Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition

Handbuch zur Software-Verteilung

PROGRAMMVERSION: 8.0 SERVICE PACK 2

Sehr geehrter Benutzer!

Wir danken Ihnen, dass Sie unser Programm ausgewählt haben. Wir hoffen, dass Ihnen diese Dokumentation bei der Arbeit behilflich sein und die damit verbundenen Fragen beantworten wird.

Das Dokument kann zukünftig ohne besondere Ankündigung geändert werden. Die neueste Version des Dokumentes finden Sie auf der Seite von Kaspersky Lab unter http://www.kaspersky.com/de/docs.

Redaktionsdatum: 25.02.2015

http://www.kaspersky.com/de/
http://support.kaspersky.com/de/

INHALT

INFORMATIONSQUELLEN ZU KASPERSKY ANTI-VIRUS

Dieser Abschnitt enthält die Beschreibung der Informationsquellen zum Programm. Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage eine passende Quelle wählen.

IN DIESEM ABSCHNITT

QUELLEN FÜR DIE SELBSTSTÄNDIGE INFORMATIONSSUCHE

Für Kaspersky Anti-Virus stehen Ihnen folgende Informationsquellen zur Verfügung:

- Seite von Kaspersky Anti-Virus auf der Webseite von Kaspersky Lab
- Seite von Kaspersky Anti-Virus auf der Webseite des Technischen Supports (Wissensdatenbank)
- Elektronisches Hilfesystem
- Dokumentation

Wenn Sie keine Lösung für Ihr Problem finden, können Sie sich an den Technischen Support von Kaspersky Lab wenden.

Für die Nutzung der Informationsquellen auf den Webseiten ist ein Internetzugang notwendig.

Seite von Kaspersky Anti-Virus auf der Webseite von Kaspersky Lab

Auf der Seite von Kaspersky Anti-Virus (http://www.kaspersky.com/de/anti-virus-windows-server-enterprise) stehen Ihnen allgemeine Informationen über das Programm, seine Funktionsmöglichkeiten und Besonderheiten zur Verfügung.

Auf der Seite für Kaspersky Anti-Virus befindet sich ein Link zum Online-Shop. Dort können Sie ein Programm kaufen oder die Nutzungsrechte für das Programm verlängern.

Seite über Kaspersky Anti-Virus in der Wissensdatenbank

Die *Wissensdatenbank* ist ein spezieller Bereich auf der Support-Webseite.

Auf der Seite von Kaspersky Anti-Virus in der Wissensdatenbank (http://support.kaspersky.com/de/wsee8) finden Sie Artikel, die nützliche Informationen, Empfehlungen und Antworten auf häufig gestellte Fragen zum Erwerb, zur Installation und zur Anwendung des Programms enthalten.

Artikel der Wissensdatenbank beantworten Fragen nicht nur in Bezug auf Kaspersky Anti-Virus, sondern auch auf andere Programme von Kaspersky Lab. Außerdem können Artikel der Wissensdatenbank auch Neuigkeiten über den Technischen Support enthalten.

Im Handbuch zur Software-Verteilung finden Sie typische Vorgehensweisen zur Installation von Kaspersky Anti-Virus in einem Unternehmensnetzwerk.

Im Installationshandbuch finden Sie Informationen über die Ausführung folgender Aufgaben:

- Vorbereitung der Installation, Installation und Aktivierung von Kaspersky Anti-Virus
- Vorbereitung von Kaspersky Anti-Virus zur Ausführung
- Reparatur und Entfernen von Kaspersky Anti-Virus

Das Administratorhandbuch bietet Informationen zur Konfiguration und Verwendung von Kaspersky Anti-Virus.

Das Handbuch für die Implementierung zum Schutz von Netzwerkspeichern bietet Informationen zur Konfiguration und Verwendung von Kaspersky Anti-Virus zum Schutz von Netzwerkspeichern.

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM FORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum (http://forum.kaspersky.com) besprechen.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben und neue Themen zur Diskussion stellen.

KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus schützt Server mit Microsoft® Windows®-Betriebssystem sowie NetApp Storage-Systeme vor Viren und anderen Bedrohungen für die Computersicherheit, die bei der Übertragung von Dateien eindringen können. Kaspersky Anti-Virus ist zum Einsatz in lokalen Netzwerken mittlerer und großer Unternehmen vorgesehen. Als Benutzer von Kaspersky Anti-Virus gelten Netzwerkadministratoren des Unternehmens und Mitarbeiter, die für die Antiviren-Sicherheit des Unternehmensnetzwerks zuständig sind.

Sie können Kaspersky Anti-Virus auf Servern installieren, die folgende Funktionen ausführen:

- Terminalserver
- Druckerserver
- Anwendungsserver
- Domain Controller
- Server zum Schutz von Netzwerkspeichern
- Dateiserver – Diese Arten von Servern unterliegen dem höchsten Infektionsrisiko, weil sie Dateien mit Benutzer-Workstations austauschen.

Sie können Kaspersky Anti-Virus auf folgende Arten verwalten:

- Über die Konsole für Kaspersky Anti-Virus, die auf einem Server mit Kaspersky Anti-Virus oder auf einem anderen Computer installiert ist.
- Mithilfe eines Befehls in der Befehlszeile.
- Über die Administrationskonsole von Kaspersky Security Center.

Sie können die Anwendung Kaspersky Security Center verwenden, die der zentralisierten Verwaltung des Schutzes mehrerer Server dient, auf denen jeweils eine Exemplar von Kaspersky Anti-Virus installiert ist.

Sie können die Leistungsindikatoren von Kaspersky Anti-Virus für die Anwendung "Systemmonitor" sowie Indikatoren und SNMP-Traps analysieren.

Komponenten und Funktionen von Kaspersky Anti-Virus

Im Lieferumfang des Programms sind folgende Komponenten enthalten:

- Echtzeitschutz für Dateien

  Kaspersky Anti-Virus untersucht Objekte, wenn darauf zugegriffen wird. Kaspersky Anti-Virus untersucht folgende Objekte:

  - Dateien
  - alternative Datenströme der Dateisysteme (NTFS-Streams)
  - MBR und Bootsektoren von lokalen Festplatten und Wechseldatenträgern

- Skript-Untersuchung

  Kaspersky Anti-Virus kontrolliert die Ausführung von Skripts, die mit Microsoft Windows Script Technologies (oder Active Scripting) erstellt worden sind, z. B. VBScript- oder JScript®-Skripts. Die Ausführung von Skripts wird nur erlaubt, wenn das betreffende Skript von Kaspersky Anti-Virus als sicher eingestuft wurde. Kaspersky Anti-Virus verbietet die Ausführung von Skripts, die als gefährlich eingestuft wurden. Wenn Kaspersky Anti-Virus ein Skript als potenziell gefährlich eingestuft hat, wird die von Ihnen festgelegte Aktion ausgeführt: Ausführung dieses Skripts erlauben oder verbieten.

- Schutz von Netzwerkspeichern

  Wenn Kaspersky Anti-Virus auf einem Server mit einem Microsoft Windows-Betriebssystem installiert ist, werden Netzwerkspeicher vor Viren und anderen Bedrohungen für die Computersicherheit geschützt, die bei der Übertragung von Dateien eindringen können.

- Virensuche

  Kaspersky Anti-Virus überprüft den angegebenen Bereich einmalig auf Viren und andere Bedrohungen der Computersicherheit. Kaspersky Anti-Virus überprüft Daten, den Arbeitsspeicher des Servers sowie Autostart-Objekte.

Das Programm verfügt über folgenden Funktionen:

- Update der Datenbanken und Programm-Module

  Für den Download von Updates für die Datenbanken und Programm-Module verwendet Kaspersky Anti-Virus die FTP- oder HTTP-Update-Server von Kaspersky Lab, den Administrationsserver von Kaspersky Security Center oder andere Update-Quellen.

- Quarantäne

  Objekte, die von Kaspersky Anti-Virus als möglicherweise infiziert eingestuft worden sind, werden in die Quarantäne verschoben, d. h. die Objekte werden von ihrem ursprünglichen Speicherort in den *Quarantäne-Ordner* verschoben. Aus Sicherheitsgründen werden die Objekte im Quarantäne-Ordner in verschlüsselter Form gespeichert.

- Backup

  Bevor ein Objekt mit dem Status *Infiziert* oder *Möglicherweise infiziert* desinfiziert oder gelöscht wird, speichert Kaspersky Anti-Virus eine verschlüsselte Sicherungskopie im *Backup*.

- Benachrichtigungen an den Administrator und die Benutzer

  Sie können die Benachrichtigung des Administrators und der Benutzer, die auf den geschützten Server zugreifen, über Ereignisse, die mit den Funktionen von Kaspersky Anti-Virus und dem Status der Antiviren-Sicherheit des Servers zusammenhängen, anpassen.

- Import und Export von Parametern

  Sie können die Einstellungen von Kaspersky Anti-Virus in eine Konfigurationsdatei im xml-Format exportieren und Einstellungen aus einer Konfigurationsdatei in Kaspersky Anti-Virus importieren. In einer Konfigurationsdatei können entweder alle Einstellungen für Kaspersky Anti-Virus oder nur die Einstellungen einzelner Komponenten gespeichert werden.

HARD- UND SOFTWARE-VORAUSSETZUNGEN

Dieser Abschnitt enthält eine Liste der Hardware- und Softwarevoraussetzungen für Kaspersky Anti-Virus.

IN DIESEM ABSCHNITT

ANFORDERUNGEN AN DEN SERVER, AUF DEM KASPERSKY ANTI-VIRUS INSTALLIERT WIRD

Vor der Installation von Kaspersky Anti-müssen Virus andere Antiviren-Anwendungen vom Server deinstalliert werden.

Sie können Anti-Virus installieren, ohne Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition oder Kaspersky Anti-Virus 6.0 bzw. 8.0 für Windows Servers® deinstallieren zu müssen.

Hardwarevoraussetzungen für den Server

Generelle Voraussetzungen:

- x86-kompatible Systeme mit Single-Core- und Multi-Core-Konfigurationen; x86-64-kompatible Systeme mit Single-Core- und Multi-Core-Konfigurationen
- Benötigter Speicherplatz:
  - für die Installation aller Programmkomponenten – 70 MB
  - für den Download und zum Speichern der Antiviren-Datenbanken des Programms – 2 GB (empfohlen)
  - zum Speichern von Objekten in Quarantäne und Backup – 400 MB (empfohlen)
  - zum Speichern von Berichten – 1 GB (empfohlen)
  - zum Speichern von Berichten – 2 GB (empfohlen)

Minimalkonfiguration:

- Prozessor – 1 Intel® Core™ 1,4 GHz
- Arbeitsspeicher – 1 GB
- Speicherplatz auf dem Datenträger – 4 GB freier Speicherplatz

Empfohlene Konfiguration:

- Prozessor – 4 Intel Core 2,4 GHz
- Arbeitsspeicher – 2 GB;
- Datenträger-Subsystem – 4 GB freier Speicherplatz

Softwarevoraussetzungen für den Server

Sie können Kaspersky Anti-Virus auf einem Server installieren, der unter einem 32-Bit- oder 64-Bit-Betriebssystem von Microsoft® Windows® läuft.

Für die Installation und Ausführung von Kaspersky Anti-Virus muss auf dem Server Microsoft Windows Installer 3.1 vorhanden sein.

Sie können Kaspersky Anti-Virus auf einem Server installieren, der unter einem der folgenden 32-Bit-Betriebssysteme von Microsoft Windows läuft:

- Windows Server 2003 Standard bzw. Enterprise Edition mit Service Pack 2
- Windows Server 2003 R2 Standard / Enterprise mit Service Pack SP2
- Windows Server 2008 Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Server 2008 Core Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher

Sie können Kaspersky Anti-Virus auf einem Server installieren, der unter einem der folgenden 64-Bit-Betriebssysteme von Microsoft Windows läuft:

- Windows Server 2003 Standard bzw. Enterprise Edition mit Service Pack 2
- Windows Server 2003 R2 Standard / Enterprise mit Service Pack SP2
- Windows Server 2008 Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Server 2008 Core Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Server 2008 R2 Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Server 2008 R2 Core Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Hyper-V® Server 2008 R2 mit Service Pack 1 oder höher;
- Windows Server 2012 Essentials, Standard, Foundation bzw. Datacenter Edition
- Windows Server 2012 R2 Essentials, Standard, Foundation bzw. Datacenter Edition;
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2

Sie können Kaspersky Anti-Virus auf folgenden Terminal-Servern installieren:

- Microsoft Terminal Services auf der Grundlage des Windows 2003 Servers;
- Microsoft Remote Desktop Services auf der Grundlage des Windows 2008 Servers
- Microsoft Remote Desktop Services auf der Grundlage des Windows 2012 Servers
- Microsoft Remote Desktop Services auf der Grundlage des Windows 2012 Servers R2;
- Citrix Presentation Server™ 4.0, 4,5;
- Citrix® XenApp® 4.5, 5.0, 6.0, 6.5;
- Citrix XenDesktop® 7.0, 7.1, 7.5.

ANFORDERUNGEN AN DEN GESCHÜTZTEN NETZWERKSPEICHER

Kaspersky Anti-Virus kann zum Schutz folgender Netzwerkspeicher eingesetzt werden:

- NetApp unter einem der folgenden Betriebssysteme:
  - Data ONTAP 7.x und Data ONTAP 8.x im Modus 7-mode
  - Data ONTAP 8.2.1 oder höher im Modus cluster-mode.
- EMC™ Celerra™ / VNX™ mit folgender Software:
  - Betriebssystem EMC DART 6.0.36 oder höher
  - Celerra Anti Virus Agent (CAVA) 4.5.2.3 oder höher
- EMC Isilon™ unter dem Betriebssystem OneFS™ 7.0 oder höher.

- Hitachi NAS auf einer der folgenden Plattformen:
  - HNAS 4100
  - HNAS 4080
  - HNAS 4060
  - HNAS 4040
  - HNAS 3090
  - HNAS 3080
- IBM® NAS Serie IBM System Storage® N series.

ANFORDERUNGEN AN DEN COMPUTER, AUF DEN DIE KONSOLE FÜR KASPERSKY ANTI-VIRUS INSTALLIERT WIRD

Hardwarevoraussetzungen für den Computer

Empfohlener Arbeitsspeicher – 128 MB oder mehr.

Freier Platz auf der Festplatte – 30 MB.

Softwarevoraussetzungen für den Computer

Sie können die Konsole für Kaspersky Anti-Virus auf einem Computer installieren, der unter einem 32-Bit- oder 64-Bit-Betriebssystem von Microsoft Windows läuft.

Für die Installation und Ausführung der Konsole für Kaspersky Anti-Virus muss auf dem Computer Microsoft Windows Installer 3.1 vorhanden sein.

Sie können die Konsole für Kaspersky Anti-Virus auf einem Computer installieren, der unter einem der folgenden 32-Bit-Betriebssysteme von Microsoft Windows läuft:

- Windows Server 2003 Standard bzw. Enterprise Edition mit Service Pack 2
- Windows Server 2003 R2 Standard / Enterprise mit Service Pack SP2
- Windows Server 2008 Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Microsoft Windows XP Professional mit Service Pack 2 oder höher;
- Microsoft Windows Vista® Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8:
- Microsoft Windows 8 Enterprise bzw. Professional;
- Microsoft Windows 8.1;
- Microsoft Windows 8.1 Enterprise bzw. Professional.

Sie können die Konsole für Kaspersky Anti-Virus auf einem Computer installieren, der unter einem der folgenden 64-Bit-Betriebssysteme von Microsoft Windows läuft:

- Windows Server 2003 Standard bzw. Enterprise Edition mit Service Pack 2
- Windows Server 2003 R2 Standard / Enterprise mit Service Pack SP2
- Windows Server 2008 Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Server 2008 R2 Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Hyper-V Server 2008 R2 mit Service Pack SP1 oder höher

- Windows Server 2012 Essentials, Standard, Foundation bzw. Datacenter Edition
- Windows Server 2012 R2 Essentials, Standard, Foundation bzw. Datacenter Edition;
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2
- Microsoft Windows XP Professional Edition mit Service Pack 2 oder höher
- Microsoft Windows Vista Editions;
- Microsoft Windows 7 Editions
- Microsoft Windows 8:
- Microsoft Windows 8 Enterprise bzw. Professional;
- Microsoft Windows 8.1;
- Microsoft Windows 8.1 Enterprise bzw. Professional.

SCHUTZ FÜR DIRECTLY ATTACHED STORAGES (DAS)

Kaspersky Anti-Virus schützt Massenspeicher, die direkt an den Server angeschlossen werden (DAS) (s. Abbildung unten).

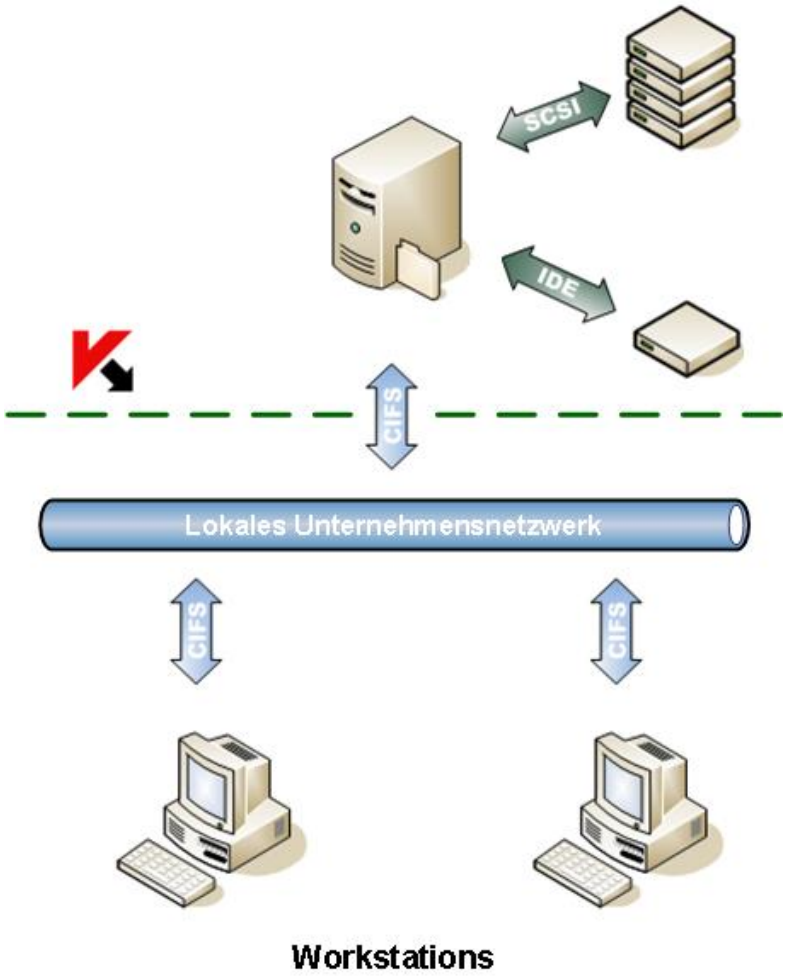

Abbildung 1: Schutzschema für Directly Attached Storages

Kaspersky Anti-Virus kontrolliert Vorgänge für Dateien, die in den Directly Attached Storages gespeichert werden. Kaspersky Anti-Virus erkennt Directly Attached Storages als lokale Dateiressourcen des Servers.

CLUSTER-SCHUTZ

Kaspersky Anti-Virus unterstützt die Installation von Servern, die in den Modi **Aktiv** / **Aktiv** und **Aktiv** / **Passiv** (s. Abbildung unten) laufen, auf Clustern.

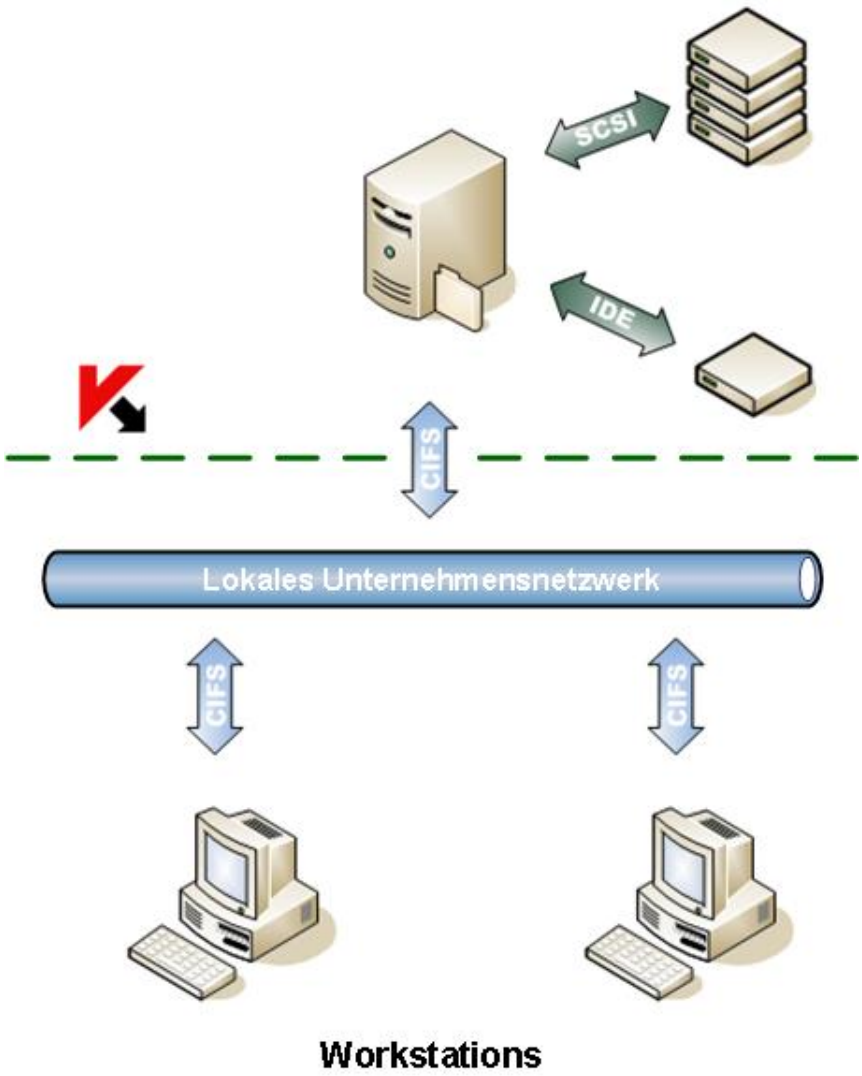

Abbildung 2: Schutzschema für Server-Cluster

Kaspersky Anti-Virus gewährleistet die fehlerfreie Funktion des Servers bei der Migration der Cluster-Ressourcen (**failover** / **failback**).

Ein umfangreicher Schutz des Clusters wird gewährleistet, wenn Kaspersky Anti-Virus auf jedem Knoten installiert wird. Kaspersky Anti-Virus schützt lokale Laufwerke des Serverdateisystems und gemeinsame Laufwerke des Clusters, die momentan dem geschützten Cluster gehören. Die Dateiressourcen, über welche der nicht geschützte Cluster-Knoten verfügt, sind nicht geschützt.

Weitere Informationen finden Sie im *Installationshandbuch zu Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition.*

SCHUTZ FÜR TERMINALSERVER

Kaspersky Anti-Virus bietet Schutz für Terminalserver (s. Abbildung unten).

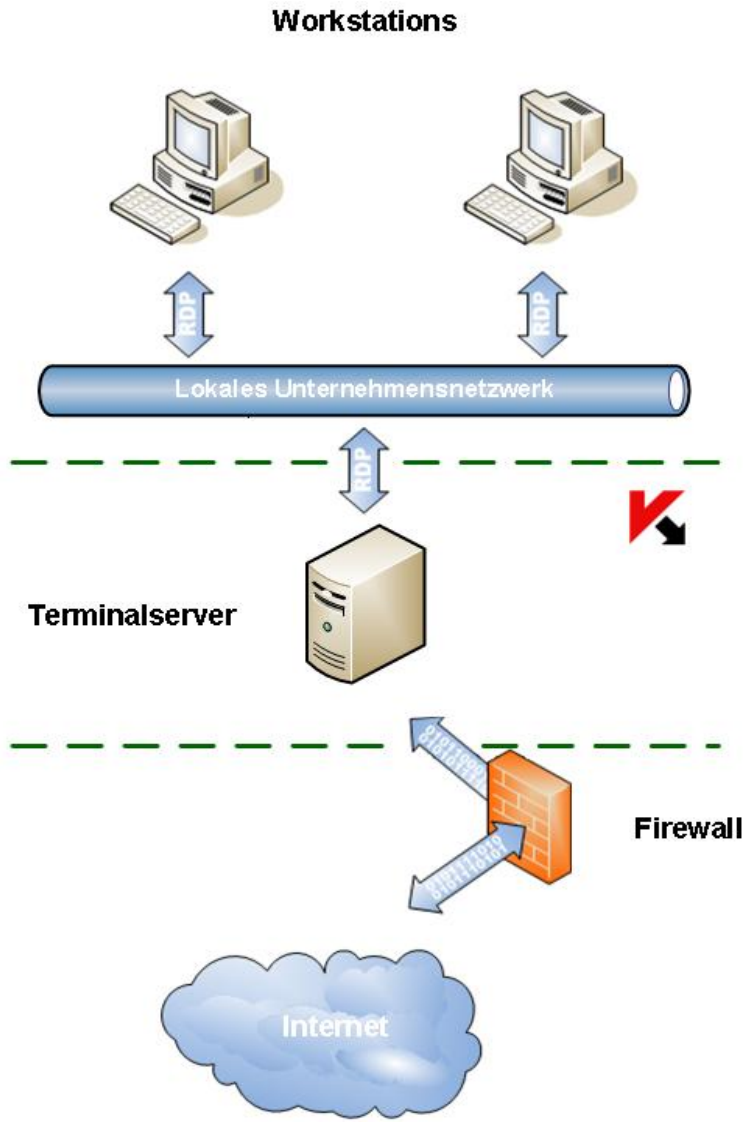

Abbildung 3: Schutzschema für Terminalserver

Kaspersky Anti-Virus bietet folgende Möglichkeiten:

- Schutz für Terminalbenutzer, die im Modus zur Desktop- und Programm-Veröffentlichung arbeiten
- Benachrichtigung der Terminalbenutzer durch den Terminaldienst
- Audit für Aktionen mit Dateien und Skripten der Terminalbenutzer

Weitere Informationen finden Sie im *Administratorhandbuch für Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition.*

SCHUTZ VON NETZWERKSPEICHERN

Wenn Kaspersky Anti-Virus auf einem Server mit einem Microsoft Windows-Betriebssystem installiert ist, werden Netzwerkspeicher vor Viren und anderen Bedrohungen für die Computersicherheit geschützt, die bei der Übertragung von Dateien eindringen können.

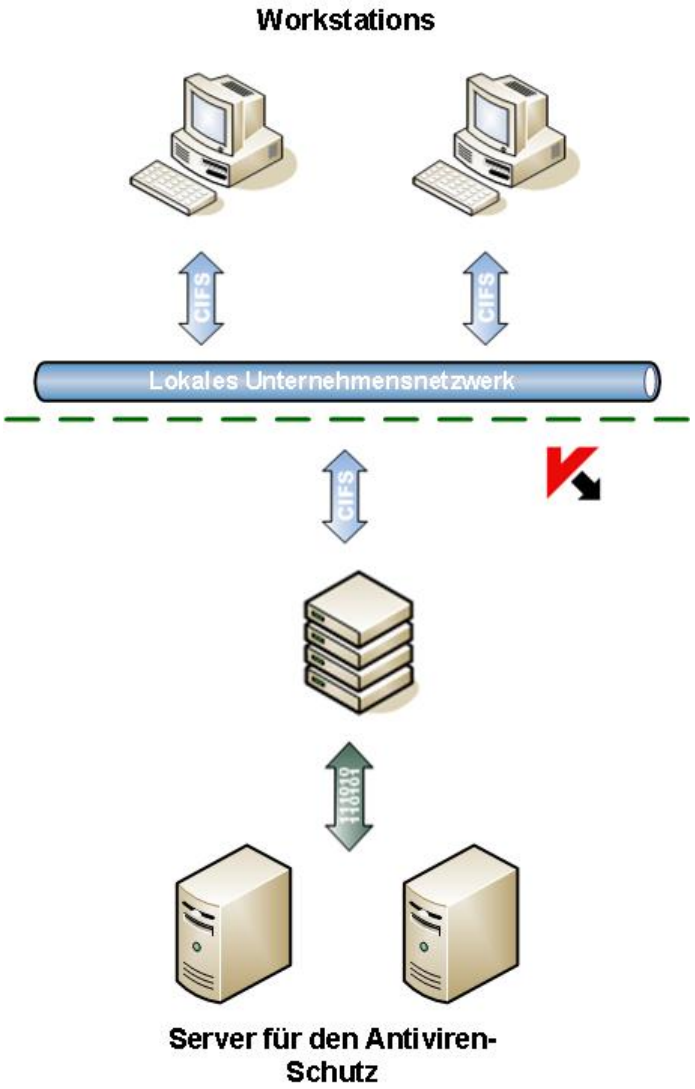

Abbildung 4: Schema des Schutzes von Netzwerkspeichern

Wenn Workstations versuchen, Dateien zu lesen oder zu ändern, die sich in den Netzwerkfreigaben (network share) eines Netzwerkspeichers befinden, werden diese Dateien von Kaspersky Anti-Virus untersucht. Der Netzwerkspeicher erlaubt das Lesen oder Ändern einer Datei, wenn Kaspersky Anti-Virus diese Datei als sicher eingestuft hat. Wenn eine Datei von Kaspersky Anti-Virus als infiziert oder möglicherweise infiziert eingestuft wurde, verbietet der Netzwerkspeicher das Lesen oder Ändern der Datei. In Kaspersky Anti-Virus können Sie Aktionen festlegen, die das Programm mit infizierten und möglicherweise infizierten Dateien ausführen soll. Folgendes Vorgehen gilt als Standard: Infizierte Dateien werden desinfiziert, irreparable Objekte werden gelöscht (sofern diese Aktion auf dem Netzwerkspeicher verfügbar ist) und möglicherweise infizierte Dateien werden in die Quarantäne verschoben. Bevor eine Datei desinfiziert oder gelöscht wird, legt Kaspersky Anti-Virus im Backup eine Sicherungskopie an.

Weitere Informationen finden Sie im *Handbuch für die Implementierung von Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition für den Schutz von Netzwerkspeichern.*

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Dieser Abschnitt beschreibt die Möglichkeiten für die technische Unterstützung und die Support-Richtlinien.

IN DIESEM ABSCHNITT

ÜBER TECHNISCHEN SUPPORT

Wenn Sie keine Lösung für Ihr Problem in der Dokumentation oder in anderen Informationsquellen zum Programm gefunden haben, empfehlen wir Ihnen, den technischen Support von Kaspersky Lab zu kontaktieren. Die Spezialisten des Technischen Supports beantworten Ihre Fragen zur Installation und Verwendung des Programms.

Der Technische Support steht nur den Benutzern zur Verfügung, die eine kommerzielle Lizenz für die Programmnutzung gekauft haben. Benutzer, die eine Testlizenz verwenden, können den Technischen Support nicht nutzen.

Bevor Sie sich an unseren Technischen Support wenden, machen Sie sich bitte mit unseren Support-Regeln vertraut (http://support.kaspersky.com/de/support/rules).

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- Telefonische Kontaktaufnahme mit dem Technischen Support von Kaspersky Lab
- Anfrage an den Technischen Support von Kaspersky Lab über den Webdienst Kaspersky CompanyAccount senden.

TECHNISCHER SUPPORT ÜBER DAS KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount (https://companyaccount.kaspersky.de/) ist ein Webservice für Unternehmen, die Kaspersky-Lab-Programme verwenden. Der Webdienst von Kaspersky CompanyAccount ist für die Interaktion der Benutzer mit den Spezialisten von Kaspersky Lab mithilfe elektronischer Anfragen vorgesehen. Im Webdienst Kaspersky CompanyAccount kann der Status der Verarbeitung elektronischer Anfragen durch Kaspersky Lab-Spezialisten zurückverfolgt sowie die Chronik der elektronischen Anfragen gespeichert werden.

Sie können alle Mitarbeiter Ihrer Firma unter einem Benutzerkonto für Kaspersky CompanyAccount registrieren. Ein Benutzerkonto ermöglicht Ihnen die zentralisierte Verwaltung von elektronischen Anfragen aller registrierter Mitarbeiter an Kaspersky Lab sowie die Verwaltung der Rechte dieser Mitarbeiter in Kaspersky CompanyAccount.

Der Webdienst Kaspersky CompanyAccount ist in folgenden Sprachen verfügbar:

- Englisch
- Deutsch
- Russisch
- Spanisch
- Polnisch
- Französisch
- Italienisch
- Portugiesisch
- Japanisch

Mehr über Kaspersky CompanyAccount erfahren Sie auf der Webseite des Technischen Supports (http://support.kaspersky.com/de/faq/companyaccount_help).

TECHNISCHER SUPPORT AM TELEFON

Bei dringenden Problemen können Sie die Spezialisten vom Technischen Support von Kaspersky Lab telefonisch kontaktieren. (http://support.kaspersky.com/de/support/contacts).

Bitte machen Sie sich mit den Regeln für die Nutzung des Technischen Supports vertraut, bevor Sie sich an den Technischen Support wenden (http://support.kaspersky.com/de/support/rules). Die Regeln enthalten Informationen darüber, zu welchen Zeiten Sie beim Technischen Support von Kaspersky Lab anrufen können und welche Daten die Spezialisten des Technischen Supports benötigen, um Ihnen helfen zu können.

PROTOKOLLIERUNGSDATEI UND AVZ-SKRIPT VERWENDEN

Wenn Sie sich mit einem Problem an die Support-Experten von Kaspersky Lab wenden, werden Sie möglicherweise darum gebeten, einen Bericht über Kaspersky Anti-Virus zu erstellen und den Bericht an den Kaspersky-Lab-Support zu schicken. Die Support-Experten von Kaspersky Lab können zusätzlich eine *Protokolldatei* anfordern. Eine Protokolldatei ermöglicht eine schrittweise Prüfung von ausgeführten Programmbefehlen. Dadurch lässt sich erkennen, auf welcher Etappe ein Fehler aufgetreten ist.

Aufgrund einer Analyse der von Ihnen eingesandten Daten können die Support-Experten von Kaspersky Lab ein AVZ-Skript erstellen, das dann an Sie geschickt wird. Mit Hilfe von AVZ-Skripten können die laufenden Prozesse auf Bedrohungen analysiert, der Computer auf Bedrohungen untersucht, infizierte Dateien desinfiziert bzw. gelöscht, und ein Ergebnisbericht über die Untersuchung des Computers erstellt werden.

GLOSSAR

A

ADMINISTRATIONSSERVER

Programmkomponente von Kaspersky Security Center, mit der die zentralisierte Speicherung von Informationen über die im Unternehmensnetzwerk installierten Programme von Kaspersky Lab sowie deren Verwaltung realisiert wird.

ANTIVIREN-DATENBANKEN

Datenbanken mit Informationen über Computer-Bedrohungen, die Kaspersky Lab beim Erscheinen der Antiviren-Datenbanken bekannt sind. Mithilfe der Einträge in den Antiviren-Datenbanken wird in den Untersuchungsobjekten schädlicher Code identifiziert. Die Antiviren-Datenbanken werden von den Experten von Kaspersky Lab gepflegt und stündlich aktualisiert.

ARCHIV

Datei, die in sich eine oder mehrere Dateien "enthält", die selbst wiederum Archive sein können.

AUFGABE

Funktionen, die von einem Programm von Kaspersky Lab ausgeführt werden und als Aufgabe durchgeführt werden, beispielsweise: Echtzeitschutz von Dateien, Vollständige Untersuchung des Computers, Datenbanken-Update.

AUFGABENEINSTELLUNGEN

Einstellungen für die Programmausführung, die für den jeweiligen Aufgabentyp gelten.

AUTOSTART-OBJEKTE

Auswahl von Programmen, die für den Start und die ordnungsgemäße Ausführung des auf Ihrem Computer installierten Betriebssystems und der Software. Diese Objekte werden bei jedem Start des Betriebssystems gestartet. Es gibt Viren, die genau diese Objekte infizieren können, was beispielsweise dazu führen kann, dass das Betriebssystem nicht gestartet wird.

B

BACKUP

Spezieller Speicher für die Aufbewahrung von Sicherungskopien der Dateien, die vor deren erster Desinfizierung oder Löschung erstellt werden.

D

DESINFEKTION DER OBJEKTE

Verarbeitungsmethode für infizierte Objekte, die eine vollständige oder teilweise Wiederherstellung der Daten zum Ergebnis hat. Nicht alle infizierten Objekte können desinfiziert werden.

F

FEHLALARM.

Situation, in der ein nicht infiziertes Objekt von einem Programm von Kaspersky Lab als infiziert eingestuft wird, weil sein Code an einen Viruscode erinnert.

H

HEURISTISCHE ANALYSE

Technologie zur Erkennung von Bedrohungen, die mithilfe der aktuellen Version der Programm-Datenbanken von Kaspersky Lab nicht bestimmt werden können. Erlaubt das Auffinden von Dateien, die möglicherweise einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten.

Dateien, in denen während der heuristischen Analyse Schadcode erkannt wurde, erhalten den Status möglicherweise infiziert.

HEURISTISCHE ANALYSE

Modul von Kaspersky Anti-Virus, das die heuristische Analyse durchführt.

I

INFIZIERBARE DATEI

Datei, die Kraft ihrer Struktur bzw. ihres Formates von Betrügern als "Behälter" für die Aufbewahrung und Verteilung von schädlichem Code verwendet werden kann. In der Regel handelt es sich hierbei um ausführbare Dateien mit den Erweiterungen com, exe, dll u. a. Das Risiko eines Eindringens von schädlichem Code in solche Dateien ist ausreichend hoch.

INFIZIERTE DATEI

Datei, innerhalb derer sich schädlicher Code befindet (bei der Untersuchung der Datei wurde Code eines bekannten Programms gefunden, das eine Bedrohung darstellt). Die Experten von Kaspersky Lab empfehlen, nicht mit solchen Dateien zu arbeiten, da dies zu einer Infizierung Ihres Computers führen könnte.

M

MÖGLICHERWEISE INFIZIERTE DATEI

Datei, innerhalb derer sich entweder modifizierter Code eines bekannten Virus, oder Code, der an einen Virus erinnert, bis jetzt jedoch Kaspersky Lab nicht bekannt war, befindet. Möglicherweise infizierte Dateien werden mithilfe der heuristischen Analyse gefunden.

O

OLE-OBJEKT

Datei, die mit einer anderen Datei verbunden oder in ihr integriert ist. Die Programme von Kaspersky Lab ermöglichen eine Untersuchung auf Viren in OLE-Objekten. Wenn Sie beispielsweise eine bestimmte Microsoft Office Excel® - Tabelle in ein Microsoft Office Word-Dokument einfügen, wird diese Tabelle als OLE-Objekt untersucht.

P

PROGRAMMEINSTELLUNGEN

Einstellungen für die Programmausführung, die für alle Aufgabentypen gleich sind, und für die Ausführung des Programms an sich gelten, beispielsweise: Einstellungen der Programmleistung, Einstellungen für das Führen von Berichten, Backup-Einstellungen.

Q

QUARANTÄNE

Ordner, in den möglicherweise infizierte Objekte verschoben werden, die Kaspersky Anti-Virus findet. Dateien werden in der Quarantäne in verschlüsselter Form gespeichert, um eine Gefährdung des Computers auszuschließen.

S

SCHWACHSTELLE

Unzulänglichkeit im Betriebssystem oder Programm, die von den Herstellern von Schadsoftware zum Eindringen in das Betriebssystem oder Programm und zur Beschädigung dessen Integrität verwendet werden kann. Eine große Anzahl von Schwachstellen im Betriebssystem macht es unsicher, da Viren, die in das Betriebssystem eindringen, Abstürze sowohl des Betriebssystems selbst als auch der installierten Programme hervorrufen können.

SIGNATURANALYSE

Technologie zum Erkennen von Bedrohungen, die die Datenbanken in Kaspersky Anti-Virus verwendet, welche eine Beschreibung der bekannten Bedrohungen und Methoden für ihre Beseitigung enthalten. Ein Schutz mithilfe der Signaturanalyse gewährleistet die minimal erforderliche Sicherheitsstufe. Gemäß der Empfehlung der Experten von Kaspersky Lab ist diese Methode immer aktiviert.

U

UPDATE

Vorgang des Austauschens bzw. Hinzufügens von neuen Dateien (Datenbanken oder Programm-Module), die vom Update-Server von Kaspersky Lab stammen.

KASPERSKY LAB

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen, die Computer vor Viren und anderer Malware, Spam, Netzwerk- und Hackerangriffen schützen.

Seit 2008 gehört Kaspersky Lab international zu den vier führenden Unternehmen im Bereich der IT-Sicherheit für Endbenutzer (Rating des "IDC Worldwide Endpoint Security Revenue by Vendor"). Nach einer Studie des Marktforschungsinstituts COMCON TGI-Russia war Kaspersky Lab 2009 in Russland der beliebteste Hersteller von Schutzsystemen für Heimanwender.

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern mit Hauptsitz in Moskau und verfügt über fünf regionale Niederlassungen, die in Russland, West- und Osteuropa, im Nahen Osten, in Afrika, Nord- und Südamerika, Japan, China und anderen Ländern aktiv sind. Das Unternehmen beschäftigt über 2.000 hochspezialisierte Mitarbeiter.

PRODUKTE. Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die Palette der Heimanwender-Produkte umfasst Antiviren-Programme für Desktops, Laptops, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Programme und Services für den Schutz von Workstations, Datei- und Webservern, Mail-Gateways und Firewalls. In Verbindung mit Administrationstools ermöglichen es diese Lösungen, netzwerkweit einen effektiven automatisierten Schutz vor Computerbedrohungen aufzubauen. Die Produkte von Kaspersky Lab sind durch namhafte Testlabore zertifiziert, mit den Programmen der meisten Softwarehersteller kompatibel und für die Arbeit mit unterschiedlichen Hardwareplattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Sie finden und analysieren jeden Tag Hunderte neuer Computerbedrohungen. Mit diesem Wissen entwickeln sie Mittel, um Gefahren zu erkennen und zu desinfizieren. Diese Informationen fließen in die Datenbanken ein, auf die die Kaspersky-Programme zurückgreifen. *Die Antiviren-Datenbanken von Kaspersky Lab werden stündlich aktualisiert*, *die Anti-Spam-Datenbanken im 5-Minuten-Takt*.

TECHNOLOGIEN. Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Softwarehersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Openwave Messaging (Ireland), D-Link (Taiwan), M86 Security (USA), GFI Software (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), Netasq+Arkoon (France), NETGEAR (USA), Parallels (USA), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

AUSZEICHNUNGEN. Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So wurde Kaspersky Anti-Virus 2010 in Tests des renommierten österreichischen Antiviren-Labors AV-Comparatives mehrfach mit dem Premium-Award Advanced+ ausgezeichnet. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 300 Millionen Anwender. Über 200.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Webseite von Kaspersky Lab:	http://www.kaspersky.com/de
Viren-Enzyklopädie:	http://www.securelist.com/de/
Viren-Labor:	newvirus@kaspersky.com (nur zum Einsenden von möglicherweise infizierten Dateien, die zuvor archiviert wurden)
Webforum von Kaspersky Lab:	http://forum.kaspersky.com

INFORMATIONEN ZUM CODE VON DRITTHERSTELLERN

Informationen zu fremden Codes finden Sie in der Datei legal_notices.txt, die sich im Installationsordner des Programms befindet.

MARKENHINWEISE

SACHREGISTER

A

P