3.1.2. Richtlinienparameter anzeigen und bearbeiten .....	40
3.2. Programmeinstellungen verwalten .....	47
ANHANG A. KASPERSKY LAB .....	55
A.1. Andere Produkte von Kaspersky Lab .....	56
A.2. Kontaktinformationen .....	67
ANHANG B. ENDBENUTZER-LIZENZVERTRAG .....	69

---

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes 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 Anti-Virus**, die zur Suche nach schädlichen Programmen und zum Löschen von gefährlichen Objekten eingesetzt werden
- **Sperren von unerwünschten SMS-Nachrichten.**

Die Installation von Kaspersky Anti-Virus erfolgt nur mit Kaspersky Administration Kit, mit dem der Administrator die folgenden Aktionen mit Kaspersky Anti-Virus ausführen kann:

- Informationen über den Zustand des Schutzes beziehen
- Informationen über die zurzeit geltenden Programmparameter beziehen
- Konfiguration der Programmparameter mit Richtlinien ändern
- Informationen über wichtige Ereignisse beziehen.

Kaspersky Anti-Virus kann dabei **nicht** mit Kaspersky Administration Kit Folgendes tun:

- Updates der Anti-Virus-Datenbanken downloaden
- Gruppenaufgaben / Globale Aufgaben / lokale Aufgaben anlegen
- Lizenzschlüssel verlängern
- Remote-Deinstallation des Programms ausführen.

Im Programm wird ein Menüsystem umgesetzt und eine einfach zu bedienende Benutzeroberfläche bereitgestellt. Auf der Benutzeroberfläche lassen sich die Parameter von Kaspersky Anti-Virus steuern (deren Änderung nicht von einer Richtlinie unterbunden ist), der aktuelle Zustand des Antiviren-Schutzes sowie das Ereignisjournal anzeigen, in dem die Programmaktionen aufgezeichnet werden.

Sollte Kaspersky Anti-Virus 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 Anti-Virus wird auf mobilen Geräten installiert, die mit den folgenden Betriebssystemen arbeiten:

- Microsoft Windows Mobile 2003, 2003SE
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

## **1.2. Lieferumfang**

Kaspersky Anti-Virus Mobile Enterprise Edition kann über das Internet bezogen werden (Programm und Dokumentation in elektronischer Form). Außerdem wird Kaspersky Anti-Virus Mobile Enterprise Edition über die Niederlassungen der Mobilfunkbetreiber vertrieben. Nähere Informationen bekommen Sie bei Ihrem Mobilfunkbetreiber.

---

# KAPITEL 2. KASPERSKY ANTI-VIRUS FÜR MICROSOFT WINDOWS MOBILE

In diesem Kapitel wird die Funktionsweise von Kaspersky Anti-Virus Mobile Enterprise Edition für mobile Geräte beschrieben, die mit einem der folgenden Betriebssysteme laufen:

- Microsoft Windows Mobile 2003, 2003SE
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

## 2.1. Kaspersky Anti-Virus installieren

Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition wird im Remote-Betrieb mit Kaspersky Administration Kit installiert.

- Anlegen eines Installationspaketes, zu dem Distributionen der Software, die Installations-Utility, der Lizenzschlüssel, Konfigurationsdateien gehören
- Installation des Installationspaketes auf dem Remote-Computer. Dabei wird auf dem Computer die Installations-Utility gestartet, die auf eine Verbindung mit dem mobilen Gerät wartet.
- Installation von Kaspersky Anti-Virus auf dem mobilen Gerät beim Anschluss des Gerätes am Computer.

*Um Kaspersky Anti-Virus Mobile Enterprise Edition zu installieren, machen Sie Folgendes:*

1. Legen Sie in der Konsolenstruktur im Ordner **Remote-Installation** (s. Abb. 1) ein Installationspaket an, das für die Remote-Installation des Programms auf dem mobilen Gerät verwendet wird.

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden

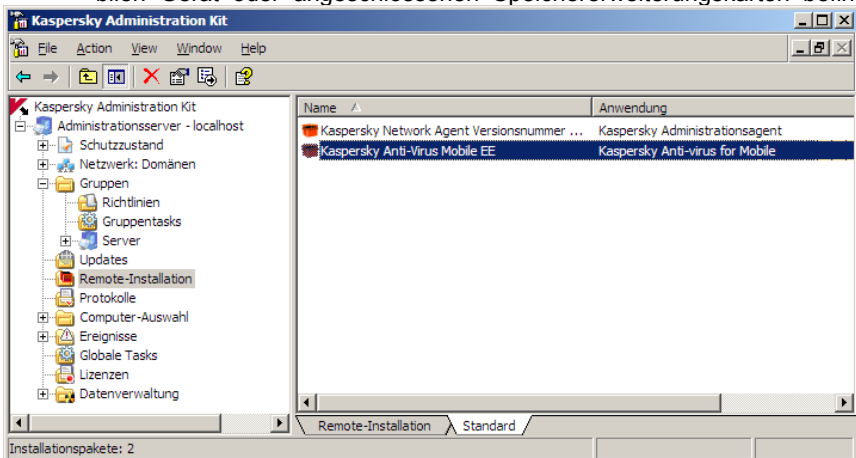


Abbildung 1. Installationspaket auswählen

Details zum Anlegen von Installationspaketen und deren Bearbeiten finden Sie im Benutzerhandbuch von Kaspersky Administration Kit.

2. Öffnen Sie das Kontextmenü für das markierte Paket und gehen Sie auf den Eintrag **Installieren**.

Die Installation des Installationspaketes erfolgt mit einem Assistenten für Microsoft Windows (Windows Wizard) und besteht aus einer Reihenfolge von Fenstern (Schritten), zwischen denen mit den Schaltflächen **Zurück** und **Weiter** navigiert werden kann. Der Assistent wird mit der Schaltfläche **Fertig** beendet. Den Assistenten können Sie an einer beliebigen Stelle mit der Schaltfläche **Abbrechen** unterbrechen.

### **Achtung!**

Zum Installationspaket gehört ein Lizenzschlüssel, der zusammen mit dem Paket auf dem mobilen Gerät installiert wird. Wenn im Installationspaket kein Lizenzschlüssel enthalten ist, wird das Programm auf dem Gerät als nicht aktiviert behandelt und funktioniert nicht.

Die Installation des Lizenzschlüssels auf einem anderen Weg wird nicht unterstützt!

3. Aufgrund der durchlaufenen Aktionen auf dem ausgewählten Computer oder Computergruppe wird die Utility **KAV Mobile EE Installer** installiert, mit deren Hilfe die weitere Installation von Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition erfolgt.
4. Verbindet sich das mobile Gerät mit dem Computer, schlägt **KAV Mobile EE Installer** dem Benutzer vor, Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition (s. Abb. 2) zu installieren.

### **Achtung!**

Damit Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition auf dem mobilen Gerät installiert wird, muss Microsoft Active Sync verwendet werden, sonst kann die Utility **KAV Mobile EE Installer** das angeschlossene Gerät nicht erkennen.

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden

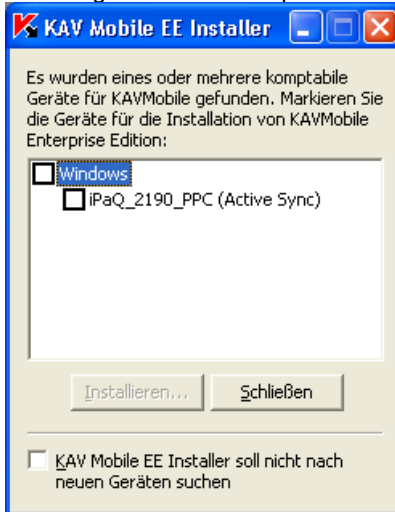


Abbildung 2. Mobiles Gerät auswählen

5. Markieren Sie das Gerät in der Liste und klicken Sie dann auf **Installieren**. Auf dem markierten mobilen Gerät beginnt die Installation von Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition.
6. Bitte lesen Sie sich auf dem mobilen Gerät die Lizenzvereinbarung durch. Wenn Sie den Punkten in der Vereinbarung zustimmen, klicken Sie auf **OK**. Um die Installation abzubrechen, klicken Sie auf **Abbrechen** (s. Abb. 3)<sup>1</sup>.



Abbildung 3. Lizenzvereinbarung

## 2.2. Arbeit mit dem Programm

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

### 2.2.1. Programm starten

*Um Kaspersky Anti-Virus Mobile Enterprise Edition zu starten, machen Sie Folgendes:*


1. Öffnen Sie auf dem mobilen Gerät das Menü **Programme**.

---

<sup>1</sup> An dieser und an weiteren Stellen in der Dokumentation befinden sich Screenshots, die auf dem Smartphone I-mate K-JAM hergestellt wurden. Die Darstellung kann sich bei anderen Modellen erheblich davon unterscheiden.

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION


**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden.
- 2. Gehen Sie auf das Symbol  **KAV Mobile**, um das Programm zu starten.

Beim ersten Start des Programms erscheint auf dem Display des mobilen Gerätes das Fenster für den Status der Basiskomponenten von Kaspersky Anti-Virus (s. Abb. 4):

- **Echtzeitschutz ist** – Verwenden des Modus Echtzeitschutz. Details s. Pkt. 2.2.3 auf S. 14.
- **Letzter vollst. Scan** – Datum für die letzte Antiviren-Untersuchung des Smartphones
- **Signaturen von** – Erstellungsdatum der von Kaspersky Anti-Virus verwendeten Antiviren-Datenbanken

**Achtung!**

Wenn das mobile Gerät nicht auf Viren untersucht worden ist / 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.

- **Anti-Spam ist** – Status des Anti-Spam-Moduls zum Filtern von SMS-Nachrichten

**Achtung!**

Auf dem PDA gibt es kein Anti-Spam!



Abbildung 4. Fenster Status der Programmkomponenten

## 2.2.2. Grafische Oberfläche

Die grafische Programmoberfläche besteht aus fünf Registerkarten, auf die Sie mit **Menü** zugreifen können (s. Abb. 6):

- Auf der Registerkarte **Untersuchung** können die Antiviren-Untersuchung des mobilen Gerätes eingestellt, die Parameter für die Antiviren-Untersuchung und der Modus Echtzeitschutz bearbeitet und ein Zeitplan für den Start einer automatischen Untersuchung konfiguriert werden.
- Auf der Registerkarte **Anti-Spam** können Sie das Filtern von eingehenden SMS- und MMS-Nachrichten einstellen.

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden
- 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.
- Auf der Registerkarte **Quarantäne** können Sie die Quarantäne verwalten, eine spezielle Ablage für infizierte und verdächtige Objekte.
- Auf der Registerkarte **Info** können das Ereignisjournal für die Programmkomponenten, allgemeine Informationen zum Programm und der verwendeten Datenbanken angezeigt sowie die allgemeinen Parameter für die Programmfunktionen bearbeitet werden.



Abbildung 6. Menü Programme

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

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

## 2.2.3. Antiviren-Untersuchung und Schutz

Auf der Registerkarte **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 des Modus Echtzeitschutz ändern, das Protokoll über die Untersuchungsergebnisse anzeigen und einen Zeitplan für den automatischen Start einer Untersuchung einrichten.

### 2.2.3.1. Echtzeitschutz und Scan auf Befehl

Der Echtzeitschutz ist ein Modus, bei dem sich ein residenter Teil von Kaspersky Anti-Virus dauerhaft im Arbeitsspeicher des mobilen Gerätes einnistet und alle Daten des Gerätes kontrolliert.

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

Außerdem kann Kaspersky Anti-Virus das Dateisystem des mobilen Gerätes komplett untersuchen.

Die Ergebnisse des Echtzeitschutzes und des Scan auf Befehls werden in einen Bericht eingetragen. Zum Anzeigen des Berichtes müssen Sie den Eintrag **Un-**

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden. Wählen Sie den Bericht **Untersuchungsbericht**. Außerdem erreichen Sie den Bericht auf der Registerkarte **Informationen** (s. Pkt. 2.2.7 auf S. 28).

*Um den Echtzeitschutz zu starten, machen Sie Folgendes:*

1. Auf der Registerkarte **Untersuchung** gehen Sie auf **Unters. konfig.**
2. Aktivieren / Deaktivieren Sie den Echtzeitschutz, indem Sie den entsprechenden Wert **Echtzeitschutz** setzen.

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

1. Auf der Registerkarte **Untersuchung** gehen Sie auf **Unters. Konfig.**
2. Geben Sie im Block **Unters. Konfig.** den Untersuchungsbereich ein, indem Sie die Dateitypen markieren, die untersucht werden sollen:
  - **Archive untersuchen** – Dateien untersuchen, die als Archiv gepackt sind
  - **Nur ausführbare** – Untersucht werden nur ausführbare Programmdateien.

3. Wählen Sie die Aktion aus, die bei Entdecken eines infizierten Objektes im Block **Bei Erkennung** ausgeführt werden soll. Damit Kaspersky Anti-Virus versucht, ein erkanntes infiziertes Objekt zu desinfizieren, setzen Sie das Häkchen in **Desinfektionsversuch**. Wenn das Objekt nicht desinfiziert werden muss, wählen Sie eine mögliche Aktion des Anti-Virus, indem Sie für den Parameter **Wenn irreparabel** einen der folgenden Werte:

- **Quarantäne** – Die erkannten infizierten Objekte werden in die Quarantäne verschoben.
- **Benutzer fragen** – 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.

Außerdem können Sie eine der angeführten Aktionen für den Fall vorgeben, wenn der Desinfektionsversuch für ein infiziertes Objekt nicht gelungen ist. Setzen Sie dazu das Häkchen in **Desinfektionsversuch** und markieren Sie die gewünschte Aktion in der Liste **Wenn irreparabel**.

*Um eine Antiviren-Untersuchung zu starten, machen Sie Folgendes:*

1. Starten Sie Kaspersky Anti-Virus (s. Pkt. 2.2.1 auf S. 10).
2. Wechseln Sie zur Registerkarte **Unters. konfig.**
  - Geben Sie im Block **Unters. Konfig.** den Untersuchungsbereich ein, indem Sie die Dateitypen markieren, die untersucht werden sollen (s. oben).
  - Wählen Sie die Aktion aus, die bei Entdecken eines infizierten Objektes ausgeführt werden soll (s. oben).
3. Auf der Registerkarte **Untersuchung** (s. Abb. 7) wählen Sie den Punkt **Alle Untersuchungen**, wenn Sie das gesamte Dateisystem des mobilen Gerätes untersuchen wollen, oder **Ordner untersuchen**, wenn Sie einen einzelnen Ordner untersuchen wollen.

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden



Abbildung 7. Registerkarte **Untersuchung**

Sollten Sie sich für den Punkt **Ordner untersuchen** entschieden haben, gelangen Sie in das Fenster, das das Dateisystem des mobilen Gerätes darstellt. Um die Untersuchung eines Ordners zu starten, setzen Sie den Cursor auf den Ordner und gehen auf **Untersuchen**.

Nachdem die Untersuchung begonnen hat, öffnet sich das Untersuchungsfenster, in dem der aktuelle Status angezeigt wird: Anzahl der untersuchten Objekte und Pfad zum Objekt, das gerade untersucht wird (s. Abb. 8).

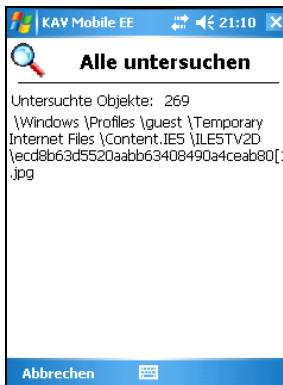


Abbildung 8. Fenster Untersuchungsfenster



Abbildung 9. Meldung eines erkannten Virus

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

## 2.2.3.2. Untersuchung nach Zeitplan

Mit Kaspersky Anti-Virus kann der Benutzer einen Zeitplan für die automatische Antiviren-Untersuchung des mobilen Gerätes erstellen. Die Untersuchung erfolgt im Hintergrund. Wenn ein infiziertes Objekt erkannt wird, wird die Aktion ausge-

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem Microsoft Windows Mobile vor schädlichen Programmen und unerwünschten Nachrichten und übernimmt die folgenden Funktionen:

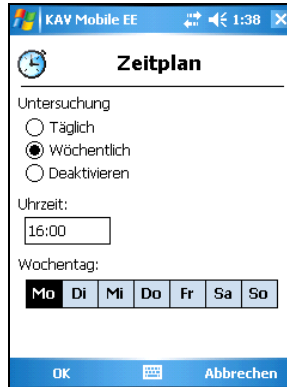
- **Echtzeitschutz** für das Dateisystem des Gerätes – Abfangen und Untersuchen:
  - aller eingehenden Objekte, die über drahtlose Verbindungen empfangen werden (Infrarot-Port, Bluetooth), EMS- und MMS-Nachrichten, bei der Synchronisierung mit dem Personalcomputer und beim Aufrufen von Dateien über den Browser
  - Dateien, die sich auf dem mobilen Gerät öffnen lassen
  - Programme, die sich auf der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befindet, die in den Untersuchungseinstellungen vorgegeben wurde (Punkt **Unters. Konfig.**).

Die Untersuchung nach Zeitplan ist standardmäßig deaktiviert.

*Um eine Untersuchung nach Zeitplan einzurichten, machen Sie Folgendes:*

Auf der Registerkarte **Untersuchung** gehen Sie auf den Punkt **Zeitplan** und richten die Untersuchungsparameter ein (s. Abb. 10):

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

Abbildung 10. Menü **Zeitplan**

## 2.2.4. Isolieren in Quarantäne

Infizierte Objekte, die in die Quarantäne verschoben worden sind, bedrohen nicht mehr die Sicherheit Ihres 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.

Damit die Anwendung bei einer Antiviren-Untersuchung automatisch infizierten Objekte in die Quarantäne verschiebt, wechseln Sie zur Registerkarte **Untersuchung**, wählen Sie den Punkt **Unters. Konfig.** und setzen Sie im Block **Bei Erkennung** für den Parameter **Basisaktion** den Wert **Quarantäne**. Für den Fall, dass das infizierte Objekt nicht desinfiziert werden konnte, setzen Sie dazu das Häkchen in **Desinfektionsversuch** und gehen Sie in der Liste **Wenn irreparabel** auf **In Quarantäne**.

Wenn Sie als Aktion **Benutzer fragen** angegeben haben, schlägt Ihnen Kaspersky Anti-Virus beim Erkennen eines infizierten Objektes vor, das Objekt zu löschen oder es in die Quarantäne zu verschieben.

Den Inhalt der Quarantäne zeigen Sie an, indem Sie zur Registerkarte **Quarantäne** wechseln (s. Abb. 12).

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden

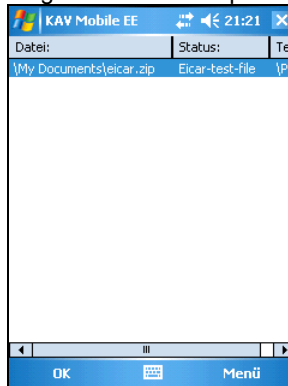


Abbildung 12. Quarantäne

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**)
- Datei auf Viren untersuchen, die in die Quarantäne verschoben wurde (Punkt **Untersuchen**)
- Aktuelles Objekt löschen (Punkt **Löschen**)
- Objekt desinfizieren, das in die Quarantäne verschoben wurde (Punkt **Desinfizieren**)
- Aktuelles Objekt aus Quarantäne in ursprüngliches Verzeichnis wiederherstellen (Punkt **Wiederherstellen**)
- Quarantäne leeren, indem der gesamte Inhalt mit den Objekten gelöscht wird (Punkt **Alle löschen**)

## 2.2.5. Anti-Spam

Eine weitere Funktion, die in Kaspersky Anti-Virus Mobile 6.0 neu ist, ist Anti-Spam, um Ihr mobiles Gerät vor unerwünschten SMS-Nachrichten zu schützen.

### **Achtung!**

**Auf dem PDA gibt es kein Anti-Spam!**

Das Filter-Prinzip für Nachrichten beruht auf der Verwendung einer so genannten „schwarzen“ und „weißen“ Liste. Nachrichten, die von Telefonnummern eingehen, die auf einer „Schwarzen“ Liste stehen, werden von Anti-Spam gesperrt. Nachrichten von Telefonnummern, die auf einer „weißen“ Liste stehen, werden nicht gesperrt.

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

1. Auf der Registerkarte **Anti-Spam** gehen Sie auf **Einstellungen**.
2. Aktivieren / Deaktivieren Sie Anti-Spam, indem Sie das Häkchen in **Anti-Spam aktivieren** setzen oder entfernen.
3. Geben Sie an, ob der Empfang von SMS-Nachrichten von Nummern zugelassen werden soll, die in keiner Liste stehen. Entfernen oder setzen Sie das Häkchen in **Empfange SMS von: Sender Unbekannt**.
4. Geben Sie an, ob der Empfang von SMS-Nachrichten von Nummern zugelassen werden soll, die in keiner Liste stehen. Entfernen oder setzen Sie dazu das Häkchen in **Empfange SMS von: meiner Kontaktliste**.

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden

## 2.2.5.1. „Schwarze“ und „Weiße“ Liste bearbeiten

Die „Schwarze“ Liste enthält Telefonnummern, von denen der Empfang von SMS-Nachrichten durch Anti-Spam gesperrt wird.

Die „Weiße“ Liste enthält Telefonnummern, von denen der Empfang von SMS-Nachrichten zugelassen ist.

Um die „schwarze“ oder „weiße“ Liste zu bearbeiten, wechseln Sie auf die Registerkarte **Anti-Spam** (s. Abb. 13) und gehen Sie auf die entsprechende Liste.



Abbildung 13. Menü **Anti-Spam**

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, die Sie in die Liste aufnehmen wollen. Die Nummer kann mit einer Ziffer oder dem Zeichen „+“ beginnen und darf nur Ziffern enthalten.

Zum Bearbeiten der Liste klicken Sie auf **OK**, um zur Registerkarte **Anti-Spam** zurückzukehren.

## 2.2.5.2. Aktionen für Nachrichten

Geht eine SMS- Nachricht von einer Telefonnummer ein, die nicht in der „schwarzen“ oder „weißen“ Liste steht, vorausgesetzt, dass in den Anti-Spam-Einstellungen der Nachrichten-Empfang von unbekanntem Nummern zugelassen ist (s. Abb. 2.2.5 auf S. 22), erscheint im Display des mobilen Gerätes eine Warnmeldung (s. Abb. 14).

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden

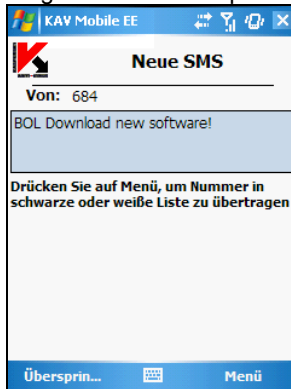


Abbildung 14. Anti-Spam warnt

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 **Nachricht überspringen**, um den Empfang der Nachricht zuzulassen. Die Telefonnummer des Absenders wird in keine Liste gespeichert.

Die Daten über gesperrte Nachrichten werden in das Journal eingetragen. Um das Journal anzuzeigen, klicken Sie auf der Registerkarte **Anti-Spam** auf **Bericht** oder auf der gleichen Registerkarte gehen Sie auf den Punkt **Anti-Spam-Bericht**. Außerdem erreichen Sie den Bericht auf der Registerkarte **Informationen** (s. Pkt. 2.2.7 auf S. 28).

## 2.2.6. Update der Anti-Virus-Datenbanken

Nach schädlichen Programmen wird mithilfe von Einträgen in einer Datenbank von Kaspersky Anti-Virus 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 und Starten eines Updates dient die Registerkarte **Update** (s. Abb. 15). Das Update erfolgt über das Internet von den Kaspersky-Lab-Servern.

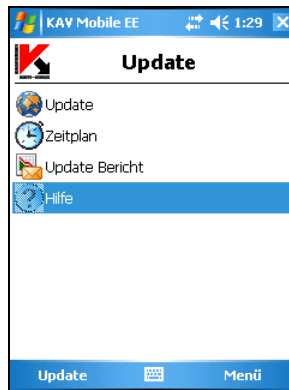


Abbildung 15. Registerkarte **Update**

Der Update-Vorgang der Datenbanken wird in das Journal eingetragen. Um das Journal anzuzeigen, gehen Sie auf der Registerkarte **Update** auf den Punkt **Update Bericht**. Außerdem erreichen Sie den Bericht auf der Registerkarte **Info** (s. Pkt. 2.2.7 auf S. 28).

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden

*Um manuell das Update der Anti-Virus-Datenbanken von den Update-Servern bei Kaspersky Lab zu starten, machen Sie Folgendes:*

1. Starten Sie Kaspersky Anti-Virus (s. Pkt. 2.2.1 auf S. 10) und wechseln Sie zur Registerkarte **Update**.
2. Gehen Sie auf **Update**, um den Update-Download zu starten.

*Um einen Zeitplan für das automatische Update der Anti-Virus-Datenbanken einzurichten, machen Sie Folgendes:*

1. Starten Sie Kaspersky Anti-Virus (s. Pkt. 2.2.1 auf S. 10) und wechseln Sie zur Registerkarte **Update**.
2. Wählen Sie **Zeitplan** aus, um zur Bearbeitung der Parameter für einen Zeitplan Automatisches Update zu wechseln.
3. Geben Sie den Update-Intervall als Wert für den Update-Parameter ein:
  - **Täglich** – Untersuchung erfolgt jeden Tag. Geben Sie zusätzlich die **Uhrzeit** des Updates vor.
  - **Wöchentlich** – Untersuchung erfolgt einmal pro Woche. Geben Sie zusätzlich den **Tag** und die **Uhrzeit** des Updates ein.

- **Deaktivieren** – Der Benutzer ruft die Untersuchung allein auf.

Auf der Registerkarte **Informationen** können Sie das Erstellungsdatum für die Anti-Virus-Datenbanken erfahren, die in Ihrem mobilen Gerät installiert sind, sowie die Summe der Virussignaturen. Gehen Sie dazu auf der Registerkarte auf den Punkt **Datenbank-Info**.

## 2.2.7. Berichte im Programmablauf

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

- Antiviren-Untersuchung
- Anti-Spam
- Update der Anti-Virus-Datenbanken.

*Um beispielsweise einen Bericht über eine Antiviren-Untersuchung anzusehen, machen Sie Folgendes:*

1. Starten Sie Kaspersky Anti-Virus (s. Pkt. 2.2.1 auf S. 10).
2. Auf der Registerkarte **Info** gehen Sie auf den Punkt **Berichte** (s. Abb. 16).
3. Im nächsten Fenster markieren Sie den Bericht für den Echtzeitschutz .



Abbildung 16. Registerkarte **Berichte**

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden.

## 2.3. Programm deinstallieren

Um Kaspersky Anti-Virus zu deinstallieren, machen Sie Folgendes:

1. Deaktivieren Sie den Echtzeitschutz (Details s. Pkt. 2.2.3 auf S. 14).

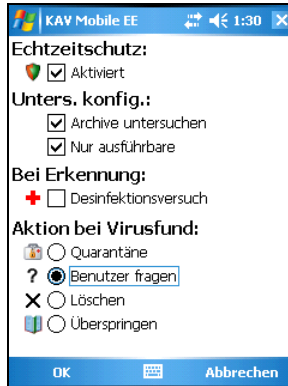


Abbildung 17. Echtzeitschutz deaktivieren

2. Schließen Sie Kaspersky Anti-Virus. Gehen Sie dazu im Menü auf den Punkt **Beenden** (s. Abb. 18).

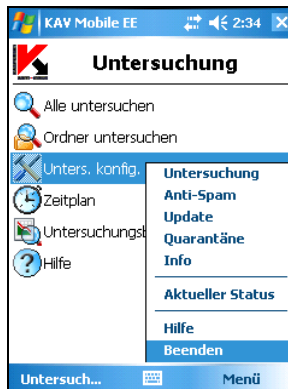


Abbildung 18. Programm beenden

3. Deinstallieren Sie das Programm. Machen Sie dazu Folgendes:
  - Klicken Sie auf die Schaltfläche **Start**, gehen Sie auf das Menü **Einstellungen** und dann auf **Programm entfernen** (s. Abb. 19):

# KAPITEL 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

**Kaspersky Anti-Virus® Mobile 6.0 Enterprise Edition** (im Weiteren auch **Kaspersky Anti-Virus**) dient zum Schutz von mobilen Geräten mit dem Betriebssystem 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- und MMS-Nachrichten, 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 der Oberfläche des Gerätes installieren lassen.
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden

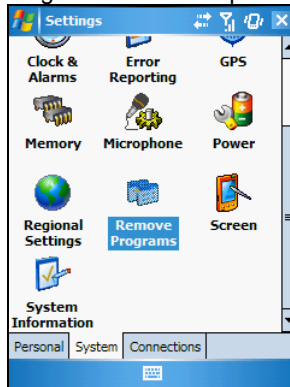


Abbildung 19. Programm-Deinstallation aufrufen

- In der Liste der installierten Programme gehen Sie auf **KAV Mobile** und klicken auf die Schaltfläche **Deinstallieren** (s. Abb. 20).

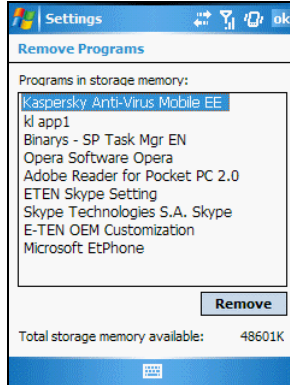


Abbildung 20. Programme auswählen

- Bei der Bestätigungsabfrage für die Programm-Deinstallation klicken Sie auf die Schaltfläche **Ja** (s. Abb. 21).

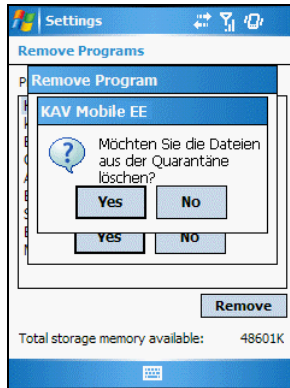


Abbildung 21. Bestätigungsabfrage für Programm-Deinstallation

---

# KAPITEL 3. VERWALTUNG DES PROGRAMMS ÜBER KASPERSKY ADMINISTRATION KIT

**Kaspersky Administration Kit** ist ein Programm für die wichtigsten administrativen Aufgaben zur Verwaltung der Sicherheit von mobilen Geräten.

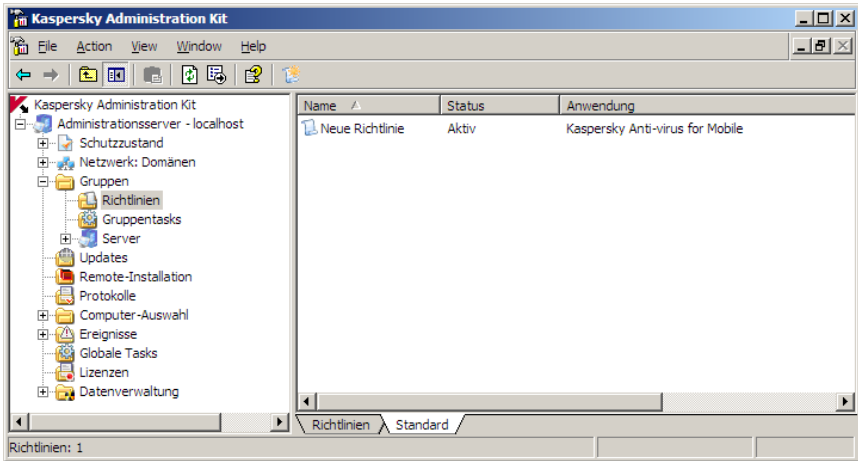


Abbildung 22. Administrationskonsole von Kaspersky Administration Kit

Bei einer zentralen Verwaltung über Kaspersky Administration Kit bestimmt der Administrator die Richtlinien und Anwendungen. Der Schutz beruht auf diesen Einstellungen.

Eine Besonderheit für die zentrale Verwaltung ist die Organisation von mobilen Geräten in Gruppen und die Verwaltung der Einstellungen über die Erstellung und Einstellung von Gruppenrichtlinien.

Eine **Richtlinie** ist eine Sammlung von Parameter für Kaspersky Anti-Virus für eine Gruppe eines logischen Netzwerkes. Die Richtlinie kann die Programmfunktionen steuern, da in ihr viele Einstellungen von Kaspersky Anti-Virus gespeichert sind.

Zu einer Richtlinie können auch mehrere Einschränkungen für die Änderung von eingegebenen Parametern bei der Programmeinstellung gehören. Diese Einschränkungen werden aus der Schnittstelle von Kaspersky Administration Kit geregelt, wenn der Benutzer die Administratorenrechte hat.

### Hinweis

Zum Verschieben des mobilen Gerätes in die Administrationsgruppe öffnen Sie die **Administrationskonsole**, wechseln Sie in den Container **Netzwerk** und konfigurieren Sie ihn in der Domänenanzeige. Nach der Anti-Virus-Installation werden bei einer Netzabfrage solche mobilen Geräte in die Gruppe **PDAGroup** verschoben.

Damit Kaspersky Administration Kit mobile Geräte immer erkennt, setzen Sie in den Eigenschaften des Administrationservers auf der Registerkarte **Einstellungen** das Häkchen in **Port für Handheld-Geräte öffnen**.

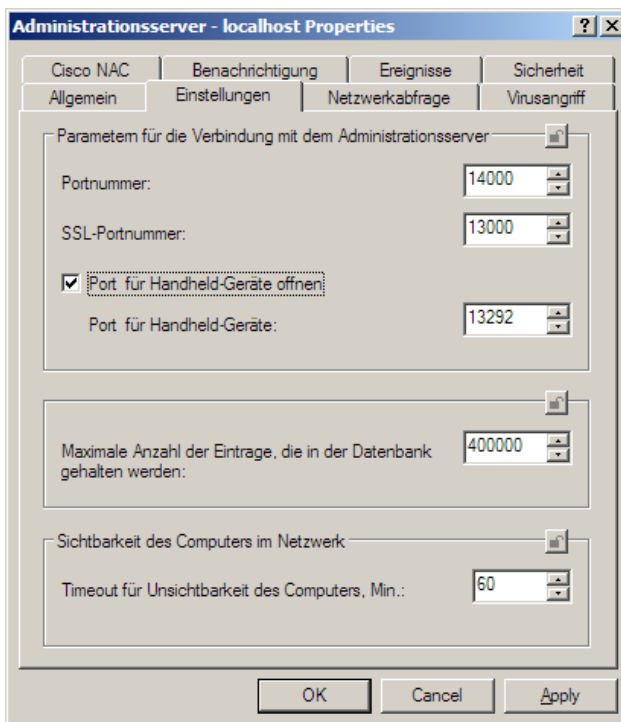


Abbildung 23. Registerkarte **Einstellungen**

## 3.1. Richtlinienverwaltung

In diesem Abschnitt stehen Informationen über die Anlage und Einstellung einer Richtlinie für Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition.


### 3.1.1. Richtlinie erstellen

Um eine Richtlinie zu erstellen, führen Sie folgende Aktionen durch:

1. Markieren Sie die Gruppe derjenigen mobilen Geräte, für die eine Richtlinie erstellt werden muss, in der Konsolenstruktur im Ordner **Gruppen**.
2. Markieren Sie den zur ausgewählten Gruppe gehörenden Ordner **Richtlinien**, öffnen Sie mit das Kontextmenü und gehen Sie auf **Richtlinie erstellen**→.

Die Anlage einer Richtlinie erfolgt mit einem Assistenten für Microsoft Windows (Windows Wizard) und besteht aus einer Reihenfolge von Fenstern (Schritten), zwischen denen mit den Schaltflächen **Zurück** und **Weiter** navigiert werden kann. Der Assistent wird mit der Schaltfläche **Fertig** beendet. Den Assistenten können Sie an einer beliebigen Stelle mit der Schaltfläche **Abbrechen** unterbrechen.

#### **Achtung!**

In jedem Schritt für die Anlage einer Richtlinie lassen sich die eingegebenen Parameter mit der Schaltfläche  fixieren. Wenn das Schloss in der Schaltfläche verschlossen ist, werden im Weiteren bei Verwendung der Richtlinie auf den mobilen Geräte Werte übernommen, die von der angelegten Richtlinie vorgegeben sind.

#### **Schritt 1. Eingabe von allgemeinen Richtliniendaten**

Erster Schritt des Eingabeassistenten. Im ersten Fenster des Assistenten müssen Sie einen Namen für die Richtlinie vergeben (Feld **Name**). Im zweiten Fenster wählen Sie das Programm **Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition** aus der Dropdown-Liste **Programmname** aus. Damit die Richtlinieneinstellungen sofort nach der Anlage in Kraft treten, muss im dritten Fenster das Häkchen **Aktive Richtlinie** im Block **Richtlinienerstellung** gesetzt werden.

## Schritt 2. Parameter für Antiviren-Untersuchung bestimmen

In diesem Schritt werden die Parameter für die Antiviren-Untersuchung des mobilen Gerätes festgelegt: Untersuchungsbereich und Zeitplan, dem zufolge die Untersuchung erfolgen wird. Außerdem wird bestimmt, ob der Echtzeitschutz gestartet wird.

Damit das mobile Gerät mit dem Echtzeitschutz läuft, setzen Sie das Häkchen in **Echtzeitschutz aktivieren** (s. Abb. 24). In Folge dessen wird der Echtzeitschutz beim Einschalten des Gerätes gestartet und läuft bis zu dessen Ausschalten.

Im Block **Virensuche** können Sie den Untersuchungsbereich auswählen, indem Sie die Dateitypen markieren, die untersucht werden sollen, sowie ob versucht werden soll, das infizierte Objekt zu desinfizieren:

- **Ausführbare Dateien untersuchen** – Untersucht werden ausführbare Programmdateien.
- **Archive untersuchen** – Dateien untersuchen, die als Archiv gepackt sind
- **Desinfektionsversuch für infiziertes Objekt** – Versuch unternehmen, das infizierte Objekt zu desinfizieren. Es lassen sich nicht alle Objekte desinfizieren.

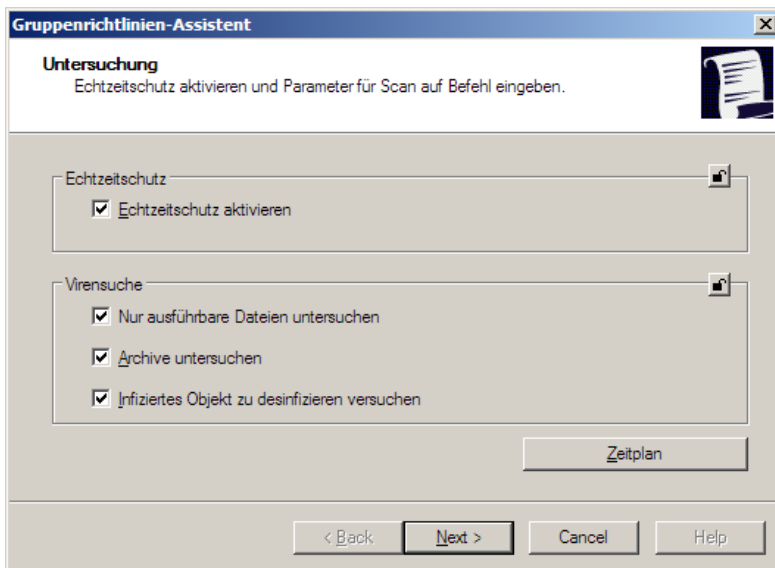


Abbildung 24. Parameter für Antiviren-Untersuchung konfigurieren

Um einen Zeitplan einzugeben, demzufolge Scan auf Befehl ausgeführt wird, klicken Sie auf **Zeitplan**. Es öffnet sich ein Dialogfenster, wo der Untersuchungsintervall eingegeben werden muss:

- **Manuell** – Die Aktion wird bei einem manuellen Start auf Wunsch des Benutzers ausgeführt.
- **Täglich** – Die Untersuchung erfolgt jeden Tag. In der Feldergruppe **Startzeit** geben Sie das Datum für den Aufgabenstart ein.
- **Wöchentlich** – Die Untersuchung erfolgt an bestimmten Wochentagen. In der Feldergruppe **Startzeit** geben Sie die Zeit für die Aktion an und wählen einen Wochentag aus, wann der Scan auf Befehl ausgeführt werden soll.

### Schritt 3. Updatequelle auswählen

In diesem Schritt wird die Updatequelle bestimmt und ein Zeitplan aktiviert, demzufolge die Updates erfolgen.

Im Block **Updatequelle** (s. Abb. 25) geben Sie die Adresse der Updatequelle im entsprechenden Feld an. Als Updatequelle kommen nur die Updateserver von Kaspersky Lab infrage.

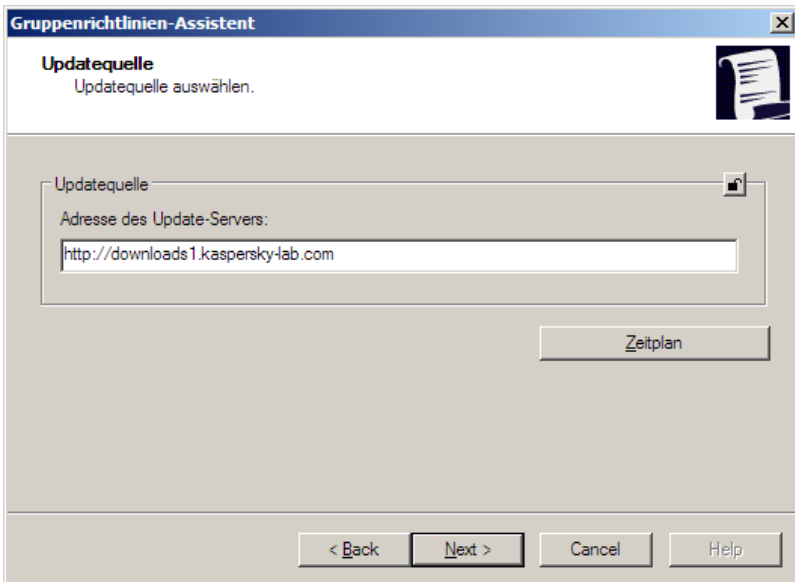


Abbildung 25. Updatequelle auswählen

Außerdem können Sie einen Zeitplan für den Update-Download eingeben. Klicken Sie dazu auf die Schaltfläche **Zeitplan**. Es öffnet sich ein Dialogfenster, wo der Untersuchungsintervall eingegeben werden muss:

- **Manuell** – Die Aktion wird bei einem manuellen Start auf Wunsch des Benutzers ausgeführt.
- **Täglich** – Die Untersuchung erfolgt jeden Tag. In der Feldergruppe **Startzeit** geben Sie das Datum für den Aufgabenstart ein.
- **Wöchentlich** – Die Untersuchung erfolgt an bestimmten Wochentagen. In der Feldergruppe **Startzeit** geben Sie die Zeit für die Aktion an und wählen einen Wochentag aus, wann der Scan auf Befehl ausgeführt werden soll.

#### Schritt 4. Zusätzliche Parameter eingeben

In diesem Schritt können Sie die Parameter des Moduls Anti-Spam einstellen und außerdem aktivieren Sie die Synchronisierung mit dem Administrationsserver.

Im Block **Anti-Spam** (s. Abb. 26) richten Sie die Parameter für das Modul Anti-Spam ein. Wenn Sie das Häkchen in **Schutz vor unerwünschten Nachrichten aktivieren** gesetzt haben, analysiert Anti-Spam eingehende Nachrichten anhand der folgenden Kriterien auf Spam:

- **Nachrichten von Nummern zustellen, die auf Kontaktliste stehen** – Kriterien für die Zugehörigkeit der Nummern zur "weißen" Liste. Nachrichten von Nummern auf der weißen Liste werden dem Benutzer immer zugestellt.
- **Nachrichten von Nummer sperren, die nicht auf der weißen Liste stehen, sowie Nachrichten von unbekanntem Empfängern** – Kriterien, anhand derer Nachrichten dem Benutzer nicht zugestellt werden.

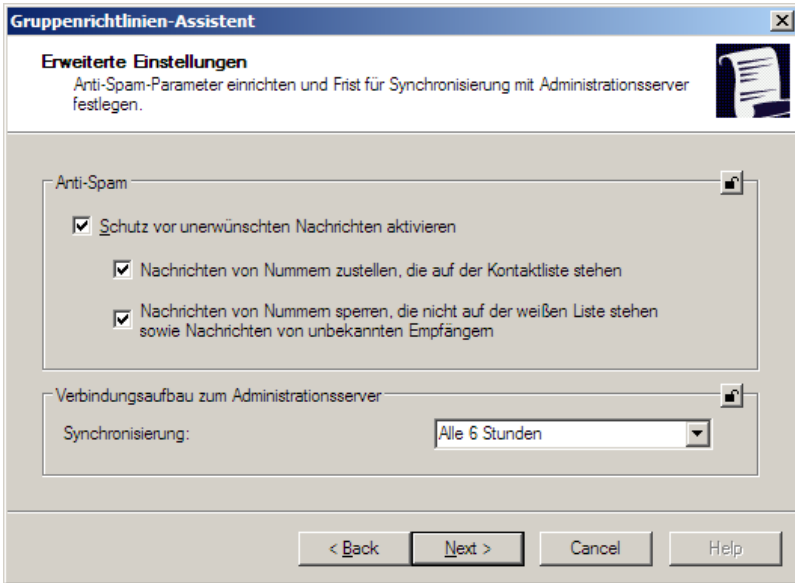



Abbildung 26. Zusätzliche Programmeinstellungen

Im Block **Verbindungsaufbau zum Administrationsserver** geben Sie den Intervall des Verbindungsaufbaus ein, indem Sie den gewünschten Wert in der Dropdown-Liste **Synchronisierung** markieren.

## Schritt 5. Richtlinienerstellung abschließen

Das letzte Fenster des Assistenten informiert Sie über den erfolgreichen Abschluss für die Erstellung der Richtlinie (s. Abb. 27).

Nach Abschluss des Assistenten zur Erstellung einer Richtlinie für Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition wird die Richtlinie im Ordner **Richtlinien** der entsprechenden Gruppe eingefügt und im Ergebnisfenster angezeigt.

Die angelegte Richtlinie können Sie mit deren Einstellungen bearbeiten und Einschränkungen für die Änderung der Parameter mithilfe der Schaltfläche  für jede Gruppeneinstellung festlegen. Der Benutzer des mobilen Gerätes kann die Einstellungen nicht ändern, die auf diese Weise fixiert worden sind. Die Verbreitung der Richtlinie auf mobile Geräte erfolgt bei der ersten Synchronisierung der Clients mit dem Server.

Sie können Richtlinien aus einer Gruppe in einer andere Gruppe kopieren und übertragen und mit den Standardbefehlen des Kontextmenüs **Kopie-**

ren / Einfügen, Ausschneiden / Einfügen und Löschen oder der analogen Einträge im Menü **Aktion** löschen.

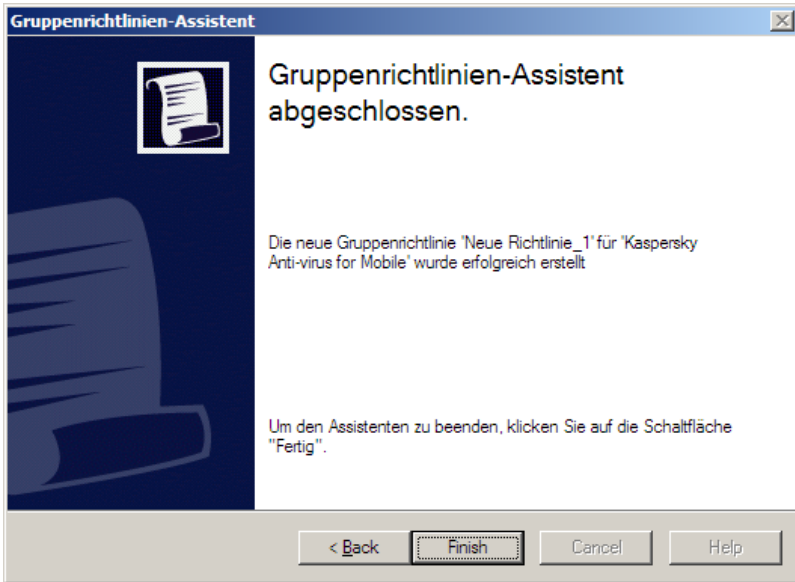


Abbildung 27. Richtlinienerstellung abschließen

### 3.1.2. Richtlinienparameter anzeigen und bearbeiten

Beim Bearbeiten können Sie eine Richtlinie ändern, können das Ändern der Parameter in den Richtlinien der untergeordneten Gruppen und in den Programm- und Aufgabeneinstellungen unterbinden.

1. Markieren Sie in der Konsolenstruktur im Ordner **Gruppen** eine Computergruppe, für die die Parameter bearbeitet werden sollen.
2. Markieren Sie den zu dieser ausgewählten Gruppe gehörenden Ordner **Richtlinien**, dabei werden im Ergebnisfenster alle Richtlinien angezeigt, die für die Gruppe erzeugt worden sind.
3. Markieren Sie in der Richtlinienliste die gewünschte Richtlinie für **Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition** (Programmname steht im Feld **Programm**).


4. Gehen Sie im Kontextmenü der ausgewählten Richtlinie auf den Eintrag **Eigenschaften**.

Es öffnet sich das Fenster zur Einstellung der Richtlinie für das Programm, das mehrere Registerkarten enthält.

Die Registerkarten **Allgemein**, **Übernahme** und **Ereignisse** sind Standard für das Programm Kaspersky Administration Kit (Details s. Administratorhandbuch von Kaspersky Administration Kit).

Die übrigen Registerkarten enthalten die Einstellungen für die Parameter von Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition. Weiter unten wird jede Registerkarte beschrieben.

#### Anmerkung

Beim Bearbeiten der Richtlinienparameter verwenden Sie die Schaltfläche , um die eingegebenen Richtliniendaten zu fixieren. Im Weiteren kann der Benutzer des mobilen Gerätes die Richtlinieneinstellungen nicht ändern, die auf diese Weise fixiert worden sind.

### 3.1.2.1. Programm-Informationen anzeigen

Auf der Registerkarte **Allgemein** (s. Abb. 28) stehen die folgenden Informationen über die Richtlinie: Name der Richtlinie, Name des Programms, für das sie erstellt wurde, Version des Programms, Datum und Uhrzeit für die Erstellung der Richtlinie, Datum und Uhrzeit der letzten Änderung.

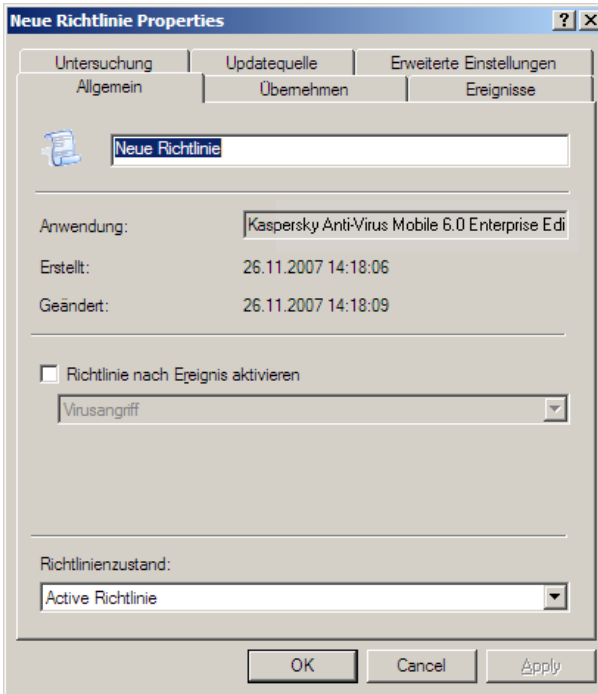


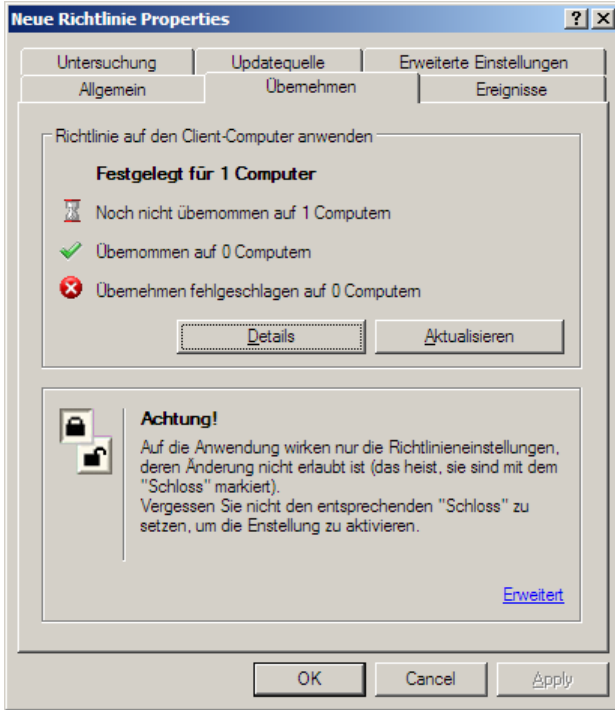
Abbildung 28. Registerkarte **Allgemein**

In dem Fenster können Sie den Namen der Richtlinie ändern, sie aktivieren oder deaktivieren sowie die Aktivierung der Richtlinie bei Eintreten eines Ereignisses konfigurieren.

### 3.1.2.2. Ergebnisse der Richtlinienübernahme anzeigen

Auf der Registerkarte **Übernahme** (s. Abb. 29) stehen Hilfestellungen zur Übernahme der Richtlinie auf mobilen Geräten der Gruppe. Es wird dabei die Menge der Geräte angegeben, auf denen:

- die Richtlinie nicht festgelegt wurde
- sie ausgeführt wird
- sie noch nicht ausgeführt wird
- die Richtlinie aufgrund eines Fehlers nicht übernommen werden konnte.

Abbildung 29. Registerkarte **Übernahme**

Details zu den Ergebnissen der Richtlinienübernahme auf jedem Client-Computer der Gruppe lassen sich im Fenster anzeigen, das sich mit einem Klick auf **Details** geöffnet werden kann (Details s. Administratorhandbuch von Kaspersky Administration Kit 6.0).

### 3.1.2.3. Parameter für Ereignisregistrierung im Programmverlauf konfigurieren

Kaspersky Anti-Virus generiert während des Programmablaufs einen bestimmten Bestand an Ereignissen. Jedes Ereignis hat eine Charakteristik, die die Priorität ihrer Bedeutung darstellt. Es gibt vier Prioritätsstufen: Kritisches Ereignis, Funktionsausfall, Warnung und informative Mitteilung.

Die Ereignisse vom gleichen Typ können verschiedene Prioritätsstufen haben, je nach Situation, in der das Ereignis eingetreten ist.

Auf der Registerkarte **Ereignisse** (s. Abb. 30) stehen die Ereignistypen, die im Programmablauf eintreten und im Bericht fixiert werden, sowie der Speicherort des Berichtes und die Art der Benachrichtigung von Administrator und / oder anderer Benutzer.

Um Ereignistypen anzuzeigen, wählen Sie die gewünschte Prioritätsstufe aus der Dropdown-Liste **Prioritätsstufe** aus. Die Ereignistypen für die ausgewählte Priorität werden im Informationsfeld dargestellt, das sich unten befindet.

Für jedes Ereignis können Sie die Option angeben, es in den Bericht aufzunehmen und eine Benachrichtigung des Administrators über das Ereignis zu konfigurieren.

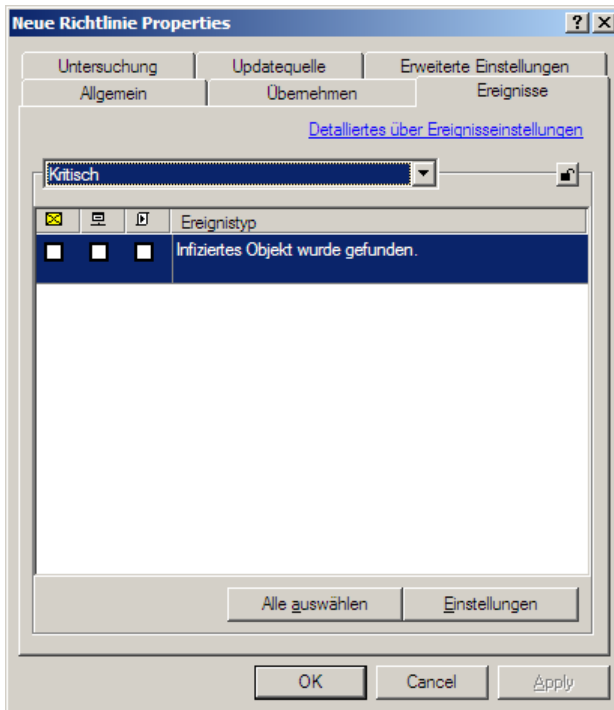


Abbildung 30. Registerkarte **Ereignisse**

Details zu den übrigen Einstellungen der Registerkarte **Ereignisse** finden Sie im Administratorhandbuch von Kaspersky Administration Kit 6.0.

### 3.1.2.4. Parameter für Antiviren-Untersuchung bestimmen

Auf Registerkarte **Untersuchung** (s. Abb. 31) werden die Parameter für Scan auf Befehl angepasst: Untersuchungsbereich, Aktion für infizierte Objekte, Zeitplan, dem zufolge die Untersuchung erfolgen wird. Außerdem wird auf der Registerkarte bestimmt, ob der Echtzeitschutz gestartet wird.

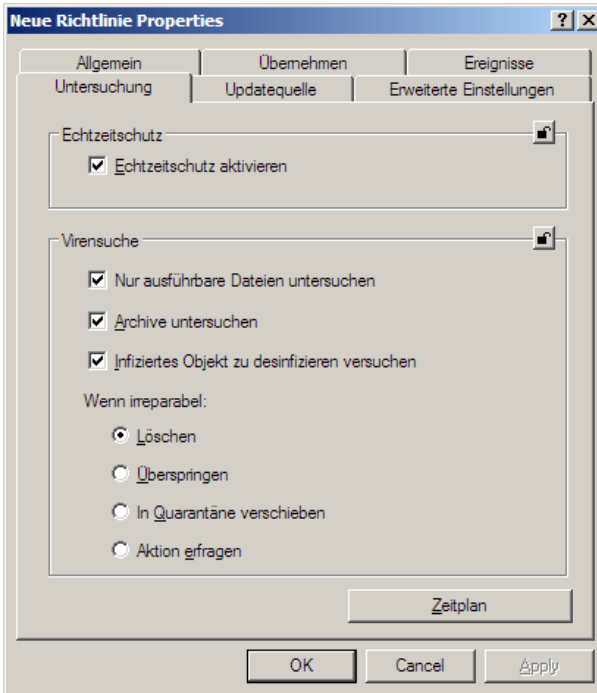


Abbildung 31. Registerkarte **Untersuchung**

Im Block **Wenn irreparabel** geben Sie die Aktion an, die beim Erkennen eines infizierten Objektes ausgeführt wird:

- **Löschen**
- **Überspringen** – Die erkannten infizierten Objekte werden ohne Änderung belassen.
- **In Quarantäne verschieben** – 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 ohne Änderung zu belassen.

Die übrigen Parameter sind analog zu den oben in Pkt. 3.1.1 auf S. 35 beschriebenen Einstellungen.

### 3.1.2.5. Updatequelle der Datenbanken von Kaspersky Anti-Virus bestimmen

Auf der Registerkarte **Updatequelle** (s. Abb. 32) wird die Updatequelle angegeben, von der die Updates der Anti-Virus-Datenbanken geladen werden. Außerdem wird auf der Registerkarte ein Zeitplan eingestellt, demzufolge die Updates erfolgen.

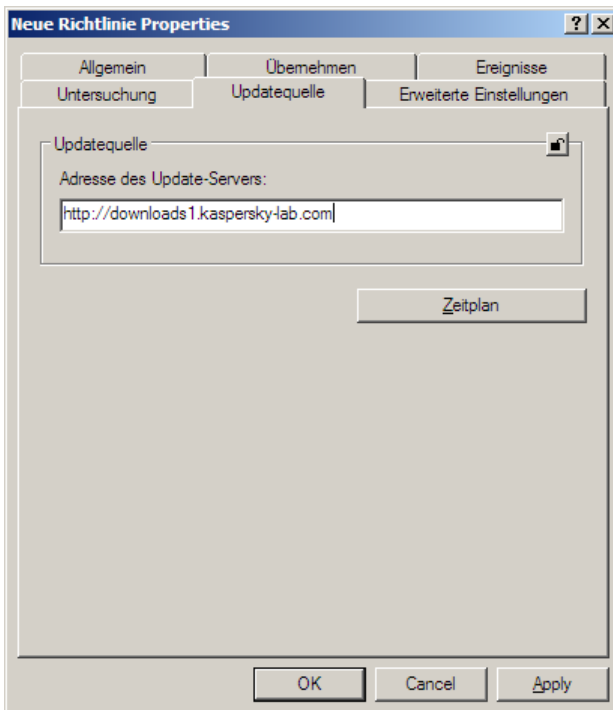


Abbildung 32. Registerkarte **Updatequelle**

### 3.1.2.6. Zusätzliche Parameter eingeben

Auf der Registerkarte **Erweiterte Einstellungen** (s. Abb. 33) werden die Einstellungen von Anti-Spam eingegeben und der Intervall für den Verbindungsaufbau mit dem Administrationsserver festgelegt.

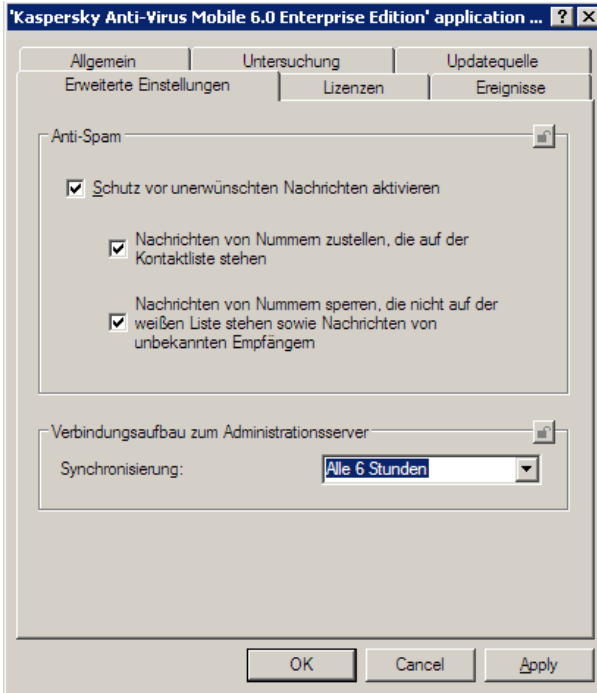


Abbildung 33. Registerkarte **Erweiterte Parameter**

## 3.2. Programmeinstellungen verwalten

Mithilfe der Programmeinstellungen können Sie die Parameter von Kaspersky Anti-Virus für einzelne mobile Geräte in einer Gruppe oder für ein lokales Gerät ändern, auf dem das Programm installiert ist. Es lassen sich nur nicht von einer Richtlinie fixierte Parameter ändern (Details s. Pkt. 0 auf S. 34).

Um die Programmeinstellungen zu ändern, machen Sie Folgendes:

1. Markieren Sie den Ordner mit dem Name der Gruppe, zu der das mobile Gerät gehört, im Ordner **Gruppen**.
2. Markieren Sie im Ergebnisfenster das Gerät, für das Sie die Programmeinstellungen ändern müssen. Im Kontextmenü oder im Menü **Aktionen** gehen Sie auf den Eintrag **Eigenschaften**.
3. Im Programmhauptfenster öffnet sich daraufhin das Dialogfenster **Eigenschaften: Computername**. Gehen Sie auf die Registerkarte **Anwendungen** (s. Abb. 34).

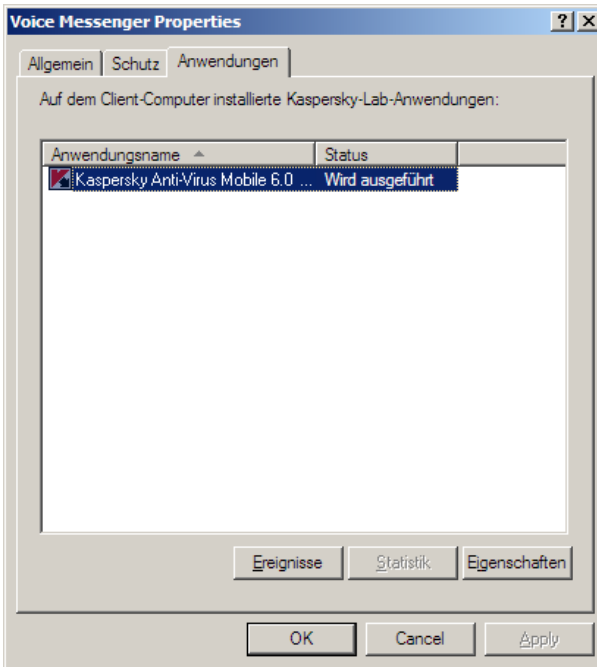


Abbildung 34. Fenster Eigenschaften des mobilen Gerätes anzeigen.  
Registerkarte **Anwendungen**

4. Markieren Sie das Programm **Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition**. Im unteren Teil des Fenster befinden sich die folgenden Schaltflächen:
  - **Ereignisse** – Ereignisse im Programmablauf anzeigen, die auf dem mobilen Gerät eingetreten und auf dem Administrationsserver registriert worden sind.

- **Statistik** - allgemeine Informationen über das Programm anzeigen.
- **Eigenschaften** – Programm im geöffneten Fenster Parameter des Programms Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition einstellen

### 3.2.1.1. Programm-Informationen anzeigen

Auf der Registerkarte **Allgemein** (s. Abb. 35) können Sie Informationen über das Programm Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition anzeigen lassen.

Im oberen Fensterteil steht der Name des installierten Programms, die Version, das Installationsdatum, dessen Status (ob das Programm auf dem mobilen Gerät gestartet oder beendet ist) sowie Angaben über den Zustand der Anti-Virus-Datenbanken.

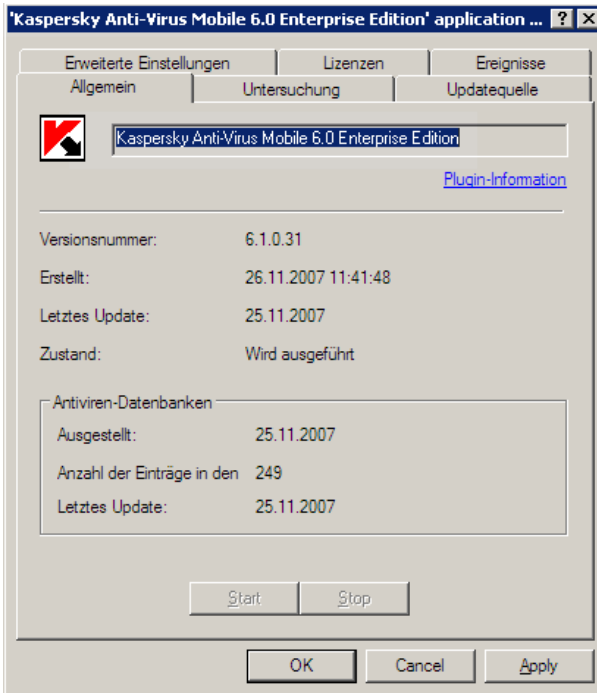


Abbildung 35. Fenster Einstellung der Programmeigenschaften. Registerkarte **Allgemein**

### 3.2.1.2. Informationen über eingestellte Parameter der Antiviren-Untersuchung anzeigen

Auf Registerkarte **Untersuchung** (s. Abb. 36) können Sie Informationen über die eingestellten Parameter für Scan auf Befehl anzeigen lassen: Untersuchungsbereich, Aktion für infizierte Objekte sowie Zeitplan, dem zufolge die Untersuchung erfolgen wird. Außerdem stehen auf der Registerkarte Angaben darüber, ob auf dem mobilen Gerät der Echtzeitschutz läuft.

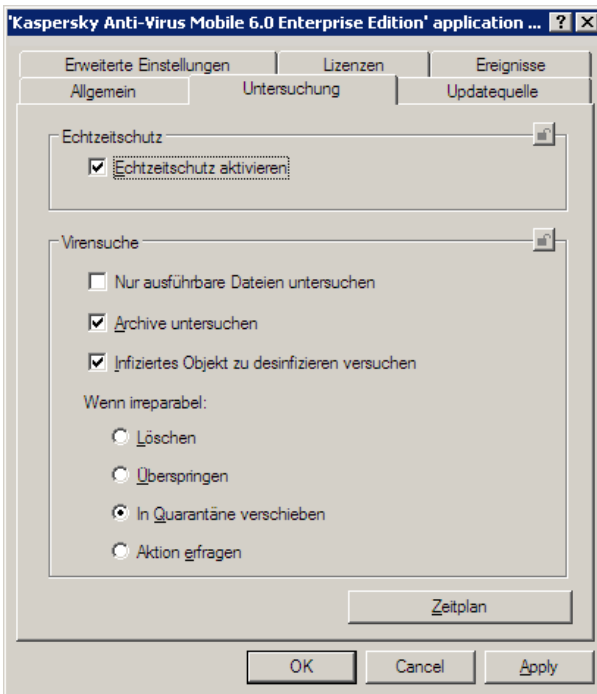


Abbildung 36. Registerkarte **Untersuchung**

### 3.2.1.3. Informationen über Updatequelle anzeigen

Auf der Registerkarte **Updatequelle** (s. Abb. 37) können Sie Informationen ergründen, von welchem Server der Update-Download für dieses mobile Gerät

eingestellt ist sowie nach welchem Zeitplan Updates auf dem gewählten mobilen Gerät Updates erfolgen.

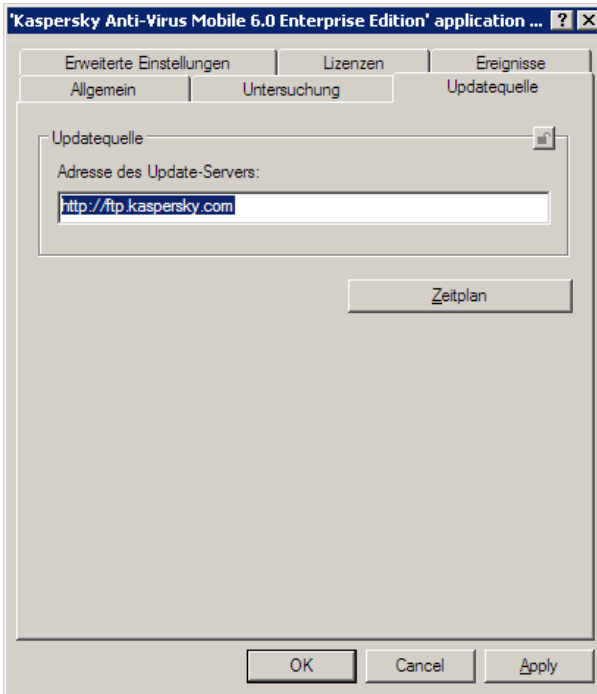
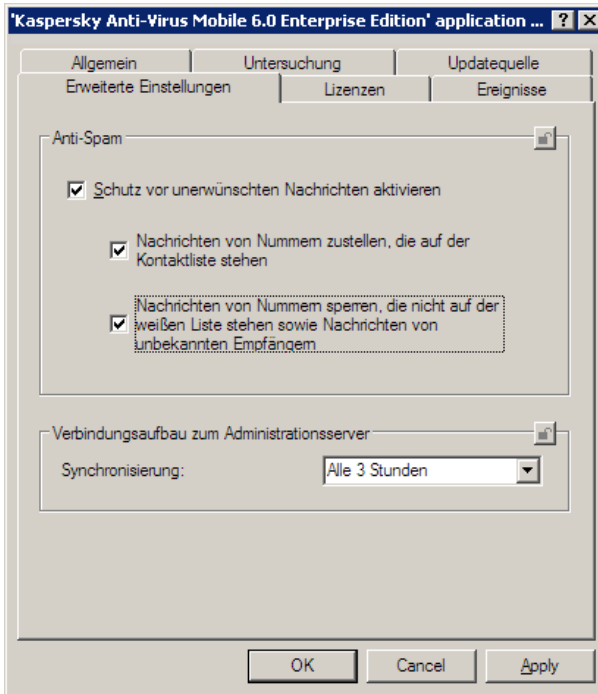


Abbildung 37. Registerkarte **Updatequelle**

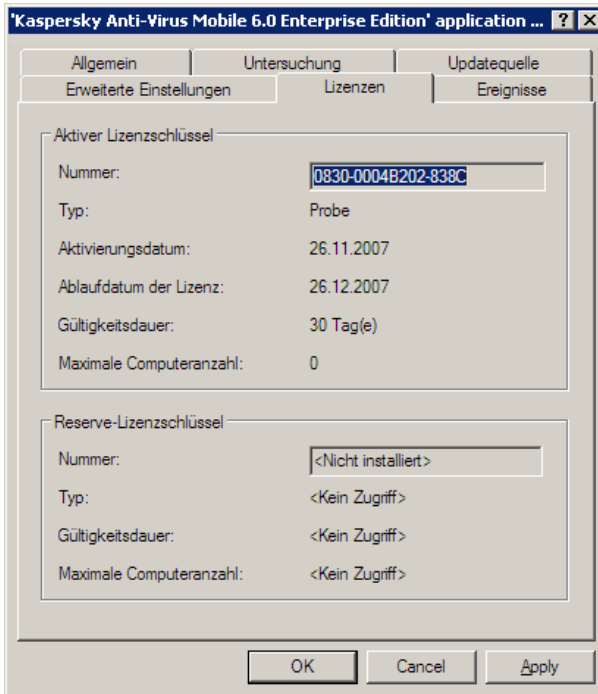
### 3.2.1.4. Informationen über zusätzliche Parameter anzeigen

Auf der Registerkarte **Erweiterte Parameter** (s. Abb. 38) können Sie Daten über die Einstellungen von Anti-Spam anzeigen und den Intervall für den Verbindungsaufbau mit dem Administrationsserver festlegen.

Abbildung 38. Registerkarte **Erweiterte Parameter**

### 3.2.1.5. Informationen über Lizenzschlüssel anzeigen

Auf der Registerkarte **Lizenz** (s. Abb. 39) stehen Informationen über den aktiven Lizenzschlüssel oder über den Reserveschlüssel, die auf diesem mobilen Gerät installiert sind. Außerdem stehen hier Informationen über den Schlüsseltyp, dessen Gültigkeitsdauer und Lizenzbeschränkungen. Für den aktiven Lizenzschlüssel befinden sich hier noch Daten über den Tag der Aktivierung und über den Tag, an dem der Lizenzschlüssel abläuft.

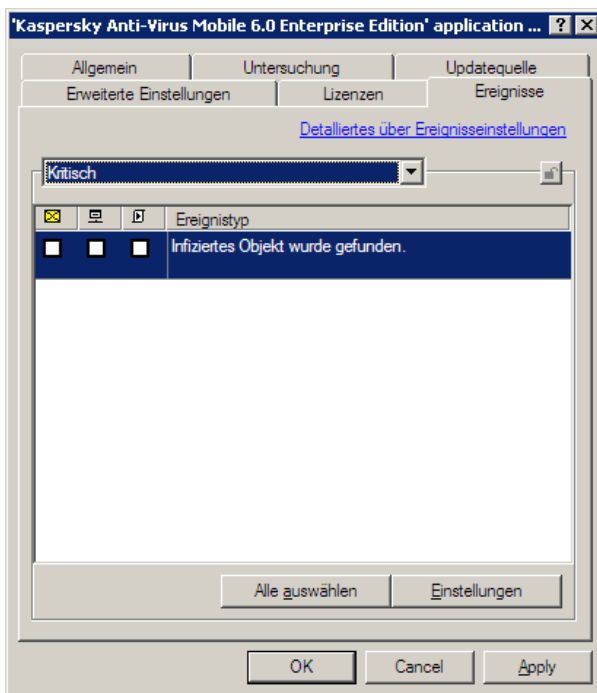
Abbildung 39. Registerkarte **Lizenz**

### 3.2.1.6. Ereignis-Informationen anzeigen

Kaspersky Anti-Virus generiert während des Programmablaufs einen bestimmten Bestand an Ereignissen. Jedes Ereignis hat eine Charakteristik, die die Priorität ihrer Bedeutung darstellt. Es gibt vier Prioritätsstufen: Kritisches Ereignis, Funktionsausfall, Warnung und informative Mitteilung.

Die Ereignisse vom gleichen Typ können verschiedene Prioritätsstufen haben, je nach Situation, in der das Ereignis eingetreten ist.

Auf der Registerkarte **Ereignisse** (s. Abb. 40) stehen die Ereignistypen, die im Programmablauf eintreten und im Bericht fixiert werden, sowie der Speicherort des Berichtes und die Art der Benachrichtigung von Administrator und / oder anderer Benutzer über das eingetretene Ereignis.

Abbildung 40. Registerkarte **Ereignisse**

---

# ANHANG A. KASPERSKY LAB

## Das Unternehmen

Kaspersky Lab ist ein weltweit führendes Unternehmen in den Bereichen Viren-, Spam- und Hacker-Schutz. Unser hoch spezialisiertes Viren-Labor reagiert stets schneller als alle anderen auf neue Bedrohungen, so dass unsere innovativen Programme seit vielen Jahren Heimanwender und Unternehmen jeder Größe zuverlässig schützen.

Bereits 1997 wurde Kaspersky Lab von dem russischen Virenexperten Eugene Kaspersky in Moskau gegründet und hat heute unter anderem Niederlassungen in Deutschland, Frankreich, Großbritannien, Polen, Japan, USA und China.

## Einzigartige Erfahrung

Weltweit beschäftigt Kaspersky Lab über 550 hochspezialisierte Mitarbeiter, darunter Mitglieder der Computer Anti-Virus Researchers Organisation (CARO) und des Virus Bulletin Technical Advisory Board. Im Laufe vieler Jahre Forschung und Kampf gegen Computerviren haben wir Wissen und Fähigkeiten erworben, die heute unser wertvollstes Kapital darstellen.

Dank unserer weit reichenden Erfahrung sind wir in der Lage, Entwicklungstrends bei Malware vorherzusehen. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab, so dass wir anderen immer einen Schritt voraus sind und unseren Kunden stets den besten Schutz bieten können.

## Kaspersky Anti-Virus

Nach vielen Jahren innovativer Entwicklungen zählt Kaspersky Lab heute zu den führenden Herstellern von Sicherheits-Software. Der hohe Standard unserer Produkte wird durch zahlreiche Auszeichnungen internationaler Forschungseinrichtungen, unabhängiger Testlabors und renommierter Fachpublikationen bestätigt.

Die Programm-Module unseres bekanntesten Programms, Kaspersky Anti-Virus, gewährleisten einen zuverlässigen Schutz für Workstations, Datei- und Web-Server, Mail-Gateways, Firewalls, Pocket-PCs und Smartphones.

Als erstes Unternehmen entwickelte Kaspersky Lab bedeutende Technologien, die heute selbst bei zahlreichen Antiviren-Programmen anderer Hersteller – wie G-Data, Aladdin und F-Secure – als Programm-Kern einen unverzichtbaren Bestandteil bilden. So vertrauen bereits über 200 Millionen Anwender unseren Innovationen, wie dem heuristischen Analysator zur Entdeckung noch unbekannter Viren, den Micro-Updates für die Antiviren-Datenbanken und dem ersten umfassenden Virenschutz für Unix/Linux-Systeme.

## **Komplexe Technologien für Ihre Sicherheit**

Moderne Viren und Schadprogramme sind komplexe Bedrohungen, so dass die bisher üblichen Schutzpakete für PCs und Netzwerke häufig nicht mehr ausreichen.

Aus diesem Grund entwickelte Kaspersky Lab mit Kaspersky Anti-Hacker eine Personal Firewall und mit Kaspersky Anti-Spam einen besonders effektiven Spam-Filter. Mit den Produkten von Kaspersky Lab können Sie Ihren Computer und Ihr Netzwerk optimal vor allen modernen virtuellen Gefahren schützen.

### **Service**

Kaspersky Lab bietet seinen Kunden eine ganze Palette zusätzlicher Dienstleistungen, die einen maximalen Schutz garantieren: Die Antiviren-Datenbanken werden stündlich aktualisiert, die Anti-Spam-Dateien 12 bis 24 Mal pro Tag. Zudem steht allen Anwendern ein rund-um-die-Uhr-Support zur Verfügung: Telefonisch oder per E-Mail – in deutscher, englischer, russischer und französischer Sprache.

# **A.1. Andere Produkte von Kaspersky Lab**

## **Kaspersky Lab News Agent**

Das Programm News Agent dient der schnellen Zustellung der Nachrichten von Kaspersky Lab, der Benachrichtigung über das "Virus-Wetter" und über neu erschienene Nachrichten. Das Programm liest in vorgegebenen Zeitabständen von den Kaspersky-Lab-Newsservern eine Liste der verfügbaren Nachrichtenkanäle und der darin enthaltenen Informationen.

News Agent verfügt außerdem über folgende Funktionen:

- Visualisierung des Zustands des "Viren-Wetters" im Infobereich der Taskleiste.
- Abonnieren und Abbestellen der Nachrichtenkanäle von Kaspersky Lab.
- Download von Nachrichten für jeden abonnierten Kanal in festgelegten Zeitabständen. Außerdem erfolgt eine Benachrichtigung über ungelesene Nachrichten.
- Anzeige von Nachrichten der abonnierten Kanäle.
- Anzeige einer Liste der Kanäle und ihrer Status.
- Öffnen der Webseite mit dem vollständigen Nachrichtentext im Browser.

News Agent funktioniert unter dem Betriebssystem Microsoft Windows. Er kann als separates Programm benutzt werden oder zu unterschiedlichen integrierten Lösungen von Kaspersky Lab gehören.

### **Kaspersky® OnLine Scanner**

Dieses Programm ist ein kostenloser Dienst, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antiviren-Untersuchung des Computers im Online-Modus erlaubt. Kaspersky OnLine Scanner wird direkt im Browser ausgeführt. Dadurch kann der Benutzer schnell eine Antwort auf Fragen erhalten, die mit einer Infektion durch schädliche Programme verbunden sind. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

### **Kaspersky® OnLine Scanner Pro**

Dieses Programm stellt einen Abonnementdienst dar, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antiviren-Untersuchung des Computers und die Desinfektion infizierter Dateien im Online-Modus erlaubt. Kaspersky OnLine Scanner Pro wird direkt im Browser ausgeführt. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

### **Kaspersky Anti-Virus® 7.0**

Kaspersky Anti-Virus 7.0 dient dem Schutz eines PCs vor schädlichen Programmen. Dabei werden traditionelle Virenschutzmethoden auf optimale Weise mit neuen proaktiven Technologien vereinigt.

Das Programm erlaubt eine komplexe Antiviren-Untersuchung, die folgende Optionen umfasst:

- Antiviren-Untersuchung des Mail-Datenstroms auf Ebene des Datenübertragungsprotokolls (POP3, IMAP und NNTP für eingehende Mails und SMTP für ausgehende Mails) unabhängig vom verwendeten Mailprogramm, sowie Untersuchung und Desinfektion von Mail-Datenbanken.

- Antiviren-Untersuchung des Internet-Datenstroms, der mit HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.
- Antiviren-Untersuchung beliebiger einzelner Dateien, Ordner und Laufwerke. Außerdem sind vordefinierte Untersuchungsaufgaben für die Virenanalyse von kritischen Bereichen des Betriebssystems und von Objekten, die beim Start des Betriebssystems Microsoft Windows gestartet werden, vorhanden.

Der Proaktive Schutz umfasst:

- *Kontrolle über Veränderungen im Dateisystem.* Das Programm erlaubt es, eine Liste der Anwendungen anzulegen, deren Komponentenbestand kontrolliert werden soll. Dadurch lässt sich die Verletzung der Integrität von Anwendungen durch Schadprogramme verhindern.
- *Überwachung von Prozessen im Arbeitsspeicher.* Kaspersky Anti-Virus 7.0 warnt den Benutzer rechtzeitig, wenn gefährliche, verdächtige oder versteckte Prozesse auftreten oder wenn aktive Prozesse auf unerlaubte Weise verändert werden.
- *Überwachung von Veränderungen in der Registrierung des Betriebssystems* durch die Kontrolle des Zustands der Systemregistrierung.
- Die *Rootkit-Suche* zur Kontrolle von versteckten Prozessen erlaubt es, Bedrohungen abzuwehren, die unter Verwendung der Rootkit-Technologie schädlichen Code im Betriebssystem verstecken.
- *Heuristische Analyse.* Bei der Untersuchung eines Programms emuliert der heuristische Analysator seine Ausführung und protokolliert alle verdächtigen Aktionen wie beispielsweise das Öffnen einer Datei, das Schreiben in eine Datei, das Abfangen von Interrupt-Vektoren usw. Auf der Grundlage dieses Protokolls wird darüber entschieden, ob das Programm eine Vireninfection verursachen kann. Die Emulation erfolgt isoliert in einer virtuellen Umgebung, wodurch eine Infektion des Computers ausgeschlossen wird.
- *Systemwiederherstellung* nach schädlicher Einwirkung von Spyware: Die Wiederherstellung wird durch die Speicherung aller Veränderungen in der Registrierung und im Dateisystem des Computers und durch das vom Benutzer initiierte Rückgängigmachen der Veränderungen ermöglicht.

## **Kaspersky® Internet Security 7.0**

Kaspersky Internet Security 7.0 ist eine komplexe Lösung für den Schutz eines PCs vor den wichtigsten Bedrohungen (Viren, Hackerangriffe, Spam und Spyware), denen Informationen unterliegen. Alle Komponenten lassen sich über eine einheitliche Benutzeroberfläche einstellen und steuern.

Die Funktion des Antiviren-Schutzes umfasst:

- *Antiviren-Untersuchung des Mail-Datenstroms* auf Ebene des Datenübertragungsprotokolls (POP3, IMAP und NNTP für eingehende Mails und SMTP für ausgehende Mails) unabhängig vom verwendeten Mailprogramm. Für die populären Mailprogramme Microsoft Office Outlook, Microsoft Outlook Express und The Bat! sind Plug-Ins und die Desinfektion von Mail-Datenbanken vorgesehen.
- *Antiviren-Untersuchung des Internet-Datenstroms*, der mit HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.
- *Schutz des Dateisystems*: Der Antiviren-Untersuchung können beliebige einzelne Dateien, Ordner und Laufwerke unterzogen werden. Außerdem sind vordefinierte Untersuchungsaufgaben für die Virenanalyse von kritischen Bereichen des Betriebssystems und von Objekten, die beim Start des Betriebssystems Microsoft Windows gestartet werden, vorhanden.
- *Proaktiver Schutz*: Das Programm führt die ununterbrochene Überwachung der Aktivität von Anwendungen und Prozessen durch, die im Arbeitsspeicher des Computers gestartet werden, verhindert gefährliche Veränderungen des Dateisystems und der Registrierung, und stellt das System nach schädlicher Einwirkung wieder her.

Der *Schutz vor Internetbetrug* beruht auf dem Erkennen von Phishing-Angriffen. Dadurch lässt sich der Diebstahl Ihrer vertraulichen Informationen verhindern (in erster Linie Kennwörter, Konto- und Kreditkartennummern, sowie Sperren der Ausführung gefährlicher Skripts auf Webseiten, Sperren von Popupfenstern und Werbebannern). Die Funktion zum *Sperren der automatischen Einwahl auf kostenpflichtige Internetressourcen* ermöglicht es, Programme zu identifizieren, die versuchen Ihr Modem für versteckte Verbindungen mit kostenpflichtigen Telefondiensten zu missbrauchen, indem diese Programme gesperrt werden. Das Modul *Schutz von vertraulichen Informationen* gewährleistet den Schutz vor dem unerlaubtem Zugriff und der Übertragung von Informationen mit vertraulichem Charakter. Die Komponente *Kindersicherung* bietet die Kontrolle über den Zugriff von Computerbenutzern auf Internetressourcen.

Kaspersky Internet Security 7.0 *erkennt Versuche zum Scannen der Ports Ihres Computers*, die häufig im Vorfeld von Netzwerkangriffen stattfinden, und wehrt bekannte Netzwerkangriffe erfolgreich ab. Auf der *Basis von vordefinierten Regeln* führt das Programm die Kontrolle aller Netzwerkaktionen durch und überwacht alle *eingehenden und ausgehenden Datenpakete*. Der *Stealth-Modus macht den Computer für die externe Umgebung praktisch unsichtbar*. In diesem Modus wird jede Netzwerkaktivität verboten, wenn sie nicht durch Ausnahmeregelungen erlaubt wird, die vom Benutzer festgelegt wurden.

Im Programm wird eine komplexe Methode zur Spam-Filterung eingehender Mails angewandt:

- Untersuchung nach schwarzen und weißen Adressenlisten (einschließlich Adressen von Phishing-Seiten)
- Phrasenuntersuchung im Mailtext
- Analyse des Mailtexts mit Hilfe eines lernfähigen Algorithmus
- Erkennung von Spam in Form von Grafiken

### **Kaspersky Anti-Virus for File-Server**

Das Produkt schützt die Dateisysteme von Servern, die unter den Betriebssystemen Microsoft Windows, Novell NetWare, Linux und Samba laufen, zuverlässig vor allen Arten schädlicher Programme. Das Produkt umfasst folgende Anwendungen von Kaspersky Lab:

- [Kaspersky Administration Kit](#)
- [Kaspersky Anti-Virus for Windows Server](#)
- [Kaspersky Anti-Virus for Linux File Server](#)
- [Kaspersky Anti-Virus for Novell Netware](#)
- [Kaspersky Anti-Virus for Samba Server](#)

Vorzüge und Funktionen:

- *Echtzeitschutz der Dateisysteme von Servern*: alle Dateien der Server werden untersucht, wenn versucht wird, sie zu öffnen und auf dem Server zu speichern.
- *Verhinderung von Viren-Epidemien*
- *Scan auf Befehl* des gesamten Dateisystems oder bestimmter Ordner und Dateien
- *Einsatz von Optimierungstechnologien* bei der Untersuchung von Objekten des Serverdateisystems
- *Systemwiederherstellung nach einer Infektion*
- *Skalierbarkeit* im Rahmen der verfügbaren Systemressourcen
- *Berücksichtigung der Systemauslastung*
- *Verwendung einer Liste mit vertrauenswürdigen Prozessen*, deren Aktivität auf dem Server nicht vom Programm kontrolliert wird.
- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung

- *Speicherung von Sicherungskopien infizierter und gelöschter Objekte*, um sie bei Bedarf wiederherzustellen.
- *Isolierung verdächtiger Objekte* in einem speziellen Speicher
- *Benachrichtigungen über Ereignisse* bei der Arbeit des Produkts für den Systemadministrator
- *Ausführliche Berichtsführung*
- *Automatisches Update der Datenbanken* des Softwareprodukts.

### **Kaspersky Open Space Security**

Kaspersky Open Space Security realisiert eine neue Art des Herangehens an die Sicherheit moderner Unternehmensnetzwerke mit beliebigem Umfang. Dabei gewährleistet es den zentralen Schutz von Informationssystemen und unterstützt externe Arbeitsplätze und mobile Benutzer.

Das Softwareprodukt umfasst vier Produkte:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Im Folgenden wird jedes Produkt genau beschrieben.

**Kaspersky Work Space Security** bietet den zentralen Schutz von Workstations innerhalb und außerhalb eines Unternehmensnetzwerks. Es schützt vor allen aktuellen Internet-Bedrohungen wie Viren, Spyware, Hackerangriffen und Spam.

Vorzüge und Funktionen:

- *Komplexer Schutz vor Viren, Spyware, Hackerangriffen und Spam*
- *Proaktiver Schutz* vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.
- *Personal Firewall* mit IDS/IPS-System
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Schutz vor Phishing-Angriffen und Spam*
- *Dynamisches Ressourcen-Management* bei der vollständigen Untersuchung des Systems

- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Unterstützung von Cisco® NAC* (Network Admission Control)
- *Untersuchung von E-Mails und Internet-Traffic in Echtzeit*
- *Sperren von Popupfenstern und Werbebannern bei der Arbeit im Internet*
- *Sichere Arbeit in Netzwerken aller Art*, einschließlich Wi-Fi
- *Mittel zum Erstellen einer Notfall-CD zur Systemwiederherstellung*, um die Folgen von Virenangriffen zu beheben.
- *Flexibles Informationssystem* für den Schutzstatus
- *Automatisches Update der Datenbanken*
- *Vollständige Unterstützung von 64-Bit-Betriebssystemen*
- *Optimiert für Notebooks* mit Intel® Centrino® Duo
- *Möglichkeit zur Remote-Reparatur* (Intel® Active Management - Intel® vPro™)

**Kaspersky Business Space Security** bietet den optimalen Schutz für die Informationsressourcen einer Firma vor Internet-Bedrohungen. Es schützt Workstations und Dateiserver vor Viren, Trojanern und Würmern, und verhindert Virus-Epidemien. Zudem überwacht es die Integrität der Daten und ermöglicht den Benutzern den schnellen Zugriff auf Netzwerkressourcen.

Vorzüge und Funktionen:

- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Unterstützung von Cisco® NAC* (Network Admission Control);
- *Schutz von Workstations und Dateiservern vor allen Internet-Bedrohungen*
- *Verwendung der iSwift-Technologie zur Vermeidung wiederholter Untersuchungen* innerhalb eines Netzwerks
- *Dynamische Auslastung der Serverprozessoren*
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*

- *Proaktiver Schutz* für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.
- *Untersuchung von E-Mail und Internet-Traffic in Echtzeit*
- *Personal Firewall* mit IDS/IPS-System
- *Schutz bei der Arbeit in Wi-Fi-Netzwerken*
- *Technologie zum Selbstschutz des Antiviren-Programms vor Schadprogrammen*
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Automatisches Update der Datenbanken*

### **Kaspersky Enterprise Space Security**

Das Produkt umfasst Komponenten zum Schutz von Workstations und Groupware-Servern vor allen aktuellen Internet-Gefahren. Viren werden aus dem E-Mail-Datenstrom gelöscht. Die Integrität der Daten sowie die schnelle und sichere Verfügbarkeit der Netzwerkressourcen werden gewährleistet.

Vorzüge und Funktionen:

- *Schutz für Workstations und Server vor Viren, Trojanern und Würmern*
- *Schutz der Mailserver Sendmail, Qmail, Postfix und Exim*
- *Untersuchung aller E-Mails auf einem Microsoft Exchange Server, einschließlich der gemeinsamen Ordner*
- *Bearbeitung von E-Mails, Datenbanken und anderen Objekten auf Lotus Notes/Domino-Servern*
- *Schutz vor Phishing-Angriffen und Spam*
- *Verhinderung von massenhaften E-Mails und Viren-Epidemien*
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Unterstützung von Cisco<sup>®</sup> NAC (Network Admission Control);*
- *Proaktiver Schutz* für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.
- *Personal Firewall* mit IDS/IPS-System
- *Schutz bei der Arbeit in Wi-Fi-Netzwerken*

- *Untersuchung des Internet-Traffics in Echtzeit*
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Dynamisches Ressourcen-Management* bei der vollständigen Untersuchung des Systems
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Berichtssystem über den Status des Schutzsystems*
- *Automatisches Update der Datenbanken*

### **Kaspersky Total Space Security**

Diese Lösung überwacht alle ein- und ausgehenden Datenströme, E-Mails, Internet-Traffic und alle Netzwerkaktionen. Kaspersky Total Space Security umfasst Komponenten zum Schutz von Workstations und mobilen Geräten, gewährleistet den schnellen und sicheren Zugriff der Anwender auf die Informationsressourcen der Firma und auf das Internet. Außerdem garantiert es Sicherheit bei der Kommunikation per E-Mail.

Vorzüge und Funktionen:

- *Komplexer Schutz vor Viren, Spyware, Hackerangriffen und Spam* auf allen Ebenen eines Unternehmensnetzwerks von der Workstation bis zur Internet-Gateway.
- *Proaktiver Schutz* für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.
- *Schutz für Mailserver und Groupware-Server*
- *Echtzeit-Untersuchung des Internet-Datenverkehrs (HTTP/FTP)*, der in ein lokales Netzwerk eintrifft.
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Sperren des Zugriffs auf infizierte Workstations*
- *Verhinderung von Viren-Epidemien*
- *Zentrale Berichte über den Schutzstatus*
- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Unterstützung von Cisco® NAC (Network Admission Control)*;
- *Unterstützung von Hardware-Proxyservern*

- *Filterung des Internet-Datenverkehrs* nach einer Liste vertrauenswürdiger Server, nach Objekttypen und nach Benutzergruppen
- *Verwendung der iSwift-Technologie zur Vermeidung wiederholter Untersuchungen* innerhalb eines Netzwerks
- *Dynamisches Ressourcen-Management* bei der vollständigen Untersuchung des Systems
- *Personal Firewall* mit IDS/IPS-System
- *Sichere Arbeit in Netzwerken aller Typen*, einschließlich Wi-Fi
- *Schutz vor Phishing-Angriffen und Spam*
- *Möglichkeit zur Remote-Reparatur* (Intel® Active Management - Intel® vPro™)
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Technologie zum Selbstschutz des Antiviren-Programms vor Schadprogrammen*
- *Vollständige Unterstützung von 64-Bit-Betriebssystemen*
- *Automatisches Update der Datenbanken*

### **Kaspersky Security for Mail-Server**

Kaspersky Security for Mail-Server schützt Mailserver und Groupware-Server gegen Schadprogramme und Spam. Das Produkt umfasst Anwendungen für den Schutz aller bekannten Mailserver wie Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix und Exim. Zudem kann auch ein separater Mail-Gateway organisiert werden. Zu dieser Lösung gehören:

- [Kaspersky Administration Kit](#)
- [Kaspersky Mail Gateway](#)
- [Kaspersky Anti-Virus for Lotus Notes/Domino](#)
- [Kaspersky Anti-Virus for Microsoft Exchange](#)
- [Kaspersky Anti-Virus for Linux Mail Server](#)

Funktionen:

- Zuverlässiger Schutz vor schädlichen und potenziell gefährlichen Programmen
- Spam-Filterung
- Scan von ein- und ausgehenden E-Mails und E-Mail-Anhängen

- Antiviren-Untersuchung aller E-Mails auf einem Microsoft Exchange Server, einschließlich der gemeinsamen Ordner
- Untersuchung von E-Mails, Datenbanken und anderen Objekten auf Lotus Notes/Domino-Servern
- Filterung von E-Mails nach Typen der Anhänge
- Isolierung verdächtiger Objekte in einem speziellen Speicher
- Komfortable Bedienung
- Verhinderung von Viren-Epidemien
- Monitoring für den Status des Schutzsystems mit Hilfe von Benachrichtigungen
- Berichtssystem über die Arbeit der Anwendung
- Skalierbarkeit im Rahmen der verfügbaren Systemressourcen
- Automatisches Update der Datenbanken

### **Kaspersky Security for Internet-Gateway**

Das Produkt gewährleistet allen Mitarbeitern eines Unternehmens den sicheren Zugriff auf das Internet. Die Lösung löscht automatisch alle schädlichen und potenziell gefährlichen Programme aus dem Datenstrom, der über die Protokolle HTTP und FTP eintrifft. Das Produkt umfasst:

- [Kaspersky Administration Kit](#)
- [Kaspersky Anti-Virus for Proxy Server](#)
- [Kaspersky Anti-Virus for Microsoft ISA Server](#)
- [Kaspersky Anti-Virus for Check Point FireWall-1](#)

Funktionen:

- Zuverlässiger Schutz vor schädlichen und potenziell gefährlichen Programmen
- Echtzeit-Untersuchung des Internet-Datenverkehrs (HTTP/FTP)
- Filterung des Internet-Datenverkehrs nach einer Liste vertrauenswürdiger Server, nach Objekttypen und nach Benutzergruppen
- Isolierung verdächtiger Objekte in einem speziellen Speicher
- Komfortable Bedienung
- Berichtssystem über die Arbeit der Anwendung

- Unterstützung von Hardware-Proxyservern
- Skalierbarkeit im Rahmen der verfügbaren Systemressourcen
- Automatisches Update der Datenbanken

### **Kaspersky® Anti-Spam**

Kaspersky Anti-Spam ist die erste in Russland entwickelte Software zum Spam-Schutz von kleinen und mittleren Unternehmen. Das Programm vereint moderne Verfahren der Sprachanalyse für Informationen in Textform, sämtliche modernen Verfahren zum Filtern von E-Mails (einschließlich RBL-Listen und formeller Prüfung von Nachrichten) sowie eine einmalige Auswahl an Dienstprogrammen, durch die der Nutzer in die Lage versetzt wird, bis zu 95 % der unerwünschten Nachrichten zu identifizieren und zu eliminieren.

Kaspersky® Anti-Spam ist ein Filterprogramm, das, am "Eingang" des firmeninternen Netzwerks installiert, sämtliche eingehenden E-Mails auf Spam überprüft. Das Programm ist kompatibel mit jedem beliebigen Mailing-System und kann sowohl auf bereits funktionierenden als auch auf separaten Mailservern installiert werden.

Die tägliche Aktualisierung der Filterdatenbank mit Mustertexten aus unserem Sprachlabor garantiert eine hohe Effizienz des Produkts. Die Datenbank-Updates erscheinen alle 20 Minuten.

### **Kaspersky Anti-Virus® for MIMESweeper**

Kaspersky Anti-Virus® for MIMESweeper bietet die Hochgeschwindigkeits-Antiviren-Untersuchung des Datenverkehrs auf Servern, die Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web verwenden.

Das Programm besitzt die Form eines Plug-Ins (Erweiterungsmoduls) und führt im Echtzeit-Modus die Antiviren-Untersuchung und die Bearbeitung der ein- und ausgehenden E-Mail-Nachrichten durch.

## **A.2. Kontaktinformationen**

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie gern umfassend per Telefon oder E-Mail beraten.

Weitere Information erhalten Sie bei:

Kaspersky Labs GmbH

Steinheilstraße 13

85053 Ingolstadt

Technischer Support	E-Mail: <a href="mailto:support@kaspersky.de">support@kaspersky.de</a>
Allgemeine Informationen	<a href="http://www.kaspersky.de/">http://www.kaspersky.de/</a> <a href="http://www.viruslist.de/">http://www.viruslist.de/</a>
Feedback zu unseren Benutzerhandbüchern	<a href="mailto:docfeedback@kaspersky.com">docfeedback@kaspersky.com</a> (Diese Adresse ist für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.)

---

# ANHANG B. ENDBENUTZER- LIZENZVERTRAG

## Endbenutzer-Lizenzvertrag für die erworbene KASPERSKY LAB SOFTWARE

WICHTIG - bitte sorgfältig lesen: Lesen Sie die in diesem KASPERSKY LAB Endbenutzer-Lizenzvertrag ("EULA") beschriebenen Rechte und Einschränkungen sorgfältig durch. Sie werden gebeten, die Bestimmungen des EULAs zu prüfen und ihnen zuzustimmen oder diese abzulehnen.

Indem Sie das Sicherheitsetikett auf der CD-Box aufreißen oder wenn Sie die SOFTWARE installieren, erklären Sie sich mit den Bestimmungen des EULAs einverstanden. Falls Sie mit den Bestimmungen des EULAs NICHT einverstanden sind, geben Sie die erworbene Software bitte innerhalb von 14 Tagen an die Einkaufsstelle zurück. Nach Eingabe des Aktivierungscodes ist eine Rückgabe der Software ausgeschlossen.

Jede Bezugnahme auf "Software" schließt den Aktivierungscode oder die Schlüsseldatei ein, den Sie von Kaspersky Lab als Teil der Software erhalten.

Dieser EULA ist ein rechtsgültiger Vertrag zwischen Ihnen, dem Besitzer eines Exemplars der SOFTWARE (entweder als natürlicher oder als juristischer Person) und KASPERSKY LAB. KASPERSKY LAB wird sich das exklusive Urheberrecht auf die Computersoftware (auf die Software und die Antiviren-Datenbanken) vorbehalten. Indem Sie die SOFTWARE installieren, erklären Sie sich damit einverstanden, durch die Bestimmungen dieses EULAs gebunden zu sein. Falls Sie den Bestimmungen dieses EULAs nicht zustimmen, sind Sie nicht berechtigt, die SOFTWARE zu installieren und zu verwenden.

Die SOFTWARE ist sowohl durch Urheberrechtsgesetze und internationale Urheberrechtsverträge als auch durch andere Gesetze und Vereinbarungen über geistiges Eigentum geschützt. Die SOFTWARE wird lizenziert, nicht verkauft.

1. LIZENZEINRÄUMUNG. Durch diesen EULA werden Ihnen folgende Rechte eingeräumt:

- Sie sind berechtigt, eine Kopie der SOFTWARE auf einem einzigen Computer zu installieren und zu verwenden. Eine Mehrplatzlizenz der SOFTWARE, dürfen Sie auf so vielen Computern installieren, wie Sie Lizenzen erworben haben.
- Sie sind berechtigt, die installierte SOFTWARE innerhalb der erworbenen Lizenzdauer zu benutzen.

## 2. EINSCHRÄNKUNGEN

- Einschränkungen im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung. Sie sind nicht berechtigt, die SOFTWARE zurückzuentwickeln (Reverse Engineering), zu dekompileieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Einschränkung, dies ausdrücklich gestattet. Sie sind nicht berechtigt, diese Software in automatischen, halbautomatischen oder manuellen Tools zu verwenden, welche dazu dienen, Virensignaturen, Virenerkennungsroutinen, sowie beliebige andere Daten oder Codes zum Erkennen von schädlichem Code oder Daten zu erstellen.
- Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.
- Supportleistungen. Nach Kauf und Aktivierung der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die Lizenzdauer. Supportleistungen verstehen sich wie folgt:
  - stündliche Updates der Antiviren-Datenbank
  - kostenloses Updates der Software
  - kostenlose technische Unterstützung sowohl per e-Mail als auch per Telefon mit KASPERSKY LAB

3. KÜNDIGUNG. Unbeschadet sonstiger Rechte ist KASPERSKY LAB berechtigt, diesen EULA zu kündigen, sofern Sie gegen die Bestimmungen dieses EULAs verstoßen. In einem solchen Fall sind Sie verpflichtet, sämtliche Kopien der SOFTWARE und alle ihre Komponenten zu vernichten.

4. URHEBERRECHT. Eigentum und Urheberrecht auf die SOFTWARE, die gedruckten Begleitmaterialien und jede Kopie der SOFTWARE liegen bei KASPERSKY LAB.

5. GEWÄHRLEISTUNG. KASPERSKY LAB gewährleistet, dass:

- die SOFTWARE den Spezifikationen im wesentlichen entspricht.
- im Falle einer physikalischen Lieferung der Originaldatenträger frei von Material- und Herstellungsfehlern ist.
- das Programm korrekt auf den Datenträger aufgezeichnet ist, die Dokumentation sämtliche Informationen enthält, die KASPERSKY LAB für die Benutzung der Software für erforderlich hält.
- die SOFTWARE binnen 90 Tagen ab der ersten Installation oder dem ersten Download, falls richtig behandelt, der in der beiliegenden Dokumentation bestimmten Funktionalität entspricht und laut derer voll funktionsfähig ist.

Gewährleistungspflichtige Mängel werden von KASPERSKY LAB oder dessen Lieferanten nach Entdeckung, auf jeden Fall aber vor Ablauf von der Gewährleistungsfrist, dem Ermessen von Kaspersky Lab nach, durch Ersatz, Reparatur, Umtausch oder Rückzahlung beseitigt, falls eine Mangelrüge rechtzeitig an Kaspersky Lab oder dessen Lieferanten gerichtet wurde. KASPERSKY LAB oder dessen Lieferanten übernehmen keine Gewährleistung für Mängel, die auf andere als für die Software vorgesehenen Einsatzbedingungen, unsachgemäße Behandlung oder dergleichen zurückzuführen sind.

ALLE ANDERE GEWÄHRLEISTUNGEN UND BEDINGUNGEN, SEIEN SIE AUSDRÜCKLICH ODER KONKLUDENT, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF, (FALLS ZUTREFFEND) JEDE KONKLUDENTE GEWÄHRLEISTUNG IM HINBLICK AUF HANDELSÜBLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, FAHRLÄSSIGKEIT ODER MANGELNDE FACHMÄNNISCHE BEMÜHUNGEN WERDEN VON KASPERSKY LAB ODER DESSEN LIEFERANTEN ABGELEHNT. ES BESTEHT EBENFALLS KEINE GEWÄHRLEISTUNG ODER BEDINGUNG VON RECHTSANSPRÜCHEN IN BEZUG AUF RECHTSINHABERSCHAFT, UNGESTÖRTES NUTZUNGSVERGNÜGEN ODER NICHTVERLETZUNG VON RECHTEN DRITTER. DAS GESAMTE RISIKO, DAS BEI DER BENUTZUNG ODER LEISTUNG DER SOFTWARE ENTSTEHT, LIEGT BEI IHNEN.

6. AUSSCHLUSS DER HAFTUNG FÜR ALLE SCHÄDEN. SOWEIT GESETZLICH ZUGELASSEN, SIND KASPERSKY LAB ODER DESSEN LIEFERANTEN IN KEINEM FALL HAFTBAR FÜR IRGENDWELCHE FOLGE-, ZUFÄLLIGEN, DIREKTEN, INDIREKTEN, SPEZIELLEN, STRAFRECHTLICHEN ODER ANDEREN SCHÄDEN WELCHER ART AUCH IMMER (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AN PERSONEN ODER SACHEN, SCHÄDEN AUS ENTGANGENEM GEWINN, GESCHÄFTSUNTERBRECHUNG, VERLUST VON GESCHÄFTLICHEN INFORMATIONEN, FÜR DEN VERLUST VON PRIVATSPHÄRE, DIE UNMÖGLICHKEIT, EINE PFLICHT ZU ERFÜLLEN (EINSCHLIESSLICH GEMÄSS TREU UND GUTEN GLAUBENS ODER VERNÜNFTIGER ANGEMESSENER SORGFALT) ZU ERFÜLLEN, FÜR FAHRLÄSSIGKEIT ODER ANDERE VERMÖGENSSCHÄDEN), DIE AUS DER VERWENDUNG DER SOFTWARE ODER DER TATSACHE, DASS SIE NICHT VERWENDET WERDEN KANN, RESULTIEREN ODER DAMIT IN ZUSAMMENHANG STEHEN, SELBST WENN KASPERSKY LAB ODER DESSEN LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WORDEN IST. DIESER HAFTUNGSAUSSCHLUSS FÜR SCHÄDEN GILT AUCH DANN, WENN ABHILFEMASSNAHMEN IHREN WESENTLICHEN ZWECK VERFEHLEN.

7. ANWENDBARES RECHT. Dieser Vertrag unterliegt der Gesetzgebung des Landes, indem das Produkt erworben wurde.