▶ KASPERSKY SYSTEMS MANAGEMENT

Mehr Sicherheit und weniger Komplexität durch zentrale IT-Verwaltungstools.

Nicht gepatchte Schwachstellen in gängigen Programmen sind eine der größten Bedrohungen für die IT-Sicherheit in Unternehmen. Dieses Risiko wird durch die zunehmende Komplexität von IT-Umgebungen noch verschärft – wenn Sie nicht wissen, welche Komponenten überhaupt vorhanden sind, wie sollen Sie diese dann schützen?

Durch Zentralisierung und Automatisierung von grundlegenden Sicherheits-, Konfigurations- und Verwaltungsabläufen, z. B. Vulnerability Assessment, Patch- und Update-Distribution, Bestandsverwaltung und Programm-Rollouts, sparen IT-Administration nicht nur Zeit, sie sorgen auch für eine optimierte Sicherheit.

Kaspersky Systems Management trägt zur Minimierung von IT-Sicherheitsrisiken bei und reduziert die Komplexität in der IT. Nun ist eine umfassende Kontrolle und Transparenz aller vorhandenen Geräte, Programme und Benutzer über eine einzige Benutzeroberfläche möglich.

- **Vulnerability Assessment und Patch Management**
- **Hardware- und Software-Bestandslisten**
- **Softwareinstallation und Troubleshooting per Fernzugriff auch in Zweigstellen**
- **Deployment von Betriebssystemen**
- **SIEM-Integration**
- **Rollenbasierte Zugriffskontrolle**
- **Zentrales Management**

VERBESSERTE SICHERHEIT

Verbesserte IT-Sicherheit und geringe Belastung bei Routineabläufen durch zeitnahe, automatisierte Patching- und Update-Funktionen. Automatische Erkennung und Priorisierung von Schwachstellen ermöglicht mehr Effizienz und reduziert die Ressourcenbelastung. Unabhängige Tests[1] beweisen, dass Kaspersky Lab die umfassendste und schnellste Patch- und Update-Distribution bietet.

KONTROLLE UND VOLLSTÄNDIGE TRANSPARENZ

Vollständige Netzwerktransparenz von einer zentralen Verwaltungskonsole beendet das Rätselraten für Administratoren: Alle Geräte und Programme inklusive Gastgeräte, die sich im Netzwerk anmelden, werden erkannt. Dies ermöglicht eine zentrale Kontrolle des Benutzer- und Gerätezugriffs auf geschäftliche Daten und Programme auf Grundlage von IT-Richtlinien.

ZENTRALES MANAGEMENT

Das Systems Management von Kaspersky Lab ist eine verwaltete Komponente von Kaspersky Security Center. Zur Automatisierung von IT-Routineaufgaben wird jede Funktion unter Verwendung einheitlicher, intuitiver Befehle und Benutzeroberflächen über diese zentrale Konsole verwaltet.

1 Von Kaspersky Lab in Auftrag gegebener und von der AV-TEST GmbH ausgeführter Test von Patch-Management-Lösungen (Juli 2013)

FUNKTIONEN

VULNERABILITY SCANNING UND PATCH MANAGEMENT

Automatisierte Scanabläufe ermöglichen eine rasche Erkennung, Priorisierung und Behebung von Schwachstellen. Patches und Updates werden automatisch innerhalb kürzester Zeit[2] für Software von Microsoft und anderen Herstellern bereitgestellt. Der Administrator wird über den Status der Patchinstallation informiert. Weniger wichtige Fixes können auf Zeiten nach Geschäftsschluss verschoben werden. Durch Wake-on-LAN-Befehle funktioniert dies sogar bei ausgeschalteten Computern. Die Multicast-Übermittlungstechnik ermöglicht die lokale Verteilung von Patches und Updates in Zweigstellen und reduziert so die Anforderungen an die Bandbreite.

HARDWARE- UND SOFTWARE-BESTANDSLISTEN

Automatische Erkennung, Bestandsaufnahme, Benachrichtigung und Nachverfolgung von Hard- und Software, inklusive Wechseldatenträgern, geben Administratoren einen detaillierten Einblick in die im Unternehmensnetzwerk verwendeten Geräte und Ressourcen. Auch Gastgeräte werden erkannt und erhalten nach Bedarf Internetzugriff. Die Lizenzkontrolle liefert einen Überblick über die Anzahl der Netzwerk-Nodes und die Ablaufdaten.

Hinweise zum Kauf

Kaspersky Systems Management ist eine Komponente des Kaspersky Security Center und ist in folgende Lösungen integriert:

- Kaspersky Endpoint Security for Business – Advanced
- Kaspersky Total Security for Business

Kaspersky Systems Management kann auch als separate Lösung erworben werden. Setzen Sie sich für Informationen und Preise mit Ihrem Vertriebspartner in Verbindung.

FLEXIBLE BEREITSTELLUNG VON BETRIEBSSYSTEM UND PROGRAMMEN

Zentrales und einfaches Erstellen, Speichern, Klonen und Deployment von optimal geschützten System-Images. Deployment nach Büroschluss per Wake-on-LAN inklusive Bearbeitung nach der Installation für mehr Flexibilität. UEFI-Unterstützung

SOFTWAREBEREITSTELLUNG

Zentrale Bereitstellung/Updates über eine Konsole. Über 100 weitverbreitete, vom Kaspersky Security Network identifizierte Programme können bei Bedarf nach Büroschluss installiert werden. Vollständige Unterstützung für Remote-Troubleshooting inklusive erweiterten Sicherheitsfunktionen mit Benutzerberechtigungen und Sitzungsprotokollen/Audits. Weniger Datenverkehr mit Zweigstellen dank Multicast-Technologie, die eine lokale Software-Distribution ermöglicht.

SIEM-INTEGRATION

Unmittelbare Meldung und Übermittlung von Ereignissen in führende SIEM-Systeme: IBM® QRadar® und HP ArcSight. Erfassung von Protokollen und anderen sicherheitsrelevanten Daten für weniger zeit- und toolintensive Analysen durch den Administrator bei gleichzeitiger Vereinfachung des unternehmensweiten Reporting.

ROLLENBASIERTE ZUGRIFFSKONTROLLE

Unterscheidung von administrativen Rollen und Aufgaben in komplexen Netzwerken. Individuelle Anpassung der Konsolenansichten gemäß Rolle und Berechtigung.

ZENTRALES MANANGEMENT

Die integrierte Verwaltungskonsole Kaspersky Security Center ermöglicht die Sicherheitsverwaltung für Desktops, Mobilgeräte und virtualisierte Endpoints im gesamten Netzwerk über eine einzige Benutzeroberfläche.

2 Von Kaspersky Lab in Auftrag gegebener und von der AV-TEST GmbH ausgeführter Test von Patch-Management-Lösungen (Juli 2013)

Kaspersky System Management/Version 0.3/Jan 15/Global

KASPERSKY lab