Kaspersky Vulnerability und Patch Management

Weniger Komplexität und mehr Sicherheit durch zentrale IT-Verwaltungstools

Wichtigste Vorteile

- Automatische Schwachstellen-Erkennung und -Priorisierung
- Automatische Verteilung von Patches und Updates für mehr als 150 Anwendungen
- Unterstützung für Patch-Testmodus
- Geplante Patch-Verteilung
- Optimierung des Datenverkehrs
- Ergebnisüberwachung und -Reporting
- Umfassende Client-Verwaltungstools
- Softwareinstallation und Troubleshooting per Fernzugriff auch in Zweigstellen
- Deployment von Betriebssystemen

Nicht gepatchte Schwachstellen in gängigen Programmen sind eine der größten Bedrohungen für die IT-Sicherheit in Unternehmen. Das Problem dabei sind nicht unbedingt Zero-Day-Schwachstellen, sondern die zunehmende IT-Komplexität, die es noch komplizierter macht, die Lücken in anfälliger Software rechtzeitig zu schließen: Wenn Sie nicht wirklich wissen, was Sie haben, wie sollen Sie dann für Sicherheit sorgen?

Die Verwaltung und Verteilung von Softwareaktualisierungen bei gleichzeitiger ständiger Überprüfung auf potenzielle Schwachstellen ist eine der wichtigsten, anspruchsvollsten und ressourcenintensivsten Aufgaben einer IT-Abteilung. Durch die Zentralisierung und Automatisierung von grundlegenden Sicherheits-, Konfigurations- und Verwaltungsabläufen wie Schwachstellenbewertung, Patch- und Update-Verteilung, Bestandsverwaltung und Anwendungsbereitstellungen spart Kaspersky Vulnerability and Patch Management nicht nur Zeit, sondern optimiert auch die Sicherheit.

Vollständige Transparenz

Vollständige Netzwerktransparenz von einer einzigen Konsole beendet das Rätselraten für Administratoren: Alle Geräte und Programme, inklusive Gastgeräte, die sich im Netzwerk anmelden, werden vollständig erkannt. Dies ermöglicht eine zentrale Kontrolle des Benutzer- und Gerätezugriffs auf geschäftliche Daten und Programme in Übereinstimmung mit IT-Richtlinien und Anforderungen an die Einhaltung von gesetzlichen Vorschriften.

Verbesserte Sicherheit

Sorgen Sie mit rechtzeitigen, automatisierten Patching- und Update-Funktionen für mehr IT-Sicherheit und weniger Arbeitslast durch Routineaufgaben.

Kaspersky Vulnerability and Patch Management bietet vollständige Transparenz, sodass Sie genau wissen, was Sie tun müssen, um für Sicherheit in Ihrem Unternehmen zu sorgen. Die Automatisierung des gesamten Zyklus für die Schwachstellenbewertung und das Patch Management – von der Erkennung und Priorisierung von Schwachstellen über Downloads, Tests und Verteilung von Patches und Updates bis hin zu Ergebnisüberwachung und Reporting – sorgt für mehr Effizienz und eine deutliche Reduzierung der Belastung von Ressourcen.

Rationalisieren von IT-Aufgaben

Kaspersky Vulnerability and Patch Management beinhaltet eine Reihe von Client-Verwaltungstools für die Automatisierung verschiedenster IT-Administrationsfunktionen. Die automatisierte Bereitstellung von Anwendungen, der überwachte Fernzugriff und das Troubleshooting minimieren den zeitlichen Aufwand und die erforderlichen Ressourcen für die Einrichtung neuer Workstations und die Bereitstellung neuer Programme.

Zentrale Verwaltung

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

Vulnerability Assessment und Patch Management

NETZWERK-SCANS FÜR DIE ERSTELLUNG EINER HARDWARE- UND SOFTWARE-BESTANDSAUFNAHME

Durch die automatisierte Erkennung sowie die Nachverfolgung von Hardware und Software erhalten Administratoren ausführliche Einblicke in alle Ressourcen im Unternehmensnetzwerk. Automatisierte Software-Scans ermöglichen eine schnelle Erkennung veralteter Software, die möglicherweise ein Sicherheitsrisiko darstellt und aktualisiert werden muss.

ERKENNUNG UND PRIORISIERUNG VON SCHWACHSTELLEN

Automatisierte Schwachstellen-Scans ermöglichen eine rasche Erkennung, Priorisierung und Beseitigung von Schwachstellen. Schwachstellen-Scans können automatisch bereitgestellt oder gemäß den Anforderungen des Administrators geplant werden. Eine flexible Richtlinienverwaltung vereinfacht die Verteilung aktualisierter, kompatibler Software sowie die Erstellung von Ausnahmen.

DOWNLOAD, TEST UND VERTEILUNG VON PATCHES UND UPDATES

Updates und Patches können automatisch über die Server von Kaspersky Lab heruntergeladen werden. Sie können vor der Verteilung getestet werden, um sicherzustellen, dass sie weder die Systemleistung noch die Effizienz der Mitarbeiter beeinträchtigen. Patches und Updates können unmittelbar verteilt werden, während das Patch-Deployment aufgeschoben werden kann.

ÜBERWACHUNG VON ERGEBNISSEN UND AUSFÜHRUNG VON BERICHTEN

Kaspersky Vulnerability and Patch Management benachrichtigt IT-Administratoren über den Status der Patch-Installation und ermöglicht ihnen die Ausführung von Berichten zu Scans, die Suche nach potenziellen Schwachstellen, die Verfolgung von Änderungen und zusätzliche Einblicke in die IT-Sicherheit ihres Unternehmens – sowie die Sicherheit aller Geräte und Systeme im gesamten Unternehmensnetzwerk.

ZEITSPARENDE SOFTWARE-VERTEILUNG

Deployment/Updates über eine einzige Konsole. Über 150 weit verbreitete, vom Kaspersky Security Network identifizierte Programme können nach Wunsch nach Büroschluss installiert werden. Dank Multicast-Technologie führt dies zu weniger Datenverkehr mit Zweigstellen.

Client Management Tools

REMOTETROUBLESHOOTING

Für kürzere Antwortzeiten, mehr Effizienz und einen rationalisierten Support für Remote-Standorte nutzt das Kaspersky Security Center RDP- und Windows-Desktopfreigabetechnologie (wie in Windows-Remoteunterstützung). Die Remote-Verbindung mit Clientcomputern über den Network Agent ermöglicht einen vollständigen Administratorzugriff auf die Daten und installierten Anwendungen auf dem Client, selbst wenn die TCP- und UDP-Ports des Clients geschlossen sind. Ein Autorisierungsmechanismus verhindert einen unbefugten Fernzugriff. Aus Gründen der Nachvollziehbarkeit und für Audits werden sämtliche Vorgänge protokolliert, die während einer Fernzugriffssitzung stattfinden.

BEREITSTELLUNG VON BETRIEBSSYSTEMEN

Kaspersky Vulnerability and Patch Management automatisiert und zentralisiert das Erstellen, Speichern und Klonen von gesicherten System-Images und unterstützt die Bereitstellung des Betriebssystems auf neuen Computer sowie Neuinstallationen. Alle Images werden in einem speziellen Inventar gespeichert und können umgehend bereitgestellt werden. Die Bereitstellung des Image für die Client-Workstation kann entweder über PXE-Server (Preboot eXecution Environment, auch für neue Computer ohne Betriebssystem) oder mithilfe von Kaspersky Vulnerability and Patch Management-Aufgaben (zur Bereitstellung von Betriebssystem-Images auf verwalteten Clientcomputern) durchgeführt werden.

Durch das Senden von Wake-on-LAN-Signalen können Sie Images automatisch auch außerhalb der Geschäftszeiten verteilen. UEFI wird ebenfalls unterstützt.

Hinweise zum Kauf
Kaspersky Vulnerability and Patch Management ist wie folgt verfügbar:

- Als Teil von Kaspersky Endpoint Security for Business – Advanced
- Als Teil von Kaspersky Total Security for Business
- Als Add-on für Kaspersky Endpoint Security for Business – Select
- Als eigenständige Targeted Solution

www.kaspersky.de
#truecybersecurity