Kaspersky®
Vulnerability & Patch
Management

Riduzione della complessità e rafforzamento della sicurezza tramite strumenti di gestione IT centralizzati

Le vulnerabilità non corrette da patch, nelle applicazioni più usate, rappresentano una minaccia significativa per la sicurezza IT delle aziende. E non sono solo le vulnerabilità zero-day a costituire un problema. La crescente complessità IT complica le attività rendendo più difficili le attività di patching dei sistemi vulnerabili: se non si conoscono esattamente le minacce, come è possibile proteggersi?

Gestire e amministrare gli aggiornamenti software monitorando al contempo le potenziali vulnerabilità è una delle attività più importanti e dispendiose in termini di tempo che un reparto IT debba svolgere. Centralizzando e automatizzando attività di sicurezza, configurazione e gestione fondamentali, come ad esempio il vulnerability assessment, la distribuzione delle patch e degli aggiornamenti, la gestione dell'inventario e il deployment delle applicazioni, Kaspersky Vulnerability and Patch Management fa risparmiare tempo e ottimizza anche la sicurezza.

Visibilità completa

Grazie alla possibilità di ottenere una visione completa della rete da una singola console, gli amministratori sono a conoscenza di ogni dispositivo e applicazione che accede alla rete, inclusi i dispositivi degli ospiti. Questa visibilità permette il controllo centralizzato dell'accesso di utenti e dispositivi ai dati e alle applicazioni software dell'azienda, in linea con i criteri IT e con i requisiti normativi.

Ottimizzazione della sicurezza

Maggiore sicurezza IT e attività di routine dispendiose in termini di tempo ridotte con l'applicazione tempestiva e automatizzata degli aggiornamenti e delle patch. Kaspersky Vulnerability and Patch Management offre visibilità completa, che consente di sapere esattamente come agire per garantire protezione all'azienda. Automatizzando l'intero ciclo di valutazione delle vulnerabilità e di gestione delle patch, che include il rilevamento e l'assegnazione delle priorità alle vulnerabilità, il download di patch e aggiornamenti, la verifica e la distribuzione, il monitoraggio e il reporting dei risultati, la soluzione offre un'efficienza superiore e riduce in modo significativo il carico sulle risorse.

Semplificazione delle attività IT

Kaspersky Vulnerability and Patch Management include un set di strumenti di controllo client per automatizzare un'ampia gamma di funzioni amministrative IT. Il provisioning automatico delle applicazioni, la verifica dell'accesso e la risoluzione dei problemi da remoto contribuiscono a ridurre al minimo il tempo e le risorse necessari per configurare nuove workstation e installare nuove applicazioni.

Gestione centralizzata

Kaspersky Vulnerability and Patch Management è un componente gestito da Kaspersky Security Center. Tramite questa console centrale si accede a ogni funzione e la si gestisce usando interfacce e comandi omogenei e intuitivi per automatizzare le operazioni IT di routine.

Vulnerability assessment e gestione delle patch

Monitoraggio dei risultati ed esecuzione di report

Kaspersky Vulnerability and Patch Management informa gli amministratori IT sullo stato dell'installazione delle patch e consente loro di eseguire report sulle scansioni, cercare potenziali punti deboli, monitorare i cambiamenti e ottenere maggiori dettagli sulla sicurezza IT dell'azienda, nonché su ogni dispositivo e sistema della rete aziendale.

Rilevamento delle vulnerabilità e assegnazione delle priorità

La scansione delle vulnerabilità automatizzata consente il rilevamento, la prioritizzazione e la correzione in tempi rapidi delle vulnerabilità. La scansione delle vulnerabilità può essere eseguita in modo automatico o essere programmata in base alle esigenze dell'amministratore. La gestione flessibile dei criteri semplifica la distribuzione di software compatibile e aggiornato, nonché la creazione di eccezioni.

Deployment rapido del software

Distribuzione o aggiornamento remoto, da una sola console. Oltre 150 applicazioni di uso comune, identificate tramite Kaspersky Security Network, possono essere installate automaticamente, anche dopo l'orario di lavoro. Risparmio sul traffico per gli uffici remoti con la tecnologia multicast, per la distribuzione locale di software.

Download, test e distribuzione di patch e aggiornamenti

Gli aggiornamenti e le patch possono essere scaricati in modo automatico tramite i server di Kaspersky Lab. Prima della distribuzione, è possibile verificare aggiornamenti e patch per garantire che non abbiano effetti sulle prestazioni del sistema e sull'efficienza dei dipendenti. Gli aggiornamenti possono essere distribuiti immediatamente mentre la distribuzione delle patch può essere rinviata con una pianifcazione oraria adeguata.

La scansione della rete consente di creare inventari software e hardware

Il rilevamento automatizzato e il monitoraggio di hardware e software fornisce agli amministratori informazioni dettagliate su ogni risorsa della rete aziendale. La scansione del software automatizzata consente il rilevamento rapido di software obsoleto che può rappresentare un rischio per la sicurezza se non aggiornato.

Strumenti di gestione client

Risoluzione dei problemi da remoto

Per tempi di risposta ridotti, efficienza superiore e supporto semplificato per i siti remoti, Kaspersky Security Center usa RDP (Remote Desktop Protocol) e la tecnologia Windows Desktop Sharing (come in Windows Remote Assistance). La connessione remota ai computer client tramite Network Agent consente agli amministratori di accedere completamente ai dati e alle applicazioni installate sul client, anche se le porte TCP e UDP dello stesso sono chiuse.

Un meccanismo di autorizzazione impedisce l'accesso remoto non autorizzato. Tutte le attività eseguite durante una sessione di accesso remoto sono registrate per garantire la tracciabilità e la verifica.

Distribuzione dei sistemi operativi

Kaspersky Vulnerability and Patch Management automatizza e centralizza la creazione, l'archiviazione e la clonazione di immagini del sistema protette e supporta la distribuzione del sistema operativo sui nuovi computer come sulle reinstallazioni. Tutte le immagini sono conservate in un inventario speciale, da cui sono facilmente accessibili durante la distribuzione.

La distribuzione delle immagini di workstation client può essere eseguita con server PXE (Preboot eXecution Environment, anche per nuovi computer senza sistema operativo) o tramite le attività di Kaspersky Vulnerability and Patch Management (per distribuire immagini del sistema operativo nei computer del client gestiti). Inviando segnali Wake-on-LAN ai computer, è possibile distribuire automaticamente le immagini dopo l'orario di ufficio. È incluso inoltre il supporto per UEFI.

Modalità di acquisto

Kaspersky Vulnerability and Patch Management è disponibile:

- In qualità di utente di Kaspersky Total Security for Business
- In qualità di utente di Kaspersky Endpoint Security for Business Advanced

Puoi anche acquistarlo come opzione aggiuntiva per Kaspersky Endpoint Security for Business Select o come soluzione mirata autonoma Kaspersky Vulnerability and Patch Management

Kaspersky Lab

Trovate il partner più vicino: **www.kaspersky.it/buyoffline**
Kaspersky per le aziende: **www.kaspersky.com/business**
True Cybersecurity: **www.kaspersky.com/true-cybersecurity**
Novità sulla sicurezza IT: **www.business.kaspersky.com**
#truecybersecurity
#HuMachine

www.kaspersky.it