

KASPERSKY LAB

Kaspersky[®] Administration Kit 6.0

Handbuch zur einföhrung

KASPERSKY® ADMINISTRATION KIT 6.0

Handbuch zur Einführung

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

Redaktionsdatum: Februar 2007

Inhalt

KAPITEL 1. KASPERSKY® ADMINISTRATION KIT	5
1.1. Kaspersky Administration Kit	5
1.2. Hardware- und Softwarevoraussetzungen	7
1.3. Lieferumfang	9
1.4. Service für registrierte Benutzer	9
1.5. Art des Dokumentes	10
1.6. Textgestaltung	10
KAPITEL 2. TYPISCHE ENTFALTUNG DES ANTIVIREN-SCHUTZES	12
2.1. Einführung des Antiviren-Schutzes auf Computern eines logischen Netzwerks	12
2.2. Aufbau eines zentralisierten Verwaltungssystems für den Antiviren-Schutz	13
KAPITEL 3. INSTALLATION VON KASPERSKY ADMINISTRATION KIT	15
3.1. Installation von MSDE aus der Distribution von Kaspersky Administration Kit.	17
3.2. Installation von Administrationsserver und Administrationskonsole auf einem lokalen Computer	19
3.3. Deinstallation der Programmkomponenten von Kaspersky Administration Kit	37
3.4. Update der Programmversion	37
KAPITEL 4. INSTALLATION UND DEINSTALLATION DES PROGRAMMS AUF DEN COMPUTERN	39
4.1. Remote-Installation des Programms	40
4.1.1. Erstellen eines Installationspakets	42
4.1.2. Anzeigen und Einstellen der Parameter für ein Installationspaket	45
4.1.3. Erstellen und Einstellen des Installationspaketes für Administrationsagenten	49
4.1.4. Erstellen und Einstellen des Installationspakets für einen Administrationsserver	53
4.1.5. Erstellen des Tasks Verbreitung eines Installationspaketes auf untergeordnete Administrationsserver	53
4.1.6. Verbreitung von Installationspaketen innerhalb einer Gruppe mit Administrationsagenten	55

4.1.7. Erstellen des Tasks Remote-Installation	58
4.1.8. Konfiguration des Tasks Remote-Installation	70
4.1.9. Task zur Produktinstallation auf die untergeordnete Server	72
4.1.10. Remote-Deinstallation eines Programms	75
4.2. Assistent für Remote-Installation	76
4.3. Lokale Installation eines Programms	81
4.3.1. Lokale Installationspaket des Administrationsagenten	82
4.3.2. Lokale Installation des Plug-Ins zur Anwendungsverwaltung	87
4.3.3. Installation von Programmen im Silent-Modus	88
ANHANG A. GLOSSAR	90
ANHANG B. KASPERSKY LAB	96
B.1. Weitere Produkte und Services von Kaspersky Lab	97
B.2. Kontaktinformationen	105
ANHANG C. ENDBENUTZER-LIZENZVERTRAG	106

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 von Anwendungen, die zum Bestand von Kaspersky-Lab-Produkten gehören, auf Computern, die unter Betriebssystemen der Windows-Familie arbeiten. 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.
- Zentralisierte Remote-Verwaltung aller Anwendungen, die zum Bestand von Kaspersky-Lab-Produkten gehören und auf Computern unter dem Betriebssystem Windows arbeiten. 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 E-Mail-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.
- 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.
- 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:
 - Microsoft Data Access Components (MDAC) in der Version 2.8 und höher
 - MSDE 2000 mit Service Pack 3¹ oder Microsoft SQL Server 2000 mit Service Pack 3¹ und höher oder MySQL Version 5.0.22 (Codepage ist standardmäßig UTF-8) oder Microsoft SQL 2005 und höher oder Microsoft SQL 2005 Express und höher
 - Microsoft Windows 2000 mit Service Pack 1 und höher, Microsoft Windows XP Professional mit Service Pack 1 und höher, Microsoft Windows XP Professional x64 und höher, Microsoft Windows Server 2003 und höher, Microsoft Windows Server 2003 x64 und höher, Microsoft Windows NT4 mit

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

Service Pack 6a 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 mit Service Pack 1 und höher, Microsoft Windows XP Professional mit Service Pack 1 und höher, Microsoft Windows XP Home Edition mit Service Pack 1 und höher, Microsoft Windows XP Professional x64 und höher, Microsoft Windows Server 2003 und höher, Microsoft Windows Server 2003 x64 und höher, Windows NT4 mit Service Pack 6a und höher, Microsoft Windows Vista, Microsoft Windows Vista x64;
 - Microsoft Management Console Version 1.2 und höher
 - Für Microsoft Windows installieren Sie Microsoft Internet Explorer 6.0.
- Hardwareanforderungen:
 - Intel Pentium II Prozessor, 400 MHz oder schneller
 - 64 MB RAM
 - 10 MB
- 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, Microsoft Windows Vista x64.
 - 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 kann bei unseren Vertriebspartnern (als verpackte Variante) nur im Verbund mit Kaspersky Anti-Virus Business Optimal und Kaspersky Corporate Suite für den Schutz von Workstations und Servern auf der Basis von Microsoft Windows oder in einem Online-Shop (z. B. www.kaspersky.com/de).

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 Programm benutzer 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 des 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 verbreiteten 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.
Hinweis	Zusatzinformationen, Hinweise
Achtung!	Sehr wichtige Informationen

Formatierung	Bedeutung
<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. TYPISCHE ENTFALTUNG DES ANTIVIREN-SCHUTZES

2.1. Einführung des Antiviren- Schutzes auf Computern eines logischen Netzwerks

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.

2.2. 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 Programmpaketes 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? Die Interaktion von Hauptserver und untergeordneten Administrationsservern sollte möglichst über schnelle Verbindungskanäle erfolgen, so dass die Belastung der Verbindung verringert und die Zulässigkeit des Systems erhöht wird.
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 des Administrationsservers auf Computern, die zum Firmennetzwerk gehört
2. Installation der Administrationskonsole auf Computern, von denen aus die Verwaltung der Produkte erfolgt
3. Benennung von 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 müssen die Hierarchie der Administrationsserver und für jeden Server die Struktur des logischen Netzwerks gebildet, die Hierarchie der Administrationsgruppen aufgebaut und die Computer auf die entsprechenden Gruppen verteilt werden.

Beim folgenden 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.

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 gehören 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 5.0 und 6.0 verwendet.

KAPITEL 3. INSTALLATION VON KASPERSKY ADMINISTRATION KIT

Bevor die Installation begonnen wird, muss sichergestellt werden, dass der Computer die Hardware- und Softwareanforderungen erfüllt, die an den Administrationsserver und Administratorarbeitsplatz gestellt werden (s. Pkt. □ auf S. 6).

Zum Speichern von Daten des Administrationsservers wird MSDE (Microsoft Data Engine) oder Microsoft SQL-Server verwendet. Wenn im Firmennetzwerk weder MSDE noch SQL-Server installiert ist, muss vor der Installation des Administrationsservers eine dieser Anwendungen installiert werden. Dazu können Sie Ihre Distributionen verwenden. Zur Installation von MSDE kann auch die Distribution von Kaspersky Administration Kit benutzt werden. Im Folgenden wird die Installationsprozedur für MSDE aus der Distribution von Kaspersky Administration Kit beschrieben (s. Pkt. 3.1 auf S. 17).

Zur Installation von Kaspersky Administration Kit sind lokale Administratorrechte für den Computer, auf dem die Installation erfolgt, erforderlich.

Das Setup schlägt Ihnen vor, auf dem Computer, von dem es gestartet wurde, die Programmkomponenten der Anwendung Kaspersky Administration Kit zu installieren: Administrationsserver und Administrationskonsole. Diese Konfiguration empfiehlt vor dem Aufbau einer zentralisierten Remote-Verwaltung.

Damit alle Komponente der Anwendung nach der Installation korrekt funktionieren, müssen auf den Computern alle notwendige Ports geöffnet werden. Eine Auflistung der Ports für Kaspersky Administration Kit ist in der Tabelle 1. aufgeführt.

Tabelle 1

Portnummer	Protokoll	Beschreibung
Administrationsserver		
13000	TCP und UDP	Unter Benutzung von SSL-Protokoll wird ausgeführt: <ul style="list-style-type: none"> • Datenerhalt von den Client-Computer; • Verbindung mit dem Updateagenten; • Verbindung mit den untergeordneten Administrationsserver; • Erhalt der Nachrichten über das Ausschalten der Computer.
13292	TCP	Verwendung zum Verbinden mit mobilen Endgeräten. ²
14000	TCP	Wird für folgende Aktionen benutzt: <ul style="list-style-type: none"> • Datenerhalt von den Client-Computer; • Verbindung des Updateagenten; • Verbindung des untergeordneten Administrationsserver.
18000	HTTP	Wird zum Datenaustausch zwischen Administrationsserver und Cisco NAC-Authentifizierungsserver benutzt.
Computer, welcher als Updateagent fungiert		
13000	TCP	Wird zur Verbindung von den Client-Computern benutzt.
13001	TCP	Wird zur Verbindung von den Client-Computern benutzt, wenn Updateagent gleichzeitig auch als Administrationsserver fungiert.

² Als mobiles Endgerät wird ein Gerät mit dem installierten Programm Kaspersky Anti-Virus 6.0 Mobile Enterprise Edition verstanden.

Portnummer	Protokoll	Beschreibung
14000	TCP	Wird zur Verbindung von den Client-Computern benutzt
14001	TCP	Wird zur Verbindung von den Client-Computern benutzt, wenn Updateagent gleichzeitig auch als Administrationsserver fungiert.
Clientcomputer mit installierten Administrationsagenten		
15000	UDP	Wird für Verbindungsanfragen mit dem Administrationsserver benutzt.

3.1. Installation von MSDE aus der Distribution von Kaspersky Administration Kit

Vor der Installation von MSDE müssen die Microsoft Data Access Components (MDAC) in der Version 2.8 und höher (Setup-Dateien liegen auf der Internetseite von Microsoft) installiert werden.

Die MSDE-Installation von der Distributions-CD von Kaspersky Administration Kit erfolgt lokal auf dem Computer.

Um MSDE zu installieren,

1. Starten Sie die ausführbare Datei **setup.exe**, die sich auf der Distributions-CD der Anwendung Kaspersky Administration Kit im Verzeichnis **MSDE2KSP3** befindet. Die Installation wird von einem Assistenten begleitet, der Ihnen die Konfiguration der Installationseinstellungen und den Start der Installation anbietet. Bitte folgen Sie den Anweisungen.
2. Die ersten Installationsschritte sind traditionell und umfassen das Entpacken der erforderlichen Dateien von der Distribution und das Speichern auf der Festplatte Ihres Computers, das Akzeptieren des Lizenzvertrags und die Eingabe des Benutzer- und Firmennamens.
3. Legen Sie im folgenden Dialogfenster **Zielordner auswählen** fest:

- im Feld **Programmdateien** – das Zielverzeichnis für die Programmdateien von MSDE. Als Standard gilt **<Datenträger>:\Programme\Microsoft SQL Server**. Sollte dieses Verzeichnis nicht vorhanden sein, dann wird es automatisch erstellt.
- im Feld **Datenbankdateien** – das Verzeichnis, das zum Speichern der Daten des MSDE-Servers benutzt wird. Als Standard gilt ebenfalls **<Datenträger>:\Programme\Microsoft SQL Server**.

Zur Auswahl alternativer Verzeichnisse dienen die Schaltflächen **Durchsuchen**.

4. Legen Sie im folgenden Dialogfenster **Name des SQL-Servers** (s. Abb. 1) den Namen fest, den dieser MSDE-Server erhalten soll.

Standardmäßig wird kein Name erstellt, zur Adressierung des Servers dient der Computernamen, unter dem der Rechner installiert wurde.

Wenn Sie einen anderen Namen angeben möchten, deaktivieren Sie das Kontrollkästchen **Standard** und geben Sie den neuen Namen im Feld **Name des SQL-Servers** ein.

Nach der Definition und dem Überprüfen der Einstellungen, kann die Installation gestartet werden. Nach dem erfolgreichen Abschluss wird MSDE auf Ihrem Computer installiert sein.

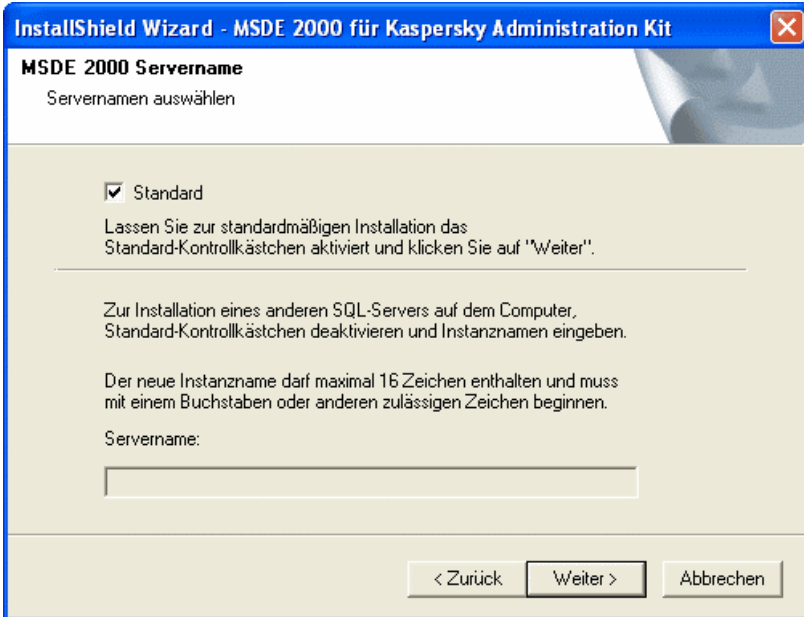


Abbildung 1. Servernamen auswählen

3.2. Installation von Administrationsserver und Administrationskonsole auf einem lokalen Computer

In diesem Abschnitt wird eine lokale Installation des Administrationsserver oder Administrationskonsole beschrieben. Wenn im Netzwerk mindestens ein Administrationsserver installiert ist, können weitere Server mit Hilfe der Remote-Installation (s. Pkt. 0 auf S. 58). Beim Erstellen des Tasks muss Installationspaket des Administrationsserver benutzt werden (S. Pkt. 4.1.4 auf S. 53).

Um den Administrationsserver und/oder die Administrationskonsole zu installieren:

1. Starten Sie die ausführbare Datei **setup.exe** von der Distributions-CD. Dadurch wird er Assistent gestartet, der Ihnen die Konfiguration

der Installationseinstellungen anbietet. Folgen Sie den Anweisungen des Assistenten.

2. Die ersten Installationsschritte sind traditionell und umfassen das Entpacken der erforderlichen Dateien von der Distribution und das Speichern auf der Festplatte Ihres Computers, das Akzeptieren des Lizenzvertrags und die Eingabe des Benutzer- und Firmennamens.
3. Legen Sie dann das Verzeichnis für die Installation der Komponenten fest. Als Standard gilt **<Datenträger>\Programme\Kaspersky Lab \Kaspersky Administration Kit**. Sollte dieses Verzeichnis nicht vorhanden sein, dann wird es automatisch erstellt. Zur Auswahl eines anderen Verzeichnisses dient die Schaltfläche **Durchsuchen**.
4. Wählen Sie danach die Komponenten von Kaspersky Administration Kit aus, die Sie installieren möchten (s. Abb. 2):
 - **Administrationsserver**. In diesem Fall können Sie auch die Installation der Standardkomponente für die Zusammenarbeit mit Cisco NAC definieren. Wenn die Installation vorgenommen werden soll, setzen Sie Häkchen **Posture Validation Server "Kaspersky Lab" für Cisco NAC**. Die Parameter für Zusammenarbeit mit Cisco NAC können in den Eigenschaften oder in der Richtlinie des Administrationsserver eingestellt werden (Details s. Beschreibung Kaspersky Administration Kit).

Administrationskonsole.

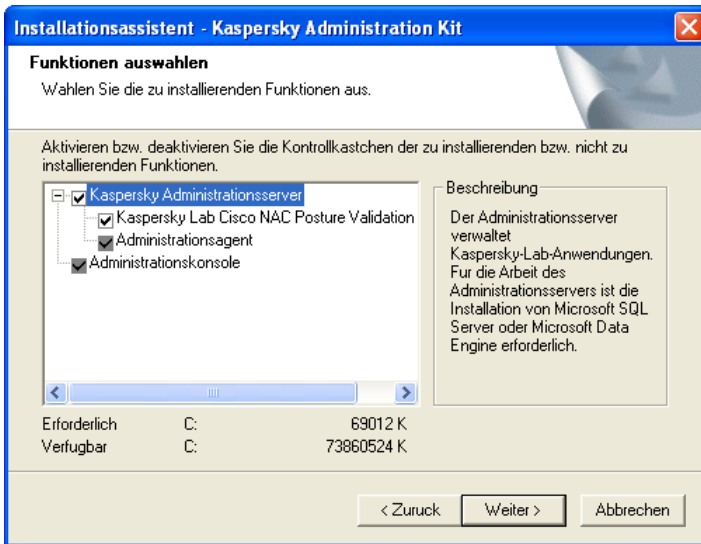


Abbildung 2. Zu installierende Komponenten auswählen

Sie können entweder alle Komponenten oder nur die Administrationskonsole zur Installation auswählen. Der Administrationsserver kann nicht ohne die Administrationskonsole zur Installation ausgewählt werden. Standardmäßig ist die Installation aller Komponenten vorgesehen.

Zusammen mit der Komponente Administrationsserver wird auf dem Computer die Serverversion des Administrationsagenten installiert. Dessen gleichzeitige Installation mit der üblichen Version des Administrationsagenten ist nicht möglich. Falls diese Komponenten bereits auf Ihrem Computer installiert sind, löschen Sie sie und starten Sie erneut die Installation des Administrationsservers.

Bitte beachten Sie folgende Informationen im Dialogfenster des Assistenten:

- im linken Teil im Feld **Beschreibung** über die ausgewählte Komponente
- im unteren Teil über den für die Installation der ausgewählten Komponenten erforderlichen Speicherplatz und den freien Speicherplatz auf dem für die Installation ausgewählten Computerlaufwerk

Wenn Sie nur die Administrationskonsole ausgewählt haben, werden die folgenden Schritte zur Konfiguration der Installationseinstellungen übersprungen und Sie können unmittelbar zur Überprüfung der Einstellungen und dem Start der Installation übergehen.

5. Wenn Sie die Installation des Administrationssservers ausgewählt haben, geben Sie auf der folgenden Etappe an, unter welchem Benutzerkonto der Administrationsserver auf diesem Computer als Dienst gestartet wird (s. Abb. 3).

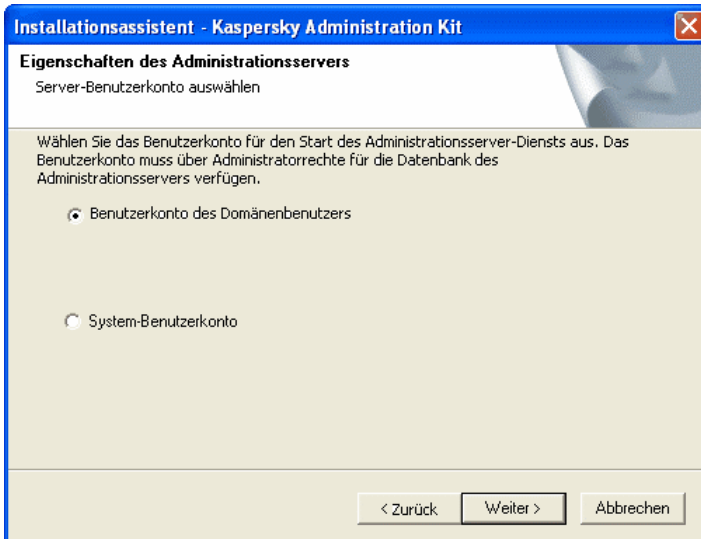


Abbildung 3. Benutzerkonto auswählen

Zwei Varianten stehen zur Auswahl:

- **Benutzerkonto des Domänenbenutzers** – Der Administrationsserver wird unter dem Konto eines Benutzers gestartet, der zu dieser Domäne gehört. In diesem Fall wird der Administrationsserver alle Operationen mit den Rechten dieses Benutzerkontos initiieren, und auf der folgenden Etappe wird Ihnen angeboten, den entsprechenden Benutzer auszuwählen, dessen Konto verwendet wird.

Wenn das Firmennetzwerk eine Windows-Domänenstruktur aufweist, wird empfohlen, für den Start des Administrationsservers das Benutzerkonto des Domänenadministrators auszuwählen. In diesem Fall wird der Administrationsserver für alle Administrationsszenarien über Zugriff auf die erforderlichen Ressourcen verfügen (s. Pkt. 0 auf S. 58).

- **System-Benutzerkonto** – Der Administrationsserver wird unter dem Benutzerkonto und mit den Rechten des **System-Benutzerkontos** gestartet. Die Auswahl dieser Variante empfiehlt sich für die Installation von Kaspersky Administration Kit in Netzwerken, die nicht über eine Windows-Domänenstruktur verfügen. In diesem Fall findet die Auswahl des Benutzers nicht statt und Sie gehen unmittelbar zur Definition der Ressource zum Speichern der Datenbanken des Administrationsservers über (s. Pkt. 7 auf S. 25).

Eine Voraussetzung für die korrekte Funktion von Kaspersky Administration Kit ist, dass das Benutzerkonto für den Start des Administrationsservers über Administratorrechte für die Ressource zum Speichern der Datenbanken des Administrationsservers verfügt.

6. Wenn Sie als Benutzerkonto für den Start des Administrationsservers das Konto eines Domänenbenutzers ausgewählt haben, wird Ihnen angeboten, diesen Benutzer zu bestimmen.

Dazu wird im Feld **Benutzerkonto** des Assistentenfensters (s. Abb. 4) mit Hilfe der Schaltfläche **Durchsuchen** oder durch manuelle Eingabe der Benutzername eines in der betreffenden Domäne registrierten Benutzers ausgewählt. Geben Sie danach das **Kennwort** des Benutzers an, mit dem er in der Domäne registriert ist.

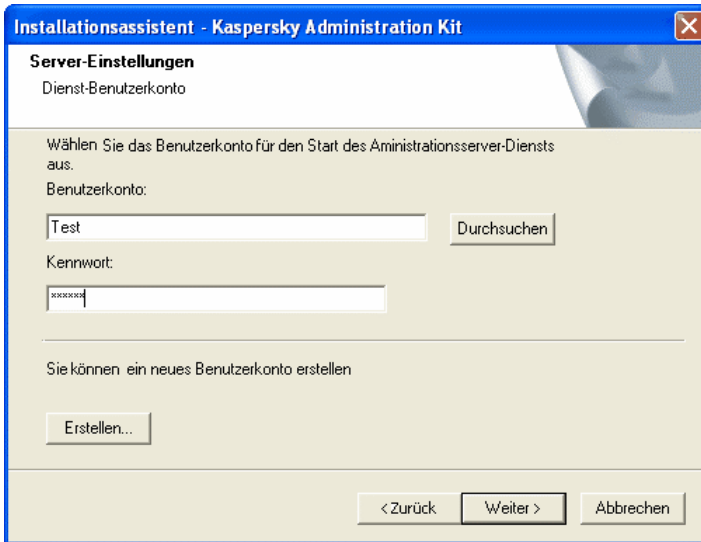


Abbildung 4. Benutzer auswählen

Wenn Sie einen Benutzer ausgewählt haben, der nicht über die Rechte des Domänenadministrators verfügt, wird der Administrationsserver unter seinem Benutzerkonto gestartet, allerdings wird die Funktionalität von Kaspersky Administration Kit eingeschränkt sein. So kann er z.B. nicht über die Rechte zum Ausführen von Tasks zur Remote-Installation mit Hilfe von Startskripts (s. Pkt. 0 auf S. 58) und zum Durchsuchen bestimmter Domänen des Windows-Netzwerks verfügen.

Damit der Administrationsserver richtig funktioniert, muss das Benutzerkonto beim Starten die folgenden Berechtigungen haben:

- Einloggen als Dienst (Log on as a service)
- Unterordnung unter das Betriebssystem (Act as part of the operating system)
- Zugriff auf den Computer aus dem Netzwerk (Access this computer from the network)
- Kennzeichen für Prozessebene austauschen (Replace a process level token)
- Speicherplatzzuweisungen für einen Prozess konfigurieren (Increase quotas/ Adjust memory quotas for a process)

Wenn der von Ihnen ausgewählte Benutzer der Domänenadministrator ist, aber nicht die oben genannte Berechtigungen hat, dann wird ihm diese Rechte zugewiesen (s. Abb. 5).



Abbildung 5. Meldung über die Zuweisung von Berechtigungen

7. Auf der nächsten Etappe werden Sie aufgefordert, die Ressource **Microsoft SQL-Server (MSDE)** oder **MySQL** (s. Abb. 6) anzugeben, die zum Speichern der Datenbank des Administrationssservers verwendet wird.

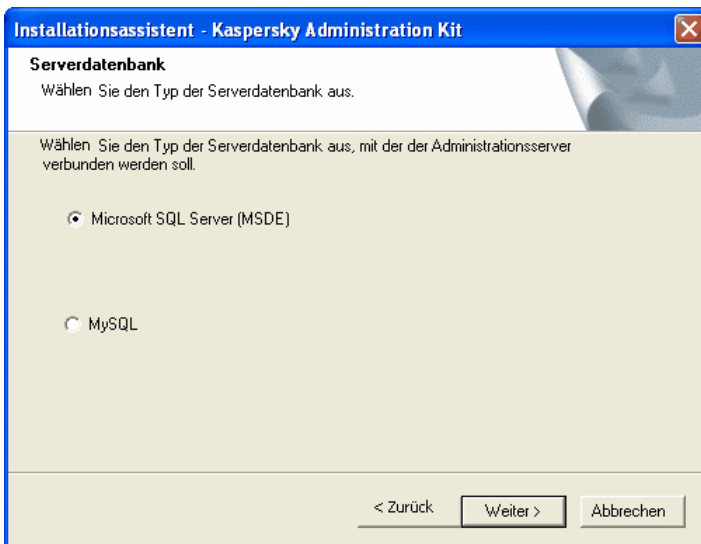


Abbildung 6. Datenbank auswählen

8. Wenn im vorangegangenen Schritt MSDE oder Microsoft SQL-Server ausgewählt wurden und Sie vorhaben, für Kaspersky Administration Kit einen Server zu verwenden, der im Firmennetzwerk installiert ist, geben Sie dessen Namen in das Feld **Name des SQL-Servers** ein und tragen Sie den Namen der Datenbank in das Feld **Name der Datenbank für SQL-Server** (s. Abb. 7) ein, die für die Aufnahme der Informationen vom

Administrationsserver angelegt wird. Standardmäßig wird die Datenbank unter dem Namen **KAV** angelegt.

Im Feld **Name des SQL-Servers** wird automatisch der Wert **(local)** vorbelegt, wenn der SQL-Server auf dem Computer vorgefunden wurde, auf dem Kaspersky Administration Kit installiert wird. Mit Hilfe der Schaltfläche **Durchsuchen** erscheint eine Liste mit allen Microsoft SQL-Servern, die im Netzwerk installiert sind.

Wenn der Administrationsserver unter dem Benutzerkonto des lokalen Administrators oder unter dem System-Benutzerkonto gestartet wird, steht die Schaltfläche **Durchsuchen** nicht zur Verfügung.

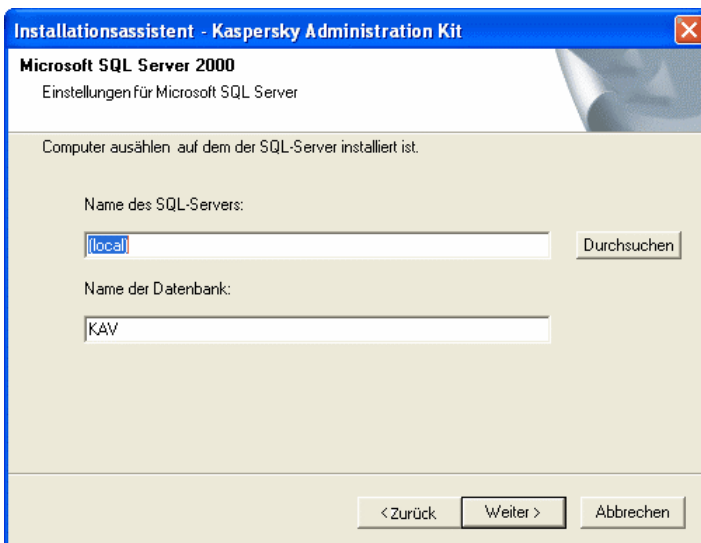


Abbildung 7. SQL-Server auswählen

Wenn in der vorangegangenen Etappe der MySQL-Server ausgewählt worden ist, geben Sie in diesem Fenster (s. Abb. 8) dessen Name im Feld **Name des MySQL-Servers** (standardmäßig gilt die IP-Adresse des Computers, auf dem Kaspersky Administration Kit installiert wird) ein und tragen Sie den Port im Feld **Port** (standardmäßig gilt der Port 3306) ein. Im Feld **Name der Datenbank des SQL-Servers** geben Sie den Namen der Datenbank ein, der für die Aufnahme der Daten vom Administrationsserver erstellt wird (standardmäßig wird die Datenbank unter dem Namen **KAV** erstellt).

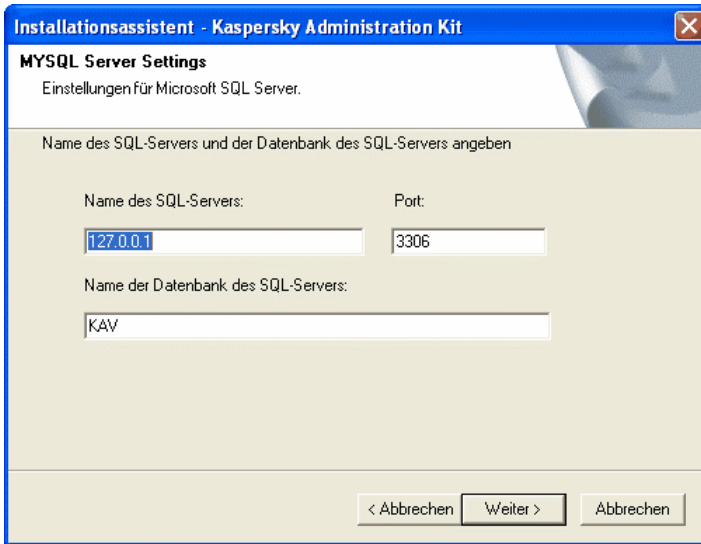


Abbildung 8. MySQL-Server auswählen

Wenn im Netzwerk kein einziger SQL-Server vorhanden ist bzw. Sie keinen derartigen Server verwenden können, müssen Sie ihn installieren (s. Pkt. 3.1 auf S. 17).

Wenn Sie den Microsoft SQL-Server auf dem Computer installieren möchten, von dem aus die Installation von Kaspersky Administration Kit erfolgt, muss die laufende Installation abgebrochen und nach der Installation des SQL-Servers erneut gestartet werden.

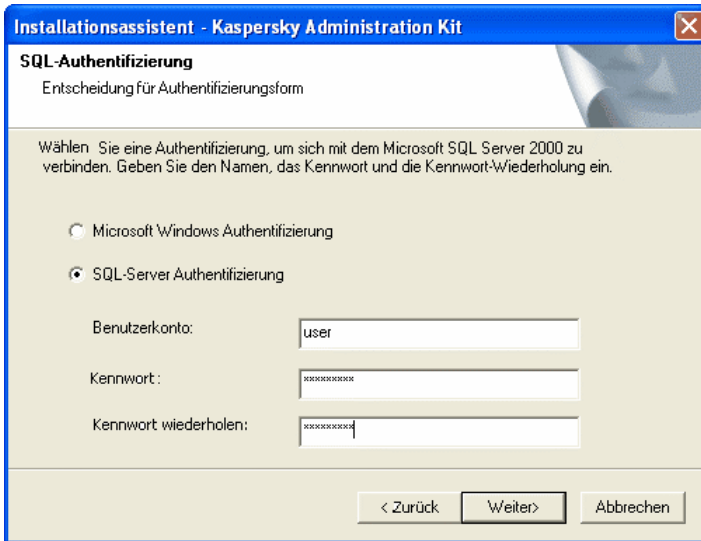
Erfolgt die Installation auf einem Remote-Computer, dann ist es nicht erforderlich, den Installationsassistenten für Kaspersky Administration Kit abzubrechen. Installieren Sie den Microsoft SQL-Server und fahren Sie danach mit der Installation von Kaspersky Administration Kit fort.

9. In diesem Schritt legen Sie die Authentifizierung fest, die für das Verbinden des Administrationsservers mit dem SQL-Server verwendet wird.

Für MSDE oder den Microsoft SQL-Server können Sie sich zwischen den beiden folgenden Varianten entscheiden (s. Abb. 9):

- **Microsoft Windows Authentifizierung** – In diesem Fall wird für die Prüfung der Rechte die Registrierung für den Aufruf des Administrationsservers herangezogen

- **SQL-Server-Authentifizierung** – In diesem Fall wird für die Prüfung der Rechte die unten eingegebene Registrierung herangezogen. Füllen Sie die Felder **Registrierung**, **Kennwort** und **Kennwort wiederholen** aus.



The screenshot shows a dialog box titled "Installationsassistent - Kaspersky Administration Kit" with a close button in the top right corner. The main heading is "SQL-Authentifizierung" and the subtitle is "Entscheidung für Authentifizierungsform". Below this, there is a paragraph of text: "Wählen Sie eine Authentifizierung, um sich mit dem Microsoft SQL Server 2000 zu verbinden. Geben Sie den Namen, das Kennwort und die Kennwort-Wiederholung ein." There are two radio button options: "Microsoft Windows Authentifizierung" (unselected) and "SQL-Server Authentifizierung" (selected). Below the options are three input fields: "Benutzerkonto:" with the text "user", "Kennwort:" with masked characters "*****", and "Kennwort wiederholen:" with masked characters "*****". At the bottom of the dialog are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

Abbildung 9. Authentifizierung am SQL-Server

Für den MySQL-Server geben Sie das Benutzerkonto und das Kennwort an (s. Abb. 10).

Installationsassistent - Kaspersky Administration Kit

Parameter der MySQL-Authentifizierung

Geben Sie das Benutzerkonto des MySQL-Servers ein.

Geben Sie das Benutzerkonto für die Verbindung zum MySQL-Server ein, dann das Kennwort und die Kennwortbestätigung

Benutzerkonto:

Kennwort:

Kennwortbestätigung:

< Zurück Weiter > Abbrechen

Abbildung 10. Authentifizierung am MySQL-Server

10. Bestimmen Sie danach (s. Abb. 11) den Speicherort und den Namen des gemeinsamen Ordners an, der verwendet wird zum:
 - Speichern der Dateien, die für die Remote-Installation von Anwendungen erforderlich sind (die Dateien werden beim Erstellen von Installationspaketen auf den Administrationsserver kopiert).
 - Speichern von Updates, die von der Update-Quelle auf den Administrationsserver kopiert werden.

Für diese Ressource erhalten alle Benutzer gemeinsamen Zugriff zum Lesen.

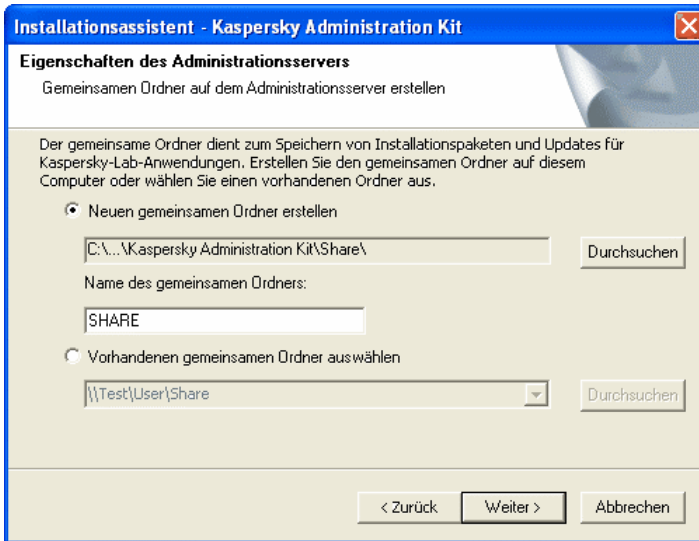


Abbildung 11. Gemeinsamen Ordner erstellen

Sie können zwischen zwei Varianten auswählen:

- **Neuen gemeinsamen Ordner erstellen** – zum Erstellen eines neuen Ordners. Geben Sie hier den Pfad des Ordners und im Feld **Name des gemeinsamen Ordners** den Ordernamen an.
- **Vorhandenen gemeinsamen Ordner auswählen** – zur Auswahl eines vorhandenen gemeinsamen Ordners.

Der gemeinsame Ordner kann lokal auf dem Computer, von dem aus die Installation erfolgt, oder entfernt auf einem beliebigen Computer, der zum Firmennetzwerk gehört, angelegt werden. Sie können sowohl einen Ordner mit Hilfe der Schaltfläche **Durchsuchen** auswählen, wie auch per Hand im Feld UNC-Pfad angeben (z. B., \\server\KLSHare).

Standardmäßig wird der lokale Ordner **KLSHare** in dem Verzeichnis erstellt, dass für die Installation der Programmkomponenten von Kaspersky Administration Kit festgelegt wurde.

11. In dem folgenden Fenster geben Sie die Adresse des Administrationsserver an (s. Abb. 12) als:
 - DNS-Name. Diese Variante wird in dem Fall benutzt, wenn ein DNS-Server im Netzwerk präsent ist, können die Client-Computer mit seiner Hilfe die Adresse von dem Administrationsserver bekommen.

- NetBIOS-Name. Diese Variante wird in dem Fall benutzt, wenn ein WINS-Server im Netzwerk präsent ist oder die Client-Computer mit Hilfe von NetBIOS-Protokoll die Adresse von dem Administrationsserver bekommen.
- IP-Adresse. Diese Variante wird in dem Fall benutzt, wenn der Administrationsserver eine statische IP-Adresse hat, welche nicht mehr geändert wird.

Setzen Sie Häkchen **Namendienst NetBIOS in dem Anti-Hacker von Kaspersky Antivirus 6.0 erlauben**, wenn es notwendig ist. Es wird dabei in dem Anti-Hacker von Kaspersky Antivirus 6.0 UDP-Port 137 geöffnet, welcher zum Ablesen der IP-Adresse des Administrationsservers benutzt wird.

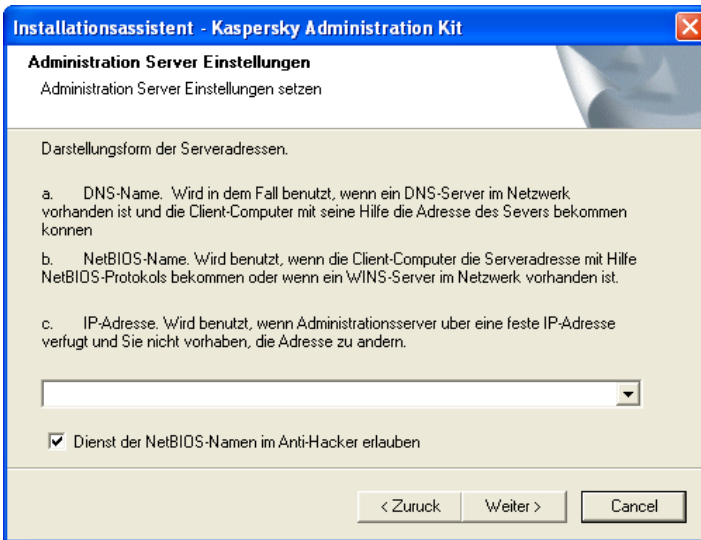


Abbildung 12. Adresse des Administrationsservers

12. Legen Sie nun die Einstellungen für die Verbindung mit dem Administrationsserver fest (s. Abb. 13):
 - Nummer des Ports, über den die Verbindung mit dem Administrationsserver erfolgt. Standardmäßig wird Port **14000** verwendet. Wenn dieser Port belegt ist, kann ein anderer Wert gewählt werden.
 - die Nummer des Ports, über den die geschützte Verbindung mit dem Administrationsserver unter Verwendung des Protokolls SSL erfolgt. Als Standard gilt Port **13000**.

Wenn der Administrationsserver unter dem Betriebssystem Microsoft Windows XP SP2 arbeitet, dann blockiert die integrierte Firewall die TCP-Ports 13000 und 14000. Für den Zugriff auf den Administrationsserver müssen diese Ports auf dem Administrationsserver-Computer manuell geöffnet werden.

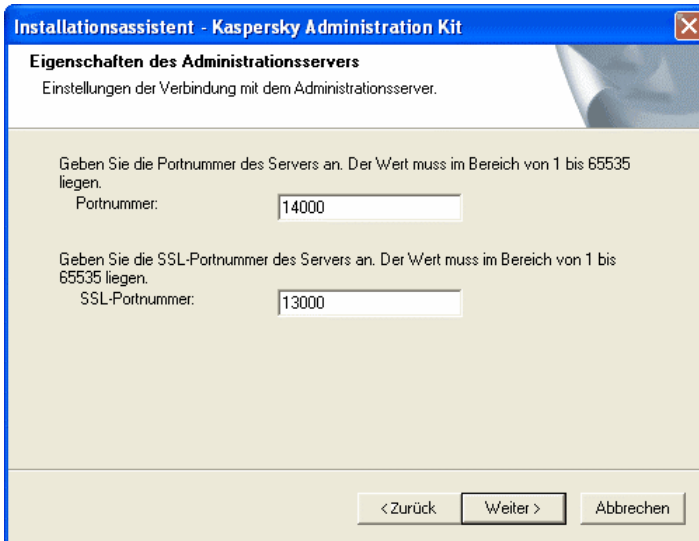


Abbildung 13. Einstellungen der Verbindung mit dem Administrationsserver

13. In diesem Fenster des Assistenten (s. Abb. 14) bestimmen Sie, wie das Zertifikat für die Authentifizierung der zu installierenden Administrationsservers erstellt wird.

Es sind zwei Möglichkeiten vorgesehen:

- **Das Zertifikat für Administrationsserver erstellen** – Entscheiden Sie sich für diese Variante, wenn Sie einen neuen Administrationsserver installieren. Damit künftig bei Bedarf die Daten und die Struktur des logischen Netzwerks leichter wiederhergestellt werden kann, speichern Sie eine Sicherungskopie vom Zertifikat. Setzen Sie dazu das Häkchen im Kontrollkästchen **Sicherungskopie vom Zertifikat erstellen**.
- **Zertifikat aus Sicherungskopie wiederherstellen** – Entscheiden Sie sich für diese Variante, wenn Sie den Administrationsserver bei fehlender Sicherungskopie

wiederherstellen. B I n diesem Fall lassen sich die Daten und die Struktur des logischen Netzwerks von Vorläufer des Administrationssservers wieder herstellen.

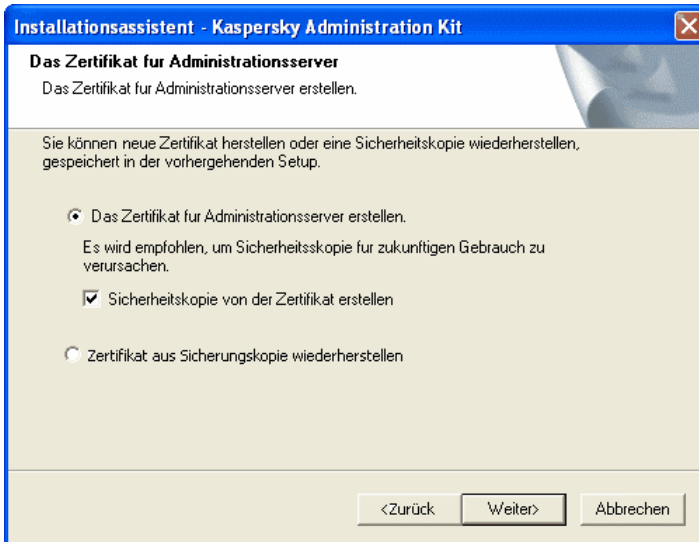


Abbildung 14. Anforderung eines Zertifikats vom Administrationsserver

14. Wenn Sie sich im vorangegangenen Schritt für das Erstellen eines neues Zertifikats und das Speichern einer Sicherungskopie entschieden haben, geben Sie im folgenden Fenster (s. Abb. 15) an:

- Verzeichnis zum Speichern der Sicherungskopie von der Zertifikatsdatei
- Kennwort, das zur Verschlüsselung beim Erstellen des Zertifikates und zum Entschlüsseln bei dessen Wiederherstellung aus der Sicherungskopie benutzt wird
- Kennwortbestätigung

Die Daten des Administrationsservers lassen sich in jedem Fall nur dann komplett wiederherstellen, wenn das Serverzertifikat gespeichert wird.

Beim Wiederherstellen des Zertifikats muss das gleiche Kennwort wie beim Erstellen der Sicherungskopie eingegeben werden. Wenn das Kennwort falsch eingegeben wird, kann das Zertifikat nicht wiederhergestellt werden.

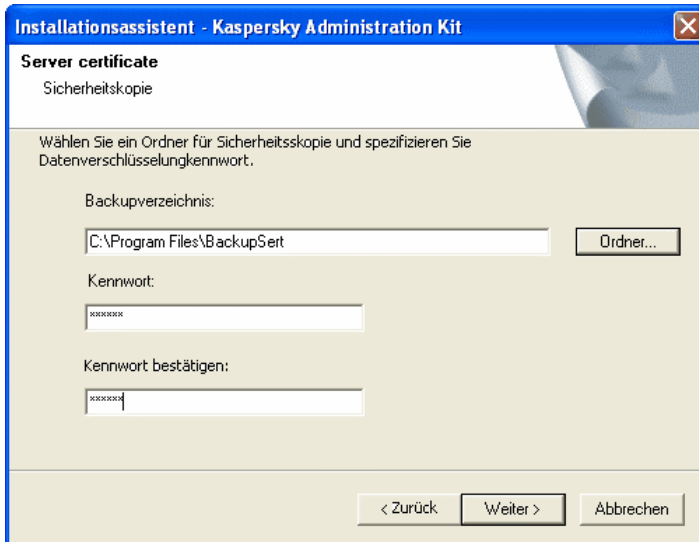


Abbildung 15. Verzeichnis für Speichern der Sicherungskopie vom Zertifikat auswählen

Wenn Sie sich im vorangegangenen Schritt für die Variante Wiederherstellen des Serverzertifikats aus der Sicherungskopie im angezeigten Fenster (s. Abb. 16) entschieden haben, geben Sie Folgendes an:

- Verzeichnis, in dem die Sicherungskopie der Zertifikatsdatei liegt
- Kennwort, das für die Verschlüsselung beim Erstellen der Sicherungskopie verwendet wurde

Nach den Einstellungen der Installationsparameter für die Komponenten von Kaspersky Administration Kit können Sie sie anzeigen und die Installation aufrufen.

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

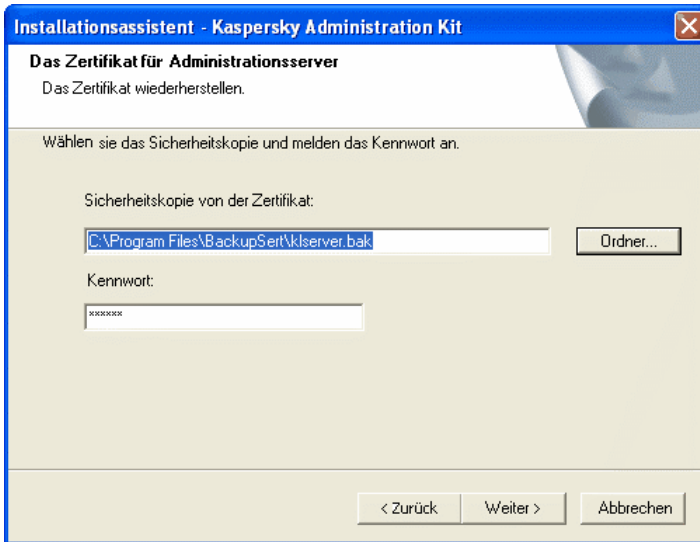


Abbildung 16. Verzeichnis für Speicherung der Sicherungskopie vom Zertifikat auswählen

Der Administrationsserver und Administrationsagent werden auf einem Computer als Dienst mit den Attributen installiert, welche der Tabelle 2 zu entnehmen sind. In der Tabelle sind auch die Attribute des Dienstes Posture Validation Server (PVS) «Kaspersky Lab» für Cisco NAC angegeben. Dieser Dienst wird auf dem Computer ausgeführt, wenn die Komponente zusammen mit dem Administrationsserver installiert wurde.

Tabelle 2

Attribut	Administrationsserver	PVS «Kaspersky Lab» für Cisco NAC	Administrationsagent
Dienstname	CSAdminServer	nacserver	klnagent
Anzeigender Dienstname	Kaspersky Administration Server	Kaspersky Lab Cisco NAC Posture Validation Server	Kaspersky Network Agent
Prozessname in dem Windows-Taskmanager	klserver.exe	klnacserver.exe	klnagent.exe
Starttyp	Automatisch beim Starten des Betriebssystem		

Attribut	Administrationsserver	PVS «Kaspersky Lab» für Cisco NAC	Administrationsagent
Benutzereintrag	Lokales Systemkonto oder Benutzerdefiniert (s. Pkt. 6 auf S. 23).		

Zusammen mit dem Administrationsserver wird auf dem Computer die Serverversion des Administrationsagenten installiert. Sie gehört zur Komponente Administrationsserver, wird gemeinsam mit ihm installiert und deinstalliert und kann nur mit dem lokal installierten Administrationsserver zusammenarbeiten. Die Verbindung von Agent und Administrationsserver muss nicht eingestellt werden, da beide programmtechnisch miteinander verknüpft sind, denn die Komponenten werden auf dem gleichen Computer installiert. Die Einstellungen stehen ebenso in den lokalen Einstellungen des Administrationsagenten auf diesem Rechner zur Verfügung. Mit diesem Aufbau ist dafür gesorgt, dass keine Zusatzeinstellungen vorgenommen werden müssen und Konflikte bei der Interaktion der Komponenten bei Einzelplatzinstallationen aus dem Weg gegangen wird.

Der Serverversion des Administrationsagenten wird mit den gleichen Attributen installiert und erfüllt die gleichen Funktionen für die Anwendungssteuerung wie der standardmäßige Administrationsagent. Für ihn gilt die Richtlinie der Gruppe, zu der der Computer mit dem Administrationsserver als Client gehört, es werden alle Tasks erstellt und ausgeführt, die für den Administrationsagenten vorgesehen sind, ausgenommen die Tasks für den Serverwechsel.

Eine separate Installation des Administrationsagenten auf dem Computer mit dem Administrationsserver wird nicht benötigt. Dessen Funktion übernimmt die Serverversion des Agenten.

Sie können mit Hilfe des standardmäßigen Windows-Verwaltungsprogramms Verwaltung → Dienste die Eigenschaften der Dienste Kaspersky Administration Server Kaspersky Administration Server, **Kaspersky Network Agent** и Kaspersky Lab Cisco NAC Posture Validation Server überprüfen und deren Arbeit verfolgen. Informationen über die Arbeit des Dienstes Kaspersky Administration Server werden im Windows-Systembericht des Computers, auf dem der Administrationsserver installiert ist, in der Verastellung Kaspersky Event Log aufgezeichnet und gespeichert.

Auf dem Computer, auf dem der Administrationsserver installiert ist, werden außerdem die Gruppen der lokalen Benutzer **KLAdmins** und **KLOperators** erstellt. Wenn der Administrationsserver unter dem Konto eines Benutzers, der zu einer Domäne gehört, gestartet wird, dann werden die Gruppen **KLAdmins** und **KLOperators** zur Gruppenliste der Domänenbenutzer hinzugefügt. Die Gruppen können mit Hilfe der standardmäßigen Microsoft Windows-Verwaltungsprogramme verwaltet werden.

3.3. Deinstallation der Programmkomponenten von Kaspersky Administration Kit

Sie können Kaspersky Administration Kit wie mit den üblichen Mitteln zur Installation und Deinstallation von Programmen unter Microsoft Windows entfernen, so auch mit Hilfe des Befehls **Kaspersky Administration Kit entfernen** in dem Menü **Start** → **Programme** → **Kaspersky Administration Kit**. Dabei wird ein Wisard gestartet, welcher alle Komponente der Anwendung von dem Computer entfernt (eingeschlossen PlugIns). Wenn während der Deinstallation Sie das Entfernen des gemeinsamen Ordners (**KLShare**) definiert haben, löschen Sie den Ordner per Hand.

Beim Deinstallieren wird Ihnen empfohlen, eine Sicherungskopie vom Administrationsserver anzulegen.

3.4. Update der Programmversion

Beim Update von der Version 4.x oder 5.x (Update-Paket 1 und Update-Paket 2) des Kaspersky Administration Kit auf eine neuere Version, muss die Vorgänger-Version deinstalliert und die neue Version laut der Beschreibung in diesem Handbuch installiert werden.

Beim Updaten der Versionen 5.0 (Update-Paket 3) und 6.0 auf eine aktuelle Version, wird die Wiederherstellung der Daten aus einer Sicherungskopie der früheren Version unterstützt.

Folgende Reihenfolge wird empfohlen:

1. Erstellen Sie eine Sicherungskopie der Daten, die auf dem Administrationsserver liegen, mit Hilfe der Utility **klbackup.exe**. Diese Utility gehört zum Lieferumfang von Kaspersky Administration Kit und nach Installation der Komponente Administrationsserver liegt sie im Wurzelverzeichnis der Installation. Achten Sie darauf, dass zu einer kompletten Wiederherstellung der Daten vom Administrationsserver das Serverzertifikat mit gespeichert werden muss. Dieser Parameter ist für die Utility **klbackup.exe** obligatorisch.
2. Starten Sie das Setup für die Update-Version von Kaspersky Administration Kit 6.0 auf dem Computer, auf dem die Vorgänger-Version des Administrationsservers und/oder Administrationskonsole installiert gewesen ist. Führen Sie das Update der Komponente aus. Bei dem Vorrang werden alle Daten

und Einstellungen der Vorläuferversion vom Administrationsserver und/oder Administrationskonsole gespeichert und auf sie kann in der aktualisierten Version zugegriffen werden. Die umgekehrte Kompatibilität zwischen neuer und aktueller Version des Administrationsservers ist gewährleistet.

3. Zum Updaten des auf den Computern im Netzwerk installierten Administrationsagenten erstellen Sie einen Gruppentask oder einen globalen Task für die Installation der aktuellen Komponentenversion. Starten Sie den Task manuell oder nach Zeitplan. Nach der Taskausführung ist die Version des Administrationsagenten auf dem neuesten Stand.

Sollten bei der Installation Probleme auftreten, können Sie die Vorläufer-Version von Kaspersky Administration Kit wiederherstellen, indem Sie die vor dem Update erstellte Sicherungskopie der Daten vom Administrationsserver heranziehen.

Wenn im Netzwerk mindestens ein Administrationsserver installiert ist, kann Update der anderen Server mit Hilfe des Tasks der Remote-Installation vorgenommen werden, dabei wird Installationspaket des Administrationsserver benutzt (Details s. Pkt. 4.1.4 auf S. 53).

KAPITEL 4. INSTALLATION UND DEINSTALLATION DES PROGRAMMS AUF DEN COMPUTERN

Bevor die Installation begonnen wird, muss sichergestellt werden, dass die Client-Computer die Hardware- und Softwareanforderungen erfüllen (s. Pkt. □ auf S. 6).

Kaspersky Administration Kit kann Programme von Kaspersky Lab auf Client-Computern eines logischen Netzwerkes auf folgende Art und Weise installieren und deinstallieren:

- zentralisiert und im Remote-Betrieb über die Administrationskonsole
- lokal auf jedem Client-Computer

Die Verbindung zwischen Administrationsserver und Client-Computern wird von der Komponente Administrationsagent gewährleistet. Deshalb muss dieser vor der Installation der Antivirenprogramme auf jedem Computer installiert sein, der an das System zur zentralisierten Remote-Verwaltung angeschlossen wird. Bei einer zentralen Installation von Anwendungen über die Administrationskonsole kann der Agent zusammen mit einer Anwendung installiert werden.

Auf dem Computer, auf dem der Administrationsserver installiert ist, kann als Agent nur die Serverversion dieser Komponente verwendet werden. Sie gehört zum Administrationsserver und wird mit ihm zusammen installiert und deinstalliert (s. Pkt. 3.2 auf S. 19).

Der Administrationsagent muss auf diesem Rechner dann nicht mehr installiert werden.

Die Installation des Administrationsagenten wird genauso durchgeführt wie die Installation von Anwendungen und kann sowohl entfernt als auch lokal erfolgen.

Die Administrationsagenten können je nach Kaspersky-Lab-Anwendung, für deren Arbeit sie installiert werden müssen, variieren. In einigen Fällen funktioniert nur eine lokale Installation des Administrationsagenten (Details siehe Handbücher für die jeweiligen Anwendungen). Der Administrationsagent wird auf einem Client-Computer ein einziges Mal installiert.

Die Oberfläche zur Anwendungsverwaltung mit Hilfe von Kaspersky Administration Kit bieten entsprechende Verwaltungs-PlugIns. Deshalb muss für

den Zugriff auf die Oberfläche zur Anwendungsverwaltung das entsprechende Plug-In am Administratorarbeitsplatz installiert sein. Bei entfernter Installation wird es automatisch installiert, wenn das erste Installationspaket für die entsprechende Anwendung erstellt wird. Bei lokaler Installation muss das Verwaltungs-Plugin vom Administrator manuell installiert werden.

In der laufenden Version Kaspersky Administration Kit wird Verwaltung von folgenden Kaspersky Lab Anwendungen unterstützt:

- Schutz der Arbeitsstationen und Fileserver:
 - Kaspersky Anti-Virus 5.0 für Windows File Servers;
 - Kaspersky Anti-Virus 6.0 für Windows Servers;
 - Kaspersky Anti-Virus 5.0 für Windows Workstations;
 - Kaspersky Anti-Virus 6.0 für Windows Workstations;
 - Kaspersky Anti-Virus 5.0 Second Opinion Solution;
 - Kaspersky Anti-Virus 5.7 für Novell NetWare;
- Perimeterschutz:
 - Kaspersky Anti-Virus 5.6 für Microsoft ISA Server 2000 Enterprise Edition.
- Schutz der Mailsysteme:
 - Kaspersky Anti-Virus 5.5 für Microsoft Exchange Server 2000/2003, Update-Paket 1;
 - Kaspersky Security 5.5 für Microsoft Exchange Server 2003, Update-Paket 1.

Detaillierte Information über Verwaltung der aufgezählten Anwendungen mit Hilfe von Kaspersky Administration Kit s. in den Anleitungen zu den entsprechenden Anwendungen.

4.1. Remote-Installation des Programms

Die Remote-Installation erfolgt vom Arbeitsplatz des Administrators aus im Programmhauptfenster von Kaspersky Administration Kit.

Einige Kaspersky-Lab-Anwendungen können auf Client-Computern nur lokal installiert werden (Details s. Handbücher der jeweiligen Anwendungen). Die Remote-Verwaltung für diese Anwendungen funktioniert trotzdem über Kaspersky Administration Kit.

Um ein Programm im Remote-Betrieb zu installieren:

1. Erstellen Sie ein Installationspaket (s. Pkt. 4.1.1 auf S. 42). In das Paket kommen die gewünschten Anwendungsdateien sowie Konfigurationsdateien für das eigentliche Installationspaket.
2. Erstellen Sie einen Task zur Remote-Installation (s. Pkt. 0 auf S. 58).

Um ein Programm auf allen Computern des logischen Netzwerkes bzw. mehreren Administrationsgruppen oder auf konkreten Computern aus verschiedenen Gruppen zu installieren, muss der Globaltask Remote-Installation erstellt werden

Um ein Programm auf allen Client-Computern einer beliebigen Administrationsgruppe zu installieren (alle eingebetteten Gruppen und untergeordnete Server), muss der Gruppentask Remote-Installation erstellt werden.

Sie können sich den Assistenten Remote-Installation (s. Pkt. 4.2 auf S. 76) zum Erstellen eines Gruppentasks oder eines Globaltask zu Nutze machen.

Der von Ihnen erstellte Task wird entsprechend seinem Zeitplan zur Ausführung gestartet. Die Parameter für die Anwendung werden auf jedem Client-Computer je nach Richtlinie der Gruppe und Standardeinstellungen dieses Programms aktiviert.

Sie können den Installationsvorgang unterbrechen, indem Sie die Taskausführung manuelle anhalten.

Alle für einen Administrationsserver erstellten Installationspakete liegen in der Konsolenstruktur in einem speziellen Container im Element **Remote-Installation**. Auf dem Administrationsserver werden die Installationspakete im angegebenen freigegebenen Ordner im Dienstverzeichnis **Packages** aufbewahrt.

Sie können die Eigenschaften des Installationspaketes anzeigen, dessen Namen ändern und im Dialogfenster **Eigenschaften: <Paketname>** (s. Abb. 20) ändern. Dieses Fenster öffnet sich mit einem Klick auf den Eintrag **Eigenschaften** im Kontextmenü oder auf den analog lautenden Eintrag im Menü **Aktion**.

Die erstellten Installationspakete können mit Hilfe von Update-Agenten auf untergeordnete Administrationsserver verbreitet werden (s. Pkt. 4.1.4 auf S. 53) sowie auf Computer innerhalb der Gruppe (s. Pkt. 4.1.6 auf S. 55).

Das gleiche Installationspaket kann mehrfach zum Erstellen von Tasks für Remote-Installation verwendet werden.

Die Installation kann auch im Hintergrund (Silent-Modus) durchgeführt werden.

4.1.1. Erstellen eines Installationspakets

Um ein Installationspaket zu erstellen:

1. Stellen Sie eine Verbindung zu dem gewünschten Administrationsserver her.
2. Wählen in der Konsolenstruktur das Element **Remote-Installation** aus. Öffnen Sie das Kontextmenü und verwenden Sie den Befehl **Neu / Installationspaket** oder den entsprechenden Punkt im Menü **Aktion**. Dadurch wird der Assistent gestartet. Folgen Sie den Anweisungen.
3. Sie werden aufgefordert, den Namen des Installationspakets festzulegen und im nächsten Schritt die zu installierende Anwendung anzugeben (s. Abb. 17).

Wenn Sie eine Anwendung installieren, für die die Option Remote-Installation über Kaspersky Administration Kit vorgesehen ist, wählen Sie aus der Dropdown-Liste die Variante **Installationspaket für Kaspersky-Lab-Anwendung erstellen** aus. Mit Hilfe der Schaltfläche **Durchsuchen** wählen Sie die Datei mit der Beschreibung der Anwendung (die Datei besitzt die Dateinamenserweiterung **.kpd** und gehört zum Lieferumfang der Distribution aller Anwendungen des Herstellers, für die eine Remote-Verwaltung über Kaspersky Administration Kit vorgesehen ist) und das selbstentpackende Archiv der Kaspersky-Lab-Anwendung aus. Dadurch werden die Felder Anwendung und Versionsnummer automatisch belegt.

Die Einstellungen des Installationspakets werden standardmäßig festgelegt und entsprechen der Anwendung, die zur Installation ausgewählt wurde. Die Einstellungen können nach der Paketerstellung im Fenster zur Ansicht der Eigenschaften geändert werden (s. Pkt. 4.1.2 auf S. 45).

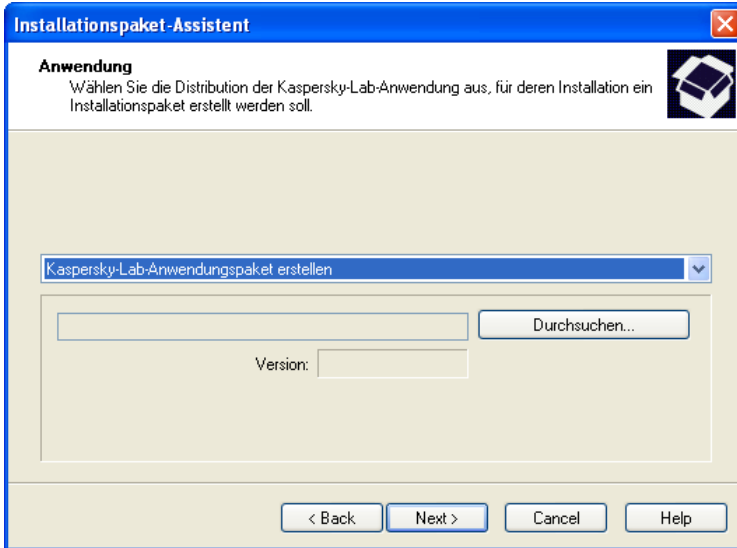


Abbildung 17. Erstellen eines Installationspaketes. Zu installierende Anwendung auswählen

Wenn Sie ein Installationspaket für andere Anwendungen erstellen, (s. Abb. 18):

- wählen Sie aus der Dropdown-Liste aus: Installationspaket für vom Benutzer angegebene Anwendung erstellen
- geben Sie den Pfad zur Distribution des Programms mit Hilfe der Schaltfläche **Durchsuchen** ein
- setzen Sie das Häkchen in **Ganzes Verzeichnis in Installationspaket kopieren**, wenn im Paket der Inhalt des ganzen Verzeichnisses stehen muss, in dem die Installationsdatei liegt
- geben Sie die Parameter für den Start der ausführbaren Datei in die Eingabezeile, wenn sie für die Installation der Anwendung gebraucht wird (beispielsweise Start im Silent-Modus mit Hilfe der Option **/s**)

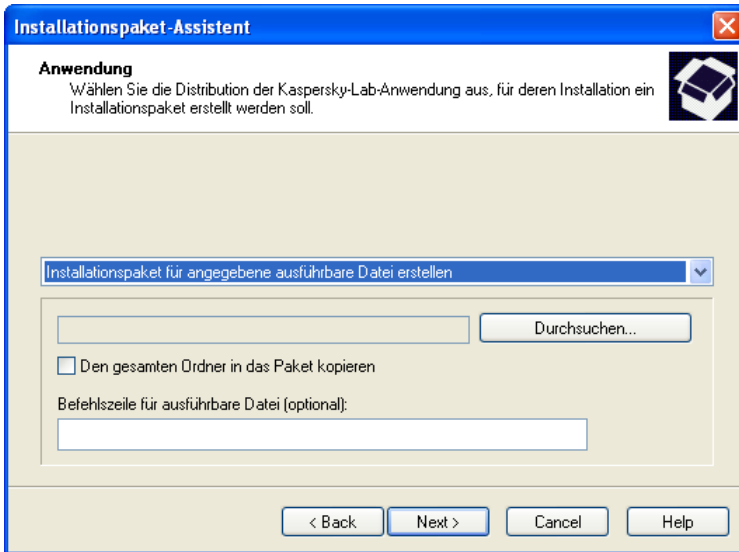


Abbildung 18. Erstellen eines Installationspaketes für eine vom Benutzer angegebene Anwendung

4. Im folgenden Fenster des Assistenten (s. Abb. 19) können Sie den Lizenzschlüssel angeben, der zu dem Installationspaket gehören soll. Klicken Sie dazu auf **Durchsuchen...** und wählen Sie die gewünschte Lizenzschlüsseldatei (mit der Dateinamenserweiterung **.key**).

Wenn Sie keinen Lizenzschlüssel in das Installationspaket einschließen möchten, klicken Sie einfach auf **Weiter**.

Beim Erstellen des Installationspaketes für Administrationsserver und Administrationsagenten muss kein Lizenzschlüssel angegeben werden.

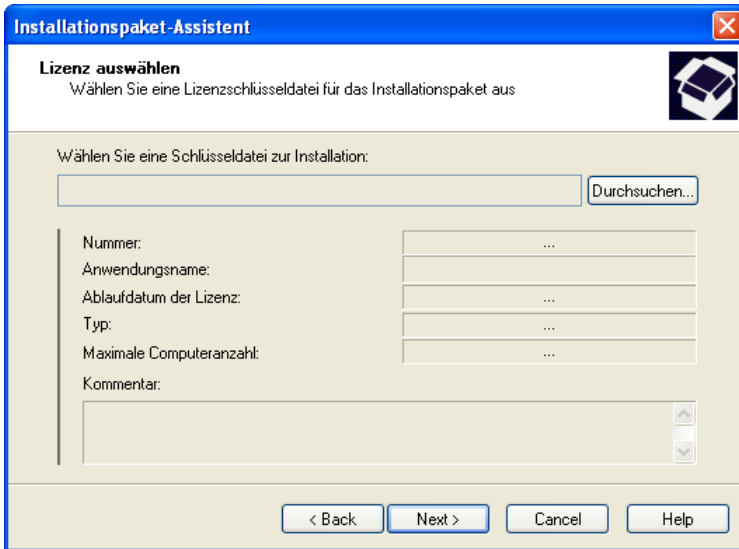


Abbildung 19. Installationspaket erstellen. Auswahl des Lizenzschlüssels

5. Danach werden die Dateien, die zur Installation der ausgewählten Anwendung auf die Client-Computer erforderlich sind, auf den Administrationsserver in den gemeinsamen Ordner geladen und es wird überprüft, ob am Arbeitsplatz des Administrators das Verwaltungs-PlugIn der ausgewählten Anwendung vorhanden ist. Wenn das Plug-In nicht installiert ist oder eine ältere Version aufweist als die in der Distribution vorhandene, dann wird es installiert oder ersetzt.

Nach dem Abschluss des Assistenten wird das erstellte Installationspaket dem Element **Remote-Installation** hinzugefügt und im Detailfenster angezeigt.

4.1.2. Anzeigen und Einstellen der Parameter für ein Installationspaket

Um die Eigenschaften eines Installationspaketes anzuzeigen, den Namen oder die Einstellungen zu ändern:

Öffnen Sie in der Konsolenstruktur das Element **Remote-Installation**, wählen Sie im Detailsfenster das gewünschte Installationspaket aus und klicken Sie auf **Eigenschaften** im Kontextmenü oder auf den analog lautenden Eintrag im Menü **Aktion**.

Es öffnet sich daraufhin das Fenster **Eigenschaften <Name des Installationspaketes>** (s. Abb. 20), das aus den Registerkarten **Allgemein**, **Einstellungen**, **Lizenzdaten** und **Neustart des BS** besteht.

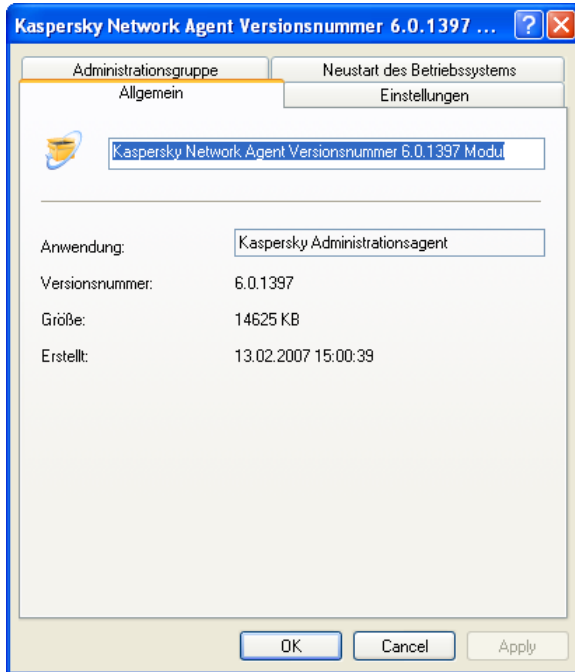


Abbildung 20. Fenster zur Ansicht der Eigenschaften eines Installationspaketes.
Registerkarte **Allgemein**

Die Registerkarte **Allgemein** (s. Abb. 20) enthält die folgenden allgemeinen Informationen zum Paket:

- Paketname
- Name und Version der Anwendung, für deren Installation das Paket erstellt wurde
- Paketgröße
- Erstellungsdatum

Die Registerkarte **Einstellungen** (s. Abb. 21) enthält die Einstellungen des Installationspakets, die der Anwendung entsprechen, für deren Installation das Paket erstellt wurde. Diese

Einstellungen werden beim Erstellen des Pakets standardmäßig festgelegt und können bei Bedarf geändert werden.

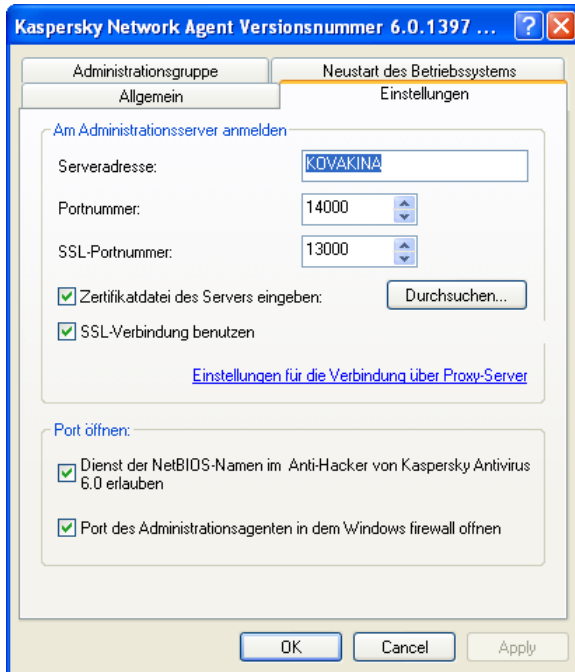


Abbildung 21. Fenster zur Ansicht der Eigenschaften des Installationspakets.
Registerkarte **Einstellungen**

Die Registerkarte **Lizenzdaten** (s. Abb. 22) enthält generelle Informationen über die Lizenz, die der Anwendung entspricht, für welche ein Installationspakete erstellt wird.

Die Registerkarte Lizenzdaten fehlt in den Eigenschaften des Installationspaketes für den Administrationsagenten und Administrationsserver.

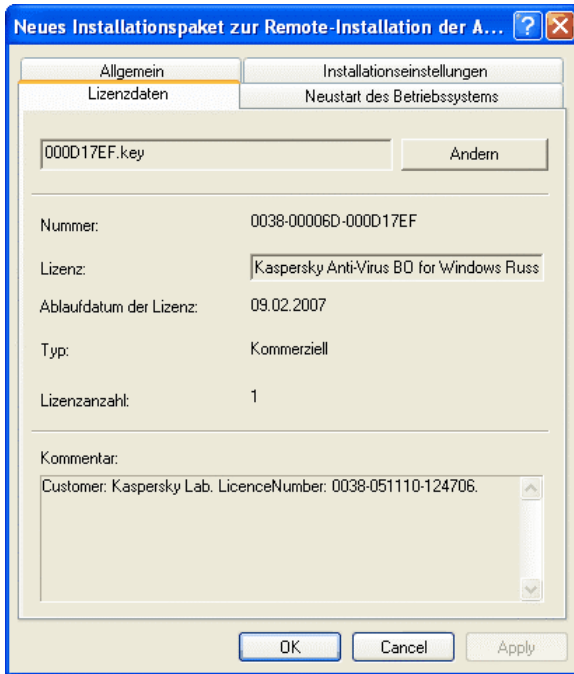


Abbildung 22. Fenster zur Ansicht der Eigenschaften des Installationspakets.
Registerkarte **Lizenzdaten**

Auf der Registerkarte **Neustart des BS** (s. Abb. 23) können Sie Aktionen bestimmen, die durchgeführt werden müssen, wenn nach Installation der Anwendung ein Neustart des Computers gefordert wird. Sie können sich für eine Variante entscheiden:

- **Betriebssystem nicht neu starten.**
- **Bei Bedarf Betriebssystem automatisch neu starten** - dabei wird das Betriebssystem nur dann neu gestartet, wenn es notwendig ist.
- **Benutzer fragen** – Sollten Sie diesen Punkt wählen, können Sie folgendes tun:
 - Informative Meldung erstellen, mit der der Benutzer benachrichtigt wird, dass das Betriebssystem neu gestartet werden muss, und zwar mit dem vorhandenen Eingabefeld
 - Häufigkeit der Benachrichtigung für den benötigten Neustart aktivieren, indem das Häkchen in **Benutzer fragen jede (Min.)** gesetzt und der Intervall angegeben wird

- Automatischen Neustart des Betriebssystems eingeben, wenn er nicht vom Benutzer nach Ablauf eines eingegebenen Zeitintervalls erfolgt, beginnend mit der Installation des Programms. Setzen Sie dazu das Häkchen in **Neustart erzwingen in (Min.)** und geben Sie die Länge des Zeitintervalls an.

Wenn Sie wollen, dass die gesperrten Arbeitsstationen neu gestartet werden, aktivieren Sie das Häkchen **Laufende Anwendungen automatisch schließen**. Standardmäßig ist das Häkchen nicht aktiviert.

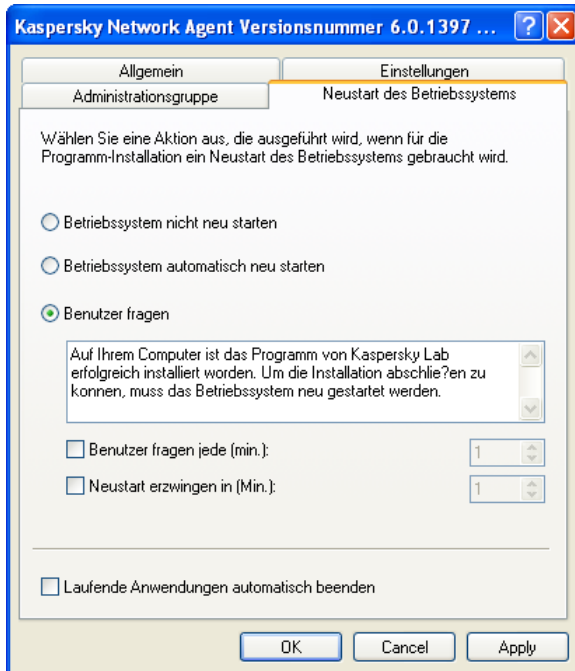


Abbildung 23. Fenster zur Ansicht der Eigenschaften des Installationspaketes.
Registerkarte **Neustart des BS**

4.1.3. Erstellen und Einstellen des Installationspaketes für Administrationsagenten

Das Installationspaket für die Remote-Installation des Administrationsagenten muss nicht manuell angelegt werden. Es wird automatisch bei der Installation der

Anwendung Kaspersky Administration Kit erstellt und befindet sich im Element **Remote-Installation**.

Wenn ein Remote-Installationspaket des Administrationsagenten gelöscht wurde, muss für seine erneute Erstellung als Beschreibungsdatei die Datei **klagent.kpd** gewählt werden, die sich im Ordner **NetAgent** des Distributionspakets Kaspersky Administration Kit befindet.

In den Einstellungen des Installationspakets für den Administrationsagenten sind die Minimalvorgaben gesetzt, die für die Funktionsfähigkeit der Komponente unmittelbar nach dessen Installation gebraucht werden. Der Wert der Parameter entspricht den standardmäßigen Anwendungseinstellungen. Bei Bedarf können Sie sie auf der Registerkarte **Einstellungen** und **Administrationsgruppe** im Fenster Anzeige der Eigenschaften des Installationspakets ändern (s. Abb. 21).

In der Registerkarte **Einstellung** (s. Abb. 21) sehen Sie die Parameter, mit denen der Agent nach der Installation auf den Client-Computern die Verbindung zum Administrationsserver aufbaut (standardmäßig werden beim Erstellen die Werte des aktuellen Servers benutzt):

- Adresse des Computers, auf dem der Administrationsserver installiert ist
- Nummer des Ports, über den die Verbindung des Agenten mit dem Administrationsserver erfolgt. Standardmäßig wird Port **14000** verwendet. Wenn dieser Port belegt ist, kann ein anderer Wert gewählt werden.
- Nummer des Ports, über den die geschützte Verbindung unter Verwendung des SSL-Protokolls erfolgt. Standardmäßig wird Port **13000** verwendet.

Für die Angabe der Portnummer ist nur die Dezimalform zulässig.

- Zertifikatsdatei für die Authentifizierung am Administrationsserver. Den Wert dieses Parameters bestimmt das Kontrollkästchen **Serverzertifikat verwenden**.

Wenn das Kontrollkästchen nicht aktiviert ist (Standard), wird die Zertifikatsdatei automatisch vom Administrationsserver beim ersten Verbindungsaufbau mit dem Agenten bezogen.

Wenn das Kontrollkästchen **Serverzertifikat verwenden** aktiviert ist, erfolgt die Authentifizierung anhand der Zertifikatsdatei, die mit einem Klick auf **Durchsuchen** vorgegeben wird. Diese Datei hat die Erweiterung **.cer** befindet sich auf dem Administrationsserver im Verzeichnis **Cert** des Installationsordners von Kaspersky Administration Kit. Sie können die Zertifikatsdatei ändern, indem Sie die gewünschte Datei mit einem Klick auf **Durchsuchen** auswählen.

- Art des Ports für die Verbindung von Administrationsagent und Server: einfach oder gesichert. Den Wert dieses Parameters bestimmt das Kontrollkästchen **SSL-Verbindung verwenden**. Wenn das

Kontrollkästchen aktiviert ist, erfolgt die Verbindung über einen gesicherten Port mit dem SSL-Protokoll. Ist das Kontrollkästchen nicht aktiv, erfolgt die Verbindung ungeschützt.

- Einstellungen für die Verbindung mit dem Proxyserver. Wenn für die Verbindung von Administrationsagent und Server ein Proxyserver verwendet wird, setzen Sie das Häkchen im Kontrollkästchen **Proxyserver verwenden**. Klicken Sie dann auf die Schaltfläche **Parameter** und im sich öffnenden Fenster geben Sie die Adresse des Proxyservers, den Benutzernamen und das Kennwort ein.
- Das Öffnen des UDP-Ports 137, welcher zum Ablesen der IP-Adresse des Administrationsserver benutzt wird, in dem Anti-Hacker von Kaspersky Antivirus 6.0. Dazu setzen Sie Häkchen **Namendienst NetBIOS in dem Anti-Hacker von Kaspersky Antivirus 6.0 erlauben**.
- UDP-Port hinzufügen, welcher für die Arbeit von Administrationsagenten notwendig ist, in die Ausnahmeliste des Firewalls von Microsoft Windows. Dazu setzen Sie Häkchen neben **Ports für Administrationsagenten in dem Microsoft Windows Firewall öffnen**.

Nach der Installation des Administrationsagenten können Sie den Wert der Parameter für die Verbindung zum Administrationsserver über die Richtlinie und die Anwendungseinstellungen ändern.

Bei einer erneuten Remote-Installation des Administrationsagenten auf dem Client-Computer werden die Werte der Verbindungseinstellungen zum Server und das Zertifikat des Administrationsservers durch neue Werte ersetzt.

In der Registerkarte **Administrationsgruppe** (s. Abb. 24) wird die Untergruppe der Gruppe **Netzwerk** festgelegt, zu der Computer nach Installation des Administrationsagenten auf diesen Rechnern hinzugefügt werden. Sie können zwischen den beiden folgenden Varianten auswählen:

- Computer in Ordner hinzufügen, **die der Stellung des Computers im Windows-Netzwerk entsprechen**: zur Domäne oder Arbeitsgruppe (standardmäßig)
- Alle Computer **In die Gruppe** einfügen, die in das Eingabefeld eingetragen worden sind. Wenn Sie sich für diese Variante entscheiden, geben Sie den Namen des Ordners im unten stehenden Feld ein. Wenn es in der Gruppe **Netzwerk** diesen Ordner nicht gibt, wird er angelegt (Sie können auch einen beliebigen Namen von dem in der Gruppe **Netzwerk** vorhandenen Ordner angeben).

In den vorgegebenen Ordner werden alle im Netzwerk erkannte Computer verschoben, auch wenn vor der Installation des Administrationsagenten der Computer von dem Administrationsserver erkannt und in einen Ordner verschoben wurde.

Nach Installation des Administrationsagenten können Sie den Ordner für das Verschieben von Computer in die Gruppe **Netzwerk** ändern. Dieser Parameter gehört nicht zu den Richtlinien und Anwendungseinstellungen.

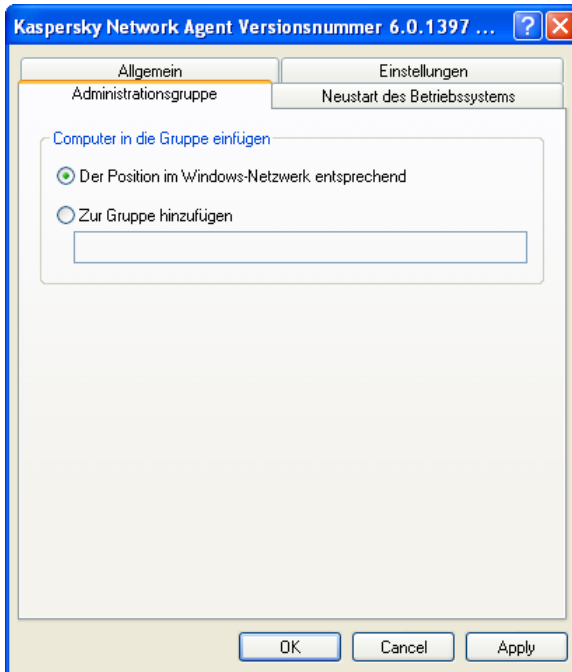


Abbildung 24. Fenster der Eigenschaften des Installationspakets für den Administrationsagenten. Registerkarte **Administrationsgruppe**

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

- mit dem Namen des Dienstes (**KLNAgent**)
- mit dem angezeigten Namen **Kaspersky Network Agent**
- mit automatischem Task-Start beim Starten des Betriebssystems
- unter der Registrierung **Lokales System**

Sie können die Eigenschaften des Dienstes **Kaspersky Network Agent** anzeigen, ihn starten, beenden und verfolgen, indem Sie die Standardmittel für das Administrieren in Windows **Systemsteuerung / Dienste** verwenden.

4.1.4. Erstellen und Einstellen des Installationspakets für einen Administrationsserver

Beim Erstellen eines Installationspakets für den Administrationsserver als einer Datei, müssen Sie die Datei **ak6.kpd** auswählen, welche sich in dem Hauptverzeichnis des Kaspersky Administration Kit Distributives befindet.

Die Einstellungen des Installationspakets für den Administrationsserver sind mit zwei Registerkarten dargestellt: **Allgemein** (s. Abb. 20) und **Betriebssystem neu starten** (s. Abb. 23). Alle anderen Einstellungen entsprechen den standardmäßigen Einstellungen des Administrationsserver.

4.1.5. Erstellen des Tasks Verbreitung eines Installationspaketes auf untergeordnete Administrationsserver

Um einen Task Verbreitung eines Installationspaketes auf untergeordnete Administrationsserver zu erstellen, tun Sie Folgendes:

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur das Element Globale Tasks aus, öffnen Sie das Kontextmenü und gehen Sie auf den Eintrag **Neu → Task** oder auf den analog lautenden Punkt im Menü **Aktion**. Es öffnet sich ein Assistent, dessen Anweisungen Sie folgen.
3. Für die Anwendung Kaspersky Administration Kit wählen Sie den Tasktyp **Verbreitung eines Installationspaketes** aus.
4. Im folgenden Fenster des Assistenten (s. Abb. 25) geben Sie an, welche Installationspakete verbreitet werden sollen. Entscheiden Sie sich für eine Variante:
 - **Alle Installationspakete**
 - **Ausgewählte Installationspakete**. In diesem Fall setzen Sie in der unten stehenden Tabelle die Häkchen neben den Namen der gewünschten Installationspakete.

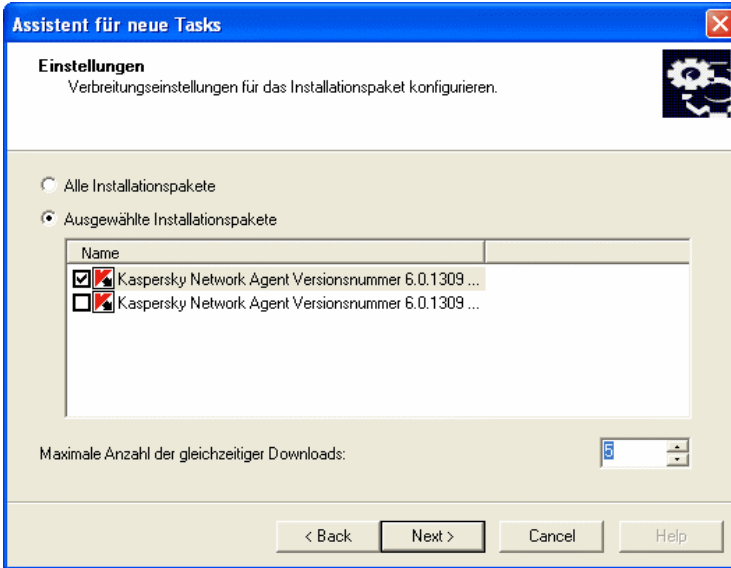


Abbildung 25. Installationspaket zusammenstellen

Im Feld **Maximale Anzahl der gleichzeitigen Downloads** geben Sie den gewünschten Wert ein.

5. Im folgenden Fenster des Assistenten (s. Abb. 26) setzen Sie die Häkchen in die Kontrollkästchen mit den Namen der untergeordneten Administrationsserver, auf die die Installationspakete verbreitet werden.
6. Im folgenden Fenster des Assistenten geben Sie einen Zeitplan für den Task-Start an (Details s. Pkt. 0 auf S. 58).
7. Zum Beenden des Assistenten klicken Sie auf die Schaltfläche **Fertig**.

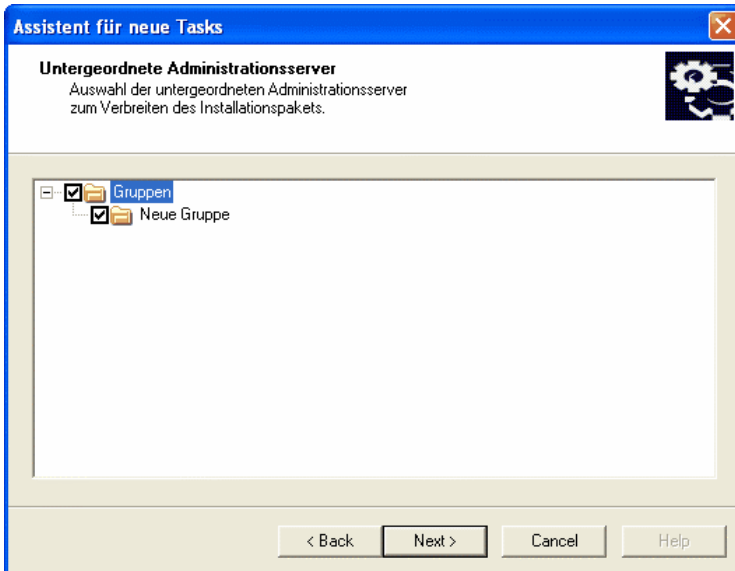


Abbildung 26. Untergeordnete Administrationsserver auswählen

4.1.6. Verbreitung von Installationspaketen innerhalb einer Gruppe mit Administrationsagenten

Zur Verbreitung von Installationspaketen innerhalb einer Gruppe lassen sich Update-Agenten einsetzen. Update-Agenten empfangen Installationspakete und Updates vom Administrationsserver und speichern sie im Installationsverzeichnis der Kaspersky-Lab-Anwendung.

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

Im Weiteren werden die Installationspakete auf die Client-Computer mit einem Mehrfach-Adressen-Versand verbreitet. Der Versand von neuen Installationspaketen innerhalb einer Gruppe erfolgt einmal. Wenn zum Versandzeitpunkt der Computer im logischen Netzwerk des Unternehmens ausgeschaltet war, dann lädt beim Start des Installationstasks der Administrationsagent automatisch das gewünschte Installationspaket vom Update-Agenten.

Um eine Liste mit Update-Agenten zu erstellen und sie für die Verbreitung von Installationspaketen auf Computern innerhalb einer Gruppe einzustellen, tun Sie Folgendes:

1. Stellen Sie eine Verbindung mit dem gewünschten Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur die gewünschte Gruppe, öffnen Sie das Kontextmenü und gehen Sie auf den Eintrag **Eigenschaften** oder klicken Sie auf den analog lautenden Befehl im Menü **Aktion**.
3. Im Eigenschaftenfenster der Gruppe erstellen Sie auf der Registerkarte **Update-Agent** (s. Abb. 27) mit den Schaltflächen **Hinzufügen** und **Löschen** eine Liste mit Rechnern, die die Rolle von Update-Agenten innerhalb einer Gruppe übernehmen.

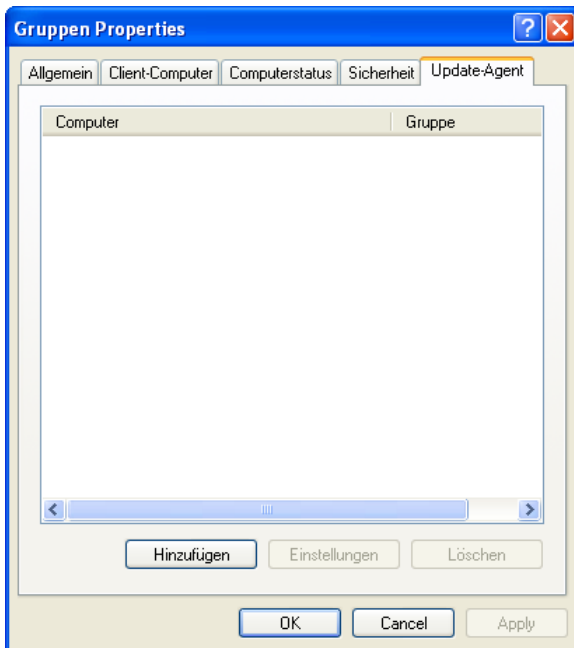


Abbildung 27. Fenster Eigenschaften der Gruppe.
Registerkarte **Update-Agenten**

4. Bearbeiten Sie die Einstellungen des Update-Agenten. Wählen Sie dazu einen Agenten in der Liste aus und klicken Sie auf die Schaltfläche **Eigenschaften**. Im sich öffnenden Fenster **<Name des Update-Agenten> Eigenschaften** (s. Abb. 28) tun Sie Folgendes:

- Geben Sie die Nummer des Ports an, über den Client-Computer und Update-Agent miteinander verbunden werden. Standardmäßig gilt der Port **14001**, wenn er belegt ist, können Sie ihn ändern.
- Geben Sie die Nummer des Ports an, mit dem eine gesicherte Verbindung von Client-Computer und Update-Agent mit dem SSL-Protokoll hergestellt wird. Standardmäßig gilt der Port **13001**.
- Setzen Sie das Häkchen im Kontrollkästchen **Multiples-IP-Versand benutzen** und befüllen Sie die Felder **IP-Versand-Adresse** und **Portnummer des IP-Versands**.

Klicken Sie auf die Schaltfläche **Übernehmen** oder **OK**.

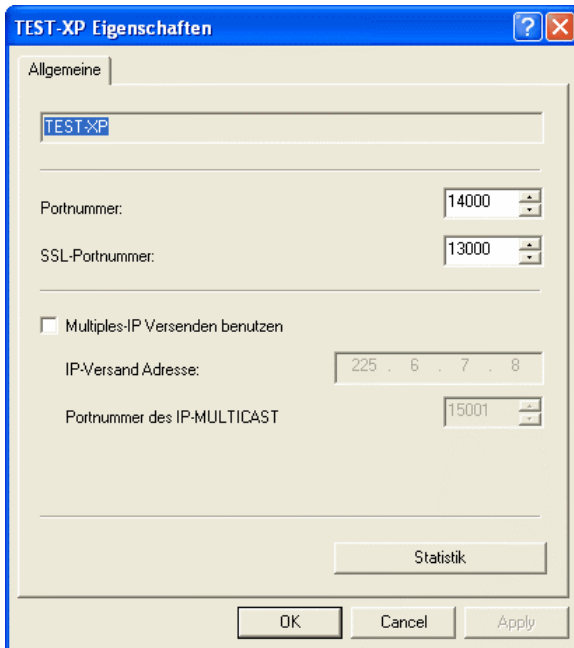


Abbildung 28. Fenster Eigenschaften des Update-Agenten

4.1.7. Erstellen des Tasks Remote-Installation

Bei der Taskausführung erfolgt die Remote-Installation von Programmen auf einen Client-Computer durch eine der folgenden Methoden: **Push-Installation** oder **Installation mit Startskript**.

Die **Push-Installation** erlaubt die entfernte Programminstallation auf konkreten Client-Computern des logischen Netzwerks. Der Administrationsserver kopiert beim Task-Start eine Auswahl von Dateien für die Anwendungsinstallation aus dem gemeinsamen Ordner in einen temporären Ordner jedes Client-Computers und nimmt auf jedem Computer den Start des Installationsprogramms vor. Zur erfolgreichen Taskausführung mit der Push-Installationsmethode muss der Administrationsserver über die Rechte für den entfernten Start von Anwendungen auf den Client-Computern des logischen Netzwerks verfügen. Empfehlenswert ist diese Methode zur Anwendungsinstallation auf Computer, die unter den Betriebssystemen Microsoft Windows NT/2000/2003/XP arbeiten, in denen diese Option unterstützt wird, oder auf Computer unter Microsoft Windows 98/Me, auf denen der Administrationsagent installiert ist.

Wenn die Verbindung zwischen Administrationsserver und Client-Computer über das Internet erfolgt oder durch eine Firewall geschützt wird, kann der gemeinsame Ordner nicht zur Datenübertragung verwendet werden. In diesem Fall können die zur Anwendungsinstallation nötigen Dateien durch den Administrationsagenten auf den Client-Computer übertragen werden. Die Installation des Administrationsagenten auf solche Computer erfolgt lokal.

Die zweite Methode, die **Installation mit Startskript**, erlaubt es, den Start eines Remote-Installationstasks an das konkrete Konto eines Benutzers (mehrerer Benutzer) zu binden. Entsprechend dem Task-Zeitplan wird in den Startskripts für die festgelegten Benutzer ein Eintrag über den Start des Installationsprogramms, das sich im gemeinsamen Ordner des Administrationsservers befindet, vorgenommen. Zum erfolgreichen Task-Start muss der Administrationsserver über das Recht zum Ändern von Startskripts in der Datenbank des Domänen Controllers verfügen. Als Ergebnis wird bei der Anmeldung des Benutzers an der Domäne 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 Microsoft Windows 95/98/Me arbeiten.

Damit der Task Remote-Installation mit Startscenario und Benutzeraufruf erfolgreich ausgeführt wird, für den das Szenario geändert werden soll, müssen auf dessen Computer die Berechtigungen des lokalen Administrators vorhanden sein.

Die Gruppentasks Remote-Installation für die Anwendung werden auf Client-Computern nur mit der Push-Installation ausgeführt. Beim Erstellen eines globalen Tasks können Sie die gewünschte Methode auswählen: Push-Installation oder Installation mit Startskript.

Um einen globalen Task Remote-Installation mit der Push-Installation zu erstellen, tun Sie Folgendes:

1. Stellen Sie eine Verbindung zum Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur das Element **Globale Tasks** aus, öffnen Sie das Kontextmenü und gehen Sie auf den Eintrag **Neu / Task** oder klicken Sie auf den analog lautenden Eintrag im Menü **Aktion**. Es öffnet sich daraufhin der Assistent für das Erstellen eines Tasks. Folgen Sie den Anweisungen.
3. Bestimmen Sie den Typ des Tasks.
4. Bei der Entscheidung für die Anwendung und beim Festlegen des Tasktyps (s. Abb. 29) aktivieren Sie jeweils die Werte **Kaspersky Administration Kit** und **Remote-Installation der Anwendung (Task zur Productinstallation)**.

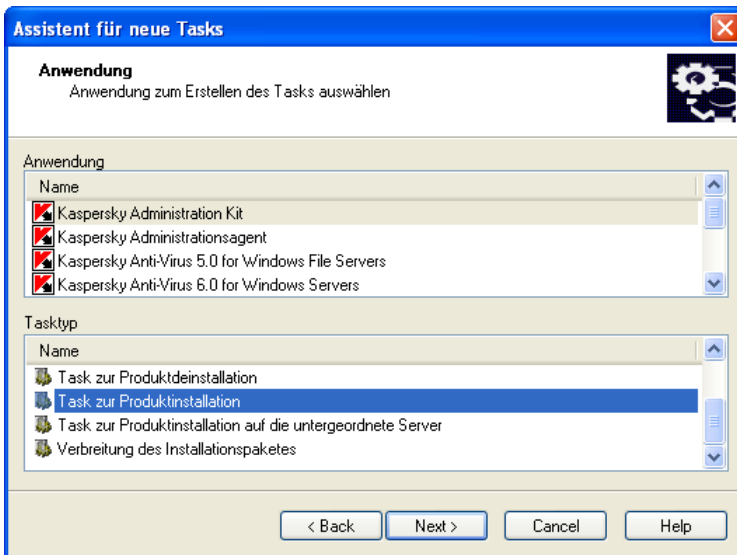


Abbildung 29. Bestimmen des Tasktyps

5. Geben Sie dann das Installationspaket an, dessen Installation bei der Ausführung dieses Tasks erfolgt (s. Abb. 30). Wählen Sie ein Installationspaket zur Installation aus, das für diesen

Administrationsserver angelegt wurde, oder erstellen Sie ein neues Paket mit Hilfe von **Neu...**

Einige Anwendungen, deren Steuerung mit Kaspersky Administration Kit erfolgt, können auf den Rechnern nur lokal installiert werden. Nähere Informationen finden Sie in den Handbüchern für die jeweilige Anwendung.

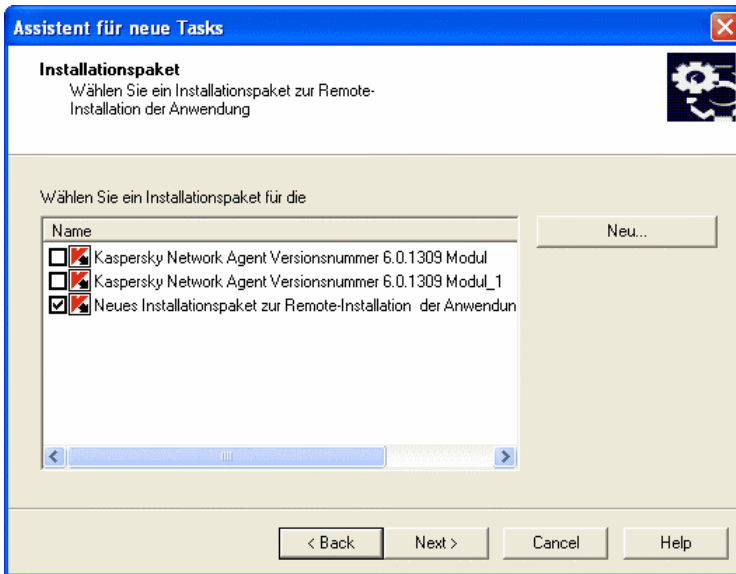


Abbildung 30. Installationspaket für Installation auswählen

- In diesem Schritt wählen Sie die Variante **Installation Erzwingen** (s. Abb. 31) aus.

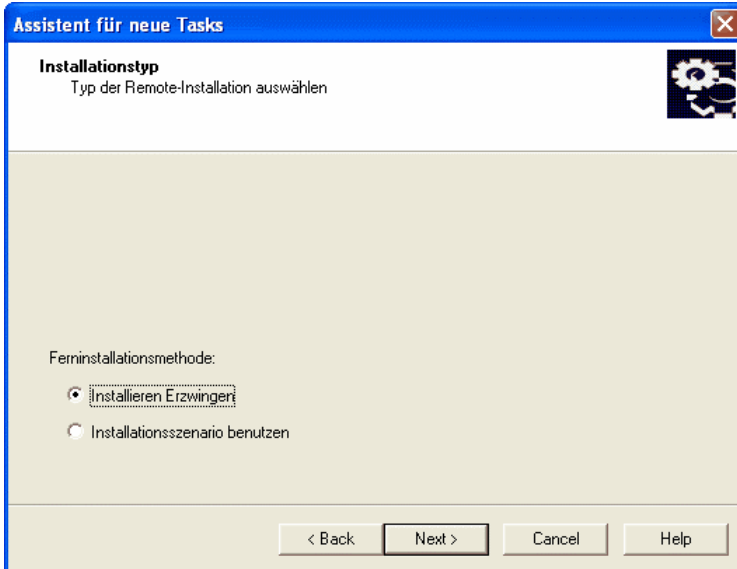


Abbildung 31. Installationsmethode auswählen

7. In diesem Fenster des Assistenten (s. Abb. 32) wird vorgeschlagen, zusätzliche Parameter für die Installation einzugeben:

- Muss die Anwendung noch einmal installiert werden, wenn es bereits auf dem Rechner vorhanden ist.

Aktivieren Sie das Kontrollkästchen **Anwendung nicht installieren, wenn sie schon installiert ist**, damit keine wiederholte Installation einer Anwendung auf Computern erfolgt (dieses Kontrollkästchen ist standardmäßig aktiviert). In diesem Fall wird auf den Computern, auf denen die Anwendung bereits lokal installiert ist bzw. auf denen wegen eines vorangegangenen Start des Tasks Remote-Installation nach Zeitplan die Anwendung bereits vorhanden ist, der Task nicht aufgerufen.

Wenn das Kontrollkästchen deaktiviert ist, wird der Task Remote-Installation solange nach Zeitplan gestartet, bis die Anzahl der Installationsversuche erreicht ist.

- Geben Sie ein, wie die für die Installation der Anwendungen benötigten Dateien auf die Client-Computer kommen sollen.

Sie müssen dazu in der Feldergruppe **Installationspakets herunterladen** Entscheidungen treffen:

- Aktivieren Sie das Kontrollkästchen **Mittels Microsoft Windows asu dem Gemeinsamem Ordner**, damit die Übertragung der für die Anwendungsinstallation erforderlichen Programmdateien auf die Client-Computer mit Windows-Mitteln über den gemeinsamen Ordner erfolgt (dieses Kontrollkästchen ist standardmäßig aktiviert)
- Aktivieren Sie das Kontrollkästchen **Mit Hilfe des Administrationsagenten**, damit die Übertragung der Dateien auf die Client-Computer durch den auf jedem Computer installierten Administrationsagenten erfolgt (dieses Kontrollkästchen ist standardmäßig aktiviert).
- Geben Sie im Feld **Maximale Downloads-Anzahl** die maximale Anzahl der Client-Computer an, die gleichzeitig Daten vom Administrationsserver herunterladen können.
- Geben Sie im Feld **Anzahl der Versuche** die Anzahl der Versuche an, die beim zeitgesteuerten Task-Start zur Anwendungsinstallation unternommen werden soll. Ein erneuter Versuch wird unternommen, wenn während der Ausführung der vorhergehenden Installation Fehler auftreten.

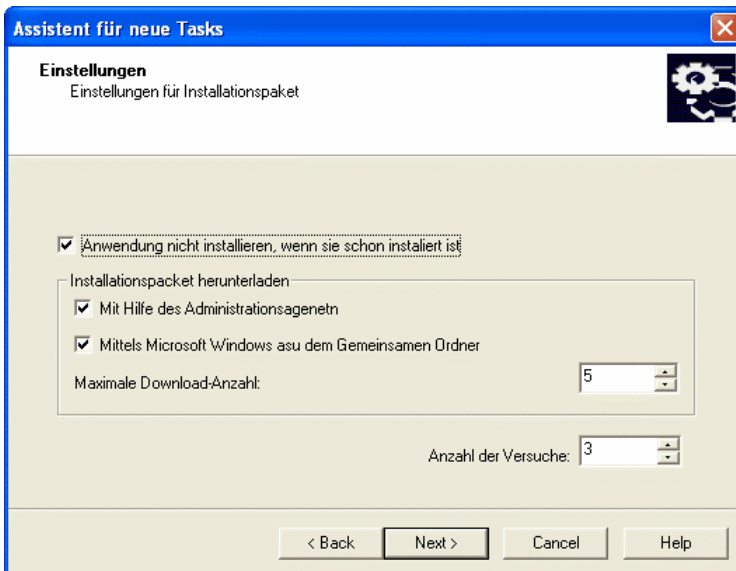


Abbildung 32. Zusätzliche Parameter für Installation

8. In diesem Schritt (s. Abb. 33) sollen Sie entscheiden, ob zusammen mit der Anwendung der Administrationsagent installiert werden soll.

Wir empfehlen Ihnen die gemeinsame Installation, um die Belastung des Administrationservers gering zu halten. Aktivieren Sie dazu das Kontrollkästchen **Kaspersky Network Agent Paket installieren** und aktivieren Sie das Kontrollkästchen neben dem Name des gewünschten Installationspaketes. Bei Bedarf erstellen Sie ein neues Installationspaket mit Hilfe der Schaltfläche **Neu**.

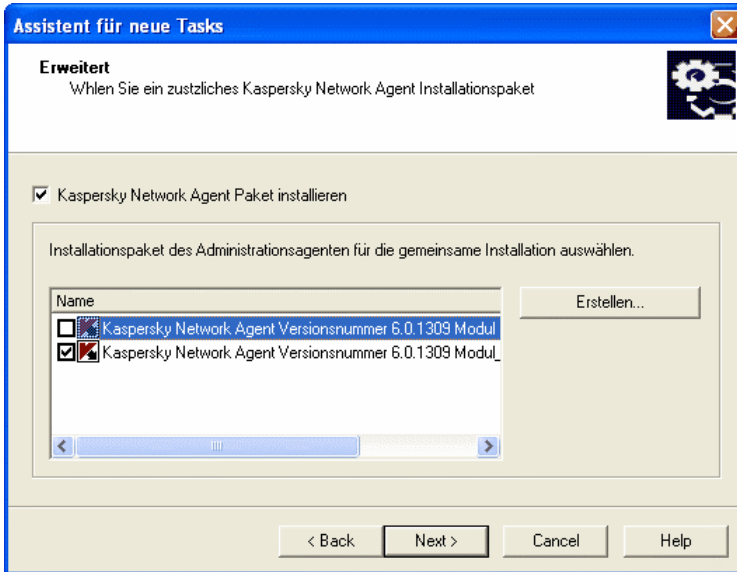


Abbildung 33. Gemeinsame Installation mit Administrationsagenten auswählen

9. Bestimmen Sie, wie die Komponenten ausgewählt werden, für die der Task erstellt wird (s. Abb. 34):
 - **Auf Basis von Daten, die sich aus dem Windows-Netzwerk ergeben.** In diesem Fall erfolgt die Auswahl der Client-Computer anhand von Daten, die sich beim Durchsuchen des Windows-Unternehmensnetzwerks durch den Administrationsserver ergeben
 - **Auf Basis von manuell einzugebenden Computeradressen.** In diesem Fall erfolgt die Auswahl der Client-Computer für die Installation manuell.

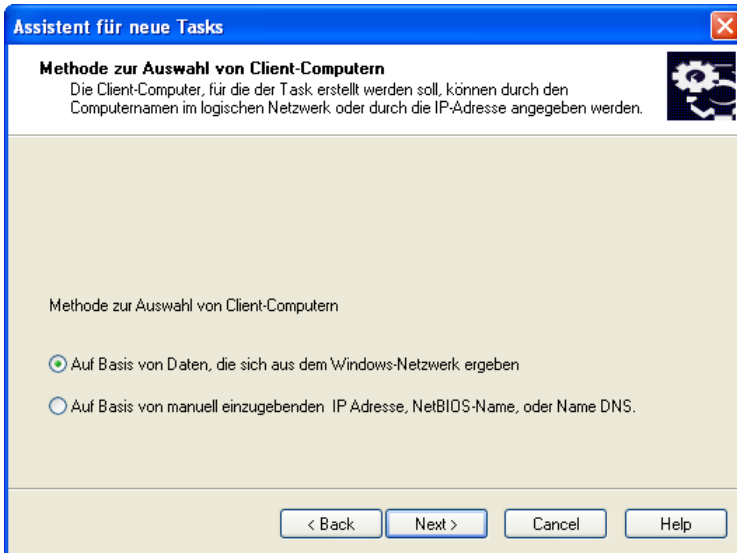


Abbildung 34. Wie Client-Computer ausgewählt werden

Wenn die Computer anhand von Daten ausgewählt werden, die beim Durchsuchen des Windows-Netzwerkes ermittelt worden sind, dann wird die Liste im Fenster des Assistenten (s. Abb. 35) erstellt und erfolgt auf die gleiche Weise, wie beim Hinzufügen von Computern in ein logisches Netzwerk (Details s. Nachschlagebuch für Kaspersky Administration Kit). Sie können Client-Computer im logischen Netzwerk (Ordner **Gruppen**) und Computer auswählen, die nicht dazu gehören (Ordner **Netzwerk**).

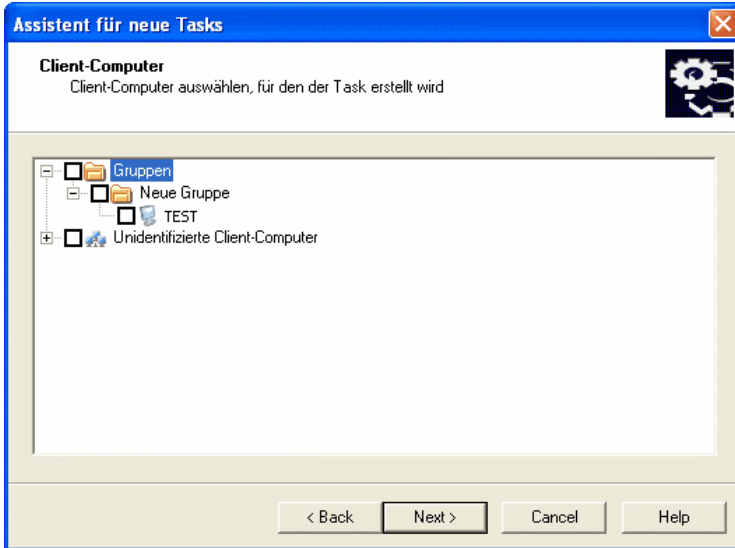


Abbildung 35. Liste mit Computern für Installation anhand der Daten aus dem Windows-Netzwerk erstellen

Wenn die Computer manuell ausgewählt werden, wird die Liste mit Hilfe eingegebener NETBIOS- oder DNS-Namen, IP-Adressen (oder Bereiche von IP-Adressen) für Computer erstellt oder es wird eine Liste aus einer *txt*-Datei importiert, in der jede Adresse in einer neuen Zeile stehen muss (s. Abb. 36).

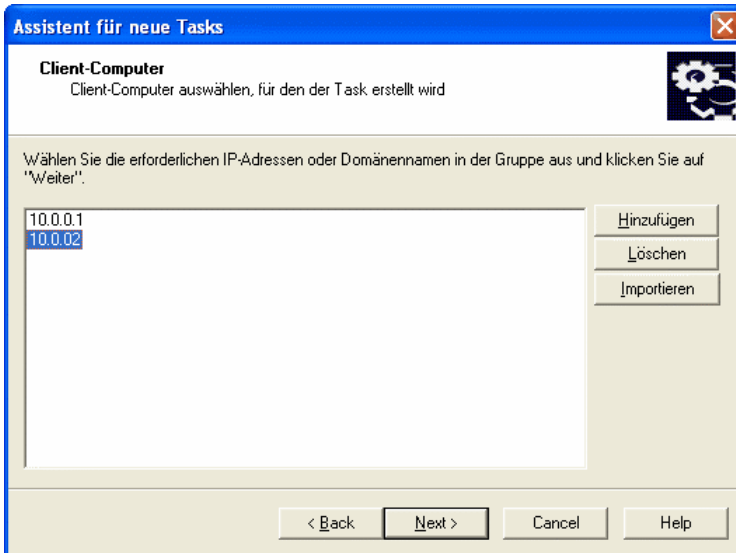


Abbildung 36. Liste mit Computern für Installation anhand von IP-Adressen erstellen

10. Geben Sie im folgenden Fenster des Assistenten an, unter welchem Benutzerkonto der Task Remote-Installation auf den Client-Computern gestartet wird (s. Abb. 37).

Das Benutzerkonto muss über Administratorrechte auf allen Client-Computern verfügen, auf denen die entfernte Installation von Programmen geplant ist.

Bei der Installation von Programmen auf Computern, die zu unterschiedlichen Domänen gehören, müssen vertrauenswürdige Beziehungen zwischen diesen Domänen und der Domäne, in welcher der Administrationsserver arbeitet, bestehen.

Wählen Sie eine der folgenden Optionen:

- **Standard-Benutzerkonto** – wenn der Administrationsserver unter dem Benutzerkonto eines Domänenbenutzers gestartet wird (s. Pkt. 3.2 auf S. 19) und das Konto über die zur Programminstallation erforderlichen Rechte verfügt.
- **Benutzerkonto festlegen** – wenn der Administrationsserver unter dem System-Benutzerkonto gestartet wird oder das Benutzerkonto des Administrationsservers nicht über Rechte zum Start eines entfernten Installationstasks verfügt.

Zur Remote-Installation der Anwendung auf Computern, die nicht zur Domäne gehören, muss der Task Remote-Installation unter dem Konto eines Benutzers gestartet werden, der über Administratorrechte für diese Computer verfügt.

Geben Sie in den unten stehenden Feldern die Attribute des Benutzers ein, dessen Konto die geforderten Bedingungen erfüllt.

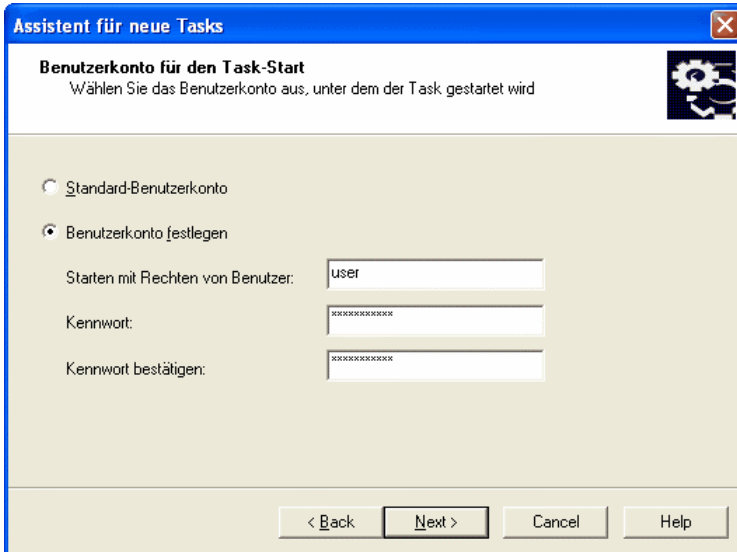


Abbildung 37. Benutzerkonto auswählen

11. Erstellen Sie nun den Zeitplan für den Task-Start (s. Abb. 38).

- Wählen Sie in der Dropdown-Liste **Start nach Zeitplan** den gewünschten Modus für den Task-Start aus:
 - **Manuell**
 - **Jede –te Stunde**
 - **Täglich**
 - **Wöchentlich**
 - **Monatlich**
 - **Einmal** – einmal (in diesem Fall wird der Task zur Remote-Installation unabhängig von den Ergebnissen der Taskausführung nur einmal auf den Client-Computern gestartet).

- **Sofort** – sofort nach dem Erstellen des Tasks (nach dem Abschluss des Assistenten).
- **Nach dem beenden eines anderen Task** (in diesem Fall wird der Remote-Installation Task erst dann gestartet, wenn vorhergegebener Task beendet wurde).
- Stellen Sie die Parameter des Zeitplans in der Feldergruppe vor, die dem gewünschten Modus entspricht (Details s. Nachschlagebuch für Kaspersky Administration Kit).

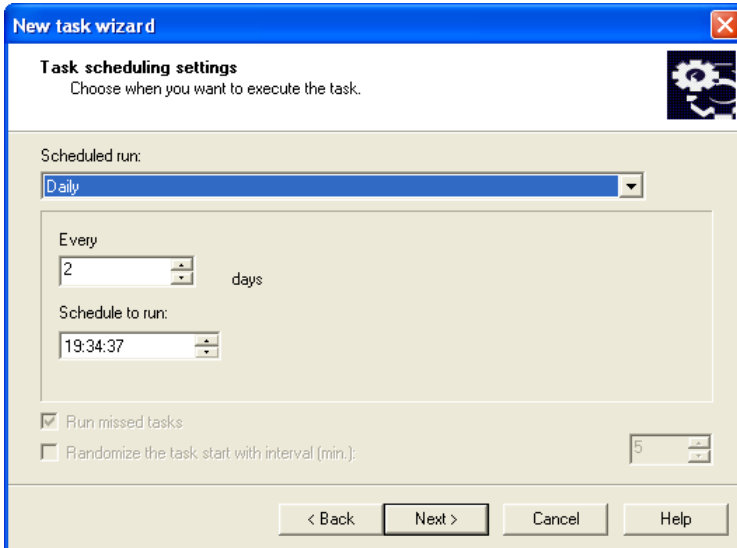


Abbildung 38. Täglicher Task-Start

Um einen globalen Task Remote-Installation mit Startscenario zu erstellen, tun Sie Folgendes:

1. Stellen Sie eine Verbindung mit dem gewünschten Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur das Element **Globale Tasks** aus, öffnen Sie das Kontextmenü und gehen Sie auf den Eintrag **Neu / Task** oder klicken Sie auf den analog lautenden Eintrag im Menü **Aktion**. Es öffnet sich daraufhin der Assistent für das Erstellen eines Tasks. Folgen Sie dessen Anweisungen.
3. Bestimmen Sie den Namen des Tasks.

4. Bei der Entscheidung für die Anwendung und beim Festlegen des Tasktyps (s. Abb. 29) aktivieren Sie jeweils die Werte **Kaspersky Administration Kit** und **Remote-Installation der Anwendung**.
5. Im folgenden Fenster (s. Abb. 30) geben Sie für die Installation das Installationspaket ab. Der Vorgang gleicht der Push-Installation (s. oben).
6. Wählen Sie danach die Variante **Installation mit Startscenario** (s. Abb. 31) aus.
7. Im folgenden Fenster des Assistenten (s. Abb. 39) wählen Sie die Benutzerkonten der Benutzer aus, für die das Startscenario geändert werden muss.

Während des Taskstarts der Installation überprüft Kaspersky Administration Kit, ob ein Startscenario von einem anderen Benutzer, asser ausgewählt, definiert wurde. Wenn ja, dann wird die Installation nicht ausgeführt. Dabei wird in den Protokoll die Information über diesen Fehler eingetragen.

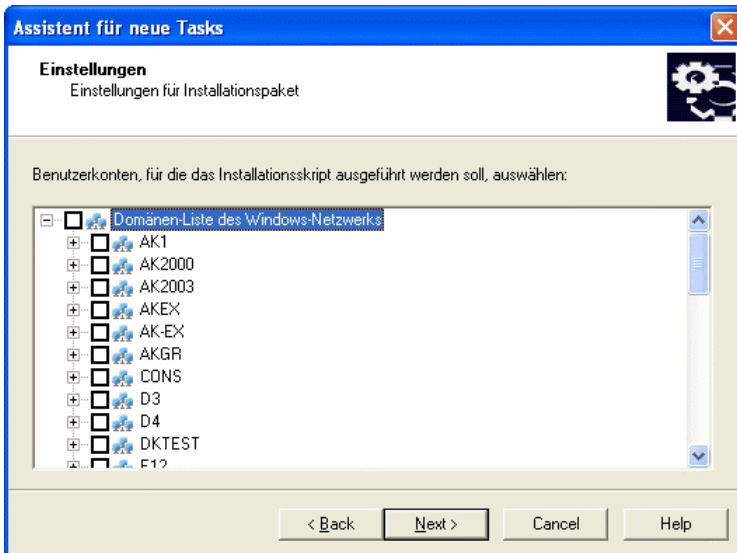


Abbildung 39. Benutzerkonten auswählen

8. Im nächsten Schritt des Assistenten (s. Abb. 37) geben Sie genauso wie bei der Push-Installation (s. oben) das Benutzerkonto an, unter dem der Task Remote-Installation auf Client-Computern gestartet wird.

9. Im Fenster **Zeitplan für Task-Start** (s. Abb. 38) erstellen Sie einen Zeitplan auf die gleiche Weise wie bei der Push-Installation(s. oben).

Nach dem Beenden des Assistenten wird der erstellte Task Remote-Installation in das Element **Globale Task** eingefügt und steht im Detailsfenster. Bei Bedarf können Sie dessen Einstellungen ändern (Details s. Pkt. 4.1.8 auf S. 70).

Tun Sie dazu Folgendes:

Wählen Sie in der Konsolenstruktur das Element **Remote-Installation** aus, markieren Sie im Detailsfenster das gewünschte Installationspaket, öffnen Sie das Kontextmenü und gehen Sie auf den Eintrag **Installieren** oder auf den analog lautenden Eintrag im Menü **Aktion**. Es öffnet sich daraufhin wie oben beschrieben der Assistent zum Erstellen eines Tasks Remote-Installation, es fehlen jedoch die Schritte zum Auswählen des Tasktyps und des Installationspaketes. Folgen Sie den Anweisungen des Assistenten.

Der Assistent für das Erstellen eines Gruppentasks für Remote-Installation lässt sich auch starten.

Tun Sie dazu Folgendes:

Wählen Sie in der Konsolenstruktur das Element **Gruppen** aus, öffnen Sie das Kontextmenü und gehen Sie auf den Eintrag **Installieren** oder auf den analog lautenden Eintrag im Menü **Aktion**. Es öffnet sich daraufhin wie oben beschrieben der Assistent zum Erstellen eines Tasks Remote-Installation, es fehlen jedoch die Schritte zum Auswählen des Tasktyps und der Computergruppe. Folgen Sie den Anweisungen des Assistenten.

4.1.8. Konfiguration des Tasks Remote-Installation

Die Konfiguration eines Tasks zur entfernten Installation entspricht der Konfiguration anderer Tasks (Details s. Nachschlagebuch für Kaspersky Administration Kit). Wir beschreiben die für diesen Tasktyp spezifischen Einstellungen genauer, die sich auf der Registerkarte **Einstellungen** befinden.

Wenn Sie einen Task bearbeiten, dessen Zweck in einer Push-Installation besteht (s. Abb. 40), können Sie Folgendes machen:

- Es kann festgelegt werden, ob eine Anwendung erneut installiert werden soll, wenn diese bereits auf dem Client-Computer installiert ist.
- Es kann festgelegt werden, auf welche Weise die für die Anwendungsinstallation nötigen Dateien auf die Client-Computer übertragen werden.

- Die Anzahl der Installationsversuche beim zeitgesteuerten Task-Start kann festgelegt werden..

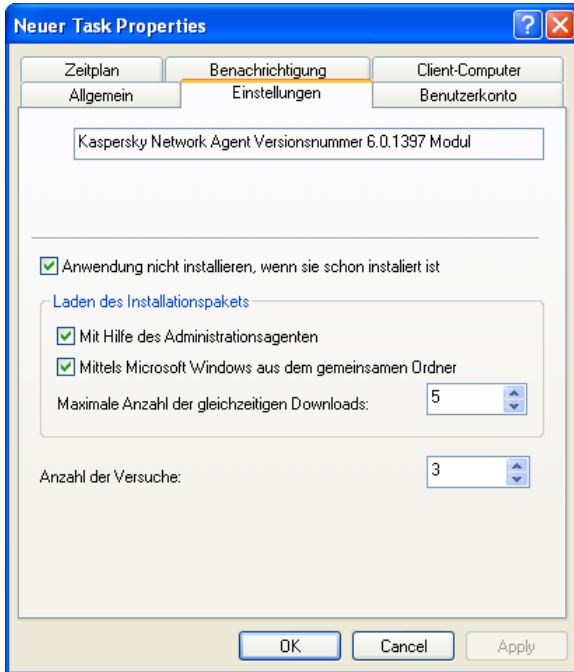


Abbildung 40. Task Remote-Installation konfigurieren.
Push-Installation

Bei der Konfiguration eines Tasks Remote-Installation mit Startskript können Sie auf der Registerkarte **Einstellungen** die Liste der Benutzerkonten ändern, für die die Änderungen in den Startskripten übernommen werden sollen (s. Abb. 41). Zum Bearbeiten der Liste dienen die Schaltflächen **Hinzufügen** und **Löschen**.

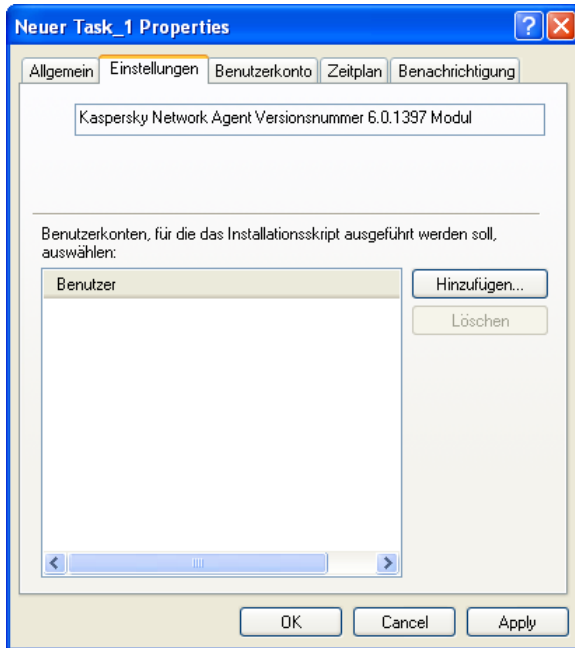


Abbildung 41. Task Remote-Installation mit Startscenario konfigurieren

4.1.9. Task zur Produktinstallation auf die untergeordnete Server

Dieser Task kann Programme von Kaspersky Lab auf untergeordnete Administrationsserver installieren.

Während des Taskstarts der Installation überprüft Kaspersky Administration Kit, ob ein Startscenario von einem anderen Benutzer, asser ausgewählt, definiert wurde. Wenn ja, dann wird die Installation nicht ausgeführt. Dabei wird in den Protokoll die Information über diesen Fehler eingetragen.

Um einen Task Task zur Produktinstallation auf die untergeordnete Server zu erstellen:

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur das Element Globale Tasks aus, öffnen Sie das Kontextmenü und gehen Sie auf den Eintrag

- Neu** → **Task** oder auf den analog lautenden Punkt im Menü **Aktion**.
Es öffnet sich ein Assistent, dessen Anweisungen Sie folgen.
3. Wählen Sie den Taskname.
 4. Für die Anwendung Kaspersky Administration Kit wählen Sie den Tasktyp **Task zur Produktinstallation auf die untergeordnete Server** aus.
 5. Setzen Sie in der unten stehenden Tabelle die Häkchen neben den Namen der gewünschten Installationspakete.
 6. Aktivieren Sie das Kontrollkästchen **Anwendung nicht installieren, wenn sie schon installiert ist**, damit keine wiederholte Installation einer Anwendung auf Computern erfolgt.

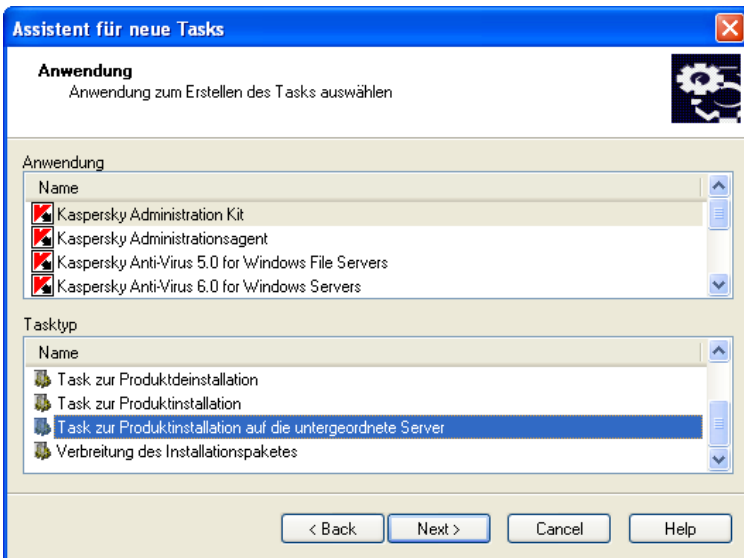


Abbildung 42. Task zur Produktinstallation auf die untergeordnete Server

7. Im folgenden Fenster des Assistenten (s. Abb. 26) setzen Sie die Häkchen in die Kontrollkästchen mit den Namen der untergeordneten Administrationsserver.

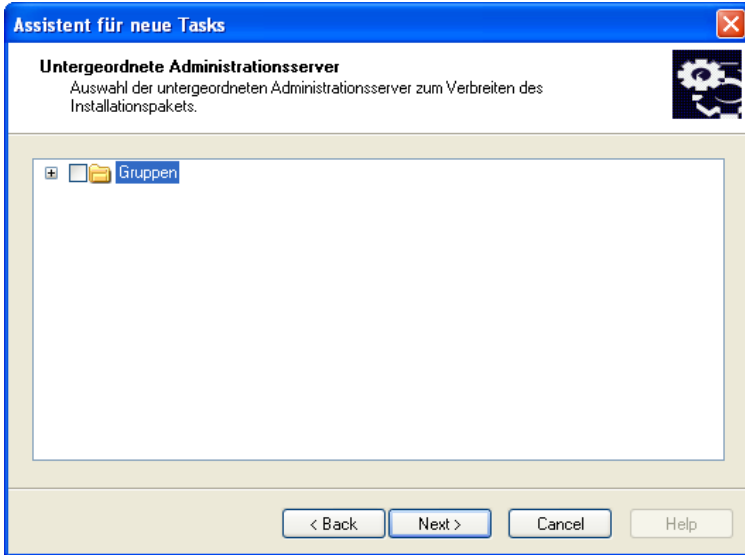


Abbildung 43. Liste der untergeordneten Administrationsserver.

8. Erstellen Sie nun den Zeitplan für den Task-Start

Nach dem Beenden des Assistenten wird der erstellte Task in das Element **Globale Task** eingefügt und steht im Detailsfenster. Bei Bedarf können Sie dessen Einstellungen ändern

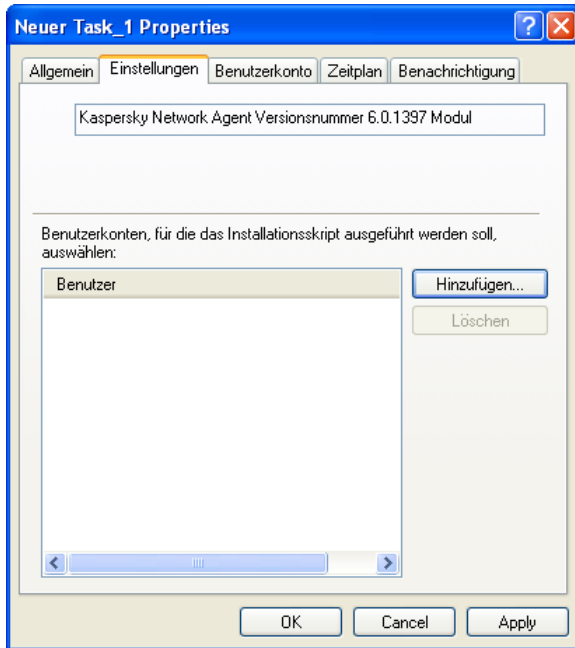


Abbildung 44. Task zur Produktinstallation auf die untergeordnete Server Registerkarte Einstellungen

4.1.10. Remote-Deinstallation eines Programms

Um eine Remote-Deinstallation eines Programms durchzuführen, tun Sie Folgendes:

Erstellen Sie einen Task analog zum Task der Remote-Installation (s. Pkt. 0 auf S. 58), als Tasktyp wählen Sie jedoch **Remote-Deinstallation einer Anwendung** aus und im Fenster **Anwendung** (s. Abb. 45) der Dropdown-Liste **Deinstallierende Anwendung** markieren Sie die gewünschte Kaspersky-Lab-Anwendung. Um eine Drittanwendung zu entfernen, aktivieren Sie das Kontrollkästchen **Drittanwendung deinstallieren** und wählen Sie eine zu deinstallierende Anwendung.

In den Dropdown-Listen stehen Anwendungen, die auf den Rechnern im logischen Netzwerk erkannt wurden, nachdem auf ihnen der Administrationsagent installiert wurde.

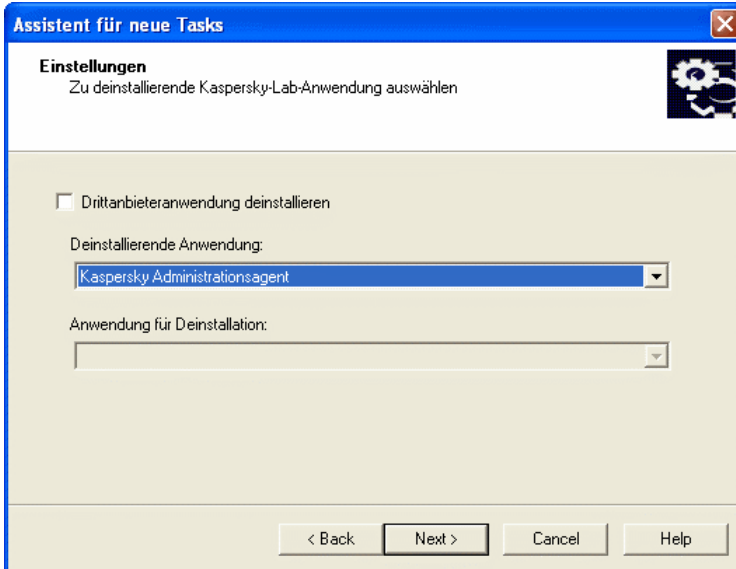


Abbildung 45. Anwendungen für Deinstallation auswählen

Der von Ihnen erstellte Task wird je nach eingestelltem Zeitplan gestartet.

4.2. Assistent für Remote-Installation

Wenn Sie Programme unseres Herstellers installieren wollen, können Sie sich den Assistenten für Remote-Installation zu Nutze machen. Der Assistent organisiert die Remote-Installation mit im Voraus angelegten Installationspaketen oder direkt von den gelieferten Dateien.

Der Assistent erledigt folgende Arbeiten:

- Er erstellt ein Installationspaket für die Installation einer Anwendung (wenn es nicht schon vorher vorhanden war). Das Paket liegt im Element **Remote-Installation** unter dem Namen, der dem Programmnamen und der Programmversion entspricht, und es lässt sich im Weiteren für die Installation der Anwendung nutzen.
- Er erstellt und startet einen globalen Task oder einen Gruppentask Remote-Installation. Der erstellte Task befindet sich dann im Ordner **Globale Tasks** bzw. **Gruppentasks** derjenigen Gruppe, für die er angelegt wurde und kann im Weiteren manuell aufgerufen werden. Der Name des Tasks entspricht dem Namen für die Installation der

Anwendung: **Installation von <Name des ausgewählten Installationspaketes>**.

Zum Installieren einer Anwendung mit dem Assistenten Remote-Installation tun Sie Folgendes:

1. Stellen Sie eine Verbindung zum Administrationsserver her.
2. Wählen Sie im Programmhauptfenster von Kaspersky Administration Kit in der Konsolenstruktur das Element des entsprechenden Administrationsservers, öffnen Sie das Kontextmenü und gehen Sie auf den Eintrag **Assistent für Remote-Installation** oder klicken Sie auf den analog lautenden Eintrag im Menü **Aktion**. Es öffnet sich der Assistent. Folgen Sie den Anweisungen.
3. Geben Sie im folgenden Fenster (s. Abb. 46) das Installationspaket an, dessen Installation erfolgen soll. Wenn Sie die Anwendungsinstallation von der Distribution vornehmen und/oder kein Installationspaket erstellt wurde, legen Sie ein neues Installationspaket an. Klicken Sie dazu auf **Neu...**, es öffnet sich der Assistent für die Erstellung eines Installationspaketes (s. Pkt. 4.1.1 auf S. 42).

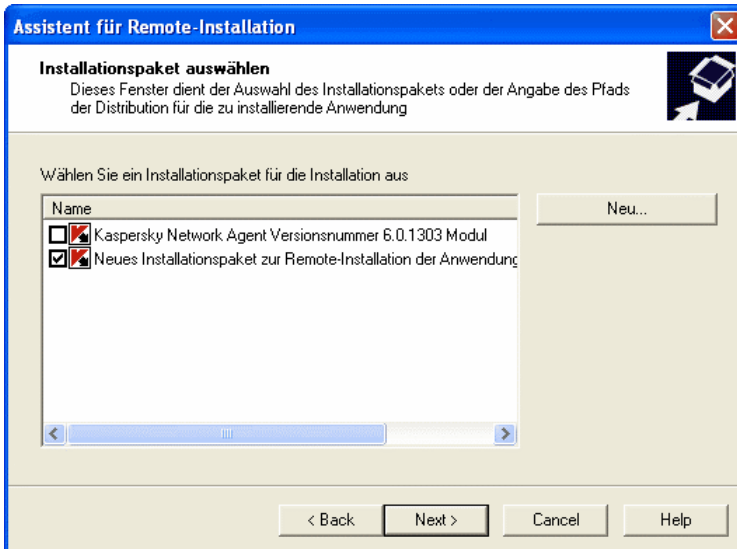


Abbildung 46. Installationspaket auswählen

4. Im folgenden Fenster des Assistenten geben Sie bei Bedarf das Installationspaket des Administrationsagenten für eine gemeinsame Installation an (Details s. Pkt. 0 auf S. 58).

5. Im nächsten Fenster des Assistenten (s. Abb. 47) bestimmen Sie, auf welchen Computern die Anwendungen installiert werden. Entscheiden Sie sich für eine der folgenden Optionen:
 - **Programm auf ausgewählten Computern installieren.** Wenn Sie sich dafür entscheiden, wird nach Abschluss des Assistenten der globale Task Remote-Installation einer Anwendung erstellt.
 - **Programm auf Computer in Administrationsgruppe installieren** – Nach Abschluss des Assistenten wird ein Gruppentask erstellt.

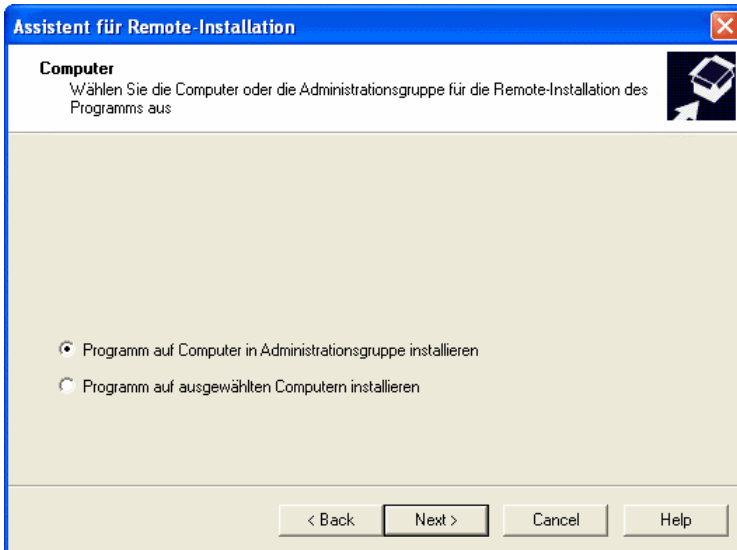


Abbildung 47. Tasktyp auswählen

6. Geben Sie des Weiteren bei Erstellung eines Gruppentasks die Gruppe an, auf deren Computer die Remote-Installation erfolgen wird (s. Abb. 48) oder wählen Sie Computer für die Installation aus. Wenn die Anwendung auf allen Client-Computern des logischen Netzwerks installiert werden soll, wählen Sie die Gruppe **Gruppen** aus.

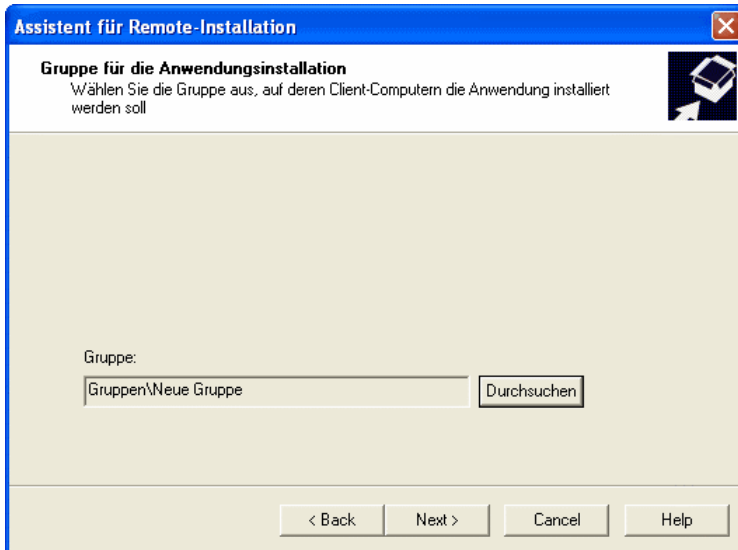


Abbildung 48. Gruppe auswählen

7. Geben Sie weiterhin an, unter welchem Benutzerkonto der Task Remote-Installation auf den Computern gestartet wird (Details s. Pkt. 0 auf S. 58).

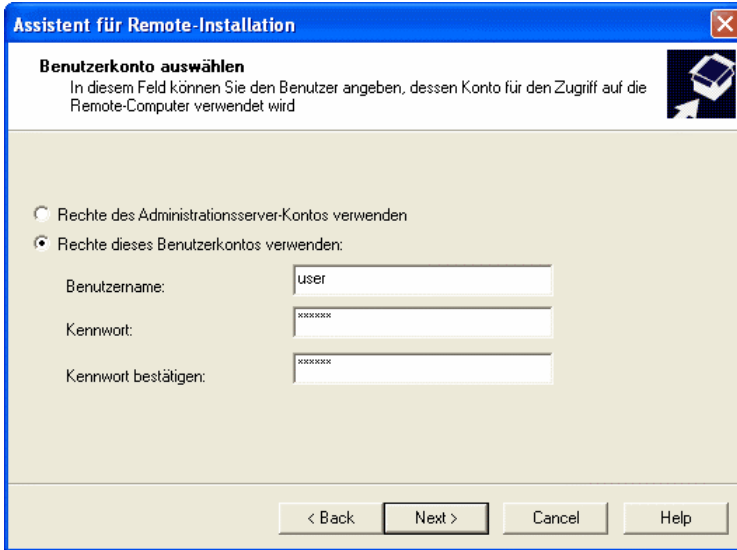


Abbildung 49. Benutzerkonto auswählen

8. Danach erscheint ein Fenster, in dem der Prozess der Verteilung und der Taskausführung Remote-Installation auf den Computern der ausgewählten Gruppe dargestellt wird (s. Abb. 50). Ausführliche Informationen über die Ergebnisse der Taskausführung auf den einzelnen Computern erhalten Sie durch Klick auf **Ergebnisse**.

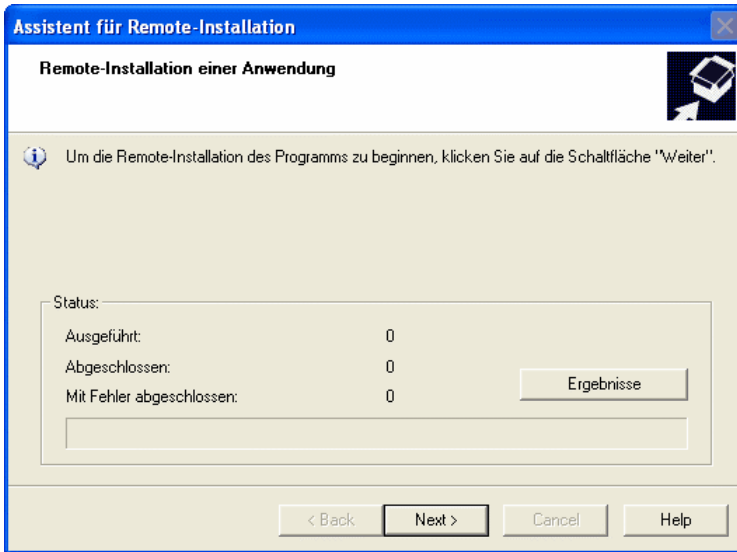


Abbildung 50. Task Remote-Installation wird ausgeführt

4.3. Lokale Installation eines Programms

Die lokale Installation erfolgt separat auf jedem Computer. Zum Ausführen sind Administratorrechte auf dem lokalen Computer erforderlich.

Eine Reihe von Anwendungen, die mit Kaspersky Administration Kit verwaltet werden, kann nur lokal auf einem Rechner installiert werden. Nähere Informationen dazu finden Sie in den Handbüchern zu den jeweiligen Anwendungen.

Das Vorgehen zur Installation von Programmen bei lokaler Einführung des Antiviren-Schutzsystems kann folgendermaßen aussehen:

- Installieren Sie den Administrationsagenten und konfigurieren Sie die Verbindung des Client-Computers mit dem Administrationsserver (s. Pkt. 4.3.1 auf S. 82).
- Installieren Sie die für das Antiviren-Schutzsystem erforderlichen Anwendungen auf den Computern. Folgen Sie dabei der Beschreibung in den entsprechenden Handbüchern.

- Installieren Sie das Verwaltungs-PlugIn für jede installierte Anwendung des Herstellers am Administratorarbeitsplatz (s. Pkt. 4.3.2 auf S. 87).

Kaspersky Administration Kit unterstützt die Option zur lokalen Anwendungsinstallation im Silent-Modus auf Basis der beim Erstellen des Installationspakets erstellten Dateien.

4.3.1. Lokale Installationspaket des Administrationsagenten

Um den Administrationsagenten lokal auf einem Computer zu installieren:

1. Starten Sie die ausführbare Datei **setup.exe** (oder **setup.msi**), die sich auf der Distributions-CD der Anwendung Kaspersky Administration Kit im Verzeichnis **NetAgent** befindet. Die Installation wird von einem Assistenten begleitet. Er bietet Ihnen die Konfiguration der Installationseinstellungen an. Folgen Sie den Anweisungen
2. Die ersten Installationsschritte sind traditionell und umfassen das Entpacken der erforderlichen Dateien aus der Distribution und das Speichern auf der Festplatte Ihres Computers, das Akzeptieren des Lizenzvertrags und die Eingabe von Informationen über Benutzer und Firma.
3. Legen Sie nun den Zielordner für den Administrationsagenten fest. Als Standard gilt **Programme\Kaspersky Lab\NetworkAgent**. Sollte dieses Verzeichnis nicht vorhanden sein, dann wird es automatisch erstellt. Zum Ändern des Ordners dient die Schaltfläche **Durchsuchen**.
4. Das nächste Fenster des Assistenten (s. Abb. 51) dient der Konfiguration der Einstellungen für die Verbindung zwischen Administrationsagent und Administrationsserver. Legen Sie fest:
 - Adresse des Computers, auf dem der Administrationsserver installiert ist oder wird. Als Computeradresse kann die IP-Adresse oder der Computername im Windows-Netzwerk benutzt werden. Der Computer kann auch mit der Schaltfläche **Durchsuchen** ausgewählt werden.
 - Nummer des Ports, über den die Verbindung des Agenten mit dem Administrationsserver erfolgt. Standardmäßig wird Port **14000** verwendet. Wenn dieser Port belegt ist, kann ein anderer Wert gewählt werden. Für die Angabe der Portnummer ist nur die Dezimalform zulässig.
 - Das Öffnen des UDP-Ports 137, welcher zum Ablesen der IP-Adresse des Administrationsserver benutzt wird, in dem Anti-Hacker von Kaspersky Antivirus 6.0. Dazu setzen Sie Häkchen

Namendienst NetBIOS in dem Anti-Hacker von Kaspersky Antivirus 6.0 erlauben.

- Nummer des Ports, über den die geschützte Verbindung unter Verwendung des SSL-Protokolls erfolgt. Standardmäßig wird Port **13000** verwendet. Wenn dieser Port belegt ist, kann ein anderer Wert gewählt werden. Für die Angabe der Portnummer ist nur die Dezimalform zulässig. Damit die Verbindung über einen geschützten Port (unter Verwendung des Protokolls SSL) erfolgt, aktivieren Sie das Kontrollkästchen **SSL-Verbindung verwenden**.

Installationsassistent - Administrationsagent

Administrationsserver

Administrationsserver auswählen

Geben Sie den Computer an, auf dem der Administrationsserver installiert ist.

Servername:

Geben Sie die Portnummer des Administrationsservers an. Der Wert muss im Bereich von 1 bis 65535 liegen.

Portnummer:

Geben Sie die SSL-Portnummer des Administrationsservers an. Der Wert muss im Bereich von 1 bis 65535 liegen.

SSL-Portnummer:

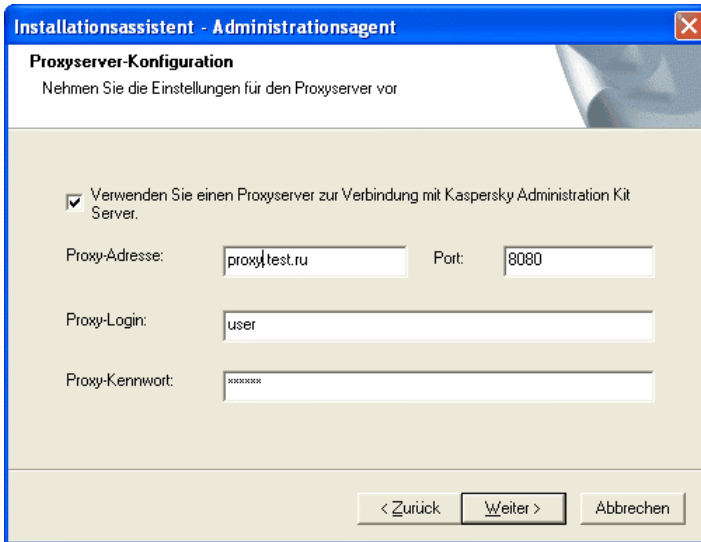
SSL-Verbindung verwenden

< Zurück

Abbildung 51. Verbindung mit Administrationsserver einstellen

5. Wenn für die Verbindung von Administrationsagent und Server ein Proxyserver verwendet wird, stellen Sie im folgenden Fenster (s. Abb. 52) die Verbindung ein:
 - Aktivieren Sie das Kontrollkästchen **Verwenden Sie einen Proxyserver zur Verbindung mit Kaspersky Administration Kit** und geben Sie die Adresse und die Portnummer für die Verbindung mit dem Proxyserver ein. Es ist nur die Dezimalform zulässig (Beispiel: **Adresse des Proxyservers:** proxy.test.ru, **Port:** 8080).
 - Wenn für den Zugang zum Proxyserver ein Kennwort gebraucht wird, nehmen Sie die Eintragungen im Feld **Benutzername** und **Kennwort** vor.

Wenn kein Proxyserver verwendet wird, lassen Sie den Schritt aus und klicken Sie auf **Weiter**.



Installationsassistent - Administrationsagent

Proxyserver-Konfiguration
Nehmen Sie die Einstellungen für den Proxyserver vor

Verwenden Sie einen Proxyserver zur Verbindung mit Kaspersky Administration Kit Server.

Proxy-Adresse: Port:

Proxy-Login:

Proxy-Kennwort:

< Zurück

Abbildung 52. Verbindung über einen Proxyserver einstellen

6. Geben Sie danach an, zu welchem Ordner der Gruppe **Netzwerk** ein Computer hinzugefügt werden soll, wenn er vom Administrationsserver beim Durchsuchen des Windows-Netzwerks gefunden wird. Wählen Sie eine der folgenden Optionen (s. Abb. 53):
 - **Standard** – Der Computer wird in den Ordner aufgenommen, der seinem Ort im Windows-Netzwerk entspricht: Domäne oder Arbeitsgruppe (diese Option ist standardmäßig ausgewählt).
 - **In die angegebene Gruppe** – Der Computer wird in den Ordner aufgenommen, der im Feld Gruppenname festgelegt wird. Wird diese Option gewählt, dann geben Sie den Ordernamen im Feld Gruppenname an. Wenn in der Gruppe Netzwerk kein solcher Ordner vorhanden ist, dann wird er erstellt (Sie können außerdem einen beliebigen Ordner aus der Gruppe Netzwerk angeben).

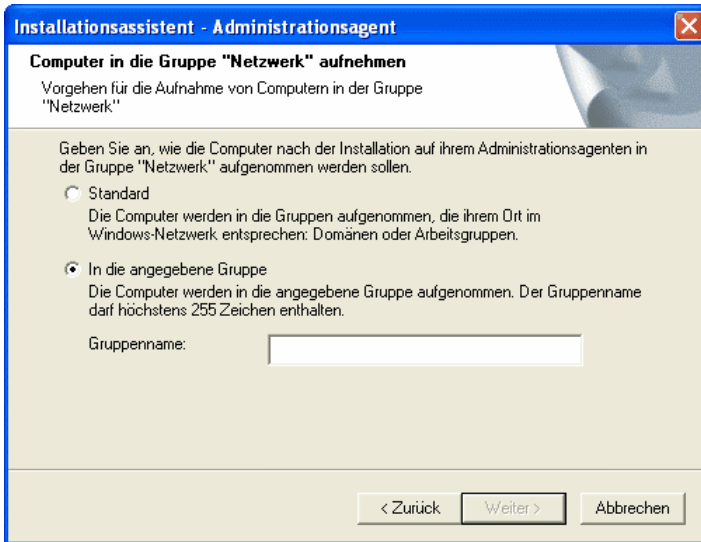


Abbildung 53. Gruppen für Computer im Ordner **Netzwerk** bestimmen

7. Beim folgenden Schritt (s. Abb. 54) wird bestimmt, auf welche Weise das Zertifikat des Administrationsservers angefordert wird, mit dem sich der Administrationsagent verbinden wird. Wählen Sie eine der Optionen:

- **Vom Administrationsservers anfordern** – Das Zertifikat des Administrationsservers wird bei der ersten Verbindung des Administrationsagenten mit dem Server angefordert (diese Option ist standardmäßig ausgewählt).
- **Vorhandenes verwenden** – Die Authentifizierung des Administrationsservers erfolgt auf Basis des Zertifikats, das vom Administrator festgelegt wird. Bei der Auswahl dieser Option muss die erforderliche Zertifikatsdatei des Administrationsservers angegeben werden.

Die Zertifikatsdatei hat die Erweiterung **.cer** und befindet sich auf dem Administrationsserver im Ordner **Cert** des Installationsordners von Kaspersky Administration Kit.

Sie können die Zertifikatsdatei in den gemeinsamen Ordner oder auf eine Diskette kopieren und zur Konfiguration der Zugriffseinstellungen für Administrationsagenten eine Kopie der Datei verwenden.

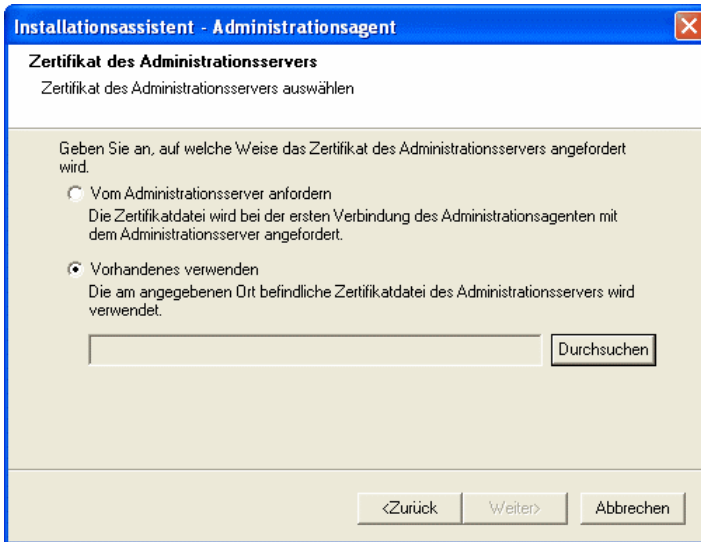


Abbildung 54. Bezug des Zertifikats für Administrationsagent einstellen

8. Im letzten Fenster des Assistenten (s. Abb. 55) wird Ihnen angeboten, den Administrationsagenten sofort nach dem Abschluss des Assistenten zu starten. Wenn Sie möchten, dass der Start später stattfindet, deaktivieren Sie das standardmäßig aktivierte Kontrollkästchen **Administrationsagent starten**.

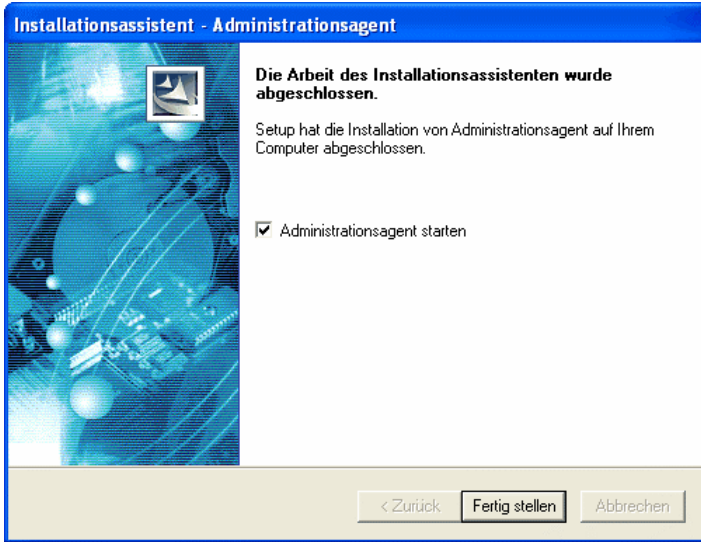


Abbildung 55. Start des Administrationsagenten einstellen

Nach Beenden des Assistenten wird der Administrationsagent auf Ihrem Computer installiert.

Sie können die Eigenschaften des Dienstes **Kaspersky Network Agent** anzeigen, ihn starten, beenden und verfolgen, indem Sie die Standardmittel für das Administrieren in Windows **Systemsteuerung / Dienste** verwenden.

Zusammen mit dem Administrationsagenten wird immer Plug-In für Arbeit mit Cisco Network Admission Control (NAC) installiert. Dieses Plug-in funktioniert in dem Fall, wenn die Anwendung Cisco Trust Agent auf dem Computer installiert ist.

4.3.2. Lokale Installation des Plug-Ins zur Anwendungsverwaltung

Um das Plug-In zur Anwendungsverwaltung zu installieren, tun Sie Folgendes:

Starten Sie auf dem Computer, auf dem die Administrationskonsole installiert ist, die ausführbare Datei **klcfiginst.exe**, die sich auf der Distributions-CD der Anwendung befindet. Diese Datei ist im Lieferumfang aller Anwendungen enthalten, die mit Hilfe von Kaspersky Administration Kit verwaltet werden können. Die

Installation wird von einem Assistenten begleitet und braucht keine Einstellungen.

Die Installationsdatei für das Verwaltungs-PlugIn des Administrationsagenten **klcfginst.exe** befindet sich im Ordner **NetAgent** des Distributionspakets von Kaspersky Administration Kit.

4.3.3. Installation von Programmen im Silent-Modus

Um die Installation einer Anwendung im Silent-Modus vorzunehmen, tun Sie Folgendes:

1. Erstellen Sie das erforderliche Installationspaket (s. Pkt. 4.1.1 auf S. 42), wenn für die Anwendung, deren Installation Sie vornehmen möchten, noch kein Installationspaket erstellt wurde.

Installationspaket wird auf dem Administrationsserver in dem Ordner gespeichert, welcher während der Installation von dem Administrationsserver in dem gemeinsamen Ordner **Packages** definiert wurde. Dabei wird jedem Installationspaket eigener eingelegerter Ordner entsprechen.

2. Wenn es nötig ist, stellen Sie die Parameter des Installationspaketes ein (s. Pkt. 4.1.2 auf S. 45).
3. Installieren Sie die Anwendung nach eine der folgenden Methoden:
 - Kopieren Sie den Ordner- welcher dem Installationspaket entspricht, von dem Administrationsserver auf den Client-Computer. Danach öffnen Sie den kopierten Ordner auf dem Client-Computer und starten Sie die ausführende Datei (Datei mit der Erweiterung **.exe**) mit der Option **/s**.
 - Von dem Client-Computer öffnen Sie den gemeinsamen Ordner, welcher dem Installationspaket entspricht. Starten Sie die ausführende Datei mit der Option **/s**.

Wenn die Anwendung Kaspersky Administration Kit im Silent-Modus installiert wird, kann eine Antworten-Datei benutzt werden. Diese Datei enthält alle Installationsparameter der Anwendung und erlaubt es, die Anwendung mehrmals mit den gleichen Parameter zu installieren.

Um eine Antworten-Datei für Kaspersky Administration Kit zu erstellen:

1. In der Befehlszeile gehen Sie zu dem Verzeichnis, in dem sich der Distributiv der Anwendung Kaspersky Administration Kit befindet, und

starten Sie die Ausführende Datei mit den Optionen **/r** und **/f1"<Dateipfad>\setup.iss"** (z. B., **setup.exe /r /f1"C:\setup.iss"**).

Auf dem Computer wird Installation der Anwendung gestartet.

2. Stellen Sie die Parameter der Anwendungsinstallation ein, in dem Sie den Anweisungen des Assistenten folgen. Z. B., kann nur die Installation des Administrationsserver oder nur der Administrationskonsole auswählen.

Es wird dabei die ausgewählte Version der Anwendung Kaspersky Administration Kit installiert, und in dem gewählten Verzeichnis eine Antworten-Datei erstellt. Die erstellte Datei muss auf den Administrationsserver kopiert werden in den Ordner des entsprechenden Installationspakets. Danach kann bei der Installation von Kaspersky Administration Kit im Silent-Modus die Konfiguration benutzt werden, welche in der Antworten-Datei vorgegeben wurde.

Mit Hilfe der Antworten-Datei kann die Anwendung Kaspersky Administration Kit im Silent-Modus upgedatet werden. Dabei kann die Datei nur für Update der gleichen Version benutzt werden, auf der die Datei erstellt wurde.

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 Antivirensicherheitsystems 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. Weitere Produkte und Services 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 Produkt 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 Antivirenuntersuchung des Computers im Online-Modus erlaubt. Kaspersky OnLine Scanner wird direkt im Webbrowser ausgeführt. Dadurch kann der Benutzer auf schnelle Weise herausfinden, ob sein Computer von einer Infektion durch schädliche Programme bedroht ist. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Antiviren-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 Antivirenuntersuchung des Computers und die Desinfektion infizierter Dateien im Online-Modus erlaubt. Kaspersky OnLine Scanner wird direkt im Webbrowser ausgeführt. Im Rahmen der Untersuchung kann der Benutzer:

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

Kaspersky Anti-Virus® 6.0

Kaspersky Anti-Virus 6.0 dient dem Schutz eines Personalcomputers vor schädlichen Programmen. Dabei werden traditionelle Virenschutzmethoden auf optimale Weise mit neuen proaktiven Technologien vereinigt.

Das Programm erlaubt eine komplexe Antivirenuntersuchung, die folgende Optionen umfasst:

- Antivirenuntersuchung 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.

- Antivirenuntersuchung des Internet-Datenstroms, der mit HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.
- Antivirenuntersuchung 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 Betriebssystem 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 6.0 warnt den Benutzer rechtzeitig, wenn gefährliche, verdächtige oder versteckte Prozesse auftreten oder wenn normale Prozesse auf unerlaubte Weise verändert werden.
- **Überwachung von Veränderungen in der Registrierung des Betriebssystems** durch die Kontrolle des Zustands der Systemregistrierung.
- **Sperren gefährlicher Makros** des Typs Visual Basic for Applications in Microsoft Office Dokumenten.
- **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 6.0

Kaspersky Internet Security 6.0 bietet Rundum-Schutz für PCs. Dabei werden traditionelle Methoden zum Schutz vor Viren auf optimale Weise mit neuen proaktiven Technologien kombiniert.

Das Programm bietet die komplexe Virenuntersuchung von Anti-Virus 6.0 sowie zusätzlich die Personal-Firewall Anti-Hacker, das Blockieren von Spam und optimalen Schutz vor Phishing:

- Schutz des E-Mail-Verkehrs. Kaspersky Internet Security 6.0 überprüft den gesamten E-Mail-Verkehr (POP3, IMAP und NNTP für alle eingehenden sowie SMTP für alle ausgehenden Nachrichten), unabhängig vom benutzten E-Mail-Programm. Für die gängigen E-Mail-Programme Microsoft Outlook, Microsoft Outlook Express und The Bat! sind PlugIns wählbar, zudem können Viren direkt in den Datenbanken des Mail-Programms entfernt werden.

- Überprüfung des Internet-Verkehrs. Kaspersky Internet Security 6.0 ermöglicht einen Echtzeit-Viren-Scan des Internet-Traffics, der über das HTTP-Protokoll eintrifft, und verhindert damit eine potenzielle Infektion – noch bevor die Dateien die Festplatte des Computers erreichen. Mit dem Plugin für den Microsoft Internet Explorer können Sie die Statistik mit allen blockierten Skripten abrufen.
- Schutz des Datei-Systems. Alle Dateien und Verzeichnisse sowie die angeschlossenen Laufwerke können jederzeit auf Viren geprüft werden. Das Programm kann aber auch nur einzelne Bereiche des Betriebssystems oder Objekte, die beim Start von Microsoft Windows geladen werden, überprüfen. Solche Scan-Aufträge können Sie selbst konfigurieren. Dadurch kann Zeit beim Viren-Scan gespart werden, da in erster Linie Bereiche und Objekte gescannt werden, die am häufigsten befallen werden.
- Proaktiver Schutz. Kaspersky Internet Security 6.0 beobachtet permanent die Aktivität der Programme und Prozesse, die im Arbeitsspeicher des Computers gestartet werden und warnt den Anwender rechtzeitig bei Entdeckung gefährlicher, verdächtiger oder getarnter Prozesse (Rootkits). Zudem verhindert es riskante Veränderungen des Datei-Systems sowie der Registry und stellt das System nach Ausführung eines schädlichen Programms wieder her.
- Schutz vor Spyware. Kaspersky Internet Security 6.0 schützt Ihre vertraulichen Daten – etwa Passwörter, Konto- und Kreditkarten-Nummern – vor unbefugtem Zugriff. Zudem werden Phishing-Mails erkannt und das Programm warnt Sie beim Aufruf gefälschter Webseiten, auf denen Login-Daten und Passwörter preisgegeben werden sollen.
- Blockierung von gefährlichen Prozessen und Bannern. Das Programm verhindert den Start gefährlicher Prozesse auf Webseiten, zudem werden Werbebanner und Popups blockiert, die nicht nur stören, sondern auch schädliche Programme auf Ihrem Computer starten können.
- Blockierung kostenpflichtiger Dialer. Auch Dialer-Programme, die Ihr Modem für die Verbindung mit kostenpflichtigen Telefon-Diensten benutzen, werden blockiert.
- Schutz vor Spam. Eine effektive Spam-Filterung wird durch die Kombination verschiedener Methoden erreicht: IP-Adressen und Phrasen im E-Mail-Text werden mit Black- und White-Lists (einschließlich der Adressen von Phishing-Webseiten) verglichen, zudem wird der E-Mail-Text von einem lernfähigen Algorithmus analysiert. Auch die Erkennung von Bild-Spam ist möglich.
- Unterstützung der bekanntesten Mail-Programme. Für Microsoft Outlook, Microsoft Outlook Express und The Bat! sind Plugins wählbar, die Ihnen

erlauben, Regeln für die Bearbeitung von E-Mails, entsprechend der Ergebnisse Ihrer Analyse, festzulegen.

- Vorab-Prüfung von E-Mails auf Spam. Die Betreffzeilen eingehender E-Mails können vor dem Herunterladen auf Ihren Computer geprüft werden. Damit ist es möglich, den Empfang bestimmter E-Mails abzulehnen – Sie sparen Zeit und laden gleichzeitig weniger Spam oder Viren auf Ihren Computer herunter.
- Schutz vor Hacker-Angriffen. Kaspersky Internet Security 6.0 bemerkt so genannte Portscans Ihres Computers, die Netz-Attacken häufig vorangehen. Es wehrt die am meisten verbreiteten Hacker-Attacken erfolgreich ab, indem es die Zusammenarbeit mit dem attackierenden Computer verbietet. Das Monitoring sämtlicher Netz-Aktivitäten ermöglicht zudem eine genaue Statistik aller Verbindungen.
- Kontrolle des Netzwerks. Auf Grundlage vorgegebener Regeln für über 250 bekannte Anwendungen kontrolliert das Programm die ein- und ausgehenden Datenpakete. Auch neue Regeln für weitere Anwendungen können formuliert werden – fertige Schablonen erleichtern die Erstellung. Beim Anschluss des Computers an ein Netzwerk können Sie den Netz-Typ wählen: Internes Netzwerk, Intranet oder Internet. Diese Auswahl definiert die Sicherheitsstufe, die von der Firewall verwendet wird.
- Stealth-Modus im Internet. Der Stealth-Modus ermöglicht Ihnen unerkanntes Surfen im Internet. Beim Aktivieren dieses Modus werden Sie für andere Nutzer im Netzwerk unsichtbar, alle Zugriffe von außen werden blockiert. Für bestimmte Webseiten oder Nutzer können Sie aber Ausnahme-Regeln festlegen.

Kaspersky® Security für PDA

Kaspersky® Security für PDA gewährleistet zuverlässigen Virenschutz für Daten auf Handheld-PCs unter Palm OS oder Microsoft Windows CE sowie für Daten, die von einem gewöhnlichen PC oder Erweiterungsspeichern, von CD-ROM oder aus Datenbanken übernommen werden. Das Programm umfasst eine optimale Auswahl an Virenschutz-Komponenten:

- einen Virenschanner, der eine Überprüfung der Daten (sowohl im Speicher des PDA selbst, als auch auf beliebigen Speicher-Erweiterungskarten) auf Anforderung des Anwenders ausführt;
- den Antivirus-Monitor, der während der Synchronisation über HotSync™ und während des Datenaustausches mit anderen PDA Virenprogramme blockiert.

Weiterhin schützt das Programm die auf dem PDA gespeicherten Informationen vor unberechtigtem Zugriff durch Verschlüsselung des Zugriffs auf das Gerät selbst wie auch auf die im Speicher des PDA und auf Speicherkarten enthaltenen Daten.

Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile bietet den Antivirenschutz für mobile Geräte, die mit den Betriebssystemen Symbian OS und Microsoft Windows Mobile arbeiten. Das Programm erlaubt es, eine komplexe Antivirenuntersuchung vorzunehmen, die folgende Optionen umfasst:

- **Scan auf Befehl** des Arbeitsspeichers, der Speicherkarten, einzelner Ordner oder einer konkreten Datei des mobilen Geräts. Wenn ein infiziertes Objekt gefunden wird, wird es in den Quarantäneordner verschoben oder gelöscht.
- **Echtzeit-Untersuchung**: alle eingehenden oder veränderten Objekte und alle Dateien, auf die versucht wird zuzugreifen, werden automatisch untersucht.
- **Untersuchung nach Zeitplan** von Informationen, die im Arbeitsspeicher des mobilen Geräts gespeichert sind.
- **Schutz vor sms- und mms-Spam.**

Kaspersky Anti-Virus® Business Optimal

Dieses Programmpaket ist die ultimative Lösung zum Schutz vor Computerviren für Unternehmen kleiner und mittlerer Größe.

Kaspersky Anti-Virus® Business Optimal bietet Rundumschutz³ vor Viren für:

- *Computerarbeitsplätze* unter Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstation, Linux.
- *Dateiserver* unter Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD und Linux; *Dateispeicher* unter Samba.
- *Mailsysteme* vom Typ Microsoft Exchange 2000/2003, Lotus Notes/Domino, postfix, exim, sendmail und qmail.
- *Internet-Gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition, Microsoft ISA Server 2004 Standard Edition.

Kaspersky Anti-Virus® Business Optimal beinhaltet außerdem das zentrale Installations- und Administrationssystem Kaspersky® Administration Kit.

Sie selbst wählen die geeigneten Virenschutzprogramme in Abhängigkeit von den in Ihrem Unternehmen verwendeten Betriebssystemen und Anwendungen.

Kaspersky® Corporate Suite

Kaspersky® Corporate Suite ist eine integrierte Softwarelösung zum Datenschutz für Ihr gesamtes Firmennetzwerk ohne Einschränkungen hinsichtlich Größe und

³ Je nach Lieferumfang

Struktur. Die enthaltenen Programmkomponenten schützen jeden Punkt ihres firmeninternen Netzes. Sie sind kompatibel mit den meisten heute verbreiteten Betriebssystemen und Anwendungen, über ein zentrales Steuerungssystem miteinander verbunden und werden über eine gemeinsame Benutzeroberfläche bedient. Mit diesem System erhalten Sie einen Virenschutz, der sich vollständig an die Systemanforderungen Ihres internen Netzes anpassen lässt.

Kaspersky® Corporate Suite bietet Rundumschutz⁴ vor Viren für:

- *Computerarbeitsplätze* unter Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstation und Linux.
- *Dateiserver* unter Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, Linux; *Dateispeicher* unter Samba.
- *Mailsysteme* vom Typ Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, sendmail, postfix, exim und qmail.
- *Internet-Gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Enterprise Edition; Microsoft ISA Server 2004 Enterprise Edition.
- *Handheld-PCs*, die unter Symbian OS, Microsoft Windows CE und Palm OS arbeiten, sowie *Smartphones*, die unter Microsoft Windows Mobile 2003 for Smartphone und Microsoft Smartphone 2002 arbeiten.

Kaspersky® Corporate Suite beinhaltet außerdem das zentrale Installations- und Administrationssystem Kaspersky® Administration Kit.

Sie selbst wählen die geeigneten Virenschutzprogramme in Abhängigkeit von den in Ihrem Unternehmen verwendeten Betriebssystemen und Anwendungen.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam ist die erste in Russland entwickelte Software zum Schutz vor unerwünschten Mailings (Spam) für Unternehmen kleinerer und mittlerer Größe. 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 Mitteilungen 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.

⁴ Je nach Lieferumfang

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

Kaspersky® SMTP Gateway

Kaspersky® SMTP-Gateway for Linux / Unix dient der Antivirenbearbeitung von E-Mails, die mit SMTP-Protokoll weitergeleitet werden. Die Anwendung umfasst eine Reihe von zusätzlichen Filterinstrumenten für den Mailverkehr (Filterung nach Namen und MIME-Typen von Attachments) sowie eine Reihe von Mitteln, die es erlauben, die Belastung des Mailsystems zu verringern und Hackerangriffe abzuwehren. Dazu zählen die Begrenzung der maximalen Mailgröße, der Anzahl von Adressaten usw. Die Unterstützung der Technologie DNS Black List schützt vor dem Empfang von Mails, die von Servern stammen, die auf diesen Listen stehen und als Verbreitungsquellen für Spam gelten.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security® for Microsoft Exchange bietet die Antivirenuntersuchung der eingehenden, ausgehenden und auf dem Server gespeicherten E-Mail-Nachrichten einschließlich der Nachrichten in gemeinsamen Ordnern. Außerdem führt er die Filterung unerwünschter Korrespondenz aus, wobei intelligente Technologien zur Spam-Erkennung in Verbindung mit Technologien der Firma Microsoft verwendet werden. Die Anwendung untersucht alle mit dem SMTP-Protokoll auf dem Exchange-Server eingehenden Nachrichten auf das Vorhandensein von Viren, wobei Antivirentechnologien von Kaspersky Lab verwendet werden, und auf Spam-Merkmale, wozu die Filterung nach formalen Kennzeichen (E-Mail-Adresse, IP-Adresse, Größe der Mail, Kopfzeile) dient. Außerdem analysiert er den Inhalt des Briefs und seiner Anhänge mit Hilfe von intelligenten Technologien, die unikale grafische Signaturen zum Erkennen von Spam in grafischer Form umfassen. Der Untersuchung werden sowohl der Nachrichtenkörper als auch angehängte Dateien unterzogen.

Kaspersky® Mail Gateway

Kaspersky® Mail Gateway ist eine universelle Lösung für den komplexen Schutz der Benutzer von Mailsystemen. Die Anwendung wird zwischen dem Unternehmensnetzwerk und dem Internet installiert und führt die Untersuchung aller Elemente einer E-Mail auf das Vorhandensein von Viren und anderen schädlichen Programmen (Spyware, Adware usw.) durch. Außerdem erfolgt die zentralisierte Filterung des E-Mail-Nachrichtenstroms auf Spam-Merkmale. Die Anwendung enthält eine Reihe von Zusatzwerkzeugen zur Filterung des Mail-Datenstroms – nach Namen und MIME-Typen der angehängten Dateien, sowie eine Reihe von Mitteln, die es erlauben, die Belastung des Mailsystems zu senken und Hackerangriffe zu verhindern.

Kaspersky Anti-Virus® for Proxy Server

Kaspersky Anti-Virus® for Proxy Server ist eine Antivirenlösung für den Schutz des Web-Datenverkehrs, der mit dem HTTP-Protokoll über einen Proxyserver

geleitet wird. Die Anwendung führt im Echtzeitmodus die Antivirenuntersuchung des Internet-Datenverkehrs durch, schützt vor dem Eindringen schädlicher Programme während des Surfens im Web und scannt Dateien, die aus dem Internet heruntergeladen werden.

Kaspersky Anti-Virus® for MIMESweeper for SMTP

Kaspersky Anti-Virus® for MIMESweeper for SMTP bietet die Hochgeschwindigkeits-Antivirenuntersuchung des SMTP-Datenverkehrs auf Servern, die Clearswift MIMESweeper verwenden.

Das Programm besitzt die Form eines Plugins für die Anwendung MIMESweeper for SMTP der Firma Clearswift und führt im Echtzeitmodus die Antivirenuntersuchung und -bearbeitung des ein- und ausgehenden Mailverkehrs 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	Tel.: +49 (0) 841 98 18 90 Fax: +49 (0) 841 98 18 918 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 dekompileieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Einschränkung, dies ausdrücklich gestattet. Sie sind nicht berechtigt, diese Software in automatischen, halbautomatischen oder manuellen Tools zu verwenden, welche dazu dienen, Virensignaturen, Virenerkennungsroutinen, sowie beliebige andere Daten oder Codes zum Erkennen von schädlichem Code oder Daten zu erstellen.
- Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.
- Supportleistungen. Nach Kauf und Aktivierung der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die Lizenzdauer. Supportleistungen verstehen sich wie folgt:
 - stündliche Updates der Antiviren-Datenbank
 - kostenloses Updates der Software
 - kostenlose technische Unterstützung sowohl per e-Mail als auch per Telefon mit KASPERSKY LAB

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

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

5. GEWÄHRLEISTUNG. KASPERSKY LAB gewährleistet, dass:

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

Gewährleistungspflichtige Mängel werden von KASPERSKY LAB oder dessen Lieferanten nach Entdeckung, auf jeden Fall aber vor Ablauf von der

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

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

6. AUSSCHLUSS DER HAFTUNG FÜR ALLE SCHÄDEN. SOWEIT GESETZLICH ZUGELASSEN, SIND KASPERSKY LAB ODER DESSEN LIEFERANTEN IN KEINEM FALL HAFTBAR FÜR IRGENDWELCHE FOLGE-, ZUFÄLLIGEN, DIREKTEN, INDIREKTEN, SPEZIELLEN, STRAFRECHTLICHEN ODER ANDEREN SCHÄDEN WELCHER ART AUCH IMMER (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AN PERSONEN ODER SACHEN, SCHÄDEN AUS ENTGANEMEM 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.