

KASPERSKY LAB

Kaspersky[®] Administration Kit 6.0

Handbuch für
Administratoren

KASPERSKY® ADMINISTRATION KIT 6.0

Handbuch für Administratoren

© Kaspersky Lab

Besuchen Sie unsere Webseite: <http://www.kaspersky.com/de/>

Redaktionsdatum: Februar 2007

Inhalt

KAPITEL 1. KASPERSKY ADMINISTRATION KIT	6
1.1. Kaspersky Administration Kit	6
1.2. Hardware- und Softwarevoraussetzungen	8
1.3. Lieferumfang	10
1.4. Service für registrierte Benutzer	10
1.5. Art des Dokumentes	11
1.6. Textgestaltung	11
KAPITEL 2. KONZEPTION VON KASPERSKY ADMINISTRATION KIT	13
2.1. Grundbegriffe	13
2.1.1. Logisches Netzwerk. Administrationsserver	13
2.1.2. Hierarchie der Administrationsserver	14
2.1.3. Client-Computer. Gruppe	15
2.1.4. Administratorarbeitsplatz	16
2.1.5. PlugIn zur Anwendungsverwaltung	17
2.1.6. Richtlinien, Einstellung und Tasks	18
2.1.7. Interaktion von Richtlinie und lokalen Anwendungseinstellungen	20
2.2. Verbindung von Client-Computern mit Administrationsserver	22
2.3. Geschützte Verbindung mit dem Administrationsserver	23
2.3.1. Zertifikat des Administrationsservers	23
2.3.2. Serverauthentifizierung bei Verbindung durch die Konsole	24
2.3.3. Serverauthentifizierung bei Verbindung durch Client-Computer	24
2.4. Identifikation von Client-Computern im logischen Netzwerk	25
2.5. Zugriffsrechte im logischen Netzwerk	25
2.6. Einführung des Antiviren-Schutzes über das logische Netzwerk	28
2.7. Aufbau eines zentralisierten Verwaltungssystems für den Antiviren-Schutz	28
2.8. Wartung des logischen Netzwerks	30
2.9. Koordination der gemeinsamen Arbeit von Administratoren	31
2.10. Konzeption der Benutzeroberfläche	31
2.10.1. Programmstart	32
2.10.2. Hauptfenster des Programms	32

2.10.3. Konsolenstruktur.....	33
2.10.4. Kontextmenü.....	35
KAPITEL 3. INSTALLATION VON KASPERSKY ADMINISTRATION KIT	43
3.1. Verbindung zum Administrationsserver.....	43
3.2. Vergabe von Rechten	44
3.3. Informationen zum Computernetzwerk anzeigen. Domänen, IP-Subnetze und Gruppen Active Directory	45
3.4. Schnellstart-Assistent	49
3.5. Struktur des logischen Netzwerks erstellen, anzeigen und ändern.....	50
3.5.1. Gruppen	53
3.5.2. Client-Computer.....	55
3.5.3. Untergeordnete Administrationsserver	57
KAPITEL 4. ARBEITEN MIT DEM PROGRAMM	60
4.1. Einstellung der Anwendungsparameter	60
4.1.1. Verwalten von Richtlinien	60
4.1.2. Lokale Anwendungseinstellungen	66
4.2. Verwaltung von Anwendungen.....	67
KAPITEL 5. UPDATE DER ANTIVIREN-DATENBANKEN UND PROGRAMMMODULE.....	74
5.1. Update-Download durch Administrationsserver.....	75
5.2. Verbreitung von Updates auf die Client-Computer	78
5.2.1. Update für Anwendungen	78
5.2.2. Automatisches Verbreiten durch Administrationsserver	78
5.3. Update untergeordneter Server und ihrer Client-Computer	80
5.4. Verbreitung von Updates mit Updaten-Agenten	81
KAPITEL 6. BEDIENUNG	83
6.1. Lizenzverlängerung.....	83
6.2. Quarantäne und Backup	85
6.3. Ereignisprotokolle. Ereignisfilter	87
6.4. Protokolle	91
6.5. Computersuche	93
6.6. Benutzerdefinierter Computer-Filter	96
6.7. Überwachung von Virenepidemien	98

6.8. Sicherheitskopieren und Wiederherstellung von Daten des Administrationsservers	102
ANHANG A. GLOSSAR	104
ANHANG B. KASPERSKY LAB.....	111
B.1. Andere Produkte von Kaspersky Lab	112
B.2. Kontaktinformationen	124
ANHANG C. ENDBENUTZER-LIZENZVERTRAG.....	125

KAPITEL 1. KASPERSKY ADMINISTRATION KIT

1.1. Kaspersky Administration Kit

Die Anwendung **Kaspersky® Administration Kit** dient der zentralisierten Lösung der wichtigsten Administrationsaufgaben zur Verwaltung des Antiviren-Sicherheitssystems eines Firmencomputernetzwerks, das auf Anwendungen des Herstellers basiert, die zu den Produkten Kaspersky Anti-Virus Business Optimal und Kaspersky Corporate Suite gehören. Kaspersky Administration Kit unterstützt die Arbeit in allen Netzwerkkonfigurationen, die das Protokoll TCP/IP verwenden.

Das Programm ist bestimmt für Administratoren von Firmencomputernetzwerken sowie für Mitarbeiter, die für den Antiviren-Schutz von Computern in Organisationen verantwortlich sind.

Die Anwendung bietet dem Administrator folgende Möglichkeiten:

- Zentralisierte Remote-Installation und -Deinstallation von Anwendungen, die zum Bestand von Kaspersky-Lab-Produkten gehören, auf Computern des Netzwerkes. Der Administrator kann die notwendige Auswahl von Kaspersky-Lab-Anwendungen einmal auf einen ausgewählten Computer kopieren und danach die Remote-Installation auf einer beliebigen Anzahl von Netzwerkcomputern vornehmen.
- Lizenzverwaltung. Erlaubt die zentralisierte Installation von Lizenzschlüsseln für alle installierten Anwendungen des Herstellers und die Kontrolle über die Einhaltung des Lizenzvertrags (Verhältnis der Lizenzanzahl zur Anzahl der im Netzwerk laufenden Anwendungen) und die Gültigkeitsdauer der Lizenz.
- Zentralisierte Remote-Verwaltung von Anwendungen, die zum Bestand von Kaspersky-Lab-Produkten gehören. Diese Option erlaubt werden das Erstellen eines mehrstufigen Antiviren-Schutzsystems und die Verwaltung der Arbeit aller Anwendungen vom Administratorarbeitsplatz. Letzteres ist besonders aktuell für Großunternehmen, in denen das lokale Netzwerk aus einer großen Anzahl von Computern besteht und mehrere territorial getrennte Gebäude oder Räume umfassen kann. Diese Option bietet folgende Funktionen:

- Zusammenfassung von Computern in *Administrationsgruppen* entsprechend der auszuführenden Funktionen und der darauf installierten Anwendungen.
 - Zentralisierte Konfiguration von Funktionseinstellungen einer Anwendung durch Erstellen und Übernehmen von *Gruppenrichtlinien (Gruppenpolicies)*.
 - Individuelle Konfiguration der Funktionseinstellungen einer Anwendung für einzelne Computer mit Hilfe der *Anwendungseinstellungen*.
 - Zentralisierte Verwaltung der Arbeit von Anwendungen durch das Erstellen und den Start von *Gruppentasks und globalen Tasks*.
 - Individuelle Funktionsschemata für Anwendungen durch das Erstellen und den Start von Tasks für eine Auswahl von Computern aus unterschiedlichen Administrationsgruppen.
- Automatisches Update der Antiviren-Datenbanken und Programmmodule auf den Computern. Diese Option erlaubt die Ausführung der zentralisierten Aktualisierung der Antiviren-Datenbanken für alle installierten Anwendungen des Herstellers ohne direkten Zugriff jedes Computers auf die Internetserver von Kaspersky Lab. Das Update kann automatisch nach einem vom Administrator festgelegten Zeitplan erfolgen. Der Administrator kann die Verteilung von Updates an die Client-Computer verfolgen.
 - Protokoll-System. Diese Option erlaubt das zentralisierte Erstellen einer Statistik über die Arbeit aller installierten Anwendungen des Herstellers, die Kontrolle über die korrekte Funktion dieser Anwendungen und das Erstellen von Protokollen auf Basis der erhaltenen Daten. Der Administrator kann ein Protokoll über die Arbeit einer Anwendung für das gesamte Netzwerk und Protokolle über die Funktion der Anwendungen auf jedem Computer erstellen.
 - Benachrichtigungsmechanismus für Ereignisse bei der Arbeit von Anwendungen. Mechanismus zum Versenden von Benachrichtigungen. Dem Administrator wird erlaubt, eine Liste von Ereignissen für die Arbeit von Anwendungen zu erstellen, bei deren Eintreten er eine Benachrichtigung erhalten wird. Zu diesen Ereignissen können z.B. ein Virusfund, der inkorrekte Abschluss der Updateprozedur für die Antiviren-Datenbanken auf einem Computer oder der Fund eines neuen Computers im Netzwerk gehören.

- Zusammenarbeit mit Cisco Network Admission Control (NAC). Diese Möglichkeit erlaubt Ihnen die Übereinstimmung zwischen Antivirenschutz und Cisco NAC Zuständen einzustellen.

Die Anwendung Kaspersky Administration Kit besteht aus drei Basiskomponenten:

- **Administrationsserver** – Diese Komponente führt die Funktionen zum zentralisierten Speichern von Daten über die im Firmennetzwerk installierten Kaspersky-Lab-Anwendungen und deren Verwaltung aus.
- **Administrationsagent** – Er dient der Kommunikation zwischen Administrationsserver und Kaspersky-Lab-Anwendungen, die auf einem konkreten Netzwerkknoten (Workstation oder Server) installiert sind. Diese Komponente ist für alle Windows-Anwendungen aus dem Bestand der Produkte des Herstellers Kaspersky Anti-Virus Business Optimal und Kaspersky Corporate Suite einheitlich. Für Novell- und Unix-Anwendungen wurden eigene Versionen des Administrationsagenten entwickelt.
- **Administrationskonsole** – Diese Komponente bietet eine Benutzeroberfläche für die Administrationsdienste von Server und Agent. Die Administrationskonsole besitzt die Form einer Erweiterungskomponente zu Microsoft Management Console (MMC).

1.2. Hardware- und Softwarevoraussetzungen

Administrationsserver

- Softwareanforderungen:
 - MSDE 2000 SP 3 oder MS SQL Server 2000 SP 31 und höher oder MySQL 5.0.22 (Codeseite als Standard ist UTF-8) oder MS SQL 2005 und höher oder MS SQL 2005 Express und höher
 - Microsoft Windows 2000 SP 1 und höher; Microsoft Windows XP Professional mit installiertem Service Pack 1 und höher, Microsoft Windows 2003 Server und höher; Microsoft Windows

¹ Zur Installation von MSDE kann die Distribution verwendet werden, die im Lieferumfang von Kaspersky Administration Kit enthalten ist.

NT4 mit installiertem Service Pack 6a und höher, MDAC 2.8 und höher, Microsoft Windows Vista, Microsoft Windows Vista x64

- Hardwareanforderungen:
 - Intel Pentium III Prozessor, 800 MHz oder schneller
 - 128 MB RAM
 - freier (verfügbarer) Speicherplatz auf der Festplatte 400 MB

Administrationskonsole

- Softwareanforderungen:
 - Microsoft Windows 2000 SP 1 und höher; Microsoft Windows XP Professional mit installiertem Service Pack 1 und höher; Microsoft Windows 2003 Server und höher; Microsoft Windows NT4 mit installiertem Service Pack 6a und höher
 - Microsoft Management Console Version 1.2 und höher.
 - Mit Microsoft Windows NT4 – Internet Explorer 6.0
- Hardwareanforderungen:
 - Intel Pentium II Prozessor, 400 MHz oder schneller
 - 64 MB RAM
 - freier (verfügbarer) Speicherplatz auf der Festplatte 10 MB

Administrationsagent

- Softwareanforderungen:
 - Für Windows-Systeme:

Microsoft Windows 98; Microsoft Windows ME; Microsoft Windows 2000 mit installiertem Service Pack 1 und höher; Microsoft Windows NT4 mit installiertem Service Pack 6a und höher; Microsoft Windows XP Professional mit installiertem Service Pack 1 und höher, Microsoft Windows 2003 Server und höher, Microsoft Windows Vista.

- Für Novell-Systeme:

Novell NetWare 6 SP3 und höher; Novell NetWare 6.5 SP3 und höher.

- Hardwareanforderungen:
 - Für Windows-Systeme:

- Intel Pentium Prozessor, 233 MHz oder schneller;
- 32 MB RAM;
- freier (verfügbarer) Speicherplatz auf der Festplatte 10 MB.
- Für Novell-Systeme:
 - Intel Pentium Prozessor, 233 MHz oder schneller;
 - 12 MB RAM;
 - freier (verfügbarer) Speicherplatz auf der Festplatte 32 MB.

1.3. Lieferumfang

Das Softwareprodukt wird kostenlos mit allen Kaspersky-Lab-Anwendungen, die zu Kaspersky Anti-Virus Business Optimal und Kaspersky Corporate Suite (als verpackte Variante) geliefert und steht außerdem auf der Webseite von Kaspersky Lab www.kaspersky.com/de zum Download bereit.

1.4. Service für registrierte Benutzer

Kaspersky Lab bietet seinen legalen Benutzern ein breites Spektrum an Serviceleistungen, die eine gesteigerte Effektivität der hauseigenen Produkte ermöglichen.

Durch den Erwerb einer Lizenz für eine Kaspersky-Lab-Anwendung, die zu Kaspersky Anti-Virus Business Optimal und Kaspersky Corporate Suite gehört, werden Sie zum registrierten Programmbenutzer von Kaspersky Administration Kit und können die folgenden Serviceleistungen in Anspruch nehmen:

- Nutzung neuer Versionen des Softwareprodukts
- Beratung in Fragen zu Installation, Konfiguration und Benutzung des betreffenden Softwareprodukts über das Telefon und mit Webformularen

Wenn Sie an den Technischen Support-Service wenden, machen Sie Angaben zur Lizenz für die Kaspersky-Lab-Anwendung, die Sie zusammen mit dem Kaspersky Administration Kit benutzen.

- Nachrichten über das Erscheinen neuer Softwareprodukte von Kaspersky Lab und über das Auftauchen neuer Viren (Dieser Service gilt für Benutzer, die den Newsletter von Kaspersky Lab abonniert haben).

Die Beratung bezieht sich nicht auf Fragen über Funktion und Benutzung von Betriebssystemen und anderen Technologien.

1.5. Art des Dokumentes

Dieses Nachschlagewerk enthält Angaben zum Programm Kaspersky Administration Kit sowie eine Schritt-für-Schritt-Anleitung für die einzelnen Programmfunktionen. Die Grundbegriffe und eine allgemeine Beschreibung für die Arbeit mit dem Programm befinden sich im Handbuch für den Administrator von Kaspersky Administration Kit. Funktionen, die im Handbuch stehen, erscheinen im Text unterstrichen.

Fragen, die Benutzer häufig an die Mitarbeiter den Technischen Kundendienstes von Kaspersky Lab stellen, können Sie auf unserer Internetseite im Abschnitt **Dienste** → **Wissensdatenbank** nachlesen. In diesem Abschnitt stehen Informationen zur Installation, zu den Einstellungen und zu den Funktionen der Programme von Kaspersky Lab sowie Angaben zum Entfernen der am meisten verbreiteteten Viren und zum Reparieren von infizierten Dateien.

1.6. Textgestaltung

Bestimmte Textteile dieser Dokumentation sind entsprechend ihrer Bedeutung durch unterschiedliche Formatierungselemente hervorgehoben. Die Textgestaltung wird in folgender Tabelle erläutert.

Formatierung	Bedeutung
Fette Schrift	Namen von Menüs, Menüelementen, Dialogfenstern, Elementen von Dialogfenstern, usw.

Formatierung	Bedeutung
Hinweis	Zusatzinformationen, Hinweise
Achtung!	Sehr wichtige Informationen
<i>Um diese Aktion durchzuführen,</i> 1. Schritt 1. 2. ...	Beschreibung einer Folge von Schritten und möglichen Aktionen, die vom Benutzer durchgeführt werden.
[Parameter] – Funktion des Parameters	Befehlszeilenparameter
Text von informativen Meldungen und Befehlszeilen	Text von Konfigurationsdateien, informativen Programm Meldungen und Befehlszeilen

KAPITEL 2. KONZEPTION VON KASPERSKY ADMINISTRATION KIT

2.1. Grundbegriffe

2.1.1. Logisches Netzwerk. Administrationsserver

Das **logische Netzwerk** ist eine Ansammlung von Computern, die ein Netzwerk bilden, die mithilfe von Kaspersky Administration Kit vereint sind, um im Remote-Betrieb die Kaspersky-Lab-Anwendungen zentralisiert zu verwalten.

Ein Computer des Firmennetzwerks, auf dem die Komponente Administrationsserver installiert ist, wird **Administrationsserver** genannt.

Der Administrationsserver wird auf einem Computer als Dienst mit den folgenden Attributen installiert:

- unter dem Namen Kaspersky Administration Server
- mit automatischem Task-Start beim Starten des Betriebssystems
- unter der Registrierung Lokales System oder unter der Registrierung Benutzerkonto je nach der Auswahl beim Installieren der Komponente.

Der Administrationsserver (oder präziser: die darauf installierte Komponente Administrationsserver) besitzt folgende Funktionen:

- Speichern der Struktur des logischen Netzwerks (Netzwerkkonfiguration)
- Speichern einer Kopie der Konfigurationsdaten von den Computern im logischen Netzwerk
- Organisation der Distributionsdateien für Kaspersky-Lab-Anwendungen
- Remote-Installation und -Deinstallation von Anwendungen auf Computern
- Update der Antiviren-Datenbanken und Programmmodule

- Verwaltung von *Richtlinien* und *Tasks* auf Computern des logischen Netzwerks
- Speichern von Informationen über Ereignisse, die auf Computern des logischen Netzwerks eintreten.
- Erstellen von Protokollen über die Arbeit der Anwendungen des logischen Netzwerks
- Verteilung von Lizenzschlüsseln auf die Computer des logischen Netzwerks, Speichern von Informationen über die Lizenzschlüssel.
- Senden von Benachrichtigungen über die auf Computern des logischen Netzwerks ausgeführten Tasks. Solche Benachrichtigungen können z.B. über einen Virenfund auf einem Client-Computer informieren.

2.1.2. Hierarchie der Administrationsserver

Die Administrationsserver können eine Hierarchie nach dem Vorbild "**Hauptserver – untergeordneter Server**" bilden. Jeder Administrationsserver kann mehrere untergeordnete Server auf einem Server oder auf verschiedenen Hierarchieebenen haben. Zu einem logischen Netzwerk des Hauptservers gehören dann die logischen Netzwerke aller untergeordneten Server. Die Tiefe der Hierarchie ist nicht begrenzt. So lassen sich separate, voneinander unabhängige Bereiche des Computer-Netzwerkes von verschiedenen Administrationsservern verwalten, die ihrerseits vom Hauptserver verwaltet werden (Details s. Pkt. 3.5.1 auf S. 53).

Der Aufbau einer Serverhierarchie kann für folgende Aufgaben genutzt werden:

- Belastung des Administrationsservers beschränken (verglichen mit Administrationsserver im Netzwerk des Servers)
- Traffic im Netzwerk verringern und Zusammenarbeit mit Remote-Offices vereinfachen. Es muss keine Verbindung mit dem Hauptserver und jedem Computer im Netzwerk hergestellt werden, die sich beispielsweise in anderen Regionen befinden. Es genügt, in jedem Segment des Netzwerks einen untergeordneten Administrationsserver zu installieren, die Computer in einem logischen Netzwerk von untergeordneten Servern zu verteilen und eine schnelle Verbindung der untergeordneten Server mit dem Hauptserver einzurichten.
- Exakte Verteilung der Zuständigkeiten unter den Administratoren für die Antiviren-Sicherheit. Der Status der Antiviren-Sicherheit lässt sich im Corporate-Netzwerk zentral steuern und überwachen.

Jeder Computer, der zur Struktur eines logischen Netzwerkes gehört, kann nur mit einem Administrationsserver verbunden sein.

Der Administrator muss selbst die Richtigkeit der Verbindung von Computern mit den Administrationsservern kontrollieren, indem er die Funktion Computer suchen nach Netzwerkattributen in logischen Netzwerken von verschiedenen Servern nutzt.

2.1.3. Client-Computer. Gruppe

Die Interaktion zwischen Administrationsserver und Computern, um:

- Informationen über den aktuellen Status der Anwendungen zu beziehen
- Steuerungsbefehle zu versenden und zu empfangen
- Konfigurationsinformationen zu synchronisieren
- den Server mit Informationen zu Ereignissen bei der Arbeit von Anwendungen zu informieren
- die Funktion des *Update-Agenten* zu gewährleisten

erledigt der Administrationsagent. Diese Komponente muss auf jedem Computer installiert sein, auf dem Kaspersky-Lab-Anwendungen mit dem Kaspersky Administration Kit gesteuert werden sollen.

Der Administrationsagent wird auf dem Computer als Dienst mit den folgenden Attributen installiert:

- mit dem Namen Kaspersky Network Agent
- mit automatischem Task-Start beim Start des Betriebssystems
- mit der Registrierung Lokales System.
- Zusammen mit dem Administrationsagenten wird auf dem Computer Plugin für Zusammenarbeit mit Cisco NAC installiert. Dieser Plugin funktioniert im Fall, wenn auf dem Computer die Anwendung Cisco Trust Agent installiert ist. Die Parameter der Zusammenarbeit mit Cisco NAC werden in den Eigenschaften des Administrationsserver definiert.

Der Computer, der Server oder die Arbeitsstation, auf dem/r der Administrationsagent und die zu steuernden Kaspersky-Lab-Anwendungen installiert sind, werden – **Clients des Administrationsserver** (oder einfach *Client-Computer*) genannt.

Je nach organisationstechnischer oder territorialer Struktur des Unternehmens sind die zu erfüllenden Funktionen und die auf den Client-Computern zu installierenden Kaspersky-Lab-Anwendungen in *Administrationsgruppen* organisiert. Diese Einheit dient dem Komfort beim Bedienen von Computern als Ganzes und ein beliebiger Inhalt von anzugebenden Grundsätze kann eingehalten werden und es lassen sich andere Vorgaben vom Administrator machen. So kann zum Beispiel die oberste Ebene aus Gruppen bestehen, die den Abteilungen entsprechen. Auf der nächsten Ebene, in den jeweiligen Abteilungen, werden dann die Computer je nach den von Ihnen erwarteten Funktionen zusammengefasst: Eine Gruppe von Computern umfasst Arbeitsstationen, die andere Gruppe hat alle Fileserver usw..

Eine **Gruppe** sind Client-Computer, die anhand eines beliebigen Merkmals vereint sind, um die Computer der Gruppe als Ganzes zu verwalten. Für jeden Client-Computer in der Gruppe werden vorgegeben:

- einheitliche Parameter für die Arbeit von Anwendungen – mithilfe von *Gruppenrichtlinien*
- einheitlicher Modus für die Arbeit von Anwendungen durch Erstellen von *Gruppentasks* (Programmfunktionen) mit vorgegebenen Parametersätzen (beispielsweise: Erstellen und Installieren eines einheitlichen *Installationspaketes*, Update der Antiviren-Datenbanken und Anwendungsmodule, Scan auf Befehl und Echtzeitschutz).

Ein Client-Computer kann nur zu einer Gruppe gehören.

Der Administrator kann eine Hierarchie von Servern und Gruppen mit beliebiger Verschachtelungstiefe erstellen, wenn so die Ausführung von Tasks für die Programmsteuerung erleichtert wird. Auf einer Hierarchieebene können sich Administrationsserver, Gruppen und Client-Computer befinden.

2.1.4. Administratorarbeitsplatz

Die Computer, auf denen die Komponente Administrationskonsole installiert ist, werden **Administratorarbeitsplätze** genannt. Von diesen Computern aus können die Administratoren zentralisiert die Remote-Verwaltung der Konfiguration aller auf den Client-Computern eines logischen Netzwerks installierten Kaspersky-Lab-Anwendungen vornehmen.

Nach dem Installieren der Administrationskonsole auf dem Computer erscheint im Menü **Start / Programme / Kaspersky Administration Kit** das Symbol für dessen Aufruf.

Die Kommunikation zwischen Administrationsserver und Client-Computern (Senden von Informationen über den aktuellen Status von Anwendungen, Senden und Empfang von Verwaltungsbefehlen, Synchronisierung von Konfigurationsdaten, Senden von Informationen über Ereignisse bei der Arbeit von Anwendungen an den Administrationsserver) übernimmt der **Administrationsagent**.

Der Arbeitsplatz des Administrators ist kein Objekt des logischen Netzwerks. Beide können aber als Client-Computer darin aufgenommen werden. Die Anzahl der Administratorarbeitsplätze ist theoretisch nicht beschränkt. Die Administratorarbeitsplätze für unterschiedliche logische Netzwerke können zusammenfallen – von jedem dieser Arbeitsplätze aus kann die Verwaltung eines beliebigen logischen Netzwerks in der Struktur des Firmennetzwerks erfolgen.

In einem logischen Netzwerk kann ein und derselbe Computer zugleich als Client des Administrationsservers, als Administrationsserver und Administratorarbeitsplatz dienen.

2.1.5. PlugIn zur Anwendungsverwaltung

Eine Verwaltungsoberfläche für die Arbeit mit einer konkreten Anwendung über die Administrationskonsole bietet die spezielle Komponente **Plug-In zur Anwendungsverwaltung**, die zum Umfang aller Kaspersky-Lab-Anwendungen zählt, deren Verwaltung mit Hilfe von Kaspersky Administration Kit möglich ist. Das Verwaltungs-Plug-In ist für jede Anwendung individuell. Das Plug-In wird am Administratorarbeitsplatz installiert und ermöglicht:

- Dialogfenster (Interface) zum Erstellen und Anpassen der *Richtlinien* einer Anwendung
- Dialogfenster (Interface) zum Erstellen und Anpassen der *Anwendungseinstellungen*
- Dialogfenster (Interface) zum Erstellen und Anpassen der *Task-Einstellungen* einer Anwendung
- Informationen über die von einer Anwendung ausgeführten *Tasks*
- Informationen über die von einer Anwendung generierten Ereignisse
- Funktionen der Administrationskonsole zur Anzeige von Informationen, die von Client-Computern stammen, über Ereignisse und Statistik der Anwendungsarbeit.

2.1.6. Richtlinien, Einstellung und Tasks

Ein **Task** ist eine Aktion, die von einer Kaspersky-Lab-Anwendung ausgeführt wird. Tasks werden nach den auszuführenden Funktionen in **Typen** unterteilt.

Jedem Task entsprechen bestimmte Einstellungen für dessen Ausführung. Die Einstellungen einer Anwendung, die für alle Tasktypen der Anwendung gelten, werden **Anwendungseinstellungen** genannt. Dagegen heißen Einstellungen der Anwendung, die für jeden Tasktyp spezifisch sind, **Task-Einstellungen**. Anwendungseinstellungen und Task-Einstellungen werden stets voneinander getrennt.

Weitere Informationen über die Tasktypen der einzelnen Kaspersky-Lab-Anwendungen finden Sie in den entsprechenden Handbüchern.

Um die Ausführung einer bestimmten Funktion zu initiieren, muss die Anwendung konfiguriert werden, ein entsprechender Task erstellt und konfiguriert und zur Ausführung gestartet werden.

Die Anwendungseinstellungen, die für einen einzelnen Client-Computer über die lokale Schnittstelle und im Remote-Betrieb über die Administrationskonsole festgelegt werden, werden als **lokale Anwendungseinstellungen** bezeichnet.

Das zentralisierte Einstellen von Parametern für Anwendungen, die auf den Client-Computern des logischen Netzwerks installiert sind, erfolgt über *Richtlinien*.

Eine **Richtlinie** ist eine Sammlung von Parametern für die Arbeit einer Anwendung in einer Gruppe. Eine **Richtlinie** enthält die Parameter für die komplette Einstellung aller Programmfunktionen, aber die Parameter ausgenommen, die für konkrete Taskexemplare individuell sind. Beispielhaft für solche Parameter sind Zeitpläne.

So gehören folgende Parameter zu einer Richtlinie:

- Anwendungseinstellungen, die für jeden Task-Typ allgemeingültig sind
- größerer Teil der Taskeinstellungen, die für jeden Task-Typ allgemeingültig sind

Das bedeutet, dass eine Richtlinie für eine Antiviren-Anwendung (s. Abb. 1), die einen Echtzeitschutz-Task und einen Scan-auf-Befehl-Task umfasst, alle notwendigen Anwendungseinstellungen für die Ausführung Einstellungen der beiden Tasktypen enthält, aber zum Beispiel nicht einen Zeitplan für den Aufruf dieser Tasks oder Parameter, die den Untersuchungsbereich betreffen.

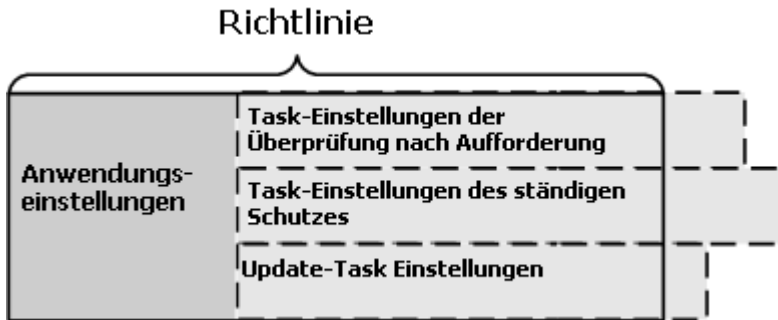


Abbildung 1. Richtlinie

Jeder in einer Richtlinie vorhandener Parameter besitzt außerdem das Attribut „Schloss“, das anzeigt, ob die festgelegten Einstellungswerte in den Richtlinien untergeordneter Hierarchieebenen (für eingebettete Gruppen und untergeordnete Administrationsserver) in den Taskeinstellungen und den lokalen Anwendungseinstellungen geändert werden dürfen. Wenn in der Richtlinie für den Parameter das „Schloss“ angezeigt wird, kann der Wert nicht verändert werden (s. Pkt. auf S.).

In einer Gruppe kann für jede Anwendung eine eigene Richtlinie angelegt werden. Für eine Anwendung können mehrere Richtlinien mit verschiedenen Werten festgelegt werden. Es kann jedoch nur eine Richtlinie für eine Anwendung gelten.

Es ist vorgesehen, eine nicht geltende Richtlinie bei einem Ereignis zu aktivieren, so dass zum Beispiel mehrere fixe Parameter des Antivirenschutzes in Zeiten von Virenepidemien aktiviert werden können.

Es lässt sich auch eine Richtlinie für mobile Benutzer einrichten. Sie tritt in Kraft, wenn der Computer vom logischen Netzwerk der Firma getrennt wird.

In verschiedenen Gruppen können sich die Parameter für die Anwendung voneinander unterscheiden. In jeder Gruppe kann eine eigene Richtlinie für eine Anwendung angelegt werden.

Eingebettete Gruppen und untergeordnete Administrationsserver erben Gruppenrichtlinien der höheren Hierarchieebene.

Im logischen Netzwerk können Tasks zentralisiert erstellt und konfiguriert werden. Ein **Gruppentask** ist einer Administrationsgruppe zugeordnet, ein **lokaler Task** einem einzelnen Client-Computer, und ein **globaler Task** mehreren Client-Computern aus unterschiedlichen Gruppen des logischen Netzwerks.

Ein Gruppentask kann auch dann für eine Gruppe festgelegt werden, wenn die Anwendung „Kaspersky Lab“ nicht auf allen Client-Computern der Gruppe installiert ist. In diesem Fall wird der Gruppentask nur für den Computer ausgeführt, auf denen die betreffende Anwendung installiert ist.

Eingebettete Gruppen und untergeordnete Administrationsserver erben die Gruppentasks der höheren Hierarchieebenen. Ein Task, der für eine Gruppe festgelegt ist, wird nicht nur auf den Client-Computern ausgeführt, die zu dieser Gruppe gehören, sondern auch auf den Client-Computern, die zu den eingebetteten Gruppen und untergeordneten Administrationsserver aller niedrigeren Hierarchieebenen gehören.

Tasks, die lokal für Client-Computer erstellt wurden, werden nur für diesen Computer ausgeführt. Bei der Synchronisierung eines Clients mit dem Administrationsserver werden lokale Tasks zur Liste der für diesen Client-Computer erstellten Tasks hinzugefügt.

Da die Richtlinie alle Parameter einer Anwendung umfasst, können in den Task-Einstellungen nur jene Werte geändert werden, deren Modifikation von der Richtlinie nicht unterdrückt wird, und außerdem Werte, die nur für einen konkreten Task festgelegt werden können. Für einen Task zur Untersuchung eines Laufwerks müssen z. B. Laufwerksname, Maske der zu untersuchenden Dateien usw. angegeben werden.

Ein Task kann automatisch (nach Zeitplan) oder manuell gestartet werden. Die Ergebnisse der Taskausführung werden auf dem Administrationsserver und lokal gespeichert. Der Administrator kann darüber benachrichtigt werden, wie ein bestimmter Task ausgeführt wurde, und Detailprotokolle einsehen.

Informationen über Richtlinien, Anwendungseinstellungen, Globale- und Gruppentasks, wie auch Task-Einstellungen werden auf dem Server gespeichert und bei der Synchronisierung an die Client-Computer verteilt. Zugleich werden in den Daten des Administrationsservers lokale Änderungen eingetragen, die auf Client-Computern erfolgten und in einer Richtlinie gespeichert wurden, sowie die Liste der auf einem Client laufenden Anwendungen, deren Status und die Liste der vorhandenen Tasks aktualisiert.

2.1.7. Interaktion von Richtlinie und lokalen Anwendungseinstellungen

Mithilfe von Richtlinien für alle zu einer Gruppe gehörenden Computer können gleichlautende Parameterwerte für eine Anwendung festgelegt werden.

Die Parameterwerte, die von einer Richtlinie eingegeben wurde, lassen sich für einzelne Computer in der Gruppe mithilfe der lokalen Anwendungseinstellungen verändern. Es lassen sich außerdem Werte nur für die Parameter vorgeben, deren Änderung nicht von einer Richtlinie gesperrt ist: Ein Parameter, der mit einem „Schloss“ gesperrt ist.

Welchen Wert die Anwendung auf dem Client-Computer verwendet (s. Abb. 2), hängt vom „Schloss“ vor dem Parameter in der Richtlinie ab:

- Wenn der Parameter nicht geändert werden darf, wird auf allen Client-Computern der gleiche Wert zugrunde gelegt, der in die Richtlinie eingegeben wurde.
- Wenn Änderungen nicht unterdrückt werden, dann verwendet die Anwendung auf jedem Client-Computer den lokalen Parameter-Wert und nicht den Wert, der in der Richtlinie angegeben ist. Außerdem lässt sich der Wert des Parameters über die lokalen Anwendungseinstellungen ändern.

So verwendet beim Ausführen von Tasks auf einem Client-Computer die Anwendung die eingegebenen Parameter:

- Die Taskeinstellungen und die lokalen Anwendungseinstellungen werden herangezogen, wenn in der Richtlinie die Änderung des Parameters nicht gesperrt wurde.
- Die Richtlinie der Gruppe wird herangezogen, wenn in der Richtlinie die Änderung des Parameters gesperrt wurde.

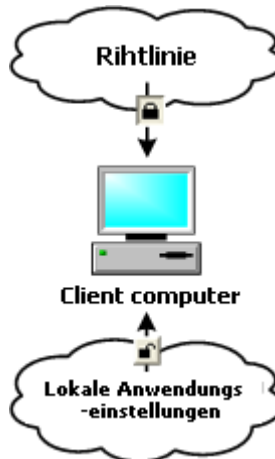


Abbildung 2. Richtlinie und lokalen Anwendungseinstellungen

Wie die lokalen Anwendungseinstellungen nach der ersten Übernahme der Richtlinie geändert werden, wird in der Anwendungsrichtlinie in dem Fenster **Erweitert** festgelegt (s. Abb. 14).

2.2. Verbindung von Client-Computern mit Administrationsserver

Die Kommunikation zwischen Client-Computern und Administrationsserver erfolgt bei der Verbindung der Clients mit dem Server (s. Pkt. 2.1 auf S. 13). Diese Funktionalität wird durch den Administrationsagenten ermöglicht, der auf den Client-Computern installiert ist.

Die Verbindung ist zur Ausführung folgender Operationen erforderlich:

- Synchronisierung der Liste von Anwendungen, die auf dem Client-Computer installiert sind.
- Synchronisierung von Richtlinien, Anwendungseinstellungen, Tasks und Task-Einstellungen
- Empfang aktueller Informationen über den Status der Anwendungen und Taskausführung durch den Server
- Senden von Informationen über Ereignisse an den Server, welche dieser bearbeiten muss.

Gewöhnlich verbindet sich der Client-Computer mit dem Server. Diese Art der Verbindung erfolgt bei der automatischen Datensynchronisierung von Client und Server, sowie beim Senden von Anwendungsereignissen an den Server.

Die automatische Synchronisierung findet entsprechend den Einstellungen des Administrationsagenten in gewissen Zeitabständen statt (z.B. alle 15 Minuten). Das Intervall zwischen den Verbindungen wird vom Administrator festgelegt.

Informationen über ein Ereignis werden sofort nach dem Ereigniseintritt an den Server gesandt.

In den Einstellungen des Client-Computers gibt es den Parameter **Verbindung mit Administrationsserver nicht trennen**, der bestimmt, ob die Verbindung zwischen Client und Server nach Abschluss der oben genannten Operationen getrennt wird. Eine ununterbrochene Verbindung ist erforderlich, wenn die ständige Kontrolle über den Status der Anwendungen nötig ist, der Server aber aus bestimmten Gründen keine Verbindung mit dem Client aufbauen kann (Client ist durch Firewall geschützt, Verbot zum Öffnen von Ports auf dem Client, unbekannte IP-Adresse des Clients, usw.).

Außerdem kann der Synchronisierungsprozess vom Administrator manuell mit Hilfe des Befehls **Synchronisieren** im Kontextmenü des Client-Computers (s. Pkt. 2.10.4 auf S. 35) gestartet werden. In diesem Fall wird die Verbindung auf andere Weise durch den Server initiiert. Dazu wird auf dem Client-Computer ein UDP-Port geöffnet. Der Server sendet eine Verbindungsanfrage auf den UDP-Port. Als Reaktion werden die Rechte des Servers zur Verbindung mit dem Client überprüft (auf Basis einer digitalen Signatur des Administrationssservers) und gegebenenfalls wird die Verbindung hergestellt.

Diese Verbindungsmethode wird auch beim Zugriff auf Daten des Clients verwendet: zum Empfang aktueller Informationen über den Status von Anwendungen, Tasks und die Statistik der Anwendungsarbeit.

2.3. Geschützte Verbindung mit dem Administrationsserver

Der Datenaustausch zwischen Client-Computern und Administrationsserver, sowie die Verbindung der Konsole mit dem Administrationsserver kann unter Verwendung des Protokolls SSL (Secure Socket Layer) erfolgen. SSL erlaubt die Authentifizierung der kommunizierenden Computer, die Verschlüsselung von zu übermittelnden Daten und den Schutz den Datenmanipulation bei der Übertragung. Die durch SSL-Protokoll geschützte Verbindung basiert auf der Verwendung von Authentifizierung der kommunizierenden Seiten und der Verschlüsselung mit einem speziellen veröffentlichten Verschlüsselungsalgorithmus ("Closed-Key-Methode").

2.3.1. Zertifikat des Administrationssservers

Bei der Verbindung der Administrationskonsole zu dem Administrationsserver und beim Datenaustausch mit Client-Computern erfolgt die Authentifizierung des Administrationssservers auf Basis des **Zertifikats des Administrationssservers**. Zertifikat wird auch für die Authentifizierung zwischen dem Haupt- und Untergeordneten-Administrationsserver benutzt.

Das Zertifikat des Administrationssservers wird bei der Installation der Komponente Administrationsserver erstellt. Es wird auf dem Administrationsserver im Installationsverzeichnis des Programms im Ordner **Cert** gespeichert.

Das Zertifikat des Administrationssservers kann nur einmal erstellt werden, bei der Installation des Administrationssservers. Es wird empfohlen während der Installation des Administrationsserver das Zertifikat zu speichern. Wenn das

Zertifikat des Administrationssservers verloren geht, muss zu dessen Wiederherstellung die Komponente Administrationsserver erneut installiert und die Daten müssen wiederhergestellt werden.

2.3.2. Serverauthentifizierung bei Verbindung durch die Konsole

Nach der Installation fordert die Administrationskonsole bei der ersten Verbindung mit dem Server das Zertifikat des Administrationssservers an und speichert es lokal am Administratorarbeitsplatz. Die gespeicherte Zertifikatkopie dient bei späteren Verbindungen mit dem Administrationsserver dieses Namens der Serverauthentifizierung.

Wenn das Zertifikat des Administrationssservers nicht mit der Zertifikatkopie übereinstimmt, die am Administratorarbeitsplatz gespeichert wurde, erfolgt eine Anfrage auf Bestätigung der Verbindung mit dem Server dieses Namens und ein neues Zertifikat wird angefordert. Im Fall der Verbindungsbestätigung speichert die Administrationskonsole eine Kopie des neuen Administrationsserverzertifikats, die künftig zur Serverauthentifizierung benutzt wird.

2.3.3. Serverauthentifizierung bei Verbindung durch Client-Computer

Bei der ersten Verbindung eines Client-Computers mit dem Server empfängt der Administrationsagent das Zertifikat des Administrationssservers und speichert es lokal.

Bei lokaler Installation des Administrationsagenten kann das Zertifikat des Administrationssservers vom Administrator manuell ausgewählt werden.

Auf Basis der empfangenen Zertifikatkopie werden bei künftigen Verbindungen die Rechte des Administrationssservers überprüft.

In Zukunft fordert der Administrationsagent bei jeder Verbindung des Client-Computers mit dem Server das Zertifikat des Administrationssservers an und vergleicht es mit der lokalen Kopie. Wenn diese nicht übereinstimmen, wird dem Administrationsserver der Zugriff auf den Client-Computer verweigert.

Wenn die Verbindung durch den Administrationsserver initiiert wurde, wird auf entsprechende Weise zuerst die über den UDP-Port empfangene Verbindungsanfrage des Administrationsservers überprüft.

2.4. Identifikation von Client-Computern im logischen Netzwerk

Die Identifikation von Client-Computern im logischen Netzwerk erfolgt auf Basis der **Namen der Client-Computer**. Der Name eines Client-Computers darf sich innerhalb der Namen von Computern, die mit dem Administrationsserver verbunden sind, nicht wiederholen.

Der Name eines Client-Computers wird dem Administrationsserver übergeben. Dies geschieht entweder beim Durchsuchen des Windows-Netzwerks und dem Fund eines neuen Computers, oder bei der ersten Verbindung des Administrationsagenten, der auf dem Client-Computer installiert ist. Standardmäßig stimmt der Name mit dem Computernamen im Windows-Netzwerk (NetBIOS-Name) überein. Wenn auf dem Administrationsserver bereits ein Client-Computer mit diesem Namen registriert ist, wird dem Namen des neuen Client-Computers eine Ordnungszahl hinzugefügt (z.B. **Name-1**, **Name-2** usw.). Unter diesem Namen wird der Client-Computer in das logische Netzwerk aufgenommen.

2.5. Zugriffsrechte im logischen Netzwerk

In Kaspersky Administration Kit sind die folgenden Berechtigungsarten für den Zugriff auf Programmfunktionen vorgesehen:

- Lesen:
 - Verbindung mit dem Administrationsserver
 - Ansicht der Struktur im logischen Netzwerk (oder Administrationsgruppen)
 - Ansicht der Werte für die Parameter von Richtlinien, Tasks und Anwendungseinstellungen

- Ausführung: Starten und Beenden von Gruppentasks und globalen Tasks; Empfangen von Protokollen über die Arbeit von Anwendungen, die auf Client-Computern installiert sind
- Schreiben:
 - Erstellen eines logischen Netzwerkes, dessen Hinzufügen zu Gruppen und Client-Computern (oder in eine Administrationsgruppe)
 - Installieren der Komponente Administrationsagent auf Client-Computer
 - Anlegen und Installieren von Installationspaketen für Antiviren-Anwendungen des Herstellers sowie der dafür benötigten Lizenzschlüssel auf Client-Computern
 - Updates der auf Client-Computern installierten Anwendungen
 - Erstellen von Richtlinien, Tasks für Computergruppen und einzelne Computer, Ändern von Anwendungseinstellungen
 - Zentralisierte Verwaltung von Anwendungen mit Diensten, die von den Komponenten Administrationsserver, Administrationsagent und Administrationskonsole zur Verfügung gestellt werden
 - Bereitstellen von Zugriffsrechten auf die Funktionen von Kaspersky Administration Kit für Benutzer und Benutzergruppen.

Nach der Installation des Administrationsservers haben standardmäßig die Rechten zum Verbinden mit dem Server und zur Arbeit mit dem logischen Netzwerk diejenigen Benutzer, die zu den Gruppen **KLAdmins** und **KLOperators** gehören.

Diese Gruppen werden bei der Installation der Komponente Administrationsserver gebildet und werden je nach dem angelegt, welches Benutzerkonto für den Dienstaufruf des Administrationsservers ausgewählt wurden:

- in der Domäne, zu der der Administrationsserver gehört, und auf dem Computer des Administrationsservers, wenn der Administrationsserver über das Benutzerkonto desjenigen Benutzers aufruft, der zur Domäne gehört
- nur auf dem Computer des Administrationsservers, wenn der Server unter dem Benutzerkonto des Systems aufgerufen wurde

Die Gruppe **KLAdmins** hat die Rechte: **Lesen, Ausführen, Schreiben**. Die Gruppe **KLOperators** hat das Recht **Lesen**. Die Rechte, die die Gruppe **KLAdmins** bekommt, lassen sich nicht ändern.

Die Benutzer, die zur Gruppe **KLAdmins** gehören, werden als **Administratoren des logischen Netzwerkes** bezeichnet, dagegen die Benutzer in der Gruppe **KLOperators** heißen **Operatoren des logischen Netzwerkes**.

Die Gruppen **KLAdmins** und **KLOperators** anzuzeigen sowie Änderungen vorzunehmen, erfolgt mithilfe der Standardmittel für das Administrieren unter Windows: **Verwaltung / Lokale Benutzer und Gruppen**.

Außer den Benutzer, die zur Gruppe **KLAdmins** gehören, erhalten Administratorenrechte noch:

- die Administratoren der Domäne, deren Computer zu diesem logischen Netzwerk gehören
- lokale Administratoren von Computern, auf denen der Administrationsserver installiert ist.

Alle von den Administratoren des logischen Netzwerks initiierten Operationen werden mit den Rechten des Administrationsserverkontos ausgeführt. Für jeden Administrationsserver kann eine eigene Gruppe **KLAdmins** angelegt werden, die nur innerhalb dieses logischen Netzwerks über Rechte verfügt.

Wenn Computer, die zu einer Domäne gehören, mehrere logische Netzwerke bilden, ist der Domänenadministrator auch der Administrator jedes dieser logischen Netzwerke. Dabei gibt es für diese logischen Netzwerke nur eine Gruppe **KLAdmins**, die bei der Installation des ersten Administrationsservers erstellt wird. Zur Anpassung dieser Gruppe dienen die Administrationstools des Betriebssystems. Die von den Administratoren des logischen Netzwerks initiierten Operationen werden mit den Rechten des entsprechenden Administrationsserverkontos ausgeführt.

Die Benutzerrechte werden in der Anwendung Kaspersky Administration Kit auf Basis der Windows-Benutzerauthentifizierung im Netzwerk zugewiesen.

Nach Installation der Anwendung kann der Administrator Folgendes tun:

- Rechte ändern, die für die Gruppen von KLOperators gelten
- Zugriffsrechte einräumen an den Programmfunktionen von Kaspersky Administration Kit für andere Benutzergruppen und Einzelbenutzer, der/die sich am Computer angemeldet hat/haben, auf dem die Administrationskonsole installiert ist
- verschiedene Zugriffsrechte für die Arbeit in jeder Administrationsgruppe einräumen.

2.6. Einführung des Antiviren-Schutzes über das logische Netzwerk

Es gibt zwei gebräuchliche Szenarien, die verdeutlichen, wie ein verlässlicher Antiviren-Schutz mit Hilfe von Kaspersky Administration Kit eingeführt werden kann:

- durch die zentralisierte Remote-Installation von Anwendungen auf den Client-Computern des logischen Netzwerks. Dabei erfolgen die Installation der Anwendungen und die Verbindung mit dem zentralisierten Remote-Verwaltungssystem automatisch, erfordern keine Interaktion des Administrators und erlauben die Installation von Antiviren-Software auf einer beliebigen Anzahl von Client-Computern.
- durch die lokale Installation von Anwendungen auf jedem Client-Computer. In diesem Fall wird die Installation der erforderlichen Komponenten auf den Client-Computern und am Administratorarbeitsplatz manuell vorgenommen, die Einstellungen für die Verbindung der Clients mit dem Server werden bei der Installation des Administrationsagenten festgelegt. Diese Variante der Einführung ist dann empfehlenswert, wenn die zentralisierte Remote-Installation nicht möglich ist.

Die Remote-Installation eignet sich für das Installieren von beliebig vielen Anwendungen, die der Benutzer vorgibt.

Es muss jedoch darauf hingewiesen werden, dass Kaspersky Administration Kit nur die Anwendungen von Kaspersky Lab verwaltet, zu deren Lieferumfang eine spezielle Komponente gehört, nämlich das Verwaltungs-Plugin für die Anwendung.

2.7. Aufbau eines zentralisierten Verwaltungssystems für den Antiviren-Schutz

Der erste Schritt beim Aufbau eines zentralisierten Verwaltungssystems für den Antiviren-Schutz eines Firmennetzwerks mit Hilfe des Programmpakets

Kaspersky Administration Kit besteht in der Planung des logischen Netzwerks. Auf dieser Etappe sind folgende Fragen zu beantworten:

1. Welche isolierten Bereiche müssen im Netzwerk vorhanden sein und wie viele Administrationsserver werden gebraucht?
2. Welche Computer im Corporate-Netzwerk fungieren als Hauptadministrationsserver und als untergeordnete Server und welche als Administratorarbeitsplatz und Client-Computer? Die Client-Computer müssen die Rechner werden, auf denen die Installation von Kaspersky-Lab-Anwendungen geplant ist.
3. Welches Kriterium dient zur Gruppierung der Client-Computer? Auf welche Weise wird die Gruppenhierarchie aufgebaut?
4. Wie wird die Antiviren-Sicherheit bei der Remote-Installation und bei einer lokalen Installation umgesetzt?

Auf der nächsten Etappe erstellt der Administrator das logische Netzwerk, indem er die entsprechenden Softwarekomponenten von Kaspersky Administration Kit auf den Netzwerkcomputern installiert:

1. Installation der Administrationskonsole auf Computern, von denen aus die Verwaltung der Produkte erfolgt
2. Installation der Administrationskonsole auf Computern, von denen aus die Verwaltung der Produkte erfolgt
3. Benennung durch Administratoren des logischen Netzwerkes, Bestimmung, welche Kategorien von Benutzern mit dem System arbeiten und Festlegung von ausführbaren Funktionen für jede Kategorie
4. Erstellen von Benutzergruppen und Einräumen von Zugriffsrechten für Benutzergruppen, um die Funktionen wahrzunehmen

Danach muss die Hierarchie der Administrationsserver und für jeden Server sowie die Struktur des logischen Netzwerks gebildet, die Hierarchie der Administrationsgruppen aufgebaut und die Computer auf die entsprechenden Gruppen verteilt werden.

Beim nächsten Schritt werden auf den Client-Computern die Komponente Administrationsagent und die erforderlichen Kaspersky-Lab-Anwendungen, sowie am Administratorarbeitsplatz die entsprechenden Plug-Ins zur Anwendungsverwaltung installiert.

Nicht alle Anwendungen von «Kaspersky Lab», welche über Kaspersky Administration Kit verwaltet werden können, können per Remote-Installation auf Client-Computer installiert werden. Detaillierte Information entnehmen Sie den entsprechenden Handbüchern.

Bei einer Remote-Installation kann der Administrationsagent gemeinsam mit einer Anwendung installiert werden. In diesem Fall wird eine separate Installation des Administrationsagenten nicht benötigt.

Der letzte Schritt besteht in der Konfiguration der installierten Anwendungen. Dazu gehört die Definition und das Übernehmen von Gruppenrichtlinien und das Erstellen der erforderlichen Tasks.

Der Schnellstart-Assistent bietet die Möglichkeit zum Aufbau eines zentralisierten Verwaltungssystems für den Antiviren-Schutz mit minimalen Einstellungen. Dabei wird angeboten, ein logisches Netzwerk zu erstellen, das der Domänenstruktur des Windows-Netzwerks entspricht, und für das Antiviren-Schutzsystem wird Kaspersky Anti-Virus for Windows Workstations verwendet.

2.8. Wartung des logischen Netzwerks

Nachdem ein logisches Netzwerk erstellt und der Antiviren-Schutz installiert und konfiguriert wurde, wird den Administratoren empfohlen, regelmäßig folgende Operationen auszuführen:

- Regelmäßige Kontrolle der Protokolle über die Arbeit der Anwendungen auf den Client-Computern.
- Lesen von Benachrichtigungen, die von Client-Computern und Administrationsservern stammen.

Eine vollständige Liste der Benachrichtigungen, die von den Anwendungen der Kaspersky-Lab-Produkte gesendet werden können, finden Sie in den betreffenden Handbüchern.

- Wenn auf einem Client-Computer eine Situation eingetreten ist, welche das Eingreifen des Administrators erfordert, kann er von seinem Arbeitsplatz aus reagieren und z.B. die Desinfektion infizierter Dateien auf diesem Computer vornehmen.
- Rechtzeitiges Update der Antiviren-Datenbanken auf den Client-Computern.

- Rechtzeitiges Update der Antiviren-Datenbanken auf den Client-Computern und der Programmmodule von Anwendungen, die auf Client-Computern installiert sind.
- Überwachen der Größe der Datenbank zum Speichern der von den Client-Computern übertragenen Informationen, die sich auf die Arbeit von Anwendungen beziehen. Gewährleistung des Vorhandenseins von freiem Speicherplatz für die übertragenen Daten auf dem Administrationsserver.
- Rechtzeitiges Hinzufügen von neu im Firmennetzwerk installierten Computern zum logischen Netzwerk und Installation der für diese Computer notwendigen Antiviren-Anwendungen.
- Regelmäßiges Anlegen von Sicherheitskopien der Daten des Administrationssystems.

2.9. Koordination der gemeinsamen Arbeit von Administratoren

Das System erlaubt gleichzeitige Arbeit von Administratoren mit den gleichen Ressourcen. Es sind jeweils die zuletzt übernommenen Einstellungen gültig. Deshalb sollte die parallele Arbeit mehrerer Administratoren koordiniert werden, um Missverständnissen vorzubeugen.

2.10. Konzeption der Benutzeroberfläche

Vom Arbeitsplatz des Administrators aus können Sie das logische Netzwerk anzeigen, erstellen, anpassen und konfigurieren sowie die Arbeit aller auf Client-Computern installierten Kaspersky-Lab-Anwendungen zentralisiert verwalten. Die Benutzeroberfläche wird von der Komponente Administrationskonsole angeboten, die ein autonomes Tool darstellt, das in Microsoft Management Console (MMC) integriert ist. Das Interface von Kaspersky Administration Kit entspricht dem Standard für MMC.

Für die lokale Arbeit mit Client-Computern ist im Programm vorgesehen, eine Remote-Verbindung mit dem Computer über die Administrationskonsole mithilfe der Standardanwendung von Microsoft Windows **Verbindung mit Remote-Desktop** herzustellen.

Um diese Option einzusetzen, muss auf dem Client-Computer eine Remote-Verbindung mit dem Desktop erlaubt worden sein.

2.10.1. Programmstart

Das Programm Kaspersky Administration Kit wird gestartet, indem der Punkt **Kaspersky Administration Kit** in der Programmgruppe **Kaspersky Administration Kit** im Standardmenü **Start \ Programme** angeklickt wird. Diese Programmgruppe wird nur auf den Administratorarbeitsplätzen beim Installieren der Komponente Administrationskonsole erstellt.

Auf die komplette Funktionalität von Kaspersky Administration Kit können Sie erst zugreifen, wenn der Administrationsserver des logischen Netzwerkes gestartet wurde.

2.10.2. Hauptfenster des Programms

Das Programmhauptfenster besteht aus Menü, Symbolleiste, Konsolenstruktur, Detailfenster, Ergebnisleiste und Taskleiste. Das Menü bietet Funktionen zur Verwaltung von Dateien und Fenstern und Zugriff auf das Hilfesystem. Die Schaltflächen der Symbolleiste erlauben den direkten Zugriff auf die gebräuchlichsten Punkte des Hauptmenüs. Die Konsolenstruktur zeigt in Form eines Konsolenbaums den Namensraum **Kaspersky Administration Kit**. Das Detailfenster enthält eine Liste der Elemente des in der Konsolenstruktur ausgewählten Objekts. Die Ergebnisleiste enthält die Taskleiste, welche einen schnellen Zugriff auf die wichtigsten Aktionen ermöglicht, welche für das in der Konsolenstruktur oder in der Ergebnisleiste mit dem Hyperlink ausgewählte Objekt vorgesehen sind. Die Ergebnisleiste kann auf zwei Arten angezeigt werden: in der Registerkarte mit dem Namen des in der Konsolenstruktur gewählten Elementes und in der Registerkarte **Standard**. Der einzelne Unterschied besteht darin, dass die Registerkarte **Standard** enthält keine Taskleiste.

Taskleiste ist nicht zugänglich und wird nicht in der Administrationskonsole angezeigt unter Betriebssystem Microsoft Windows 2000.

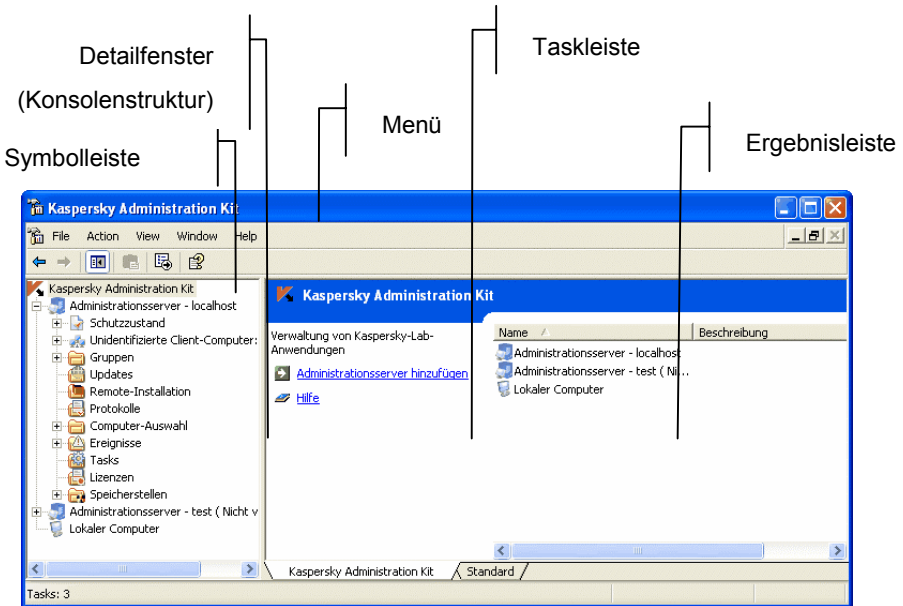


Abbildung 3. Hauptfenster des Programms Kaspersky Administration Kit

2.10.3. Konsolenstruktur

Die Konsolenstruktur dient der Darstellung von im Firmennetzwerk angelegten logischen Netzwerken, der Zugriffsrechte auf die Einstellungen des logischen Netzwerkes und der Eigenschaften des lokalen Computers, auf dem die Administrationskonsole installiert ist.

Der Namensraum **Kaspersky Administration Kit** kann mehrere Elemente mit den Namen der Server (je nach Anzahl der installierten und in die Konsolenstruktur aufgenommenen Administrationsserver) enthalten.

Das Element (**<Name des Administrationsservers>**) ist ein Container und stellt die Struktur und Einstellungen des logischen Netzwerkes eines ausgewählten Administrationsservers dar. Der Container (**<Name des Administrationsservers>**) enthält folgende Ordner:

- Zustand des Schutzes
- Netzwerk
- Gruppen

- Update
- Remote-Installation
- Protokolle
- Benutzerdefinierte Computer
- Ereignisse
- Tasks
- Lizenzschlüssel
- Backups

Der Ordner **Zustand des Schutzes** stellt Informationen über den Zustand des Antivirenschutzes auf den Client-Computern des logischen Netzwerkes sowie im gesamten Computernetzwerk dar. Im Ordner sind Protokollseiten eingebettet, die die Informationen auf die folgende Weise strukturieren:

- **Netzwerk** – Mitteilungen über Computer, die nicht zum logischen Netzwerk gehören, sowie Ergebnisse der laufenden oder vorangegangenen Abfrage durch den Administrationsserver des logischen Netzwerkes.
- **Gruppen** – Zustand des Antivirenschutzes auf den Client-Computern des logischen Netzwerkes.
- **Antivirenschutz** – Statistik über Virenaktivität und Status für Tasks des Echtzeitschutzes auf den Client-Computern des logischen Netzwerkes.
- **Update** - Zustand der von den Anwendungen zugrunde gelegten Antiviren-Datenbanken.

Der Ordner **Netzwerk** ist für die Darstellung des Computernetzwerkes vorgesehen, in dem der Administrationsserver installiert ist. Die Daten über die Netzwerkstruktur und über die dazu gehörenden Computer empfängt der Administrationsserver bei den regelmäßigen Abfragen des Windows-Netzwerkes und der IP-Subnetzes, die im Computernetzwerk der Firma angelegt worden sind.

Der Ordner **Gruppen** dient zum Speichern, Anzeigen, Konfigurieren und Anpassen der Struktur des logischen Netzwerkes, der Gruppenrichtlinien und Gruppentasks.

Die Objekte, die sich im Stamm des Ordners **Gruppen** befinden, entsprechen der höchsten Hierarchieebene des logischen Netzwerkes. Zu ihnen gehören die für jedes Objekt obligatorischen Ordner **Administrationsserver**, **Richtlinien** und

Tasks. Diese Ordner dienen der Arbeit mit den Administrationsservern, Richtlinien und Tasks der obersten Hierarchieebene.

Der Ordner **Update** enthält eine Liste der vom Administrationsserver empfangenen Updates, die an Client-Computer verteilt werden können.

Der Ordner **Remote-Installation** enthält eine Liste der Installationspakete, die zur Remote-Installation von Anwendungen auf Client-Computer des logischen Netzwerks verwendet werden können.

Der Ordner **Protokolle** enthält eine Liste der Vorlagen für Protokolle über den Status des Antiviren-Schutzsystems auf den Computern des logischen Netzwerks.

Das Element **Benutzerdefinierte Computer** ist für die Suche nach Client-Computern anhand eingegebener Kriterien, für die Speicherung und für die Anzeige der Suchergebnisse in einzelnen Ordnern vorgesehen.

Das Element **Ereignisse** enthält benutzerdefinierte Ereignisse, in denen Informationen über Ereignisse stehen, die bei der Programmarbeit registriert wurden, sowie die Ergebnisse der Taskausführung.

Der Ordner **Globale Tasks** enthält eine Liste der globalen Tasks, die für die ausgewählten Computer des logischen Netzwerks festgelegt wurden.

Der Ordner **Lizenzschlüssel** enthält eine Liste der Lizenzschlüssel, die auf Client-Computern installiert sind.

Der Ordner **Backups** ist für die Arbeit mit Objekten vorgesehen, die von den Antiviren-Anwendungen auf Client-Computern in Quarantäne-Verzeichnisse verschoben wurden sowie für Sicherungskopien von Objekten, die in das Backup verschoben wurden. Die eigentlichen Objekten werden nicht auf den Administrationsserver übertragen.

Die in der Administrationskonsole stehenden Informationen werden nur für die Elemente automatisch aktualisiert.

Damit die Informationen im Detailfenster aktualisiert werden, müssen Sie die Taste **F5** drücken oder im Menü oder im Kontextmenü auf den Eintrag **Aktualisieren** oder Sie klicken auf den Hyperlink Aktualisieren der Taskleiste.

2.10.4. Kontextmenü

Jede Kategorie von Objekten des Namensraums **Kaspersky Administration Kit** besitzt ein Kontextmenü. Außer den Standardbefehlen des MMC-Menüs stehen Befehle zur Verfügung, die zur Arbeit mit den Objekten dienen. Tabelle 1 enthält eine Liste der Objekte und die ihnen entsprechenden Zusatzbefehle des Kontextmenüs.

Tabelle 1

Objekt	Befehl	Funktion des Befehls
Kaspersky Administration Kit	Neu/ Administration sserver	Administrationsserver zur Konsolenstruktur hinzufügen
<Servername>	Mit Administration sserver verbinden	Mit Administrationsserver verbinden
	Von Adm inistrationssser ver trennen	Von Administrationsserver trennen
	Schnellstart-Assistent	Schnellstart-Assistent starten
	Assistent für Remote-Installation	Task für Remote-Installation erstellen und starten
	Computer suchen	Einstellungsfenster für Computersuche
	Eigenschaften	Eigenschaften-Fenster des Administrationsservers öffnen
Alle Tasks/ Parameter für Erkennen eines Virenangriffs	Parameter für Erkennen eines Virenangriffs auf die Computer des logischen Netzwerkes einstellen	
Netzwerk	Computer suchen	Fenster für Computersuche im Ordner Netzwerk öffnen
	Assistent für Remote-Installation	Task für Remote-Installation erstellen und starten

Objekt	Befehl	Funktion des Befehls
	Ansicht/Domäne	Struktur des Computernetzwerkes als Hierarchie der Windows-Domänen und Workgroups darstellen
	Ansicht/Active Directory	Struktur des Computernetzwerkes je nach Struktur im Active Directory darstellen
	Ansicht/IP-Subnetze	Struktur des Computernetzwerkes als IP-Subnetze darstellen
	Ansicht/Admini- strationsserver	Übergang zum Element Administrationsserver, zu dem der Ordner Netzwerk gehört
	Neu/IP-Subnetz	IP-Subnetz für Computerdarstellungen erstellen
	Alle Tasks/ Computeraktivität	Parameter für Reaktion des Administrationsservers auf fehlende Aktivität von Computern im Netzwerk einstellen
Gruppen	Anwendung installieren	Task Remote-Installation für Gruppen erstellen und starten
	Anwendung aktualisieren	Task für automatische Update-Verteilung erstellen
	Neue Protokollvorlage	Neue Protokollvorlage für ausgewählte Gruppe erstellen

Objekt	Befehl	Funktion des Befehls
	Computer suchen	Fenster für Computersuche in Gruppe öffnen
	Virenzähler zurücksetzen	Virenzähler auf allen Client-Computern der Gruppe zurücksetzen
	Synchronisierung erzwingen	Daten auf allen Computern der Gruppe synchronisieren
	Neu/ Gruppe	Neue Gruppe in der Struktur des logischen Netzwerks erstellen
	Neu/ Client-Computer	Neuen Computer zur Gruppe hinzufügen
	Alle Tasks/ Computeraktivität	Parameter für Reaktion des Administrationsservers auf fehlende Aktivität von Computern im Netzwerk einstellen
	Alle Tasks/ Sicherheit	Zugriffsrechte für Gruppe einstellen
	Alle Tasks/ Richtlinien	Übergang zum Ordner Richtlinien für gewählte Gruppe
	Alle Tasks/ Tasks	Übergang zum Ordner Gruppentasks für gewählte Gruppe
	Alle Tasks/ Untergeordnete Server	Übergang zum Ordner Administrationsserver für gewählte Gruppe

Objekt	Befehl	Funktion des Befehls
Richtlinien	Neu/Richtlinie	Neue Gruppenrichtlinie erstellen
	Ansicht / Geerbte Richtlinien	Die geerbten Richtlinien in der Liste anzeigen.
Gruppentasks	Neu/ Task	Neuen Gruppentask erstellen
	Alle Tasks/ Importieren	Task aus Datei importieren
	Ansicht / GeerbteTasks	Geerbte Tasks In der Ergebnisliste anzeigen.
Update	Updates downloaden	Task für Update-Download durch Administrationsserver starten
	Parameter Update-Download	Parameter des Tasks Update-Download durch Administrationsserver einstellen
	Protokoll über Versionen der Antiviren-Datenbanken	Protokoll über Versionen der Antiviren-Datenbanken erstellen und anzeigen
Remote-Installation	Assistent für Erstellen des Tasks Remote-Installation	Task Remote-Installation einer Anwendung erstellen

Objekt	Befehl	Funktion des Befehls
	Protokoll über Programmversionen	Protokoll über auf den Computern installierten Versionen der Kaspersky-Lab-Anwendungen erstellen und anzeigen
	Neu/ Installationspaket	Neues Installationspaket erstellen
	Alle Tasks/ Assistent für Erstellen des Tasks Programmdeinstallation	Task Remote-Deinstallation einer Anwendung erstellen
Protokolle	Neu/ Protokoll	Neue Protokollvorlage erstellen
Benutzerdefinierte Computer	Neu/Neue Definition	Neue Benutzerdefinition für Suche nach Computern
Ereignisse	Neu/Neue Definition	Neue Benutzerdefinition für Suche und Anzeige von Ereignissen
	Alle Tasks/ Protokoll über Virenaktivität	Protokoll über Virenaktivität im Netzwerk erstellen und anzeigen
Globale Tasks	Neu/ Task	Neuen globalen Task erstellen
	Alle Tasks/ Importieren	Task aus Datei importieren
Lizenzschlüssel	Lizenzschlüssel hinzufügen	Neuen Lizenzschlüssel installieren

Objekt	Befehl	Funktion des Befehls
	Protokoll über Lizenzschlüssel	Protokoll über auf den Client-Computern installierten Lizenzschlüsseln erstellen und anzeigen

Auch im Detailfenster besitzt jedes Element eines in der Konsolenstruktur ausgewählten Objekts ein Kontextmenü, dessen Befehle der Arbeit mit dem Element dienen. Tabelle 2 enthält die wichtigsten Typen von Elementen und die ihnen entsprechenden Befehle.

Tabelle 2

Element	Befehl	Funktion des Befehls
Client-Computer	Schutz	Informationen über den Zustand der Antiviren-Sicherheit auf einem Client-Computer anzeigen
	Tasks	Eigenschaftenfenster des Client-Computers mit der Registerkarte Tasks öffnen
	Anwendungen	Eigenschaftenfenster des Client-Computers mit der Registerkarte Anwendungen öffnen
	Ereignisse	Fenster öffnen für Anzeige der Ereignisse, die bei der Programmarbeit auf dem Client-Computer registriert wurden
	Assistent für Remote-Installation	Task Remote-Installation für Client-Computer erstellen

Element	Befehl	Funktion des Befehls
	Synchronisieren	Datensynchronisierung auf Client-Computer und Administrationsserver vornehmen
	Virenzähler zurücksetzen	Virenzähler auf dem Client-Computer zurücksetzen
	Mit Remote-Desktop verbinden	Fenster Verbindung mit Remote-Desktop öffnen
Installationspaket	Installieren	Task Remote-Installation erstellen
Protokollvorlage	Neu	Protokoll nach ausgewählter Vorlage erstellen und anzeigen
	Protokollversand	Task für automatisches Erstellen und Versenden von Protokollen nach gewählter Vorlage erstellen

KAPITEL 3. INSTALLATION VON KASPERSKY ADMINISTRATION KIT

3.1. Verbindung zum Administrationsserver

Nach dem Start von Kaspersky Administration Kit enthält das Programmhauptfenster die Konsolenstruktur, in der die oberste Hierarchieebene des Namensraums **Kaspersky Administration Kit** angezeigt wird. Um die Struktur und Einstellungen des logischen Netzwerks in das Hauptfenster zu laden, muss in die Konsolenstruktur ein Objekt ein Server eingefügt und die Verbindung mit dem gewünschten Administrationsserver hergestellt werden (s. Abb. 2). Das Programm empfängt vom Administrationsserver Informationen über die Struktur des logischen Netzwerks und zeigt diese in der Konsolenstruktur an.

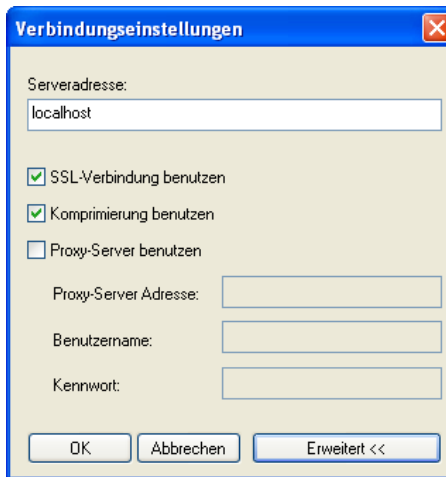


Abbildung 4. Herstellen einer Verbindung mit dem Administrationsserver

Benutzern, die nicht über Verbindungsrechte verfügen, wird der Zugriff auf den Administrationsserver verweigert. Die Überprüfung der Benutzerrechte erfolgt auf Basis der Windows-Benutzerauthentifizierung im Netzwerk.

Wenn in der Netzwerkstruktur der Firma mehrere Administrationsserver installiert sind, können Sie mit dem logischen Netzwerk jedes Administrationsservers vom einheitlichen Administratorarbeitsplatz aus arbeiten. Zum Wechsel in ein anderes logisches Netzwerk, können Sie sich am gewünschten Administrationsserver anmelden oder der Konsolenstruktur mehrere Server hinzufügen und sich an jeder davon anmelden.

Sie können nur dann parallel mit den logischen Netzwerken mehrerer Administrationsserver arbeiten, wenn Sie für jedes dieser Netzwerke über Operator- oder Administratorrechte des logischen Netzwerks verfügen oder die entsprechenden Rechte dafür haben.

3.2. Vergabe von Rechten

Nach Installation des Administrationsservers haben diejenigen Benutzer die Rechte für die Verbindung zum Server und für das Arbeiten mit dem logischen Netzwerk, die zu den Gruppen **KLAdmins** und **KLOperators** (s. Pkt. 2.5 auf S. 25) gehören.

Sie können die Zugriffsrechte für die Gruppe **KLOperators** ändern, Rechte vergeben im logischen Netzwerk für Benutzergruppen und einzelne Benutzer, die am Computer angemeldet sind, auf dem die Administrationskonsole installiert ist.

Die Zugriffsrechte auf jedes Objekt des logischen Netzwerkes werden im Einstellungsfenster für die Eigenschaften des Administrationsservers auf der Registerkarte **Sicherheit** (s. Abb. 5) vergeben.

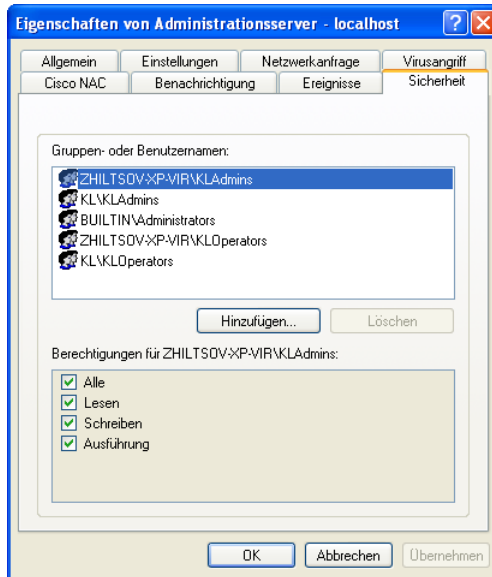


Abbildung 5. Vergabe von Zugriffsrechten auf den Administrationsserver

Es ist die Option vorgesehen, einzelne Zugriffsrechte für jede Gruppe im logischen Netzwerk zu vergeben. Diese Einstellung erfolgt im Eigenschaftensfenster der Gruppe auf der Registerkarte **Sicherheit**.

Der Administrator kann Benutzeraktionen mithilfe von Ereignissen bei der Ausführung des Administrationsservers unterordnen, die im Ereignisprotokoll eingetragen sind. Diese Ereignisse haben den Rang **Informative Mitteilung**, die Ereignisarten beginnen mit dem Wort **Audit**. In der Konsolenstruktur werden die Ereignisse im Element **Ereignisse**, Ordner **Audit-Ereignisse** angezeigt.

3.3. Informationen zum Computernetzwerk anzeigen. Domänen, IP-Subnetze und Gruppen Active Directory

Die Informationen über die Struktur des Computernetzwerkes und über die dazu gehörenden Computer stehen im Ordner **Netzwerk** der Konsolenstruktur.

Nach Installation von Kaspersky Administration Kit enthält der Ordner **Netzwerk** eine Hierarchie von Ordnern, die die Struktur der Domänen und Arbeitsgruppen im Windows-Netzwerk des Unternehmens darstellen. Jeder Ordner auf der obersten Ebene enthält eine Liste von Computern, die der jeweiligen Domäne oder Arbeitsgruppe angehören, die aber nicht zum logischen Netzwerk gehören. Wird ein solcher Computer in eine Gruppe übernommen, werden seine Informationen sofort aus dem Ordner entfernt. Wird ein Computer aus dem logischen Netzwerk entfernt, erscheinen seine Informationen erneut in dem entsprechenden Ordner des Elementes **Netzwerk**.

Die Hierarchie der Ordner für das Element **Netzwerk** lässt sich auch anhand der Struktur eines Active Directory oder in einem Netzwerk von IP-Subnetzen darstellen. Klicken Sie dazu im Kontextmenü des Elementes **Netzwerk** auf den Menüpunkt **Ansicht / Active Directory** bzw. **Ansicht / IP-Subnetze**.

Sollte das Element **Netzwerk** als IP-Subnetze angezeigt werden, kann dessen Struktur durch den Administrator über Erstellen von IP-Subnetzen und Ändern der Parameter gebildet werden.

Standardmäßig werden als IP-Subnetze nur solche IP-Subnetze angezeigt, zu den der Administrationsserver gehört.

Wenn Sie die Ordner in der Konsolenstruktur markieren, werden die darin befindlichen Computer im Detailfenster in Tabellenform angezeigt, so dass sich folgende Inhalte ergeben:

- **Name** – Name des Computers im logischen Netzwerk (NetBios-Name oder IP-Adresse des Computers)
- **Art des Betriebssystems** – название операционной системы, установленной на клиентском компьютере.

Je nach Art des Betriebssystems steht neben dem Computernamen das Symbol  für den Server und  für eine Workstation.

- **Domäne** – Windows-Domäne oder Arbeitsgruppe, zu der der Computer gehört.
- **Agent / Antivirus** – Status der auf dem Computer installierten Anwendungen. Für den Administrationsagenten oder die Antiviren-Anwendung, die mit Kaspersky Administration Kit gesteuert werden können, erscheint das Symbol "+" (Pluszeichen), wenn diese Komponenten auf dem Rechner installiert sind. Wenn keine Anwendungen installiert sind, erscheint das Symbol "-" (Minuszeichen).

- **Sichtbarkeit im Netzwerk** – Daten, wann der Computer das letzte Mal vom Server im Netz erkannt wurde
- **Letztes Update** – Daten des letzten Updates für die Antiviren-Datenbank und die Anwendungen auf dem Computer.
- **Status** – aktueller Status des Computers (OK / Warnung / Kritisch) anhand von Kriterien, die der Administrator festgelegt hat.
- **Datenaktualisierung** – Daten der letzten Aktualisierung von Informationen über Computer
- **DNS-Domäne** – DNS-Domäne, der der Computer angehört
- **Domänenname** – DNS-Name des Computers
- **IP-Adresse** – IP-Adresse des Computers
- **Serververbindung** – Uhrzeit der letzten Verbindung des auf dem Client-Computer installierten Administrationsagenten mit dem Administrationsserver

Der Ordner **Netzwerk** ist eine Abbildung der gleichnamigen Dienstgruppe. Das Erstellen und Unterstützen der Gruppe **Netzwerk** erfolgt im aktuellen Status vom Administrationsserver. Er fragt in regelmäßigen Abständen das Firmennetzwerk ab, ob neue Computer angeschlossen oder Rechner entfernt worden sind.

Ein Administrationsserver kann folgende Netzwerkabfragen durchführen (s. Abb. 6):

- *Schnelle Windows-Netzwerkabfrage.* In diesem Fall wird nur Information über NetBIOS-Namen der Computer aus aller Domänen und Arbeitsgruppen.
- *Volle Windows-Netzwerkabfrage.* Dabei werden zusätzliche Informationen über Computer eingeholt: Betriebssystem, IP-Adresse, DNS-Name u.ä.
- *Abfrage der IP-Subnetze.* Dabei fragt der Administrationsserver die Erstellten IP-Bereiche mit Hilfe von ICMP-Pakete ab und holt vollständige Informationen über die darin enthaltenen Computer ein.
- *Abfrage der Active Directory Gruppen.* Dabei werden in die Datenbank des Administrationsservers Informationen über die Struktur der Organisationseinheiten aus Active Directory geschrieben, wie auch Informationen über DNS-Namen der Computer.

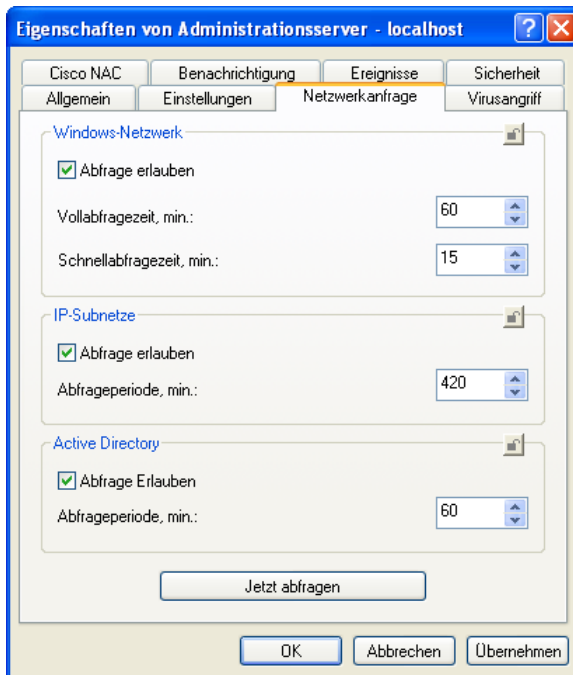


Abbildung 6. Einstellungen der Netzwerkabfrage durch den Administrationsserver

Anhand der empfangenen Informationen und Daten über die Struktur des logischen Netzwerks aktualisiert der Administrationsserver die Gruppe **Netzwerk**, deren Zusammensetzung und den Inhalt des Ordners **Netzwerk**. In Verbindung damit können im Netzwerk erkannte Computer automatisch in die vom Administrator vordefinierte Ordner der Gruppe **Netzwerk**, eingebunden werden oder in das logische Netzwerk einer bestimmten Administrationsgruppe. Es ist außerdem die Option vorgesehen die Abfrage von Computern zu deaktivieren, die der Gruppe **Netzwerk** angehören sowie darin befindliche Untergruppen.

In dem Ordner **Netz** des Administrationsserver werden auch die Computer angezeigt, welche zum logischen Netzwerk des untergeordneten Administrationsserver gehören und umgekehrt.

3.4. Schnellstart-Assistent

Das Programm Kaspersky Administration Kit bietet an, mit einem Schnellstart-Assistenten einen Minimalsatz von Parametern zu konfigurieren, die zum Aufbau eines zentralisierten Verwaltungssystems für den Antiviren-Schutz erforderlich sind. Bei seiner Arbeit erstellt der Assistent:

- ein logisches Netzwerk, dessen Struktur der Administrator vorgeben kann:
 - Automatisches Erstellen anhand der Domänen- und Arbeitsplatzstruktur im Windows-Netzwerk
 - Manuelles Erstellen

Wenn ein Computer beim Erstellen des logischen Netzwerks aus beliebigem Grund vom Assistenten nicht in die Gruppe **Netzwerk** aufgenommen wird (ausgeschaltet, im Netzwerk nicht erreichbar), dann wird er dem logischen Netzwerk nicht hinzugefügt. Der Computer kann jedoch später manuell hinzugefügt werden.

Das Erstellen eines logischen Netzwerks mithilfe des Schnellstart-Assistenten verletzt dessen Integrität nicht: Neue Gruppen werden hinzugefügt, ersetzen aber nicht die vorhandenen Gruppen. Ein Client-Computer kann nicht wiederholt aufgenommen werden, weil die Gruppe **Netzwerk** nur Computer enthält, die nicht zum logischen Netzwerk gehören.

- die Einstellungen für das Versenden von E-Mail-Benachrichtigungen über Ereignisse, die bei der Arbeit des Administrationsservers und aller anderen Kaspersky-Lab-Anwendungen registriert werden.
- eine Richtlinie und eine minimale Auswahl von Tasks der höchsten Hierarchieebene für Kaspersky Anti-Virus for Windows Workstations, Versionen 5.0 und 6.0, sowie globale Tasks: Update-Download für den Administrationsserver und Sicherheitskopieren von Daten.

Die Richtlinien für Kaspersky Anti-Virus for Windows Workstations der Versionen 5.0 und 6.0 wird nicht erstellt, wenn im Ordner **Gruppen** bereits eine Richtlinie für diese Anwendungen vorhanden ist.

Wenn Gruppentasks für die Gruppe **Gruppen** und globale Update-Tasks und Tasks für Sicherungskopien mit diesen Namen bereits erstellt wurden, werden diese ebenfalls nicht mehr erstellt.

Der Vorschlag für den Aufruf des Schnellstart-Assistenten erscheint zuerst, wenn nach der Installation des Administrationssservers eine Verbindung zu ihm aufgebaut werden soll. Um den Assistenten künftig aufzurufen, klicken Sie im Kontextmenü des Administrationssservers auf den Eintrag **Schnellstart-Assistent**.

3.5. Struktur des logischen Netzwerks erstellen, anzeigen und ändern

Die Struktur des logischen Netzwerks, nämlich die Hierarchie der untergeordneten Administrationsserver, die Liste mit den Gruppen und die Zusammensetzung der Gruppen, wird in der Projektierungsphase festgelegt. Das logische Netzwerk wird im Programmhauptfenster von Kaspersky Administration Kit in dem speziellen Ordner **Gruppen** (s. Abb. 7) so gebildet, dass die Hierarchie der Gruppen angelegt sowie Client-Computer und untergeordnete Administrationsserver hinzugefügt werden.

Unmittelbar nach der Installation von Kaspersky Administration Kit enthält der Ordner **Gruppen** keinerlei Objekte, die Ordner **Administrationsserver**, **Richtlinien** und **Gruppentasks** sind leer. Wenn der Administrator die Struktur des logischen Netzwerks erstellt, können in den Ordner **Gruppen** Client-Computer und darin eingebundene Gruppen übernommen werden.

Die Gruppen werden in der Ordneransicht dargestellt. Jeder Ordner hat eine Struktur, die analog zur Struktur des Ordners **Gruppen** gestaltet ist:

- Bei jedem Erstellen einer Gruppe werden automatisch die eingebetteten Ordner Administrationsserver, Richtlinien und Gruppentasks für das Speichern und Arbeiten mit den Administrationsservern, mit den Richtlinien und mit den Tasks dieser Gruppe angelegt.
- Wenn Client-Computer in die Gruppe übernommen werden, werden deren Informationen in Tabellenansicht im Detailfenster dargestellt.
- Wenn eine eingebettete Gruppe hinzugefügt wird, wird ein Ordner erstellt, der die gleiche Struktur hat.

Wenn Sie den Ordner in der Konsolenstruktur im Detailfenster markieren, wird der Inhalt angezeigt.

Für jeden Client-Computer wird neben seinen Informationen in der Tabelle des Ordners **Netzwerk** Folgendes angezeigt:

- **Scan auf Befehl** – Datum und Uhrzeit der letzten kompletten Untersuchung für den Client-Computer, ob Viren vorhanden sind
- **Viren erkannt** – Menge der auf dem Client-Computer erkannten Viren seit Installation der Antiviren-Anwendung (Erstuntersuchung des Computers) oder seit der letzten Zurücksetzung dieser Wertgröße (Zähler für erkannte Viren). Der Wert kann mithilfe des Eintrags **Virenzähler zurücksetzen** im Kontextemenü oder im Menü **Aktion** gelöscht werden.
- **Status des Echtzeitschutzes** – aktueller Status für den Echtzeitschutz des Client-Computers
- **IP-Adresse der Verbindung** – IP-Adresse der Verbindung von Client-Computer mit Administrationsserver

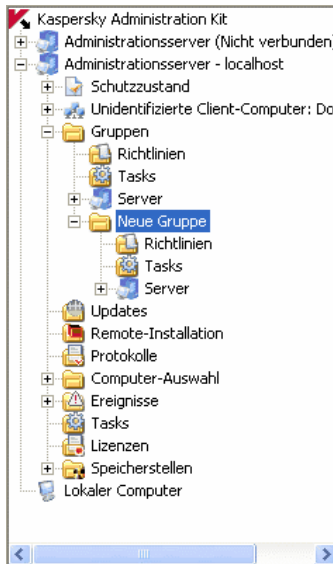


Abbildung 7. Anzeige der Objekte im logischen Netzwerk

Die Arbeit mit den Objekten des Ordners **Gruppen** erfolgt mithilfe den Einträgen im Kontextemenü (s. Pkt. 2.10.4 auf S. 35) und den Hyperlink in der Taskspalte.

Soll ein logisches Netzwerk mit der Struktur erstellt werden, die mit der Domänen- und Arbeitsgruppenstruktur im Windows-Netzwerk identisch ist, können Sie mit dem Schnellstart-Assistenten arbeiten (s. Pkt. 3.3 auf S. 45).

Um eine bereits vorprojektierte Struktur eines logischen Netzwerkes manuell zu erstellen, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.
2. Legen Sie eine Hierarchie der Gruppen beim nachfolgenden Erstellen von eingebetteten Gruppen fest.
3. Fügen Sie der Gruppe Client-Computer hinzu.
4. Fügen Sie untergeordnete Administrationsserver hinzu.

Die Struktur des logischen Netzwerkes wird im Ordner **Gruppen** angezeigt. Sie können Informationen über jedes Objekt im logischen Netzwerk empfangen: über untergeordnete Server, Gruppen und Client-Computer. Es werden Daten angezeigt, wann das Objekt erstellt wurde und wann dessen Parameter zuletzt bearbeitet wurden (s. Abb. 8). Außerdem können Sie erkennen, und auf Wunsch, die Parameter der Interaktion von Objekten (mit untergeordnetem Server, Client-Computer oder mit allen Client-Computern in der Gruppe) und des Administrationsservers ändern.

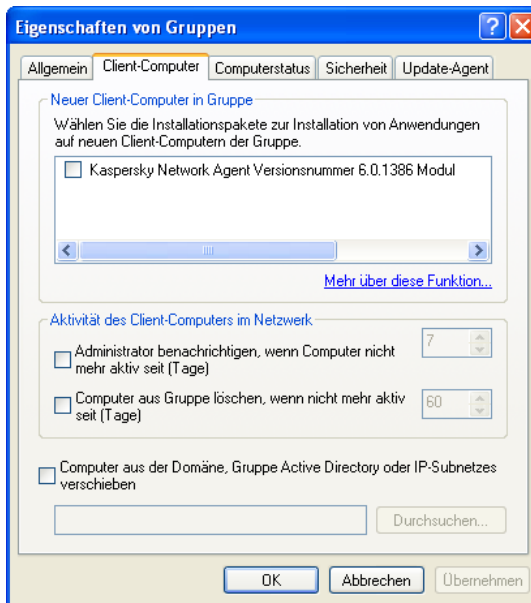


Abbildung 8. Anzeige der Gruppeneigenschaften.
Registerkarte **Client-Computer**

Um Informationen über konkrete Client-Computer zu bekommen, können Sie die Suchfunktion des Computers im logischen Netzwerk mit einzugebenden Kriterien nutzen (s. Pkt. 6.5 auf S. 93). Bei der Suche lassen sich die Informationen über die logischen Netzwerke untergeordneter Administrationsserver verwenden. Für die Suche, Speicherung und Anzeige von Informationen über Computer in einem einzelnen Ordner der Konsolenstruktur nutzen Sie die Funktion Erstellung einer Benutzerdefinition.

Bei Änderungen der Konfiguration des Firmennetzwerks müssen rechtzeitig entsprechende Änderungen in der Struktur des logischen Netzwerks erfolgen. Sie können:

- dem logischen Netzwerk beliebig viele Gruppen unterschiedlicher Ebenen hinzufügen (in die Gruppe können untergeordnete Administrationsserver eingebettet sein, die die folgende Hierarchiestufe bilden).

Außerdem können Sie festlegen, welche Kaspersky-Lab-Anwendungen automatisch auf allen neu in eine Gruppe aufgenommenen Client-Computern installiert werden sollen.

Damit Programme von Kaspersky Lab auf neuen Computern mit den Betriebssystemen Microsoft Windows 98/ME installiert werden können, ist auf ihnen vorsichtshalber der Administrationagent zu installieren.

- dem logischen Netzwerk beliebig viele Client-Computer hinzufügen.
- die Hierarchie der Objekte im logischen Netzwerk ändern, indem Sie einzelne Client-Computer und ganze Gruppen in andere Gruppen verschieben.
- aus dem logischen Netzwerk Gruppen und Client-Computer entfernen.
- dem logischen untergeordnete Administrationsserver hinzufügen, damit die Belastung für den Hauptserver verringert, der interne Traffic eingedämmt und die Zuverlässigkeit des Systems der Remote-Steuerung verbessert wird.
- Client-Computer aus einem logischen Netzwerk in ein anderes Netzwerk umsetzen.

3.5.1. Gruppen

Um eine neue Gruppe hinzuzufügen, klicken Sie auf den Eintrag **Neu / Gruppe** im Kontextmenü der Gruppe, in die die Gruppe eingebettet wird. Daraufhin erscheint in der Konsolenstruktur im Element **Gruppen** (s. Abb. 7) im von Ihnen angegebenen Ordner ein neuer Ordner mit dem eingegebenen Namen. Im

Ordner werden automatisch die darin eingebetteten Ordner **Richtlinien**, **Gruppentasks** und **Administrationsserver** angelegt. Befüllt werden sie in der Phase, wenn die Richtlinien der Gruppe festgelegt, Gruppentasks gebildet und untergeordnete Server eingerichtet werden.

In eine Gruppe können Client-Computer und untergeordnete Gruppen übernommen werden, welche die nächste Hierarchieebene bilden. Es kann die das Anzeigen der geerbten Richtlinien und Gruppentasks in den untergeordneten Gruppen eingestellt werden.

Sie können auch vorgeben, welche Kaspersky-Lab-Anwendungen automatisch auf allen der Gruppe neu hinzugefügten Client-Computern installiert werden sollen.

Damit Programme von Kaspersky Lab auf neuen Computern mit den Betriebssystemen Microsoft Windows 98/ME automatisch installiert werden können, ist auf ihnen vorsichtshalber der Administrationagent zu installieren.

Des Weiteren können Sie den Namen der Gruppe ändern, die Gruppe in andere Gruppe verschieben oder sie löschen.

Die Gruppe wird zusammen mit allen eingebetteten Gruppen, untergeordneten Administrationsservern, Client-Computern, Gruppenrichtlinien und Gruppentasks vorgehalten. Ihr werden allen Einstellungen zugeordnet, die ihrer Position in der Hierarchie von Objekten im logischen Netzwerk entsprechen.

Gruppen werden mit den Standardbefehlen im Kontextmenü **Ausschneiden** / **Einfügen** oder mit den analogen Einträgen im Menü **Aktion**, oder mit den üblichen Drag- und Drop-Bewegungen der Maus verschoben.

Wenn Gruppen verschoben werden, muss auf die Unikalität von Gruppennamen im Rahmen einer Hierarchieebene geachtet werden. Um einem Namenskonflikt aus dem Weg zu gehen, muss der Name einer Gruppe vor deren Verschieben geändert werden. Sollte die Regel der Unikalität für einen Namen nicht eingehalten werden, bekommt der Gruppenname automatisch Die Endung _1, _2 usw. zugewiesen.

Sie können den Namen des Ordners **Gruppe** nicht ändern, da er in die Administrationkonsole fest eingebaut ist.

Die Gruppe kann aus dem logischen Netzwerk entfernt werden, wenn keine untergeordneten Administrationsserver, eingebettete Gruppen und Client-Computer sowie keine Gruppentasks oder Richtlinien mehr vorhanden sind. Die gewählte Gruppe wird mit dem Eintrag **Entfernen** im Kontextmenü oder mit dem analog lautenden Eintrag im Menü **Aktion** entfernt.

3.5.2. Client-Computer

Client-Computer werden zu einer Gruppe hinzugefügt, indem Sie auf den Eintrag **Neu / Computer** im Kontextmenü für eine Gruppe klicken, in die der Rechner übernommen werden soll. Es wird ein Assistent gestartet. Beim Bearbeiten des Assistenten werden in die Gruppe Computer eingefügt und im Detailfenster unter den Namen der Administrationsserver dargestellt, die für sie installiert wurden (s. Abb. 9).

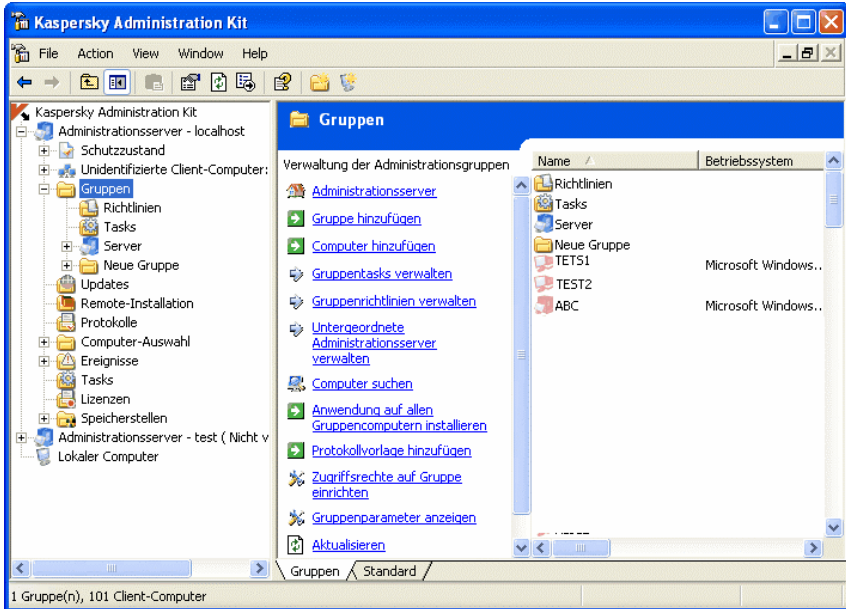


Abbildung 9. Client-Computer in einer Gruppe

Das Hinzufügen von Client-Computern in ein logisches Netzwerk lässt sich so einstellen, dass der Administrationsserver eigenständig alle neu im Windows-Netzwerk erkannten Rechner in eine bestimmte Administrationsgruppe aufnimmt. Es müssen dazu jedoch die entsprechenden Parameter in den Gruppeneigenschaften **Netzwerk** (s. Abb. 10) konfiguriert werden.

Das Hinzufügen eines Computers geht auch mit der Maus im Hauptfenster von Kaspersky Administration Kit, indem Sie den Computer aus dem Ordner **Netzwerk** in den Ordner des logischen Netzwerks ziehen.

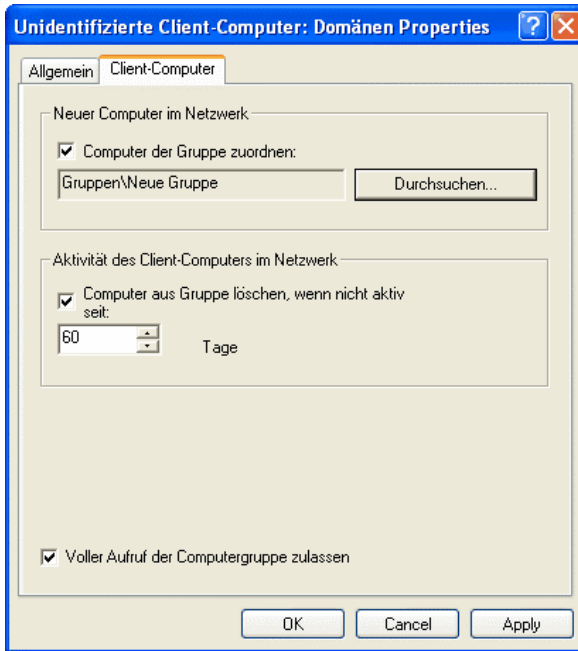


Abbildung 10. Automatisches Hinzufügen neuer Computer in die Gruppe

Sie können Client-Computer aus einer Gruppe in eine andere Gruppe verschieben, von einem logischen Netzwerk mit den Standardeinträgen im Kontextmenü **Ausschneiden / Einfügen** und **Löschen** oder den analog lautenden Punkten im Menü **Aktion** entfernen. Die aus dem logischen Netzwerk entfernten Computer kommen in die Gruppe **Netzwerk**. Der Verschiebevorgang lässt sich auch mit der Maus und Drag-and-Drop erledigen.

Es besteht die Option, Client-Computer aus einem logischen Netzwerk in ein anderes logisches Netzwerk zu verschieben. Wenn beispielsweise ein untergeordneter Administrationsserver hinzugefügt wird, können Sie Client-Computer aus dem logischen Netzwerk des Hauptserver in das logische Netzwerk eines untergeordneten Server verschieben. Es müssen zu diesem Zweck die Client-Computer mit dem neuen Administrationsserver verbunden werden.

Das Zuweisen eines Client-Computers zu einem anderen Administrationsserver erfolgt durch das Erstellen und den Start des Tasks **Administrationsserver wechseln**. Möglich ist das Verschieben einzelner Computer durch das Erstellen eines globalen Tasks, wie auch aller Client-Computer aus einer bestimmten Administrationsgruppe mit Hilfe eines Gruppentasks. Als Ergebnis der

Ausführung des Tasks zum Ändern des Servers werden die Client-Computer, für die der Task erstellt und erfolgreich ausgeführt wurde, vom alten Administrationsserver getrennt und erscheinen in der Gruppe **Netzwerk** des neuen Servers. Das Entfernen der Client-Computer aus der Administrationsgruppe des alten logischen Netzwerks und das Hinzufügen zum neuen logischen Netzwerk erfolgt manuell über die Administrationskonsole.

Sie können einen [Client-Computer mit einem anderen Administrationsserver lokal verbinden](#) vom Client-Computer aus.

Dieser Vorgang erfolgt mit der Utility **klmover.exe**, die zum Lieferumfang des Administrationsagenten gehört. Nach Installation des Administrationsagenten steht diese Utility im Wurzelverzeichnis der Installation zur Verfügung.

3.5.3. Untergeordnete Administrationsserver

Mithilfe der Serverhierarchie können für jeden untergeordneten Administrationsserver und ihm vom Hauptserver zugeordneten Client-Computer die folgenden Vorgänge ausgeführt werden:

- Erstellen und Verbreiten einer *Richtlinie für Anwendungen*
- Anlegen und Verbreiten von *Gruppentasks* (mit Task für Remote-Installation)
- Verbreitung von *Updates* und *Installationspaketen*, die der Hauptserver empfangen hat
- Erstellen von *Protokollen*, in denen die Informationen von allen untergeordneten Administrationsservern zusammengefasst werden

Richtlinien und Tasks, die vom Hauptadministrationsserver empfangen wurden, können auf dem untergeordneten Administrationsserver nicht geändert werden.

Einen untergeordneten Server fügen Sie hinzu, indem Sie auf den Eintrag **Neu / Administrationsserver** für das Objekt des Administrationsservers in der gewünschten Gruppe klicken. Es öffnet sich daraufhin der [Assistent für das Hinzufügen eines untergeordneten Servers](#). Folgende Vorgänge lassen sich im Nachgang erledigen:

- Hinzufügen eines untergeordneten Administrationsservers
- Verbinden der Administrationskonsole mit einem untergeordneten Server

- Konfiguration der Verbindungseinstellungen mit dem Hauptserver
- Hinzufügen von Informationen über den untergeordneten Server in die Datenbank des Hauptadministrationservers
- Verbindungsphasen und Einstellungen überspringen, so dass Sie sie manuell ausführen müssen. Bauen Sie dazu eine Verbindung von Administrationskonsole und dem Server auf, der als untergeordneter Server fungieren wird, und geben Sie die Parameter für dessen Verbindung zum Hauptserver ein.

Nachdem ein untergeordneter Administrationsserver erfolgreich hinzugefügt worden ist, werden das Symbol und der Name des Servers im Ordner **Administrationsserver** in der jeweiligen Gruppe angezeigt.

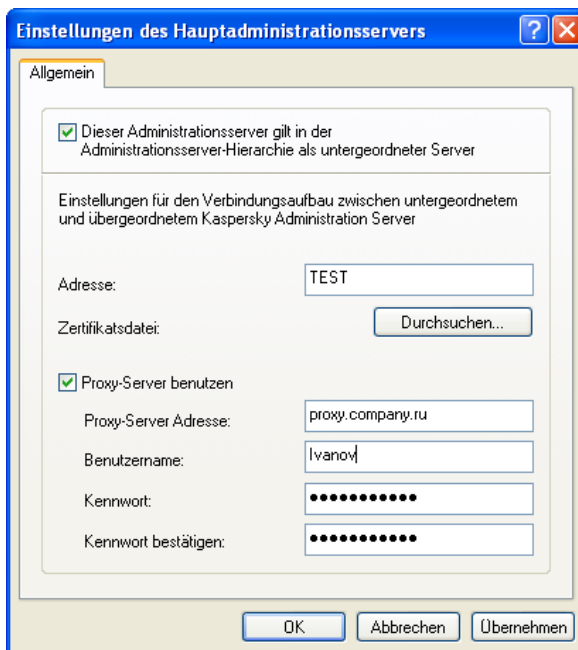








Abbildung 10. Konfiguration der Verbindungseinstellungen zum Hauptadministrationsserver

Sie können mit dem logischen Netzwerk des untergeordneten Administrationservers über das Element **Administrationsserver** im logischen Netzwerk des Hauptservers so oder auch direkt arbeiten, indem Sie den Server in die Konsolenstruktur als neuen Administrationsserver einfügen.

Ein untergeordneter Server ist ein vollwertiger Administrationsserver und erfüllt alle Funktionen eines Administrationsservers in seinem logischen Netzwerk.

Der untergeordnete Administrationsserver vererbt vom Hauptserver die Gruppentask und Richtlinien dieser Gruppe, zu der er gehört. Die vererbten Richtlinien und Tasks werden auf dem untergeordneten Server auf folgende Weise dargestellt:

- Neben dem Namen der Richtlinie, die vom Hauptadministrationsserver empfangen wurde, steht das Symbol  (übliches Richtlinienkennzeichen ist ).
- Die Parameterwerte einer vererbten Richtlinie lassen sich auf dem untergeordneten Server nicht ändern.
- Die in einer vererbten Richtlinie für Änderungen nicht zugelassenen Parameter sind in allen Anwendungsrichtlinien auf dem untergeordneten Server für Änderungen gesperrt (Symbol ) und verwenden Werte, die in der vererbten Richtlinie vorgegeben wurden.
- Die Parameterwerte, deren Änderung in der vererbten Richtlinie nicht gesperrt ist, können in den Richtlinien des untergeordneten Servers geändert werden (Symbol ). Wenn ein Parameter in einer Richtlinie des untergeordneten Servers nicht einem „Schloss“ verriegelt ist, lässt er sich auch in den Anwendungseinstellungen und in den Taskeinstellungen ändern.
- Neben dem Namen des Gruppentasks, der vom Hauptadministrationsserver empfangen wurde, erscheint das Symbol  (übliches Taskkennzeichen ist ).

Globales Tasks für Remote-Installation werden auf untergeordnete Server nicht übertragen. Die Übertragung von Gruppentasks wird in den Taskeigenschaften eingestellt.

Das Update von Client-Computern eines untergeordneten Administrationsservers kann so eingestellt werden, dass nach dem Update-Download durch den Hauptserver automatisch der Task Update-Download durch den untergeordneten Server und nach dessen erfolgreicher Ausführung der Task Update der Anwendungen auf den jeweiligen Client-Computern des untergeordneten Servers gestartet wird (s. Pkt. 5.3 auf S. 80).

KAPITEL 4. ARBEITEN MIT DEM PROGRAMM

Kaspersky Administration Kit unterstützt nur die Verwaltung der Kaspersky-Lab-Anwendungen, die mit einer speziellen Komponente, dem Steuerungs-PlugIn, geliefert werden.

4.1. Einstellung der Anwendungsparameter

4.1.1. Verwalten von Richtlinien

Das Erstellen einer Richtlinie für eine Anwendung geht nur, wenn auf dem Administratorarbeitsplatz das Verwaltungs-PlugIn für diese Anwendung installiert ist.

Klicken Sie zum Erstellen einer Richtlinie auf den Hyperlink **Neu / Richtlinie** im Kontextmenü des Ordners **Richtlinie**. In der Phase Erstellen einer Richtlinie werden die minimalen Parameter eingestellt, ohne die das Programm nicht funktioniert. Die restlichen Werte werden nach dem Standard gesetzt und entsprechen den Standardwerten für eine lokale Programminstallation.

Eine detaillierte Beschreibung zur Einstellung einer Richtlinie für eine Kaspersky-Lab-Anwendung finden Sie in den jeweiligen Handbüchern.

Des Weiteren können Sie Parameterwerte ändern, deren Änderung in Richtlinien von eingebetteten Gruppen und in den Anwendungseinstellungen sperren (s. Abb. 11).

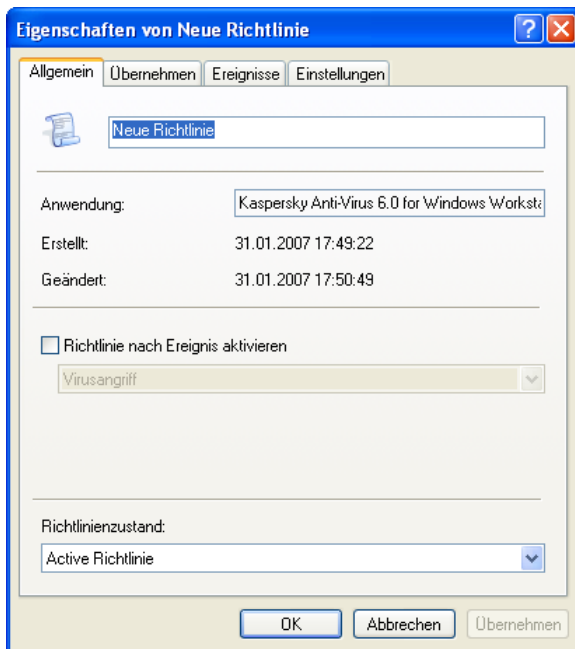


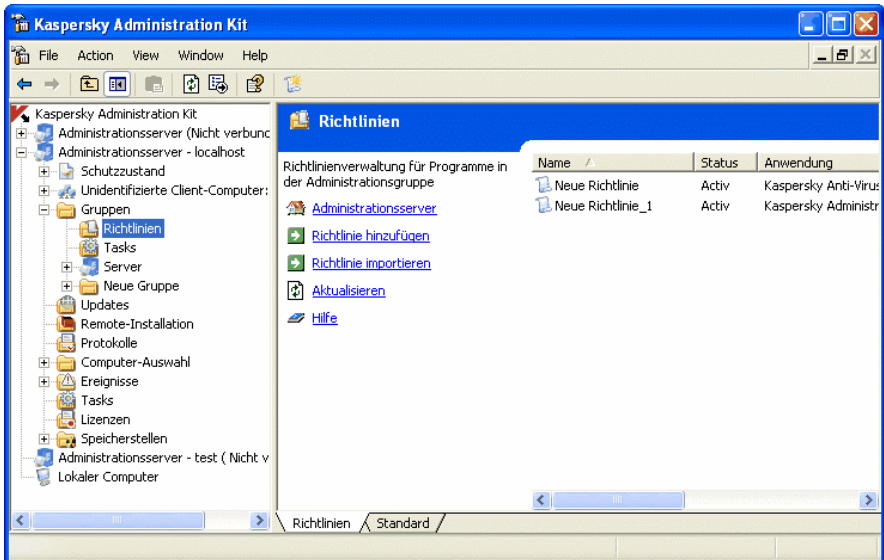


Abbildung 11. Richtlinie bearbeiten

Neben Parametern, die zu einer Richtlinie gehören, deren Änderung unterbunden werden soll, steht das Symbol . Zum Einrichten des Verbots klicken Sie mit der linken Maustaste darauf. Das Symbol verwandelt sich in . Solche Parameter sind in den Anwendungseinstellungen, den Taskeinstellungen und in den Richtlinien von eingebetteten Gruppen und untergeordneten Administrationsservern künftig für Änderungen gesperrt.

Die lokalen Anwendungseinstellungen haben vor den Richtlinieneinstellungen Priorität. Wenn Sie wollen, dass für einen Parameter ein in eine Richtlinie eingegebener Wert gilt, müssen Sie die Änderungssperre für diesen Parameter aufheben.

Nach dem Erstellen wird die Richtlinie in den Ordner **Richtlinien** (s. Abb. 12) der entsprechenden Gruppe eingefügt und auf alle zu ihr gehörenden eingebetteten Gruppen und untergeordneten Administrationsserver als ererbte Richtlinie verbreitet.

Abbildung 12. Ordner **Richtlinie**

Eine erstellte Richtlinie können Sie löschen, kopieren, aus einer Gruppe in eine andere Gruppe mit dem Eintrag im Kontextmenü der im Detailfenster gewählten Richtlinie exportieren und importieren.

Für jede Anwendung können mehrere Gruppenrichtlinien erstellt werden, es kann aber immer nur eine Richtlinie gelten. In den Parametern für so eine Richtlinie muss der Parameter **Aktive Richtlinie** gesetzt sein.

Die Aktivierung einer Richtlinie erfolgt automatisch, wenn ein bestimmtes Ereignis eintritt. Die Rückkehr zur vorangegangenen Richtlinie geschieht jedoch manuell.

Außerdem lässt sich eine Richtlinie für mobile Benutzer erstellen, die unmittelbar nach Trennung des Computers vom logischen Netzwerk in Kraft tritt.

Ein Computer wird als „vom logischen Netzwerk getrennt“ betrachtet, wenn drei Verbindungsversuche des Administrationsservers erfolglos blieben. Zeitabstand zwischen den Verbindungsversuchen wird in den Parameter des Administrationsagenten, im Feld **Synchronisationsperiode (Min.)** vorgegeben, und beträgt standardmäßig 15 Minuten.

Die Ergebnisse einer Richtlinienverbreitung lassen sich über die Administrationskonsole im Fenster Richtlinieneigenschaften anzeigen (s. Abb. 14).

Wie sich die Werte der lokalen Parameter der Anwendung auf jedem Client-Computer verändern hängt davon ab, welche Variante wurde in dem Fenster **Erweitert** gewählt (s. Abb. 14). Dieses Fenster wird durch den Klick auf den Hyperlink **Erweitert** in der Registerkarte **Anwenden** in dem Fenster der Richtlinieneigenschaften.

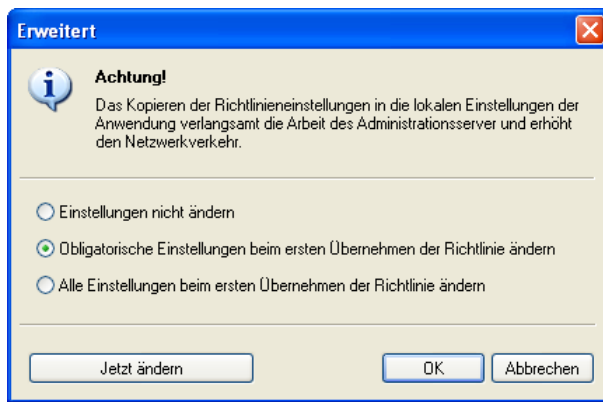



Abb. 13. Einstellung der Richtlinienanwendung



Das Ändern der lokalen Parameter wird automatisch vorgenommen entsprechend der gewählten Variante beim ersten Anwenden der Richtlinie auf dem Client-Computer, das heißt:

- Hinzufügen des Client-Computers in den Bereich, wo die Richtlinie gültig ist;
- Aktivierung der Richtlinie;
- Das Installieren der Antivirenanwendung auf dem Client-Computer, für den die Richtlinie erstellt wurde.

Es kann eine der folgenden Varianten gewählt werden:

- **Die Parameter nicht ändern.** In diesem Fall werden nur die Parameter angewendet, welche mit dem Ikon  in den Richtlinieneinstellungen markiert sind. Andere Parameter werden den lokalen Einstellungen entsprechen. Diese Variante ist Standardmäßig eingestellt.

Nach dem Entfernen oder Außerkraftsetzen einer Richtlinie kehren alle lokalen Parameter zu den Werten zurück, welche vor dem Anwenden der Richtlinie gültig waren.

- **Zwangsläufige Parameter beim ersten Anwenden der Richtlinie ändern.** In diesem Fall werden nur die Parameter angewendet, welche mit dem Icon  in den Richtlinieneinstellungen markiert sind. In diesem Fall nach dem Entfernen oder Außerkraftsetzen einer Richtlinie kehren zu den ursprünglichen Einstellungen nur die Parameter, Bearbeitung dessen in der Richtlinie nicht verboten wurde (diese Parameter sind mit dem Icon  markiert).
- **Alle Parameter beim ersten Anwenden der Richtlinie ändern.** In diesem Fall werden alle lokalen Parameter entsprechend der Richtlinie geändert. Nach dem Entfernen oder Außerkraftsetzung der Richtlinie wird die Anwendung mit den in der Richtlinie definierten Einstellungen weiter arbeiten. Später können die Einstellungen per Hand geändert werden.

Sie können die Parameter auch per Hand anwenden. Dazu klicken Sie auf **Sofort anwenden** (s. Abb. 14). Die Richtlinie wird mit den gewählten Parametern angewendet.

Auf welche Weise sich die Werte der lokalen Anwendungsparameter auf jedem Client-Computer ändern, hängt vom Kontrollkästchen Nichtpflichtfelder bei Erstübernahme ändern ab.

Außerdem können Sie Parameterwerte je nach der manuell getroffenen Wahl und unabhängig von der Richtlinieübernahme festlegen. Klicken Sie dazu auf die Schaltfläche **Jetzt ändern** (s. Abb. 14).

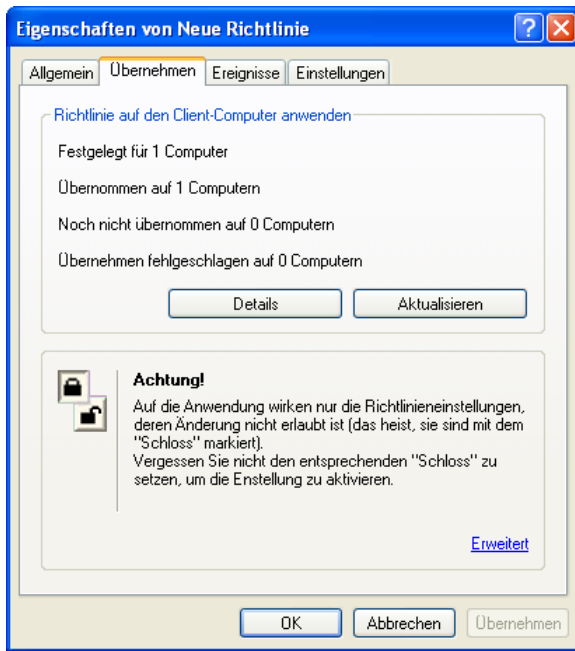


Abbildung 14. Einstellung einer Richtlinienübernahme

Eine Richtlinie wird auf die folgende Weise übernommen: Wenn auf dem Client-Computer Residenztasks (Echtzeitschutz) ausgeführt werden, werden sie ohne Unterbrechung mit den neuen Parameterwerten fortgeführt. Die aufgerufenen periodischen Tasks (Scan auf Befehl, Update der Antiviren-Datenbanken) werden mit den alten Werten ausgeführt, der Neustart erfolgt mit den geänderten Parameterwerten. Die Parameterwerte des Programms, die nach Übernahme der Richtlinie aktiviert worden sind, können Sie in der Administrationskonsole im Eigenschaftenfenster des konkreten Client-Computers sehen.

Bei einer hierarchischen Administrationsserverstruktur erhalten die untergeordneten Server die Richtlinien vom Hauptadministrationsserver und verteilen sie an die Client-Computer. Die Richtlinienparameter können auf dem Hauptadministrationsserver geändert werden. Danach passen die untergeordneten Administrationsserver ihre Richtlinien entsprechend an und verteilen diese an die untergeordneten Client-Computer.

Wenn die Verbindung zwischen Haupt- und untergeordneten Administrationsserver unterbrochen wird, setzt der untergeordnete Administrationsserver seine Arbeit mit den vorigen Einstellungen fort. Die auf dem Haupt-Administrationsserver geänderten Richtlinien werden nach dem

wiederherstellen der Verbindung auf den untergeordneten Administrationsserver propagiert.

Wenn die Verbindung zwischen Administrationsserver und Client-Computer unterbrochen wird, tritt auf dem Client-Computer die Richtlinie für mobile Benutzer in Kraft (wenn solche definiert ist), oder die Richtlinie wird mit den vorigen Einstellungen beibehalten, bis die Verbindung wiederhergestellt wird.

Die Ergebnisse der Richtlinienverteilung an untergeordnete Administrationsserver werden im Eigenschaftenfenster der Richtlinie des Hauptadministrationsservers angezeigt.

Auf analoge Weise können auch die Ergebnisse der Richtlinienverteilung auf die Client-Computer im Eigenschaftenfenster der Richtlinie des untergeordneten Administrationsservers angezeigt werden, nachdem zuvor eine Verbindung mit diesem aufgebaut wurde.

Eine detaillierte Beschreibung der Richtlinien für Kaspersky-Lab-Anwendungen steht in den Handbüchern für das jeweilige Programm. Die Einstellung der Richtlinie für den Administrationsagenten und den Administrationsserver ist im Benutzerhandbuch für den Kaspersky Administration Kit beschrieben.

4.1.2. Lokale Anwendungseinstellungen

Das Verwaltungsprogramm Kaspersky Administration Kit bietet die Option der Remote-Steuerung von lokalen Anwendungseinstellungen auf Client-Computern über die Administrationskonsole (s. Abb. 15). Mithilfe der Anwendungseinstellungen können Sie individuelle Parameterwerte für das Programm auf jedem einzelnen Client-Computer in der Gruppe bestimmen. Sie können die Werte aber nur für die Parameter ändern, deren Modifikation von der Gruppenrichtlinie für diese Anwendung nicht gesperrt ist, das heißt, der Parameter darf nicht mit einem Schloss verriegelt sein.

Die Einstellung der lokalen Parameter erfolgt für jeden Client-Computer getrennt im Fenster **Parameter der Anwendung** "<Anwendungsname>". Dieses Fenster wird von der Registerkarte **Anwendungen** im Fenster **Eigenschaften: <Computername>** aufgerufen.

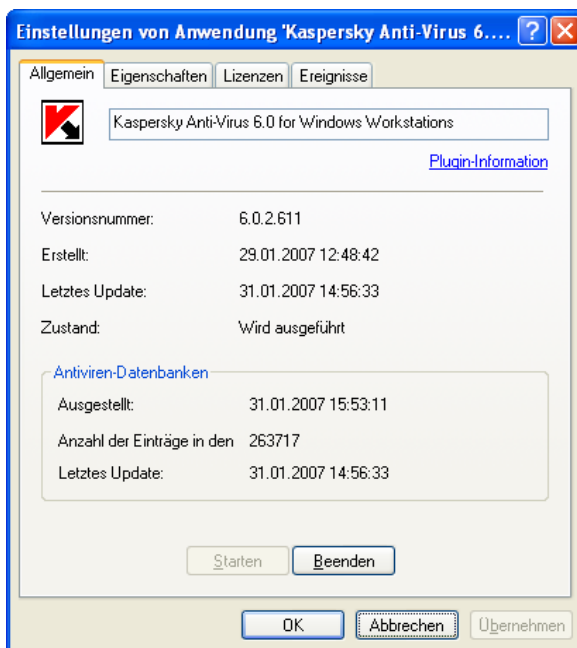


Abbildung 15. Fenster Einstellung der lokalen Anwendungsparameter

Die lokalen Parameter sind für jede Kaspersky-Lab-Anwendung unterschiedlich. Eine genaue Beschreibung finden Sie in den Handbüchern der jeweiligen Anwendung.

Eine detaillierte Beschreibung der Einstellungen für den Administrationsagenten und für den Administrationsserver finden Sie im Benutzerhandbuch von Kaspersky Administration Kit.

4.2. Verwaltung von Anwendungen

Anwendungen, die auf den Client-Computern des logischen Netzwerks installiert sind, verwalten Sie mit dem Erstellen und Starten von Tasks, mit denen jede Grundfunktion ausgeübt werden kann: Installation von Anwendungen, Aktivierung von Lizenzschlüsseln, Untersuchung von Dateien, Update der Antiviren-Datenbanken und Anwendungsmodule usw.

Kaspersky Administration Kit unterstützt alle Tasktypen, die für die lokale Arbeit mit einer Anwendung vorgesehen sind. Außerdem gibt es noch die Option,

Anwendungen mit den entsprechenden Steuerungstasks für den Administrationsagenten im Remote-Betrieb zu starten und zu beenden. Eine genaue Beschreibung der Tasktypen finden Sie für jede Kaspersky-Lab-Anwendung in den jeweiligen Benutzerhandbüchern.

Über die Administrationskonsole erfolgt im Remote-Betrieb das Starten und Beenden der Anwendung mit den entsprechenden Tasks.

Tasks können für Anwendungen nur dann erstellt werden, wenn auf dem Arbeitsplatz des Administrators das Steuerungs-PlugIn für diese Anwendung installiert ist.

Um das Netzwerk zu schützen, kann der Administrator beliebig viele verschiedene Tasks (außer Einzeltasks) für jede Anwendung erstellen, deren Steuerung mit Kaspersky Administration Kit geschieht.

Damit beispielsweise Client-Computer, die Arbeitsstationen sind, auf schädlichen Programmcode untersucht werden, muss der Task Scan auf Befehl für Kaspersky Anti-Virus Windows Workstations angelegt werden.

Die Steuerungsfunktionen für die Anwendungen und die üblichen Servicevorgänge realisieren die Tasks der Komponenten von Kaspersky Administration Kit, der Administrationsserver und der Administrationsagent. Folgende Tasktypen sind für diese Komponenten festgelegt:

- Administrationsservern wechseln
- Start / Beenden einer Anwendung
- Remote-Installation einer Anwendung
- Remote-Deinstallation einer Anwendung
- Update-Download durch Administrationsserver
- Erstellen einer Sicherungskopie vom Administrationsserver
- Versand von Protokollen
- Verbreitung eines Installationspaketes

Diese Tasktypen unterscheiden sich in zahlreichen Dingen bei Erstellung und Start. Eine detaillierte Beschreibung dazu finden Sie im Benutzerhandbuch von Kaspersky Administration Kit.

Für alle Tasktypen können Sie Gruppentasks, globale Tasks und lokale Tasks erstellen.

Für den Task **Remote-Installation** lassen sich Gruppentasks und globale Tasks erstellen. Für die Tasks **Update-Download**, **Erstellen einer Sicherungskopie** und **Versand von Protokollen** lassen sich nur globale Tasks erstellen.

Die Tasks **Update-Download** und **Erstellen einer Sicherungskopie vom Administrationsserver** können nur ein einziges Mal angelegt und nur für einen einzigen Computer ausgeführt werden, nämlich auf dem Administrationsserver.

Klicken Sie zum Erstellen des Tasks auf den Eintrag **Neu / Task** im Kontextmenü für den Ordner **Gruppentasks** oder **Globale Tasks**.

Die erstellten Gruppentasks liegen dann in den eingebetteten Ordnern **Gruppentasks** der jeweiligen Gruppen (s. Abb. 16). Die globalen Tasks befinden sich dann in einem speziellen Container der Konsolenstruktur, in den **Globalen Tasks**. Die Liste mit den lokalen Tasks eines Client-Computers ergründen Sie im Eigenschaftenfenster.

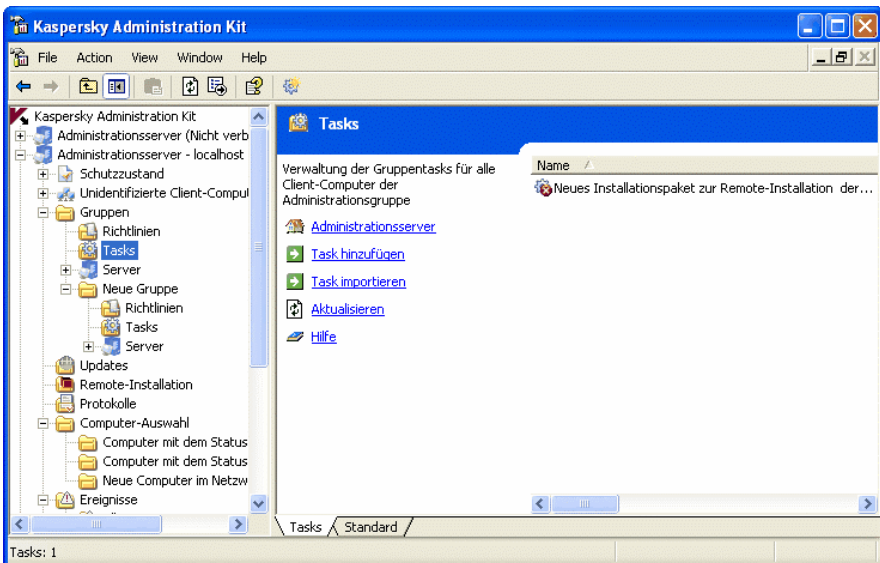


Abbildung 16. Gruppentasks

Die Informationen zu Tasks werden zwischen der lokalen Anwendung und der Informationsdatenbank von Kaspersky Administration Kit dann ausgetauscht, wenn eine Verbindung des Administrationsagenten mit dem Server zu Stande kommt. Tasks, die lokal erstellt wurden, gehen dann in die Datenbank des Administrationsservers ein.

Sie können die Taskeinstellungen ändern, die Taskausführung verfolgen, Tasks aus einer Gruppe in eine andere Gruppe exportieren bzw. importieren sowie Tasks mit den Einträgen im Kontextemenü löschen.

Die Parameter der Anwendung für die Taskausführung auf einem Client-Computer werde je nach der Gruppenrichtlinie, den Taskeinstellungen und den Einstellungen der jeweiligen Anwendung auf dem Client-Computer ativiert.

Die meisten Parameter bestimmt die Richtlinie, die diesen Task ausführt. Zum Beispiel die Aktionen für infizierte Objekte bei deren Erkennung, die Update-Ressourcen für die Antiviren-Datenbanken usw. Sollte die Änderung dieser Parameter gesperrt sein, lassen sich in den Taskeinstellungen nicht ändern (s. Abb. 17).

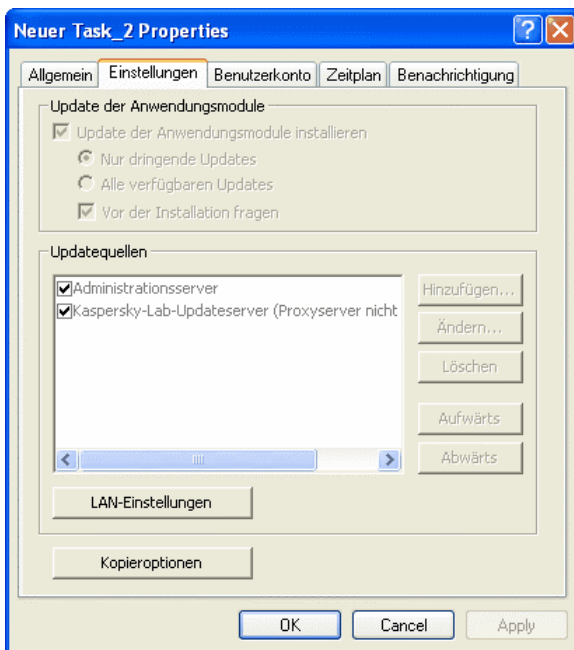


Abbildung 17. Parameter eines Tasks, deren Änderung gesperrt ist

Einige Einstellungen sind jedoch individuell für einen konkreten Task: Zeitplan für Taskstart, Benutzerkonto, unter dem der Task gestartet wird, Untersuchungsbereich für den Task Scan auf Befehl usw. Die Werte dieser Parameter werden für jeden Task in dessen Einstellungen festgelegt und können nach dem Erstellen des Task geändert werden (s. Abb. 18).

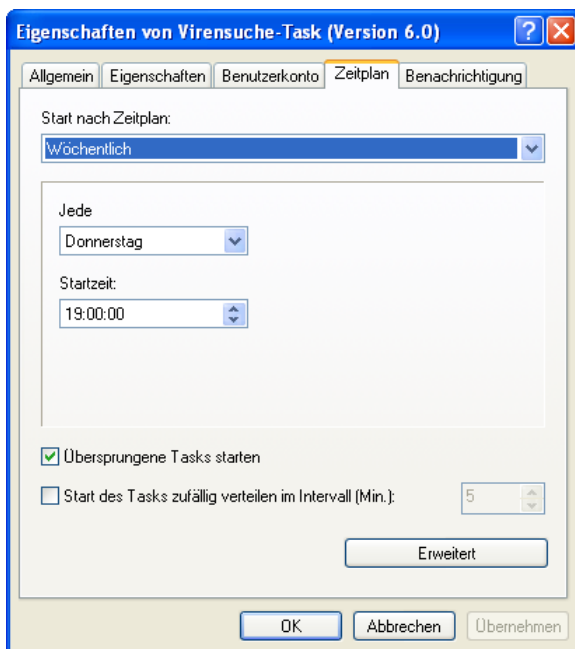


Abbildung 18. Zeitplan für den Taskstart

Tasks werden zu ihrer Ausführung je nach Zeitplan gestartet. Computer, die während der im Zeitplan eingestellten Startzeit ausgeschaltet sind, kann automatisch das Betriebssystem mit der Funktion Wake On Lan hochgefahren werden. Dazu muss im Fenster, das sich mit einem Klick auf die Schaltfläche **Erweitert** auf der Registerkarte **Zeitplan** (s. Abb. 18) öffnet, das entsprechende Häkchen gesetzt werden (s. Abb. 19).

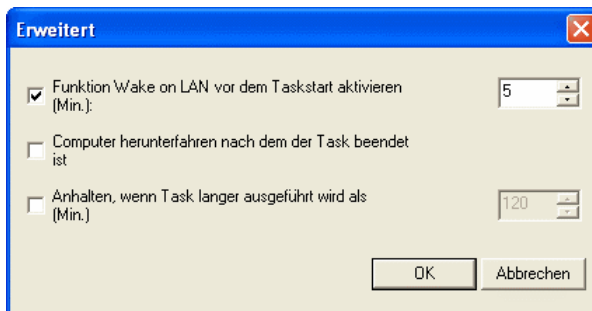


Abbildung 19. Automatisches Hochfahren des Betriebssystems aktivieren

Außerdem lässt sich eingeben, dass der Computer nach der Taskausführung laut Zeitplan automatisch wieder heruntergefahren wird.

Die Ausführungszeit für den Task kann eingegrenzt werden. In so einem Fall wird er nach Ablauf einer eingerichteten Frist beendet. Es ist vorgesehen, einen Task nach Zeitplan zu deaktivieren. Dabei wird der Task nicht gelöscht, sondern lediglich nicht gestartet.

Sie können auch manuell einen Task starten, unterbrechen, anhalten oder wiederaufnehmen, indem Sie die Befehle im Kontextmenü und im Fenster für die Taskeinstellungen anklicken (s. Abb. 20).

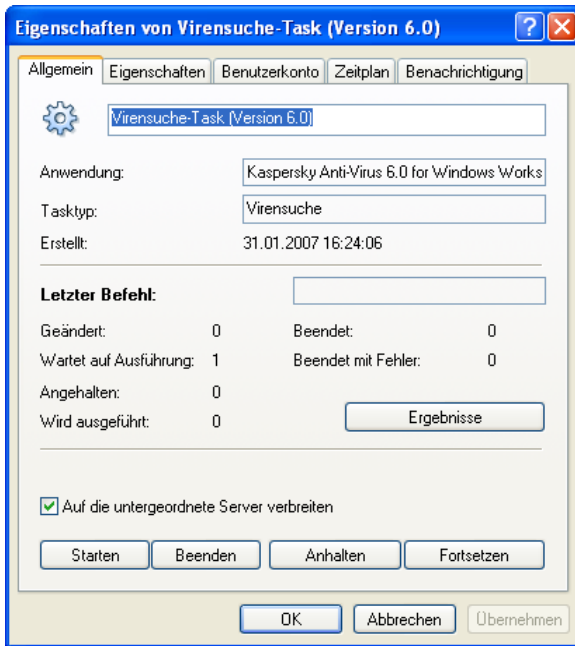


Abbildung 20. Steuerung der Taskausführung

Der Start von Tasks auf einem Client-Computer findet nur dann statt, wenn die entsprechende Anwendung gestartet wurde. Beim Beenden einer Anwendung wird die Ausführung aller gestarteten Tasks abgebrochen.

Tasks verfolgen und Ergebnisse anzeigen können Sie im Fenster Taskeinstellungen (s. Abb. 20).

Die Ausführungsergebnisse des Tasks werden entsprechend den Einstellungen im Ereignisprotokoll von Windows und des Kaspersky Administration Kit wie zentralisiert auf dem Administrationsserver, so auch lokal auf jedem Client-Computer festgehalten und gespeichert. Dabei kann die Benachrichtigung über die Ergebnisse an den Administrator und andere Benutzer erfolgen. Form und Art der Benachrichtigung werden ebenfalls durch die Task-Einstellungen bestimmt.

Sie können die Ergebnisse der Taskausführung, die im Ereignisprotokoll von Kaspersky Administration Kit gespeichert sind, über das Element **Ereignisse** in der Konsolenstruktur anzeigen lassen. Die Ergebnisse der Taskausführung für jeden Client-Computer finden Sie im Fenster der Task-Eigenschaften.

Die Anzeige von Informationen über die Ergebnisse der Taskausführung, die lokal auf einem Client-Computer gespeichert sind, erfolgt über die lokal auf dem betreffenden Computer installierte Administrationskonsole.

Bei einer hierarchischen Administrationsserverstruktur erhalten die untergeordneten Server, wenn in den Taskeinstellungen der entsprechende Parameter aktiviert ist (s. Abb. 20), die Gruppentasks vom Hauptadministrationsserver und verteilen diese an die Client-Computer. Die Parameter der Gruppentasks können auf dem Hauptadministrationsserver verändert werden. Danach passen die untergeordneten Administrationsserver ihre Gruppentasks entsprechend an und verteilen diese an die untergeordneten Client-Computer.

Die Ergebnisse des Verteilens eines Gruppentasks an untergeordnete Administrationsserver werden im Fenster **Ergebnisse der Taskausführung** im Eigenschaften-Fenster des Gruppentasks des Hauptadministrationsservers angezeigt.

Auf entsprechende Weise können auch die Ergebnisse des Verteilens eines Gruppentasks auf die Client-Computer im Eigenschaften-Fenster des Gruppentasks des untergeordneten Administrationsservers angezeigt werden, nachdem zuvor eine Verbindung mit diesem aufgebaut wurde.

KAPITEL 5. UPDATE DER ANTIVIREN-DATENBANKEN UND PROGRAMMMODULE

Wichtige Faktoren für die Zuverlässigkeit des Antiviren-Schutzsystems sind die rechtzeitige Aktualisierung der zur Untersuchung infizierter Objekte verwendeten Antiviren-Datenbanken und die Installation kritischer Updates der Programmmodule für Anwendungen, sowie die regelmäßige Aktualisierung deren Versionen.

Die Antiviren-Datenbanken auf den Kaspersky-Lab-Webseiten werden stündlich aktualisiert. Wir empfehlen Ihnen, die Antiviren-Datenbanken in den gleichen Intervallen zu aktualisieren und umgehend alle kritischen Updates für Programmmodule zu installieren.

Zur Aktualisierung der Antiviren-Datenbanken und Programmmodule für die Anwendungen, die mit Hilfe von Kaspersky Administration Kit verwaltet werden, muss ein globaler Task zum Update-Download durch die Anwendung Kaspersky Administration Kit erstellt werden. Als Ergebnis der Taskausführung werden die Antiviren-Datenbanken und Updates der Programmmodule den Task-Einstellungen entsprechend von der Update-Quelle kopiert. Die empfangenen Daten werden auf dem Administrationsserver im Verzeichnis **Updates** des freigegebenen Ordners gespeichert und können auf die Client-Computer und untergeordneten Administrationsserver automatisch nach dem Update-Vorgang verbreitet werden. Der freigegebene Ordner wird bei der Installation des Administrationsservers angelegt. Als Standard gilt als freigegebener Ordner das Verzeichnis **KLShare**, das sich im Installationsverzeichnis der Komponente Administrationsserver (**<Datenträger>:\Program Files\Kaspersky Lab\Kaspersky Administration Kit**) befindet.

Auf die Client-Computer werden die Updates mit Update-Tasks für Anwendungen verbreitet. Die untergeordneten Administrationsserver werden mit Update-Tasks durch den Administrationsserver aktualisiert. Diese Tasks lassen sich automatisch nach dem Update-Download durch den Hauptserver starten, unabhängig von einem Zeitplan, der in den Taskparameter angegeben ist.

5.1. Update-Download durch Administrationsserver

Das Task Update-Download durch den Administrationsserver ist ein globaler Task und kann nur ein einziges Mal erstellt werden. Dieser Task wird so nur für einen einzigen Computer erstellt und gestartet, für den Computer, auf dem die Komponente Administrationsserver installiert ist.

Wenn Sie mit dem Schnellstart-Assistenten gearbeitet haben, ist der Task Update-Download durch Administrationsserver bereits erstellt und er befindet sich in der Konsolenstruktur im Element Globale Tasks.

Starten Sie zum Erstellen des Tasks Update-Download durch den Administrationsserver den Assistenten für das Erstellen von Tasks für das Element **Globale Tasks**. Wählen Sie als Anwendung, für die der Task angelegt werden soll, das Programm **Kaspersky Administration Kit**, als Tasktyp bitte **Update-Download durch Administrationsserver** (s. Abb. 21) aus.

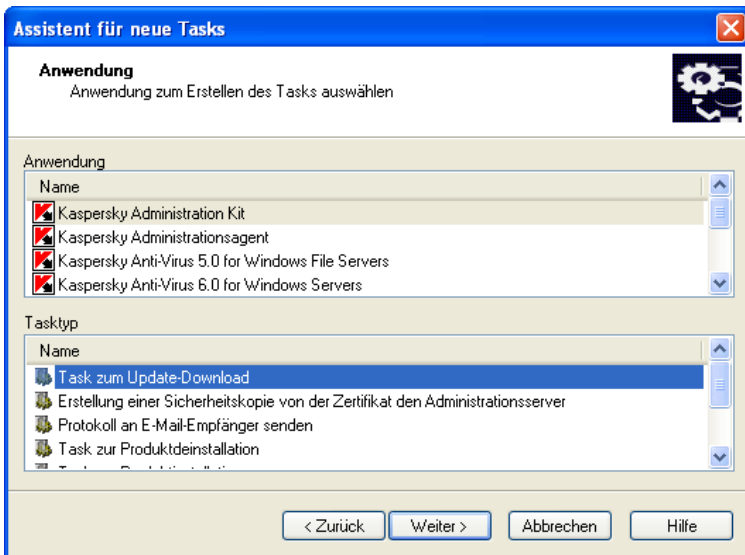


Abbildung 21. Erstellen des Update-Tasks. Wahl von Anwendung und Tasktyp

Wenn im logischen Netzwerk eine Hierarchie von Administrationsservern vorhanden (oder geplant) ist, muss in den Taskeinstellungen auf dem

Hauptserver zur automatischen Verbreitung von Updates auf untergeordnete Server das Kontrollkästchen **Update der untergeordneten Server erzwingen** gesetzt sein (s. Abb. 22). In diesem Fall werden nach dem Update-Download durch Hauptserver die Update-Tasks für die untergeordneten Server gestartet (wenn sie erstellt worden sind).

Wenn ein Häkchen im Kontrollkästchen Update der untergeordneten Server erzwingen steht, erfolgt kein automatisches Erstellen des Tasks Update-Download auf untergeordneten Administrationsservern. Diese Tasks müssen separat und manuell für jeden untergeordneten Server angelegt werden.

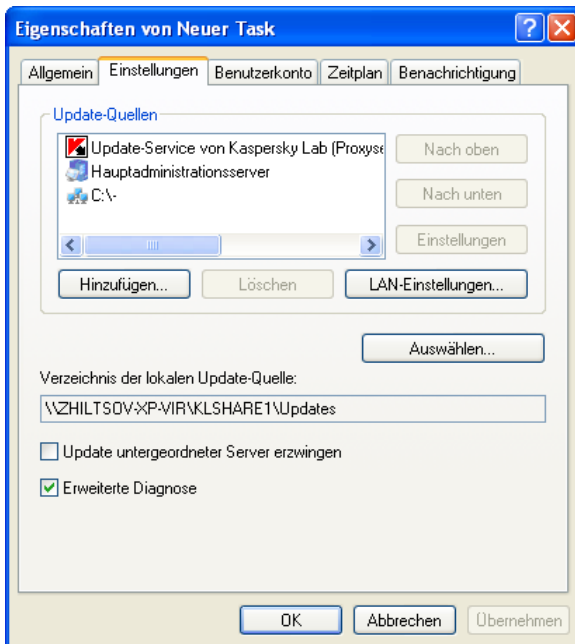


Abbildung 22. Einstellung des Tasks Update-Download

Aufgrund der Taskausführung Update-Download durch Administrationsserver werden die Updates der Antiviren-Datenbanken und Programmmodule von Anwendungen von der Update-Quelle geholt und im freigegebenen Ordner abgelegt.

Aus dem freigegebenen Update-Ordner werden sie dann auf die Client-Computer (s. Pkt. 5.2 auf S. 78) und untergeordneten Administrationsserver (s. Pkt. 5.3 auf S. 80) verbreitet.

Als Update-Quelle für den Administrationsserver kommen folgende Ressourcen in Frage:

- Update-Server von Kaspersky Lab
- Hauptadministrationsserver
- ftp-/http-Server oder Update-Verzeichnis des Netzwerkes

Als Update-Verzeichnis kann eine lokale Update-Quelle vorgegeben werden, in die die empfangenen Updates für Kaspersky Anti-Virus for Windows Workstations in den Versionen 5.0 und 6.0, Kaspersky Anti-Virus 5.0 for Windows File Servers und Kaspersky Anti-Virus 6.0 for Windows Servers kopiert.

Die Entscheidung für die Ressource hängt von den Taskeinstellungen ab.

В случае обновления с ftp- / http-сервера или из сетевого каталога для корректного обновления Сервера на эти ресурсы должна быть скопирована правильная структура папок с обновлениями, совпадающая со структурой формируемой при копировании обновлений программными средствами Лаборатории Касперского.

Informationen anzeigen über empfangene Updates können Sie in der Konsolenstruktur im Container **Update**, die Update-Liste steht im Detailfenster (s. Abb. 23).

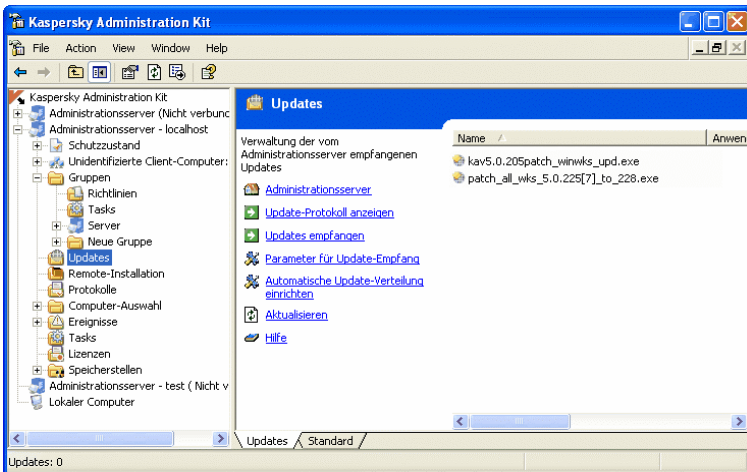


Abbildung 23. Anzeige der empfangenen Updates

5.2. Verbreitung von Updates auf die Client-Computer

5.2.1. Update für Anwendungen

Um die Zuverlässigkeit der Antiviren-Sicherheit zu erhöhen, müssen Tasks für den Update-Download von Updates für alle Anwendungen erstellt werden, die zum System der Antiviren-Sicherheit für die Computer im logischen Netzwerk gehören.

Damit auf den Client-Computern im logischen Netzwerk die gleichen Versionen der Antiviren-Datenbanken und Programmmodule installiert sind, muss in den Taskeinstellungen für den Task Update-Download für Anwendungen als Update-Quelle der Administrationsserver ausgewählt werden.

Wenn im Task Update für Anwendungen als Update-Quelle der Administrationsserver ausgewählt wurde, dann werden bei einer hierarchischen Serverstruktur die Client-Computer von dem Server aus aktualisiert, mit dem sie verbunden sind, d. h. von dem untergeordneten Server und nicht vom Hauptserver.

Die Tasks Update für Anwendungen und ihre Erstellung werden in den Handbüchern für die jeweiligen Anwendungen detailliert beschrieben.

5.2.2. Automatisches Verbreiten durch Administrationsserver

Die Remote-Verwaltung bietet die Option, Updates auf Client-Computer automatisch zu verbreiten, auf denen Kaspersky Anti-Virus for Windows Workstations in den Versionen 5.0 und 6.0, Kaspersky Anti-Virus for Windows File Servers und Kaspersky Anti-Virus for Windows Servers installiert ist, nachdem der Administrationsserver Updates empfangen hat.

Dazu müssen das Häkchen im Kontrollkästchen **Updates der Antiviren-Datenbanken sofort auf Client-Computer verbreiten** in den Eigenschaften des Elementes **Update** (s. Abb. 24) gesetzt sein.

Wenn das Kontrollkästchen aktiviert ist, werden nach dem ersten Download von Updates durch den **Administrationsserver** im Ordner **Gruppentasks** der Gruppe **Gruppen** vier spezielle Tasks erstellt: **Automatisches Update** und

Antiviren-Signaturen (je ein Task pro Anwendung). Diese Tasks werden automatisch nach jedem erfolgreichen Update-Download durch den Server gestartet. Wenn der Modus eines automatischen Verbreitens von Updates deaktiviert (Häkchen entfernt) wird, werden die Tasks gelöscht.



Abbildung 24. Einstellen für automatisches Update von Client-Computern

Wir empfehlen Ihnen, sich für das automatische Verbreiten der Updates zu entscheiden, um den Traffic und die Anfragen der Client-Computer an den Administrationsserver zu verringern sowie möglichen Ungenauigkeiten und Fehlern beim Erstellen von Update-Tasks für logische Netzwerke mit vielen Client-Computern aus dem Weg zu gehen.

Bei einer hierarchischen Struktur von Administrationsservern muss der Modus Automatisches Verbreiten von Updates auf Client-Computer nur für den Hauptadministrationsserver installiert werden. Die Tasks **Automatisches Update** und **Antiviren-Signaturen** werden nach der Hierarchie auf die Client-Computer der untergeordneten Server verbreitet.

Bei einer hierarchischen Struktur der Administrationsserver werden die Tasks **Automatisches Verbreiten von Updates auf Client-Computer** von untergeordneten Servern nach dem erfolgreichen Update dieses Servers gestartet, mit dem sie verbunden sind, also vom untergeordneten Server und nicht vom Hauptserver.

In den Einstellungen der Tasks **Automatisches Update** und **Antiviren-Signaturen** ist als Update-Quelle Administrationsserver voreingestellt. Damit die Client-Computer von untergeordneten Servern gleichzeitig Updates über diese Tasks erhalten, muss der Modus **Automatisches Update untergeordneter Server** in den Taskeinstellungen Update des Hauptservers eingestellt sein.

Um die Belastung für die Administrationsserver zu verringern, wird empfohlen, Update-Agenten zu verwenden, mit denen die Updates in der Administrationsgruppe verteilt werden.

5.3. Update untergeordneter Server und ihrer Client-Computer

Wenn in einem logischen Netzwerk eine hierarchische Struktur von Administrationsservern vorhanden ist, muss Folgendes getan werden, um dafür zu sorgen, dass Updates von untergeordneten Servern empfangen und auf angeschlossene Client-Computer verbreitet werden:

- Ein Task **Update-Download** muss für jeden untergeordneten Administrationsserver erstellt werden.
- In den Einstellungen für den Task **Update-Download** für untergeordnete Server muss als Update-Quelle **Hauptadministrationsserver** (s. Abb. 25) ausgewählt werden.
- In den Einstellungen für den Task **Update-Download** durch Hauptadministrationsserver muss der Modus **Automatisches Verbreiten von Updates auf untergeordnete Server** aktiviert sein. Setzen Sie dazu das Häkchen im Kontrollkästchen **Update untergeordneter Server erzwingen** (s. Abb. 22).
- Bei Bedarf müssen Update-Agenten im Rahmen der Administrationsgruppe angegeben werden (s. Pkt. 5.4 auf S. 81).
- Es muss der Modus **Automatisches Verbreiten von Updates auf Client-Computer** mit installiertem **Kaspersky Anti-Virus for Windows**

Workstations in den Versionen 5.0 und 6.0, Kaspersky Anti-Virus 5.0 for Windows File Servers und Kaspersky Anti-Virus 6.0 for Windows Servers aktiviert oder Tasks für den Update-Download vom Administrationsserver eingerichtet werden.

Der Update-Download von Anwendungen erfolgt von jenem Administrationsserver, mit dem der Client-Computer verbunden ist, das heißt vom untergeordneten Server und nicht vom Hauptserver.

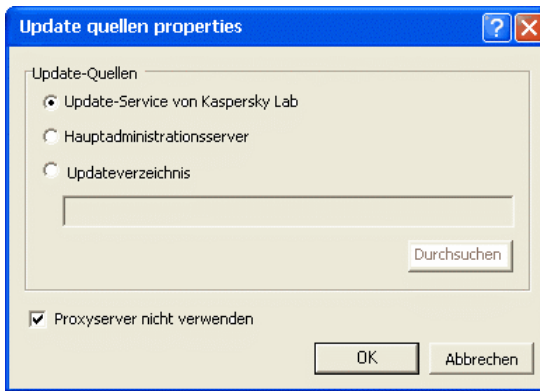


Abbildung 25. Update vom Hauptadministrationsserver

5.4. Verbreitung von Updates mit Updaten-Agenten

Um Updates auf Client-Computer einer Gruppe zu verbreiten, lassen sich *Update-Agenten* einsetzen. Es handelt sich dabei um Computer, die als Zwischenrechner für die Verbreitung von Updates und Installationspaketen im Rahmen der Administrationsgruppe fungieren. Sie empfangen Updates vom Administrationsserver und speichern sie im Installationsverzeichnis einer Anwendung. Kopiert werden nicht nur Updates, die in der Gruppe gebraucht werden. In einem weiteren Schritt wenden sich die Client-Computer einer Gruppe an die Agenten und fragen Updates ab.

Den Speicherort des Verzeichnisses, in dem die Updates und Installationspakete liegen, und dessen Größe können Sie nicht ändern.

Der Erstellen einer Liste mit mit Update-Agenten und deren Einstellung erfolgt im Eigenschaftfenster der Gruppe auf der Registerkarte **Update-Agenten** (s. Abb. 26).

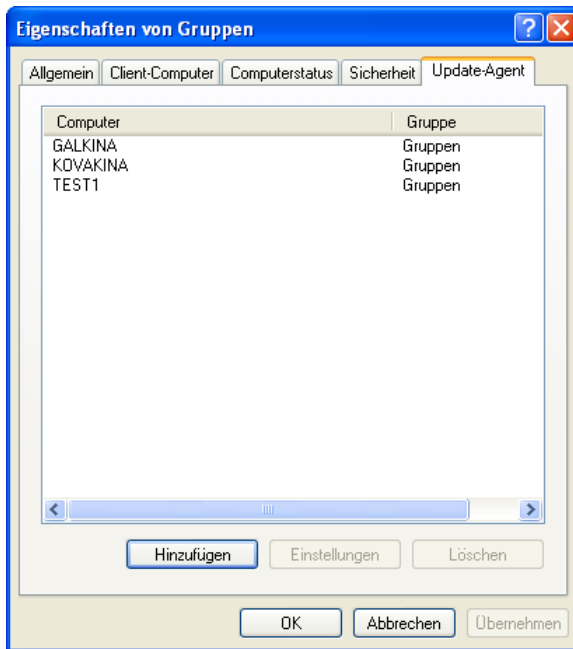


Abbildung 26. Erstellen einer Liste mit Update-Agenten

KAPITEL 6. BEDIENUNG

6.1. Lizenzverlängerung

Das Recht zur Nutzung der Software von Kaspersky Lab wird auf Basis des beim Kauf abgeschlossenen Lizenzvertrags gewährt.

Während der Gültigkeitsdauer der Lizenz erhalten Sie folgende Möglichkeiten:

- Verwendung der Antiviren-Funktionalität der Anwendung
- Aktualisierung der Antiviren-Datenbanken
- Versionsupdates für diese Anwendung
- Beratung in Fragen zu Installation, Konfiguration und Benutzung des betreffenden Softwareprodukts, per Telefon und mit Webformularen zur Anfrage an den Technischen Support-Service, die sich auf den Internetseiten von Kaspersky Lab befinden
- Möglichkeit zum Einsenden von gefundenen infizierten und verdächtigen Objekten zur Analyse an Kaspersky Lab.

Kaspersky Administration Kit braucht keinen Lizenzschlüssel für seine Arbeit!

Wenn Sie Support kontaktieren, benutzen Sie die Information über Lizenz für beliebige erworbene Anwendung von «Kaspersky Lab», welche mit Hilfe von Kaspersky Administration Kit verwaltet wird.

Die Anwendung Kaspersky Administration Kit erkennt das Vorhandensein einer Lizenz und ermittelt deren Gültigkeitsdauer nach dem Lizenzschlüssel, der einen obligatorischen Bestandteil jedes Kaspersky-Lab-Produkts darstellt. Eine Anwendung kann nur einen aktiven Lizenzschlüssel besitzen. Dieser enthält die Benutzungsbeschränkungen der Software, zu deren Kontrolle spezielle Mechanismen der Anwendung dienen.

Bei Ablauf der Gültigkeitsdauer der Lizenz werden die oben genannten Optionen eingeschränkt. Die Verlängerung der Lizenz erfolgt durch Erwerb und Installation eines neuen Lizenzschlüssels.

Die Anwendung Kaspersky Administration Kit verfügt über eine Option zur zentralen Kontrolle über den Status der auf den Client-Computern des logischen Netzwerks installierten Lizenzschlüssel und der Verlängerung von Lizenzen.

Bei der Installation eines Lizenzschlüssels werden mit Hilfe der Dienste von Kaspersky Administration Kit alle entsprechenden Daten auf dem Administrationsserver gespeichert. Auf diesen Daten basierend, werden die Protokolle über den Status der installierten Lizenzschlüssel erstellt und es erfolgt eine Benachrichtigung über den Ablauf der Gültigkeitsdauer und über die Überschreitung der im Schlüssel festgelegten Höchstzahl der Anwendungen, welche den Schlüssel verwenden dürfen. Die Parameter für die Benachrichtigung über den Status der Lizenzschlüssel werden in den Einstellungen des Administrationsservers bearbeitet.

Um ein Protokoll über den Status der Lizenzschlüssel zu erstellen, die auf Client-Computern im logischen Netzwerk aktiviert sind, können Sie auf die mitgelieferte Vorlage **Protokoll über Lizenzschlüssel** klicken oder eine neue Vorlage mit gleichem Namen erstellen.

Im Protokoll, das mit der Vorlage **Protokoll über Lizenzschlüssel**, erstellt wird, stehen alle Angaben über jeden auf den Client-Computern installierten Lizenzschlüssel, der aktiv ist oder in Reserve gehalten wird, mit Angabe der Rechner, auf denen sie benutzt werden und mit Angabe von Lizenz einschränkungen.

Eine vollständige Liste der auf den Client-Computern installierten Lizenzschlüssel befindet sich im Element **Lizenzen**. Für jeden Lizenzschlüssel sind folgende Informationen vorhanden:

- **Seriennummer** – Seriennummer des Lizenzschlüssels
- **Typ** – Typ des installierten Lizenzschlüssels, z.B. Kommerziell, Probe
- **Einschränkung** – Lizenz einschränkung für den Schlüssel
- **Gültigkeitsdauer** – Gültigkeitsdauer des Lizenzschlüssels

Informationen darüber, welche Lizenzschlüssel für eine Anwendung auf einem konkreten Client-Computer installiert sind, erhalten Sie im Eigenschaften-Fenster der Anwendung.

Zur Installation eines neuen Lizenzschlüssels muss der Task **Installation des Lizenzschlüssels** erstellt und gestartet werden.

Der Task zur Lizenzschlüssel-Installation kann als Gruppentask, globaler oder lokaler Task erstellt werden. Der globale Task Installation eines Lizenzschlüssels lässt sich mithilfe eines Assistenten anlegen.

Um einen bereits installierten Lizenzschlüssel zu ersetzen oder ihn zu aktivieren, können Sie den zuvor erstellten Task benutzen, indem Sie zunächst dessen Einstellungen ändern.

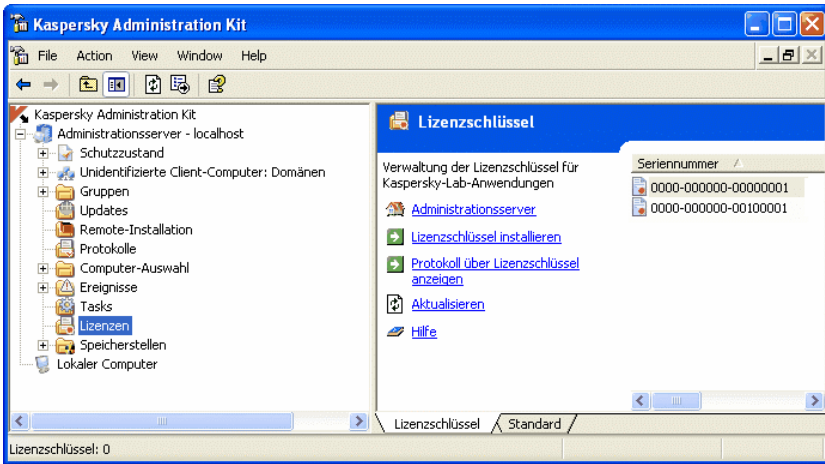


Abbildung 27. Lizenzschlüssel

6.2. Quarantäne und Backup

Das Arbeiten mit Quarantäne und Backup geht nur mit Kaspersky Anti-Virus for Windows Workstations und Kaspersky Anti-Virus for Windows Servers in den Versionen 5.0 und 6.0.

Die Antiviren-Anwendungen haben die Funktion, Objekte in speziellen Ablagen zu speichern. Für jeden Computer gibt es individuelle Quarantäne- und Backup-Verzeichnisse, die sich lokal auf jedem Computer befinden. In der Quarantäne liegen verdächtige Objekte und im Backup befinden sich Sicherungskopien von infizierten Objekten vor dem Reparieren oder Löschen.

In der Anwendung Kaspersky Administration Kit wird eine zentralisierte Liste mit Objekten geführt, die von Kaspersky-Lab-Anwendungen in Ablagen verschoben worden sind. Diese Daten werden von den Client-Computern durch die Administrationsagenten übertragen und in der Informationsdatenbank des Administrationsserver gespeichert. Außerdem können Sie über die Administrationskonsole die Eigenschaften der Objekte einsehen, die sich in den Ablagen auf lokalen Computern befinden, die Antiviren-Untersuchung der Ablagen starten und Objekte darin löschen.

Um die Funktion einer Remote-Verwaltung von Objekten in lokalen Ablagen ausüben zu können, müssen in der Richtlinie für den Administrationsagenten die Häkchen in den Kontrollkästchen Informationen über Objekte an Administrationsserver übertragen, die in Quarantäne liegen **und** Informationen

über Objekte an Administrationsserver übertragen, die im Backup liegen (**s. Abb. 28) gesetzt sein.**

Die Einstellung der Ablagenparameter erfolgt für jede Anwendung individuell in der Richtlinie oder in den Anwendungseinstellungen.

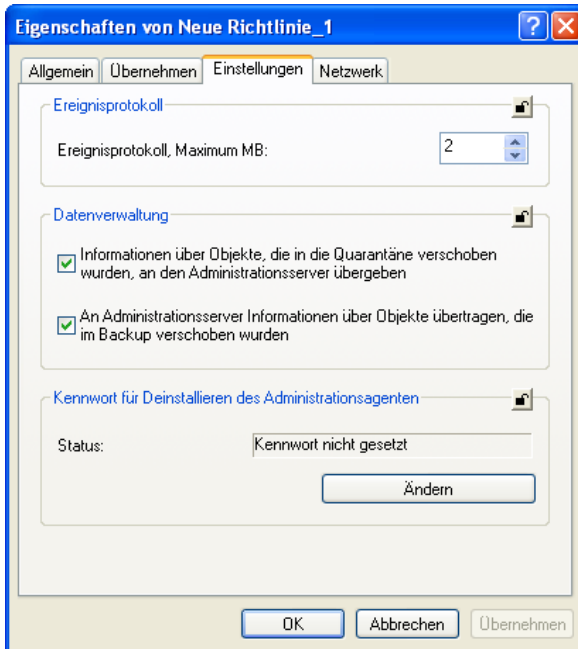


Abbildung 28. Einstellung von Remote-Ablagen

Die in den Ablagen auf den Client-Computern des logischen Netzwerkes verschobenen Objekte und die Arbeit mit den Objekten erfolgen im Ordner **Ablagen** (s. Abb. 29).

Kaspersky Administration Kit kopiert keine Objekte auf den Administrationsserver. Alle Objekte liegen in den lokalen Verzeichnissen der Client-Computer.

Die Wiederherstellung der Objekte geschieht auf dem Computer, wo die *Administrationskonsole* installiert ist, in einem Verzeichnis, das vom Administrator festgelegt wurde.

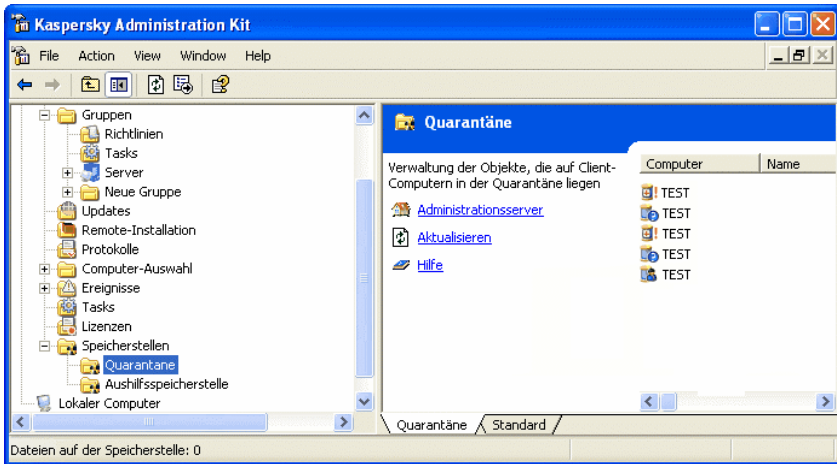


Abbildung 29. Anzeige des Inhalts in Ablage

6.3. Ereignisprotokolle. Ereignisfilter

Die Anwendung Kaspersky Administration Kit bietet ausgezeichnete Möglichkeiten zur Überwachung der Arbeit des Antiviren-Schutzsystems.

Es ist vorgesehen, Ereignisprotokolle für die Arbeit des Administrationsservers und aller Anwendungen zu führen, die von Kaspersky Administration Kit verwaltet werden. Die Daten können im Systembericht von Microsoft Windows oder im Ereignisprotokoll von Kaspersky Administration Kit gespeichert werden.

In den Protokollen werden Ereignisse gespeichert, die bei der Programmarbeit registriert werden, sowie die Ergebnisse der Taskausführung.

Sie können eine Liste der bei der Arbeit jeder Anwendung zu registrierenden Ereignisse anlegen, sowie das Vorgehen zur Benachrichtigung des Administrators und anderer Benutzer für jede Administrationsgruppe festlegen. Diese Parameter werden durch die Gruppenrichtlinie der Anwendung festgelegt. Die Konfiguration erfolgt im Eigenschaften-Fenster der Gruppenrichtlinie auf der Registerkarte Ereignisse (s. Abb. 30).

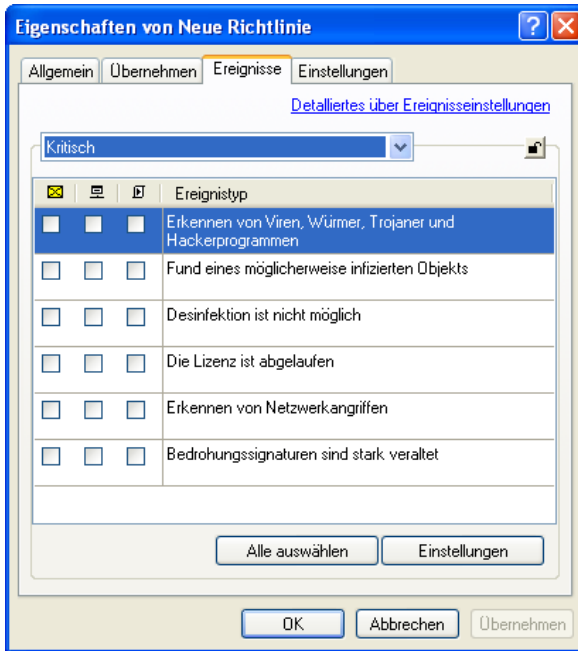


Abbildung 30. Bearbeiten der Richtlinie. Registerkarte **Ereignisse**

Die Vorgaben für die Speicherung der Ergebnisse bei der Taskausführung, die Form sowie die Art und Weise der Benachrichtigungen werden in den Taskeinstellungen bestimmt.

Die Benachrichtigung über den Eintritt eines Ereignisses kann durch das Senden einer Nachricht per E-Mail oder über das Netzwerk, sowie mit Hilfe eines bestimmten Programms oder Skripts erfolgen.

Informationen über registrierte Ereignisse und die Ergebnisse der Taskausführung können zentralisiert auf dem Administrationsserver oder für jeden Client-Computer lokal gespeichert werden.

Der Zugriff auf die Informationen, die im Systembericht von Microsoft Windows gespeichert sind, erfolgt mithilfe der standardmäßigen MMC-Erweiterung **Ereignisanzeige**. Die Informationen des Ereignisprotokolls von Kaspersky Administration Kit, die auf dem Administrationsserver gespeichert sind, werden in der Konsolenstruktur über das Element **Ereignisse angezeigt** (s. Abb. 31).

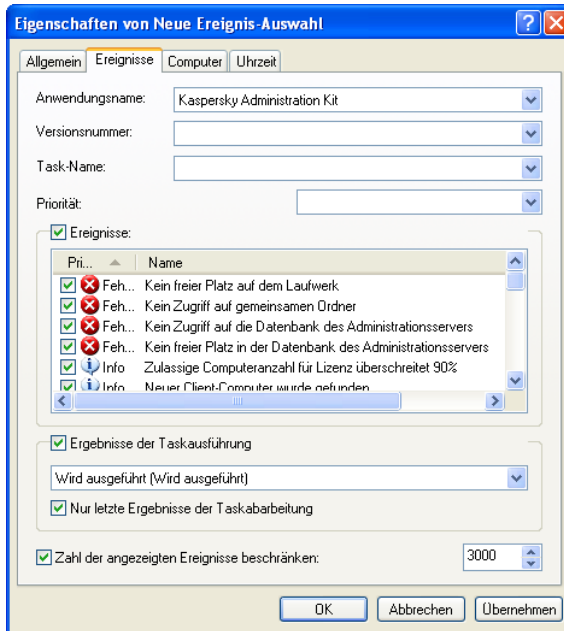


Abbildung 32. Einstellung des Ereignisfilters

Registrierte Ereignisse werden automatisch nach Ablauf der in der Richtlinie festgelegten Speicherdauer oder manuell mit Hilfe des Kontextmenübefehls **Löschen** gelöscht. Sie können einzelne Ereignisse, die im Detailfenster ausgewählt wurden, alle Ereignisse oder Ereignisse, die bestimmte Bedingungen erfüllen, löschen.

Die Liste der Ereignisse, die bei der Arbeit einer Anwendung registriert wurden, können Sie für jeden Client-Computer in dessen Eigenschaften-Fenster anzeigen. Es werden Informationen des Ereignisprotokolls von Kaspersky Administration Kit angezeigt, die auf dem Administrationsserver gespeichert sind. Klicken Sie zum Suchen nach Informationen auf Ereignisfilter.

Die Anzeige des Ereignisprotokolls von Kaspersky Administration Kit, die lokal auf dem Client-Computer gespeichert sind, erfolgt über die lokal auf diesem Computer installierte Administrationskonsole.

6.4. Protokolle

Sie können anhand von Daten, die im Ereignisprotokoll von Kaspersky Administration Kit auf dem Administrationsserver gespeichert sind, Protokolle über den Zustand des Antiviren-Schutzsystems empfangen.

Der Zustand des Antivirenschutzes lässt sich auch auf dem Client-Computer verfolgen, mit Hilfe von der Information, welche durch den Administrationsagenten in das System Registry geschrieben wird.

Protokolle lassen sich erstellen für:

- Systeme der Antivirensicherheit im Ganzen
- Computer, die zu einer bestimmten Administrationsgruppe gehören
- Client-Computer aus verschiedenen Administrationsgruppen
- Systeme der Antivirensicherheit logischer Netzwerke mit untergeordneten Administrationsservern

Es sind die folgenden Protokolltypen vorgesehen:

- **Protokoll über Versionen der Antiviren-Datenbanken** – Protokoll über Versionen der Antiviren-Datenbanken, die die Programme verwenden
- **Fehler-Protokoll** – Protokoll über Fehler (Funktionsstörungen), die in der Funktion der Programme vorhanden sind, die auf den Client-Computern installiert sind
- **Protokoll über Lizenzschlüssel** – Protokoll über den Status der Lizenzschlüssel, die von den Anwendungen benutzt werden und über die Einhaltung der aktivierten Lizenzbeschränkungen
- **Protokoll über Infektionshäufigkeit der Clients** – Protokoll über die am häufigsten infizierten Client-Computer, bei deren Untersuchung am meisten verdächtige und infizierte Objekte auffinden lassen
- **Protokoll über Antiviren-Schutzniveau** – Protokoll mit Angaben zu den Client-Computern, die kein ausreichendes Schutzniveau haben
- **Protokoll über Programmversionen** – Protokoll über die Versionen von Kaspersky-Lab-Anwendungen, die auf den Client-Computern installiert sind

- **Protokoll über Virenaktivität** – Protokoll über die Ergebnisse der Antiviren-Untersuchung auf den Client-Computern des logischen Netzwerks
- **Protokoll über Drittanwendungen** – Protokoll von Anwendungen von Dritten oder Kaspersky-Lab-Anwendungen, die auf Client-Computern installiert sind, deren Verwaltung Kaspersky Administration Kit nicht übernehmen kann
- **Protokoll über Netzwerkangriffe** – Protokoll über Netzwerkangriffe, die auf Client-Computern registriert worden sind
- **Protokoll über Anwendungstypen** enthält Informationen über die im logischen Netzwerk installierte Antivirenanwendungen, wie auch Informationen über infizierte Objekte, welche von diesen Anwendungen gefunden worden sind und an den Objekten vorgenommene Handlungen.
- **Protokoll über Anwendungen für Arbeitsstationen und Fileserver** enthält detaillierte Informationen über installierte Anwendungen zum Schutz von Arbeitsstationen und Fileserver, wie auch Informationen über infizierte Objekte, welche von diesen Anwendungen gefunden worden sind und an den Objekten vorgenommene Handlungen.
- **Protokoll über Anwendungen für Perimeterschutz** enthält detaillierte Informationen über Antivirenanwendungen für Perimeterschutz, wie auch Informationen über infizierte Objekte, welche von diesen Anwendungen gefunden worden sind und an den Objekten vorgenommene Handlungen.
- **Protokoll über Anwendungen zum Schutz der Mailsysteme** enthält detaillierte Informationen über installierte Antivirenanwendungen zum Schutz von Mailsystemen, wie auch Informationen über infizierte Objekte, welche von diesen Anwendungen gefunden worden sind und an den Objekten vorgenommene Handlungen.

Sie können Protokolle erstellen nach einem Muster. Eine Großzahl der Protokollvorlagen befindet sich im Container **Protokolle** der Konsolenstruktur (s. Abb. 33). Sie können auch einige zusätzliche Protokollvorlagen im Protokollvorlagen-Wisard auswählen.

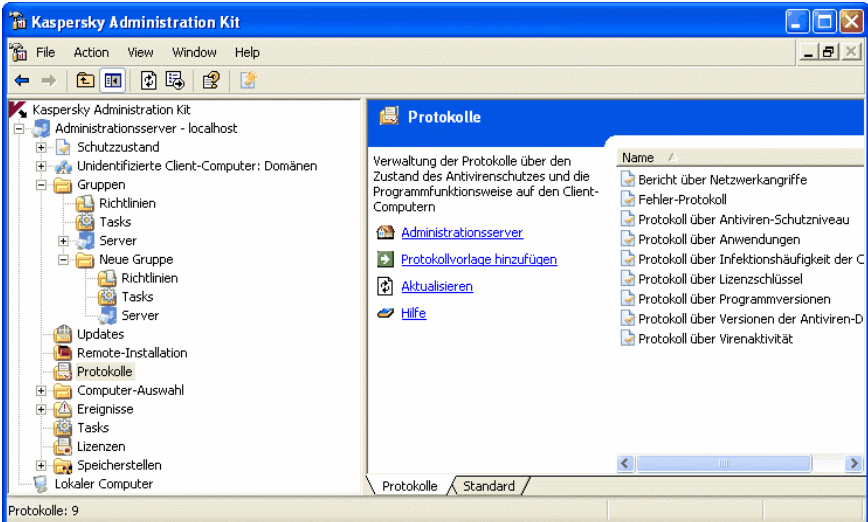


Abbildung 33. Anzeige der Ergebnisse der Taskausführung, die auf dem Administrationsserver gespeichert sind

Es sind 13 Standardvorlagen vorhanden, die den Typen der Protokolle über den Zustand des Antiviren-Schutzsystems entsprechen.

Sie können neue Vorlagen erstellen, löschen, anzeigen lassen und ihre Einstellungen bearbeiten.

Um Protokolle anzeigen zu lassen, wird der Browser herangezogen, der als Standard installiert ist.

Bei einer hierarchischen Struktur der Administrationsserver lassen sich allgemeine Protokolle erstellen, die Angaben über untergeordnete Administrationsserver enthalten.

Wenn einige Administrationsserver nicht verfügbar sind, dann erscheint eine Information darüber im Protokoll.

6.5. Computersuche

Um Informationen über einen konkreten Computer oder eine konkrete Computergruppe zu bekommen, klicken Sie auf die Funktion Computersuche anhand einzugebender Kriterien. Beim Suchen können Daten von

untergeordneten Administrationsservern einbezogen werden. Die Suchergebnisse können in einer Textdatei gespeichert werden.

Die Suchfunktion findet Folgendes:

- Client-Computer in logischen Netzwerken, Administrationsserver und dessen untergeordnete Server
- Computer, die nicht zu einem logischen Netzwerk gehören, jedoch Computernetzwerken angehören, wo der Administrationsserver und dessen untergeordnete Server installiert sind
- Alle Computer in Netzwerken, in denen der Administrationsserver und dessen untergeordneten Server installiert sind, unabhängig davon, ob der Computer zum logischen Netzwerk gehört oder nicht

Klicken Sie zur Computersuche auf den Eintrag **Computer finden** im Kontextmenü für den in der Konsolenstruktur des Elementes gewählten Administrationsserver, den gewählten Ordner **Netzwerk** oder die gewählte Administrationsgruppe (s. Abb. 34).

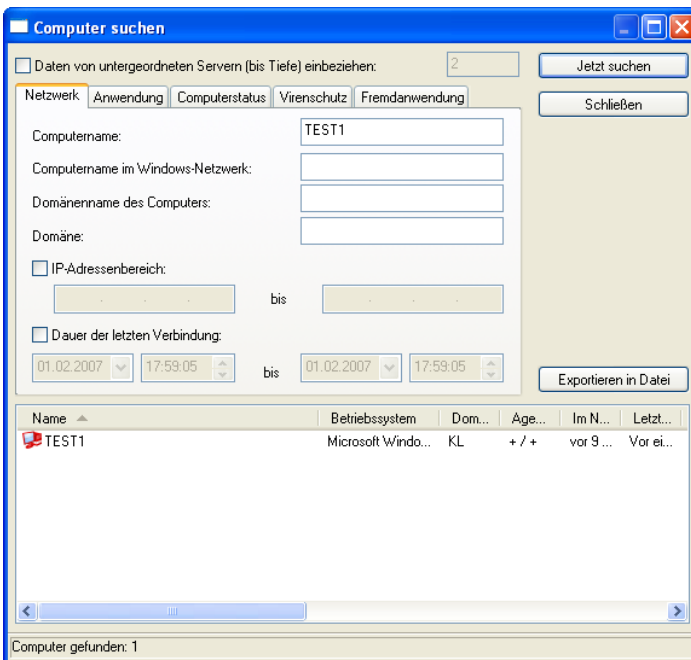


Abbildung 34. Computersuche

Je nach dem, für welches Element die Suche gelten soll, kommen folgende Ergebnisse zu Stande:

- Gruppe **Gruppe** – Suche nach Client-Computern, die mit dem logischen Netzwerk dieses Administrationsserver verbunden sind, zu dem eine ausgewählte Gruppe gehört

Die Suche erfolgt anhand von Informationen über die Struktur des logischen Netzwerks und der Netzwerke untergeordneter Administrationsserver (wenn in den Suchparametern das Häkchen **Daten von untergeordneten Servern einbeziehen** gesetzt ist).

- Gruppe **Netzwerk** – Suche nach Computern im Netzwerk, in dem der Administrationsserver installiert ist, der nicht zum logischen Netzwerk gehört.

Die Suche erfolgt anhand von Daten, die bei der Abfrage des Computernetzwerks durch den Administrationsserver und die untergeordneten Server gewonnen wurden (wenn in den Suchparametern das Häkchen **Daten von untergeordneten Servern einbeziehen** gesetzt ist).

Die Suchergebnisse sind Client-Computer, die zur für die Suche gewählten Gruppe **Netzwerk** gehören und zur Gruppe **Netzwerk** aller untergeordneten Server (wenn in den Suchparametern das Häkchen **Daten von untergeordneten Servern einbeziehen** gesetzt ist).

- Administrationsserver <Servername> – komplette Computersuche

Die Suche erfolgt anhand von Informationen über die Struktur des logischen Netzwerks und von Daten, die bei der Abfrage des Computernetzwerks durch den ausgewählten Administrationsserver und die untergeordneten Administrationsserver (wenn in den Suchparametern das Häkchen **Daten von untergeordneten Servern einbeziehen** gesetzt ist).

Die Suchergebnisse sind:

- Client-Computer, die zum logischen Netzwerk des gewählten Administrationsservers und aller ihm untergeordneter Server (wenn in den Suchparametern das Häkchen **Daten von untergeordneten Servern einbeziehen** gesetzt ist).
- Computer, die zur Gruppe **Netzwerk** des gewählten Administrationsservers gehören und zur Gruppe **Netzwerk** aller ihm untergeordneter Server (wenn in den Suchparametern das Häkchen **Daten von untergeordneten Servern einbeziehen** gesetzt ist).

Klicken Sie zum Suchen, Speichern und Anzeigen der Computerinformationen in den separaten Ordner der Konsolenstruktur auf die Funktion Filter erstellen.

6.6. Benutzerdefinierter Computer-Filter

Um den Zustand von Client-Computern im logischen Netzwerk mit den Status **Kritisch** und **Warnung** und Computer flexibler kontrollieren zu können, die im Netzwerk in den letzten Tagen erkannt wurden, steht in einem separaten Element der Konsolenstruktur der **Benutzerdefinierte Computer-Filter** (s. Abb. 35).

Die Diagnose zum Zustand der Client-Computer erfolgt anhand von Informationen über den Status der Antiviren-Sicherheit auf einem Computer und anhand von Daten über dessen Netzaktivität. Die Einstellung der Diagnoseparameter geschieht für jede Administrationsgruppe separat auf der Registerkarte **Computerstatus** (s. Abb. 36).

Informationen über neue Computer gehen nach Abfrage des Computernetzwerks durch den Administrationsserver in die Ergebnisse ein.

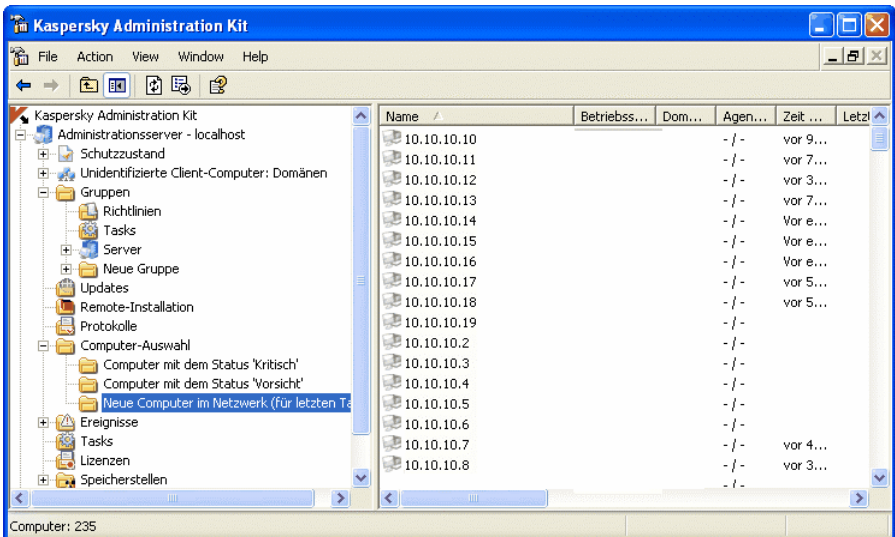


Abbildung 35. Benutzerdefinierte Computer-Filter

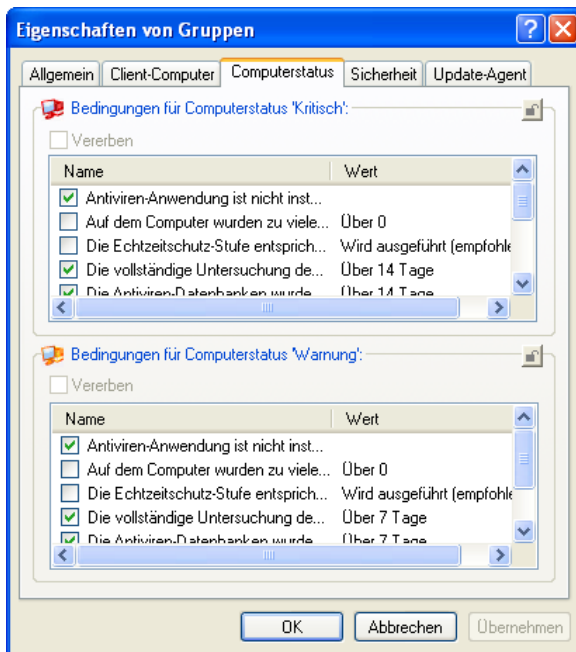


Abbildung 36. Einstellen der Diagnose für Client-Computer

Vorgesehen ist die Option, zusätzliche benutzerdefinierte Filter zu erstellen. Klicken Sie dazu auf den Eintrag **Neu / Neuer Filter** im Kontextmenü für das Element **Benutzerdefinierte Computer-Filter**. Daraufhin wird in der Konsolenstruktur im Element **Benutzerdefinierte Computer** der neue Ordner mit dem eingegebenen Namen. Damit zum benutzerdefinierten Filter weitere Computer hinzugefügt werden können, stellen Sie die Parameter des Filters ein (s. Abb. 37). Der Filter kann zur Suche und zum weiteren Verschieben von erkannten Computern in Administrationsgruppen herangezogen werden. Das Verschieben geschieht mit der Maus.

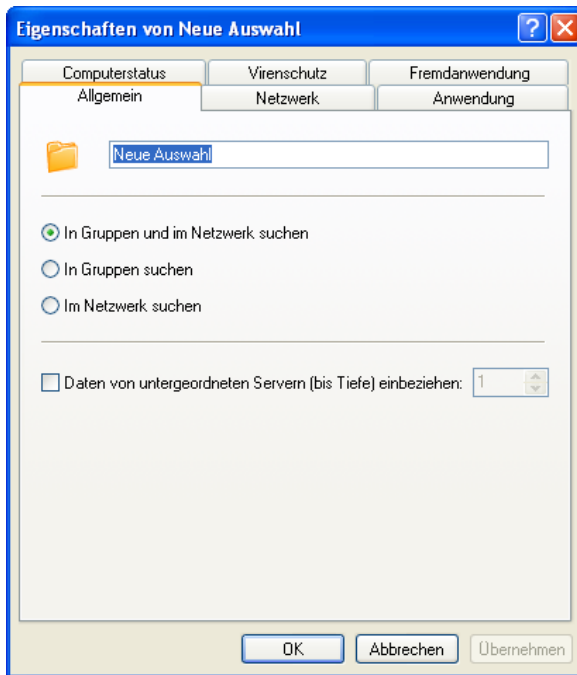


Abbildung 37. Einstellen von benutzerdefinierten Computer-Filtern

6.7. Überwachung von Virenepidemien

Kaspersky Administration Kit bietet die Option, die Virenaktivität auf Client-Computer im logischen Netzwerk mit dem Ereignis **Virenangriff** zu kontrollieren, der in der Komponente Administrationsserver registriert wird.

Diese Funktion hat einen sehr großen Wert in Zeiten von Virenepidemien und gewährleistet ein rechtzeitiges Reagieren auf drohende Attacken von Viren.

Die Kriterien, anhand derer ein Ereignis **Virenangriff** festgehalten wird, werden in den Einstellungen des Administrationsservers auf der Registerkarte **Virenangriff** (s. Abb. 38) eingestellt.

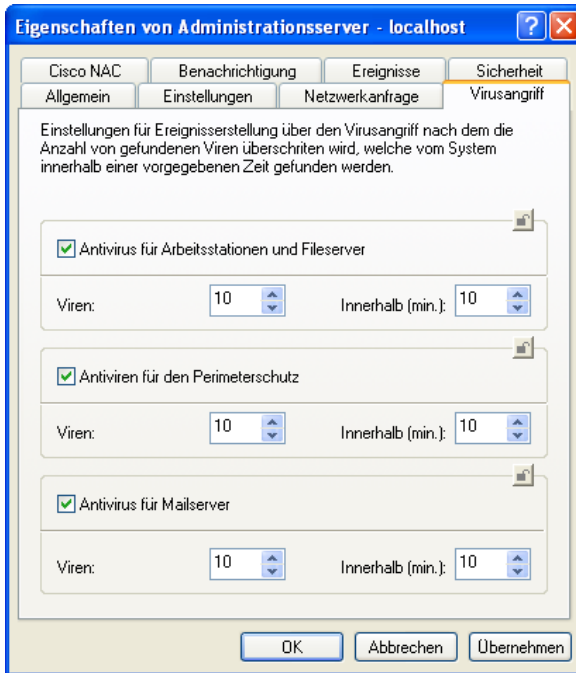


Abbildung 38. Einstellen der Kriterien für Erkennen eines Virenangriffs

Ereignis kann für mehrere Anwendungstypen registriert werden. Um das Erkennen eines Virenangriffs einzuschalten, aktivieren Sie Kontrollkästchen neben den gewünschten Anwendungstypen:

- Antiviren für Arbeitsstationen und Fileserver;
- Perimeterschutz-**Aktivieren**;
- Mailsysteme-**Antiviren**.

Geben Sie für jede Anwendung die Grenze der Virenaktivität an. Wenn diese Grenze überschritten ist, wird der Ereignis **Virenangriff** ausgelöst:

- In dem Feld **Viren** – Anzahl der Viren, welche in dem logischen Netzwerk von den Anwendungen dieses Typs gefunden worden;
- In dem Feld **Innerhalb von (Min.)** – Zeitraum, innerhalb dessen die oben genannte Anzahl der **Viren** gefunden wurde

Das Ereignis Virenangriff wird anhand von Ereignissen mit der Bezeichnung **Virus gefunden** und **Auffinden von Viren, Würmer und Hackerprogramme** in

den Antiviren-Anwendungen bestimmt. Aus diesem Grund müssen für ein erfolgreiches Erkennen einer Virenepidemie alle Daten über Ereignisse vom Typ **Virus gefunden** auf dem Administrationsserver gespeichert werden. Dazu müssen die entsprechenden Parameter in den Richtlinien für jede Antiviren-Anwendung aktiviert sein (auf der Registerkarte **Registrierung** (s. Abb. 39) in dem Eigenschaften-Fenster der Ereignisse **Virus gefunden** und **Auffinden von Viren, Würmer und Hackerprogramme** muss das Häkchen **Auf dem Administrationsserver speichern für (Tage) aktiviert werden**).

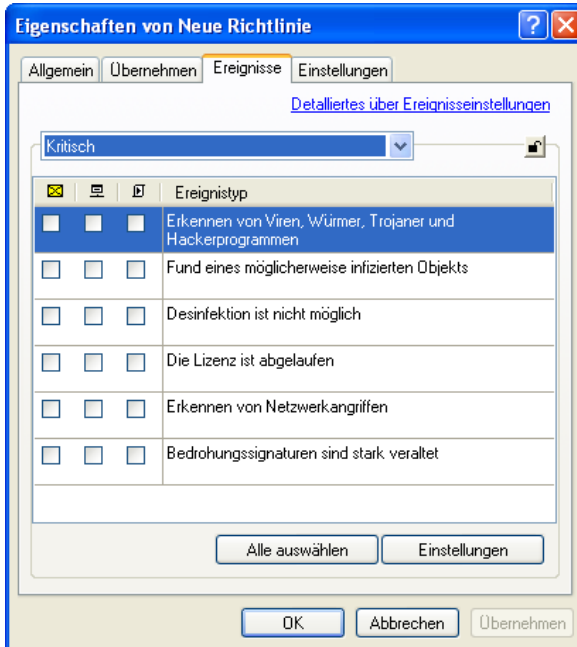


Abbildung 39. Einstellen der Ereignisregistrierung

Die Reihenfolge der Benachrichtigung über das Ereignis **Virenangriff** wird in den Einstellungen des Administrationsservers auf der Registerkarte **Benachrichtigung** (s. Abb. 40) definiert.

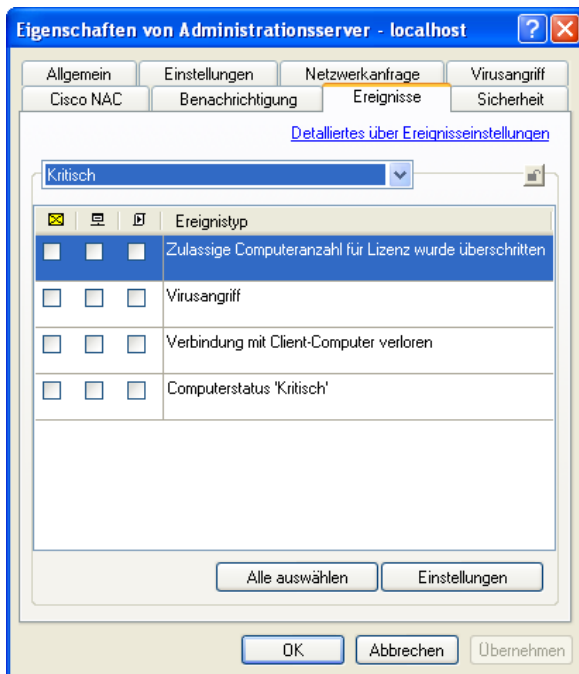


Abbildung 40. Einstellen der Parameter für die Ereignisbenachrichtigung

Als Reaktion auf eine Virenepidemie kann auch der automatische Wechsel der aktuellen Anwendungsrichtlinie vorgegeben werden. Dazu muss in den Richtlinienparametern das Häkchen im Kontrollkästchen **Richtlinie nach Ereigniseintritt aktivieren** stehen und das Ereignis **Virenangriff** (s. Abb. 11) ausgewählt sein.

Beim Berechnen der Ereignisse **Virus gefunden** und **Auffinden von Viren, Würmer und Hackerprogramme** werden nur die Daten von Client-Computern des Hauptadministrationsservers berücksichtigt.

Es wird für jeden untergeordneten Server das Ereignis **Virenangriff** separat eingestellt.

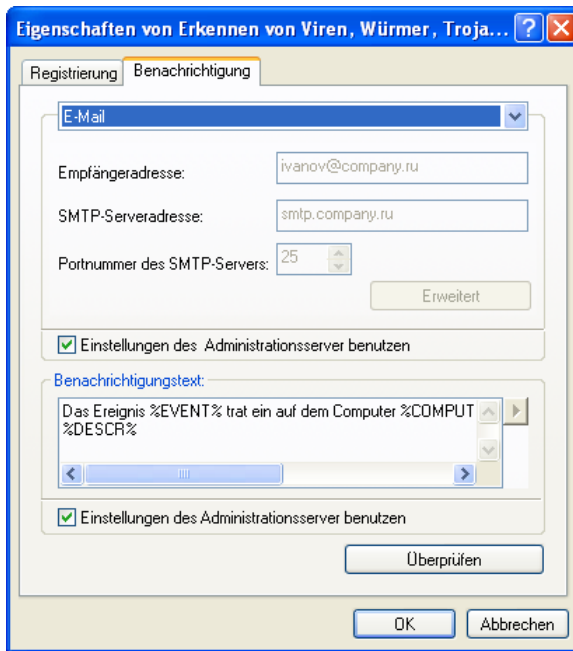


Abbildung 41. Parametereinstellungen für Ereignisbenachrichtigung

6.8. Sicherheitskopieren und Wiederherstellung von Daten des Administrationsservers

Das Sicherheitskopieren erlaubt dem Administrationsserver, von einem Computer auf den anderen Computer ohne jegliche Verluste Daten zu übertragen und Daten beim Umzug der Informationsdatenbank des Administrationsservers zu einem anderen Computer oder beim Umstieg auf eine aktuelle Version des Kaspersky Administration Kit wiederherzustellen.

Wenn der Administrationsservers auf dem Computer mit Kaspersky Administration Kit deinstalliert werden soll, wird immer nach der Sicherungskopie der Daten gefragt.

Beim Sicherheitskopieren fallen unter die Speicherung und Wiederherstellung:

- Datenbank des Administrationssservers (Richtlinien, Tasks, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse).
- Konfigurationsinformationen über die Struktur des logischen Netzwerks und der Client-Computer
- Speicherort der Programmdistributionen für die Remote-Installation (Inhalt der Ordner Packages, Uninstall, Updates)
- Zertifikat des Administrationssservers

Die Wiederherstellung der Daten bei einem Umstieg auf eine aktuelle Version der Anwendung wird unterstützt, beginnend mit dem Kaspersky Administration Kit, Version 5.0, Maintenance Pack 3.

Wenn sich beim Wiederherstellen der Daten vom Administrationsserver der Pfad zum allgemein freigegebenen Ordner geändert hat, muss die Richtigkeit der Tasks kontrolliert werden, wo dieser Pfad verwendet wird (Tasks für Update, Remote-Installation) und gegebenenfalls die Einstellungen geändert werden.

Das Kopieren von Daten des Administrationssservers zum Backup und zur nachfolgenden Wiederherstellung kann mit dem Task **Sicherheitskopieren von Daten** automatisiert werden oder manuell mithilfe der Utility **klbackup** erledigt werden, die zum Lieferumfang von Kaspersky Administration Kit gehört. Die Wiederherstellung von Daten kann nur mithilfe der Utility **klbackup** erfolgen.

Nach Installation des Administrationssservers wird die Utility **klbackup** im Installationsverzeichnis der Komponente gespeichert und führt beim Starten aus der Befehlszeile je nach den verwendeten Schlüsseln das Kopieren oder Wiederherstellen der Daten aus.

Der Task Sicherheitskopieren wird per Hand nach Ausführung des Schnellstart-Assistenten erstellt und liegt im Knoten **Globale Tasks**. Um das Sicherheitskopieren der Daten aufzurufen, müssen die Parameter dieses Tasks eingrichtet werden. Sie können auch manuell den Task Sicherheitskopieren der Daten erstellen: Als Anwendungen, für die der Task erstellt wird, geben Sie **Kaspersky Administration Kit** an. Als Tasktyp legen Sie **Erstellen einer Sicherheitskopie vom Administrationsserver** fest.

ANHANG A. GLOSSAR

Im Text des Handbuches kommen Fachausdrücke vor, die im Kontext des Antiviren-Schutzes eine spezielle Bedeutung tragen. Hier werden die Bedeutungen dieser Begriffe erläutert. Alle Einträge des Glossars sind alphabetisch geordnet, um das Auffinden zu erleichtern.

A

Administrationsagent – Komponente der Anwendung Kaspersky Administration Kit, welche der Kommunikation zwischen dem Administrationsserver und den Kaspersky-Lab-Anwendungen dient, die auf einem konkreten Netzwerkobjekt (Workstation oder Server) installiert sind. Diese Komponente ist für alle Windows-Anwendungen des Herstellers, die zu den Produkten Kaspersky Anti-Virus Business Optimal und Kaspersky Corporate Suite gehören, einheitlich. Für Novell und Unix-Anwendungen von Kaspersky-Lab wurden eigene Versionen des Administrationsagenten entwickelt.

Administrationsgruppe – Eine Auswahl von Computern, die nach den auszuführenden Funktionen und den darauf installierten Kaspersky-Lab-Anwendungen zusammengefasst werden. Die Gruppierung erlaubt die einheitliche Verwaltung aller Computer. Eine Gruppe kann andere Gruppen beinhalten. In einer Gruppe können Gruppenrichtlinien für jede in der Gruppe installierte Anwendung angelegt und Gruppentasks erstellt werden.

Administrationskonsole – Komponente der Anwendung Kaspersky Administration Kit, welche eine Benutzeroberfläche für die Administrationsdienste des Administrationsservers und Administrationsagenten enthält.

Administrationsserver – Komponente der Anwendung Kaspersky Administration Kit, welche Funktionen zum zentralisierten Speichern von Daten über die im Firmennetzwerk installierten Kaspersky-Lab-Anwendungen bietet und deren Verwaltung dient.

Administrator des logischen Netzwerks – Ein Benutzer, der die Installation, Konfiguration und Wartung von Kaspersky Administration Kit vornimmt und die Kaspersky-Lab-Anwendungen auf den Computern des logischen Netzwerks entfernt verwaltet.

Administratorarbeitsplatz – Computer, auf dem die Komponente Administrationskonsole von Kaspersky Administration Kit installiert ist. Über diese Komponente erfolgen Aufbau und Verwaltung des zentralisierten, auf Kaspersky-Lab-Anwendungen basierenden Antiviren-Schutzsystems eines Firmennetzwerks.

Aktiver Lizenzschlüssel – Lizenzschlüssel, der für einen bestimmten Zeitraum für die Arbeit einer Kaspersky-Lab-Anwendung installiert und verwendet wird. Er bestimmt die Gültigkeitsdauer der Lizenz und die für das Produkt gültige Lizenzpolitik.

Antiviren-Datenbanken – Datenbanken, die von Kaspersky-Lab-Spezialisten erstellt werden und eine detaillierte Beschreibung aller im Moment existierenden Viren und dafür notwendigen Erkennungs- und Desinfektionsmethoden enthalten. Die Antiviren-Datenbanken befinden sich auf Kaspersky-Lab-Webseiten und werden beim Auftauchen neuer Viren regelmäßig aktualisiert. Registrierte Benutzer von Kaspersky Lab besitzen Zugriff auf die Updates. Um die Effektivität der Virenerkennung zu steigern, wird empfohlen, die Updates der Antiviren-Datenbanken regelmäßig zu kopieren.

Anwendungseinstellungen – Auswahl von Parametern einer Anwendung, die für alle Tasktypen der Anwendung gültig sind.

B

Backup – Kopieren von Daten des Administrationsservers als Sicherheitskopien und zur späteren Wiederherstellung, wozu die Backup-Utility dient. Die Utility erlaubt die Wiederherstellung:

- der Datenbank des Administrationsservers (Richtlinien, Tasks, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse).
- der Konfigurationsdaten über die Struktur des logischen Netzwerks und Client-Computer.
- des Speichers der Programmdistributionen für die Remote-Installation (Inhalt der Ordner Packages, Uninstall, Updates).
- des Zertifikats des Administrationsservers.

Backup-Speicher – spezielles Verzeichnis zum Speichern von Sicherheitskopien der Daten des Administrationsservers. Die Kopien werden mit Hilfe einer Backup-Utility angefertigt.

C

Client des Administrationsservers (oder **Client-Computer**) – Computer, Server oder Workstation, auf dem/der der Administrationsagent und die zu verwaltenden Kaspersky-Lab-Anwendungen installiert sind.

D

Direkte Anwendungsverwaltung – Verwaltung einer Anwendung über ein lokales Interface.

Drittanwendung – Antiviren-Anwendung von einem Drittanbieter oder Kaspersky-Lab-Anwendung, deren Verwaltung nicht von Kaspersky Administration Kit unterstützt wird.

G

Globaler Task – Task, der für eine Auswahl von Client-Computern auf beliebigen Administrationsgruppen des logischen Netzwerks festgelegt wurde und darauf ausgeführt werden soll.

Grenzwert für Virenaktivität – Anzahl der innerhalb eines bestimmten Zeitraums gefundenen Viren. Die Überschreitung dieses Werts gilt als erhöhte Virenaktivität und als das Ereignis **Virenaktivität** (Virusangriff). Diese Eigenschaft besitzt große Bedeutung während Virusepidemien und erlaubt dem Administrator die rechtzeitige Reaktion auf drohende Virusangriffe.

Gruppenrichtlinie – Auswahl von Einstellungen einer Anwendung in einer durch Kaspersky Administration Kit verwalteten Administrationsgruppe. Die Einstellungen einer Anwendung können für verschiedene Gruppen unterschiedlich sein. Für jede Anwendung wird eine eigene Richtlinie definiert. Die Richtlinie umfasst Parameter zur vollständigen Konfiguration der gesamten Anwendungsfunktionalität.

Gruppentask – Task, der für eine Gruppe festgelegt wurde und auf allen Client-Computern dieser Administrationsgruppe ausgeführt werden soll.

Gültigkeitsdauer der Lizenz – Der Zeitraum, während dem Sie die Möglichkeit besitzen, die volle Funktionalität von Kaspersky Anti-Virus[®] zu nutzen. Die Gültigkeitsdauer der Lizenz wird durch den Lizenzschlüssel festgelegt und beträgt in der Regel ein Kalenderjahr ab der Installation des Schlüssels. Nach dem Ablauf der Lizenzgültigkeit wird die Funktionalität des Produkts eingeschränkt.

I

Installation mit Startskript – Methode zur entfernten Installation von Kaspersky-Lab-Anwendungen, die es erlaubt, den Start eines Remote-Installationstasks an das konkrete Konto eines Benutzers (mehrerer Benutzer) zu binden. Bei der Anmeldung des Benutzers an der Domäne wird versucht, die Anwendungsinstallation auf dem Client-Computer durchzuführen, von dem aus sich der Benutzer anmeldet. Diese Methode wird empfohlen für die Installation von Anwendungen des

Herstellers auf Computern, die unter den Betriebssystemen MS Windows 98/Me arbeiten.

Installationspaket – Auswahl von Dateien, welche zum Durchführen der Remote-Installation von Kaspersky-Lab-Anwendungen auf Client-Computern des logischen Netzwerks erstellt wurde. Ein Installationspaket wird auf Basis einer speziellen Datei mit der Dateinamenserweiterung **.kpd** erstellt, die zum Umfang der Anwendungsdistribution gehört, und enthält eine minimale Auswahl von Parametern, welche die Funktionsfähigkeit der Anwendung sofort nach der Installation gewährleisten. Die Einstellungswerte entsprechen der Standardkonfiguration der Anwendung.

K

Kaspersky Administration Kit – Anwendung, die zum Umfang der Produkte Kaspersky Business Optimal und Kaspersky Corporate Suite zählt und zur zentralisierten Lösung der wichtigsten Administrationsaufgaben zur Verwaltung des Antivirensicherheitssystems eines Firmencomputernetzwerks dient, welches auf Kaspersky-Lab-Anwendungen basiert.

L

Lizenzschlüssel – Eine Datei mit der Dateinamenserweiterung *.key, die Ihren persönlichen "Schlüssel" darstellt und für die Arbeit mit Kaspersky-Lab-Anwendungen erforderlich ist. Der Lizenzschlüssel ist im Lieferumfang des Produkts enthalten, wenn Sie es bei einem Händler von Kaspersky Lab erwerben, oder er wird Ihnen per E-Mail zugesandt, wenn das Produkt im Online-Shop erworben wird.

Lokaler Task – Task, der für einen einzelnen Client-Computer festgelegt wurde und darauf ausgeführt werden soll.

O

Operator des logischen Netzwerks – Benutzer, der die Kontrolle über den Zustand und die Arbeit des Antiviren-Schutzsystems vornimmt, das mit Hilfe von Kaspersky Administration Kit verwaltet wird.

P

Plug-In zur Anwendungsverwaltung – Eine spezielle Komponente, welche das Interface für die Remote-Verwaltung von Anwendungen mit Hilfe der Administrationskonsole bietet. Das Verwaltungs-Plug-In ist für jede Anwendung individuell und gehört zum Umfang aller Kaspersky-Lab-

Anwendungen, deren Verwaltung mit Hilfe von Kaspersky Administration Kit möglich ist.

Prioritätsstufe eines Ereignisses – Eigenschaft eines Ereignisses, das bei der Arbeit einer Kaspersky-Lab-Anwendung festgehalten wird. Es gibt vier Prioritätsstufen:

- Kritisches Ereignis
- Fehler
- Warnung
- Info

Ereignisse des gleichen Typs können verschiedene Prioritätsstufen besitzen, was von der Situation abhängig ist, in der das Ereignis eingetreten ist.

Push-Installation – Methode zur entfernten Installation von Kaspersky-Lab-Anwendungen auf konkreten Client-Computern des logischen Netzwerks. Zur erfolgreichen Taskausführung mit der Push-Installationsmethode muss der Administrationsserver über die Rechte für den Remote-Start von Anwendungen auf den Client-Computern des logischen Netzwerks verfügen. Empfehlenswert ist diese Methode zur Anwendungsinstallation auf Computern, die unter den Betriebssystemen MS Windows NT/2000/2003/XP arbeiten, in denen diese Option unterstützt wird, oder auf Computern unter MS Windows 98/Me, auf denen der Administrationsagent installiert ist.

R

Remote-Installation – Installation von Kaspersky-Lab-Anwendungen mit Hilfe von Diensten, die von der Anwendung Kaspersky Administration Kit angeboten werden.

Reserve-Lizenzschlüssel – Lizenzschlüssel, der für die Arbeit einer Anwendung von Kaspersky Lab installiert, aber nicht aktiviert wurde. Abhängig von den Einstellungen kann die Aktivierung automatisch nach dem Ablauf der Gültigkeit des aktiven Schlüssels oder manuell erfolgen.

Richtlinie – s. **Gruppenrichtlinie**.

S

Status des Antiviren-Schutzes – Der aktuelle Zustand des Antiviren-Schutzes, der das Sicherheitsniveau des Computers charakterisiert.

T

Task – Benannte Aktion, die von einer Kaspersky-Lab-Anwendung ausgeführt werden soll.

Task-Einstellungen – Parameter einer Anwendung, die für jeden Tasktyp spezifisch sind.

U

Update – Vorgang zum Ersetzen/Hinzufügen neuer Dateien (Antiviren-Datenbanken oder Programmmodule der Anwendung), die von den Kaspersky-Lab-Updateservern heruntergeladen wurden.

Update-Agenten – Computer, die als Zwischenzentren Updates und Installationspakete im Rahmen einer Administrationsgruppe verbreiten.

Updateserver von Kaspersky Lab – Eine Liste von http- und ftp-Servern von Kaspersky Lab, von denen Kaspersky Anti-Virus® die Antiviren-Datenbanken auf Ihren Computer kopiert.

V

Verfügbare Updates – Service Packs, die eine Auswahl von dringenden Updates enthalten, die innerhalb eines bestimmten Zeitraums gesammelt wurden, sowie Änderungen der Anwendungsarchitektur.

W

Wiederherstellung – Wiederherstellung von Daten des Administrationsservers mit Hilfe der Backup-Utility. Die Wiederherstellung basiert auf Daten, die in einem Backup-Speicher gespeichert werden. Die Utility erlaubt die Wiederherstellung:

- der Datenbank des Administrationsservers (Richtlinien, Tasks, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse).
- der Konfigurationsdaten über die Struktur des logischen Netzwerks und Client-Computer.
- des Speichers der Programmdistributionen für die Remote-Installation (Inhalt der Ordner Packages, Uninstall, Updates).
- des Zertifikats des Administrationsservers.

Z

Zentralisierte Anwendungsverwaltung – Verwaltung einer Anwendung mit Hilfe der Administrationsserver von Kaspersky Administration Kit.

Zertifikat des Administrationsservers – Zertifikat auf dessen Basis bei der Verbindung der Administrationskonsole und beim Datenaustausch mit Client-Computern die Authentifizierung des Administrationsservers stattfindet. Das Zertifikat des Administrationsservers wird bei der Installation des Administrationsservers erstellt und im Installationsverzeichnis des Programms im Ordner **Cert** gespeichert.

ANHANG B. 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.

B.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 Abonnementsdienst 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 Pop-up-Fenstern 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 Mobile

Kaspersky Anti-Virus Mobile bietet den Antiviren-Schutz für mobile Geräte, die mit den Betriebssystemen Symbian OS und Microsoft Windows Mobile arbeiten. Das Programm erlaubt eine komplexe Antiviren-Untersuchung, die folgende Optionen umfasst:

- *Scan auf Befehl* des Arbeitsspeichers, der Speicherkarten, einzelner Ordner oder einer konkreten Datei eines mobilen Geräts. Beim Fund eines infizierten Objekts wird es in die Quarantäne verschoben oder gelöscht.
- *Echtzeit-Untersuchung*: Alle eingehenden und veränderten Objekte, sowie Dateien, auf die versucht wird zuzugreifen, werden automatisch untersucht.
- *Schutz vor sms- und mms-Spam*

Kaspersky Anti-Virus für 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 Pop-up-Fenstern 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® 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 eintritt.
- *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 für Mail-Server

Kaspersky Security für 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 für 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.

B.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: support@kaspersky.de
Allgemeine Informationen	WWW: http://www.kaspersky.de/ http://www.viruslist.de/
Feedback zu unseren Benutzerhandbüchern	docfeedback@kaspersky.com (Diese Adresse ist für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.)

ANHANG C. 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 Aktivierungscode sind 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 dekomplieren 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.