



W H I T E P A P E R

# Kaspersky Administration Kit

Top-Features für kleine und mittelständische Unternehmen



Für den Schutz von Computern und kompletten Netzwerken sind Kaspersky-Lösungen erste Wahl. Dabei liegt ein Schwerpunkt der Entwicklung natürlich auf den Top-Erkennungsraten und dem fortschrittlichen proaktiven Schutz. Aber das ist für Unternehmen nur die halbe Miete, denn die sicherste und leistungsfähigste Security-Software nützt nichts, wenn sie zu aufwändig zu administrieren, zu komplex zu bedienen und zu unflexibel ist, um auf die sich stets ändernden Anforderungen zu reagieren. Mit dem Administration Kit liefert Kaspersky eine zentrale und vielseitige Management-Komponente für seine Security-Produkte, die alle Ansprüche einer modernen und leistungsfähigen Unternehmens-IT erfüllt. Das Administration Kit gewährt dem IT-Personal Vollzugriff auf alle Kaspersky-Lösungen im Netzwerk und erlaubt so die zentrale Verwaltung der netzwerkweiten Security-Software von einem Standard-PC aus.

Das Administration Kit besteht aus drei Komponenten: Der Administration Server ist das Herzstück des Administration Kit. Er ist für die Installation und Deinstallation auf entfernten Rechnern zuständig, verwaltet Lizenzschlüssel und speichert die Einstellungen der verteilten Installationen. Darüber hinaus startet er festgelegte Tasks, überwacht deren Ausführung, beobachtet den Schutzstatus der Antiviren-Lösung und aktualisiert die Antiviren-Datenbank sowie die Programm-Module. Zudem sammelt er Daten für Statistiken und zeichnet Events auf, versendet Benachrichtigungen und erstellt Reports. Der Administration Server arbeitet ressourcenschonend und kann auf vorhandener Hardware installiert werden. Seine Skalierbarkeit erlaubt aber auch den Aufbau einer Hierarchie von Servern.

Die Network Agents, die automatisiert auf jedem PC installiert werden, sind für die Kommunikation zwischen den zu überwachenden Clients und dem Administration Server zuständig. Sie empfangen die Tasks und verarbeiten die Informationen über Client-Einstellungen, die der Server verschickt. Ihrerseits senden sie wieder Statusmeldungen an den Server zurück. Der große Vorteil beim Einsatz dieser Agenten ist, dass über sie auch die Abwicklung von Remote-Installationen abläuft, für die sie die dafür nötigen Zugriffsrechte besitzen.

Die Administration Console ist ein Snap-in für die Microsoft Management Console (MMC) und fungiert als Schnittstelle für den Administration Server. So können Administratoren die Antivirus-Lösungen bequem von Ihrem Arbeitsplatz aus verwalten oder greifen über RDP zentral vom Server aus zu

### 1. Höchste Sicherheit rund um die Uhr

Mit dem Kaspersky Administration Kit gewährleisten Sie den Schutz aller Computer in Ihrem Netz, und das 24 Stunden am Tag, sieben Tage die Woche ohne großen Aufwand. So spielen die eingebauten Automatisierungen beispielsweise Updates ohne Zutun der Nutzer und Administratoren ein und halten die verwendete Schutz-Software selbständig auf dem aktuellen Stand. Außerdem kontrollieren Richtlinien die Einhaltung der festgelegten Schutzstandards. Über definierbare Tasks reagiert das Kaspersky Administration Kit selbständig auf bestimmte Vorkommnisse - etwa einen Virenausbruch oder den Ausfall eines Update-Servers. So sind die IT-Systeme auch dann geschützt, wenn die Administratoren nicht vor Ort sind.

Per Synchronisation halten sich Server und Clients, aber auch Administrations-Server und Agenten untereinander immer auf dem aktuellsten Stand. Alle 15 Minuten melden sich die Network Agents beim zuständigen Server und berichten über den aktuellen Status. Für den Problemfall, etwa einen Virenausbruch, können Administratoren neue Richtlinien hinterlegen oder direkt mit vordefinierten Tasks antworten - auch das funktioniert vollautomatisch.

### 2. Schutz für das gesamte Netz

Das Kaspersky Administration Kit stellt die Schutzzentrale für das gesamte Netzwerk dar – sowohl in reinen Windows-Umgebungen als auch in heterogenen Netzen etwa mit Linux-Workstations und –File-Servern. Der Administrator versorgt die Maschinen lediglich mit den aktuellsten Programmen, Updates und den richtigen Einstellungen.

Außerdem wichtig: Flexible Einstellungsmöglichkeiten passen den Schutz zielgenau auf unterschiedliche Nutzergruppen an. Das Kaspersky Administration Kit bietet dafür die Sicht auf ein logisches Netzwerk. PCs können unabhängig von der technischen Anbindung in Gruppen eingeteilt werden, für die die gleichen Einstellungen gelten. Scan-Parameter sind für einzelne Domains, Workgroups, Active Directories und Subnetze individuell einstellbar.

Neue Rechner, egal ob mit oder ohne Security-Software, tauchen automatisch in der Übersicht auf und können per Task mit Agent und Schutz-Software versorgt werden. Mit einem IP-Subnetz-Scan werden komplette Subnetze gefunden und in Administrations-Gruppen eingeteilt.

### 3. Kostenlos und maßgeschneidert

Wer Unternehmens-Lizenzen eines Kaspersky-Security-Produkts erwirbt, kann ohne Extrakosten das Administration Kit für deren Verwaltung nutzen. Kunden erhalten dabei aber kein System von der Stange, sondern eine hoch flexible Software, die mit zahlreichen Features an die eigenen Bedürfnisse der IT-Infrastruktur anpassbar ist.

So ist es möglich, eine hierarchische Struktur von Administrations-Servern zu bauen, etwa wenn in einer Firma große Abteilungen existieren oder Außenstellen angebunden werden sollen. Dabei gibt es immer einen Master-Server, der wiederum andere Slave-Server verwaltet. Noch flexibler ist eine Struktur mit speziellen Agenten, die auf Client-PCs laufen und einige Aufgaben des Servers wie Updates übernehmen.

### 4. Zentrale Steuerung aller Funktionen

Schon bei wenigen PCs stellt die lokale Verwaltung von Security-Software einen hohen Aufwand dar, der mit einer zentralen Management-Software wie dem Kaspersky Administration Kit erheblich reduziert werden kann. Für typische Mittelständler sind etwa 20 bis 200 aus Servern und Workstations bestehende PCs üblich, die unterschiedliche Betriebssysteme einsetzen. Immer mehr kommen auch mobile Arbeitsstationen zum Einsatz, etwa Notebooks von Außendienstmitarbeitern. Die Schwierigkeit besteht darin, nicht nur die Security-Software zu warten, sondern auch die unterschiedlichsten Anforderungen zu gewährleisten. Das geht mit dem Administration Kit sehr einfach und fängt beim Deployment an:

Das Administration Kit startet beim ersten Einsatz mit einem Assistenten, der Nutzer beim Anlegen eines logischen Netzwerks unterstützt, welches mit der vorhandenen Domänenstruktur übereinstimmt. Mit den im Administration Kit integrierten Hilfswerkzeugen kann die Verwaltungsstruktur aber auch anders angelegt werden. Das Programm zeigt unter dem Menüpunkt Netzwerk: Domänen eine Übersicht der vorhandenen Netzwerk-Rechner - nach Domänen und Arbeitsgruppen - unterteilt an. Administratoren können entweder das komplette Windows-Netz, ein vorhandenes Active Directory oder IP-Subnetze nach PCs absuchen. Praktisch: Das Administration Kit passt die Anzeige der Struktur an. So kann diese beispielsweise nach IP-Subnetzen unterteilt werden, damit auch größere Installationen übersichtlich dargestellt werden.

Die Zusammenfassung von Rechnern zu logischen Gruppen bringt den Vorteil, dass Nutzer mit Gruppentasks einmal eine Aufgabe definieren und diese dann auf alle PCs in dieser Gruppe anwenden können. Neben der 1:1-Abbildung der vorhandenen IT-Struktur lassen sich die Gruppen auch manuell verwalten und etwa gemäß der Firmenstruktur Gruppen für Vertrieb, Entwicklung, Marketing anlegen.

Natürlich ist ein Administration-Server auch für zentrale Updates geeignet. Der Admin-Server verbindet sich mit einem Kaspersky-Webserver und versorgt dann seinerseits die Clients im Netz. Weitere Admin-Server kontaktieren entweder den Master-Server oder laden selbst die Updates aus dem Internet. Alternativ können die Clients sich auch direkt über den Kaspersky-Server aktualisieren. Durch diesen redundanten Aufbau kann der Ausfall einer Update-Quelle ohne Sicherheits-einbußen verkraftet werden.

Ein zusätzliches Plus an Sicherheit: Für Updates stehen ein Pull- sowie ein Push-Mechanismus bereit. Pull ist die oben beschriebene Methode, wenn die Clients von sich aus aktiv werden. Beim Push-Verfahren initiiert der Administrationsserver die Verteilung, etwa über einen Gruppen-Task.

### 5. Eingebaute Kontroll-Tools

Um eine Security Policy ohne großen Zeitaufwand umzusetzen und deren Einhaltung zu kontrollieren, hat das Administration Kit alles Nötige an Bord. Mit Gruppen-Richtlinien (Policies) und Gruppen-Tasks bleiben alle Rechner stets geschützt:

#### Richtlinien

Über Richtlinien verwaltet der Administrator alle Einstellungen an den Komponenten der verwendeten Security-Software. Zum Beispiel lässt sich mit einer Richtlinie die Sicherheitsstufe des Virenschanners in einzelnen Gruppen anpassen oder eine Abschaltung des Schutzes selbst bei lokalen Admin-Rechten verhindern. Das Kit unterscheidet zwischen aktiven und inaktiven Richtlinien, letztere können bei Bedarf – etwa einem Virusausbruch – schnell aktiviert werden. Ein Spezialfall sind Richtlinien für mobile Nutzer.

#### Tasks

Die zentrale Steuerung von Installationen, Updates, Key-Management und auch die Virensuche steuern so genannte Tasks. Beispielsweise ist mit nur wenigen Mausklicks ein Task angelegt, der alle Festplatten der Marketing-Gruppe auf Viren hin überprüft. Für die Festlegung von Richtlinien und Tasks stehen leistungsfähige Wizards bereit.

Zusätzlich stehen globale Tasks zur Verfügung, welche nicht nur auf eine Gruppe, sondern auf das gesamte logische Netzwerk angewendet werden.

## 6. Kompatibel mit unterschiedlichsten Systemen

Das Kaspersky Administration Kit verlangt keine bestimmte Netzwerkarchitektur, es passt sich vielmehr flexibel an verschiedenste Bedürfnisse an. Ein Highlight ist etwa die dynamische Active-Directory-Integration; Änderungen am Active-Directory werden sofort im Administration Kit wirksam.

Außerdem verwaltet das Administration Kit sowohl Windows Workstations, Windows Server als auch Exchange, Lotus Notes/Domino, ISA Server, SMTP-Gateways sowie Linux-Workstations und -Fileserver.

Als Datenbank können bereits im Netz befindliche Server wie Microsoft SQL Server 2000, Microsoft SQL Server 2005 oder die leichtgewichtigen Varianten Microsoft SQL Server Desktop Engine 2000 (MSDE 2000) und Microsoft SQL Server 2005 Express Edition genutzt werden. Ebenso wird MySQL unterstützt.

Umfangreiche Funktionen lassen den Administrator die Security-Einstellungen auf unterschiedliche Anwendergruppen zuschneiden und spezielle Rechte und Optionen festlegen. Neue Gruppen können - auf der Active-Directory-Strukturbasierend-aufSubnetz-Ebene, nach Domänen oder komplett frei angelegt werden.

## 7. Schnelle Reaktion, zielgenaues Monitoring, umfangreiches Reporting

Nicht nur auf Bedrohungen durch Schadroutinen, sondern auch auf Änderungen in den internen IT-Prozessen kann das Administration Kit schnell reagieren. Durch die Abbildung der IT-Systeme auf logische Gruppen ist die gezielte Festlegung von Security-Strategien möglich.

Gegen akute Virenausbrüche helfen vordefinierte Tasks, die im Fall der Fälle angewendet werden. Außerdem sorgen Richtlinien dafür, dass im Problemfall die IT-Systeme geschützt sind. Über ein eingebautes Benachrichtigungssystem, das auf eingetretene Ereignisse reagiert, können sich Administratoren per E-Mail über Probleme informieren lassen und sind so im Ernstfall sofort gewarnt.

Immer schnell und übersichtlich informiert: Die Monitoring- und Reporting-Funktionen des Kaspersky Administration Kit unterrichten Administratoren etwa über den Schutzzustand, zeigen Statistiken über das Netzwerk, die definierten Gruppen, eine Aufstellung der Virenaktivität und den Update-Status.

Auch kritische Ereignisse wie einen nicht aktuellen Virens Scanner haben Administratoren mit dem Kaspersky Administration Kit sofort im Blick. Zudem zeigt die Computer-Auswahl PCs mit dem Status »kritisch« separat an.

Virenfunde werden lokal auf den Clients in Quarantäne geschickt und können von der Konsole aus analysiert werden. Dabei liefert der Agent alle Informationen automatisch an den Server.

## 8. Software-Verteilung inklusive

Über das Administration Kit lassen sich sämtliche Kaspersky-Programme verteilen, installieren, konfigurieren und auch wieder entfernen. Dabei kommunizieren Server und Agent auf den jeweiligen PCs miteinander. Der Vorteil dabei: Der Agent hat alle Rechte, um Software auf dem Remote-System zu installieren. Resultat: Über spezielle Zugriffs- oder Benutzerrechte muss sich niemand mehr Gedanken machen. Die Software-Verteilung funktioniert auch per Multicast auf mehrere Computer gleichzeitig

Ein weiteres Highlight: Das Administration Kit kann PCs, die nicht mit Kaspersky-Software geschützt sind, ausblenden oder die darauf befindlichen Virens Scanner deinstallieren.

### Kaspersky Lab

Kaspersky Lab reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crime-ware, Hacker, Phishing-Attacken und Spam.

Die Produkte des global agierenden Unternehmens mit Hauptsitz in Moskau haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und minimalen Reaktionszeiten einen Namen gemacht.

Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen.

### Kontakt

Kaspersky Labs GmbH  
Steinheilstr. 13  
85053 Ingolstadt

Telefon: +49 (0)841 981 89 0  
Telefax: +49 (0)841 981 89 100

info@kaspersky.de  
www.kaspersky.de