Kaspersky®
Vulnerability & Patch
Management

Weniger Komplexität und mehr Sicherheit durch zentrale IT-Verwaltungstools

Nicht gepatchte Schwachstellen in gängigen Programmen sind eine erhebliche Bedrohung für die IT-Sicherheit in Unternehmen. Das Problem dabei sind nicht nur Zero-Day-Schwachstellen, sondern auch die zunehmende IT-Komplexität, die es noch schwieriger macht, Lücken in anfälliger Software rechtzeitig zu schließen: Wenn Sie nicht wissen, welche Komponenten überhaupt vorhanden sind, wie sollen Sie diese dann schützen?

Die Verwaltung von Software-Updates bei gleichzeitig ständiger Überprüfung auf potentielle Schwachstellen ist eine der wichtigsten, aber auch mühsamsten und zeitintensivsten Aufgaben von IT-Abteilungen. Durch die Zentralisierung und Automatisierung von grundlegenden Sicherheits-, Konfigurations- und Verwaltungsabläufen wie Schwachstellenbewertung, Patch- und Update-Verteilung, Bestandsverwaltung und Programm-Rollouts spart Kaspersky Vulnerability und Patch Management Zeit und optimiert die Sicherheit.

Vollständige Transparenz

Vollständige Netzwerktransparenz von einer einzigen Konsole setzt dem Rätselraten für Administratoren ein Ende 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.

Sicherheit verbessern

Sorgen Sie mit rechtzeitigen, automatisierten Patching- und Update-Funktionen für mehr IT-Sicherheit und weniger zeitintensive 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 deutlich weniger 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

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.

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 Ausnahmeregelungen.

Zeitsparende Softwareverteilung

Nutzen Sie die Fern-Bereitstellung oder -Updates über eine einzige Konsole. Über 150 gängige, vom Kaspersky Security Network identifizierte Programme können automatisch installiert werden – bei Bedarf sogar nach Büroschluss. Dank Multicast-Technologie führt dies zu weniger Datenverkehr mit Zweigstellen.

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 sofort verteilt werden, während sich die Patchbereitstellung auch auf einen geeigneteren Zeitpunkt verschieben lässt.

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 bei fehlender Aktualisierung ein Sicherheitsrisiko darstellen könnte.

Client-Verwaltungstools

Remote Troubleshooting

Für kürzere Antwortzeiten, erhöhte Effizienz und optimierten Support für Remote-Standorte nutzt das Kaspersky Security Center die RDP(Remote Desktop Protocol)- und Windows-Desktopfreigabetechnologie (wie bei der Windows-Remote-Unterstützung). 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 den unbefugten Zugriff aus der Ferne. Zu Rückverfolgbarkeits- und Auditzwecken werden sämtliche Vorgänge während einer Remote-Sitzung protokolliert.

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 Total Security for Business
- Als Teil von Kaspersky Endpoint Security for Business – Advanced

Auch als Add-on für Kaspersky Endpoint Security for Business oder als eigenständige Targeted Solution Kaspersky Vulnerability und Patch Management erhältlich

Kaspersky Lab

Informationen zu Partnern in Ihrer Nähe finden Sie hier:
https://www.kaspersky.de/partners
Kaspersky for Business: **www.kaspersky.de/business-security**
True Cybersecurity: **www.kaspersky.de/true-cybersecurity**
IT-Sicherheitsnachrichten: **www.business.kaspersky.com**
#truecybersecurity
#HuMachine

www.kaspersky.de