Gestione delle patch per il data center

È difficile dormire sonni tranquilli con le notizie che circolano su vulnerabilità e minacce, e con il timore di cadere vittima di simili eventi. I software dei sistemi degli utenti sono sempre aggiornati e protetti. Ma i server dei data center? In un mondo in cui gli hacker usano addirittura tool preconfezionati, le organizzazioni devono poter proteggere i server dei data center aziendali con metodi efficaci e sostenibili con le risorse IT attuali.

La strategia di sicurezza deve quindi includere la gestione delle patch per rafforzare i server, proteggere i dati e renderli sempre disponibili, e salvaguardare la reputazione aziendale. È importante implementare le ultime patch, e allo stesso tempo continuare a perseguire gli obiettivi di business.

Occorre poter eseguire report accurati e controllare con precisione l'intero processo di patching: rilevamento, inventario e distribuzione di tutte le patch disponibili nell'ambiente, in modalità continua e programmata in base alle esigenze aziendali.

Per molte organizzazioni, tuttavia, è difficile mantenere i server dei data center aggiornati con tutti gli ultimi update per i sistemi operativi e le applicazioni di terze parti, come Microsoft Windows® e VMware vSphere® Hypervisor. Il problema è che i server e i data center aziendali presentano problematiche di gestione delle patch diverse da quelle dei sistemi client.

Rilevamento e interventi correttivi per l'intero data center

Per garantire un elevato livello di accuratezza delle patch nel proprio ambiente è necessario esaminare facilmente i sistemi per rilevare le patch mancanti e distribuirle rispettando i criteri aziendali per l'intero ambiente. Senza una chiara visione dell'ambiente e informazioni approfondite che consentano di capire quali sono i sistemi più vulnerabili, è impossibile comprendere i rischi a cui si è esposti. Le molteplici configurazioni presenti nei data center non facilitano certo il compito.

Spesso, a causa di vincoli di tempo e budget associati a un ambiente data center virtuale (come il tempo che serve per avviare, applicare le patch e quindi riavviare le macchine virtuali), si finisce per ignorare gli ambienti virtuali, nonostante i rischi che ciò comporta. Ponendo l'attenzione solo sui server fisici si espone l'azienda sia al pericolo delle minacce, sia al rischio di non superare un controllo di audit. È necessario trovare le vulnerabilità, esaminare il sistema alla ricerca delle patch mancanti e implementare tali patch sui sistemi sia fisici che virtuali, in modo facile, senza interferire con i carichi di lavoro dei server né ostacolare l'operatività aziendale. Inoltre, in termini di compliance, non ci si può permettere di ignorare i sistemi offline. Le patch e gli aggiornamenti dei software devono essere erogati a tutti i sistemi, anche a quelli che non sono in rete.

Applicazione rapida delle patch

Tenendo conto di tutto ciò, quanto tempo richiede attualmente l'aggiornamento dei software del data center? Alcune settimane, o addirittura qualche mese? Per ridurre l'esposizione ai rischi, bisogna ridurre questa finestra temporale a pochi giorni o persino poche ore.

I dati dimostrano che il 50% degli attacchi che sfruttano una vulnerabilità avviene entro le prime 2-4 settimane dal rilascio della relativa patch. Imponendosi un limite di 14 giorni per l'implementazione delle patch ci si può quindi proteggere contro la maggior parte degli attacchi. Tuttavia, i processi manuali e l'utilizzo di più strumenti che non sono in grado di supportare l'intero ambiente aggiungono complessità ed estendono il tempo necessario a individuare, definire e distribuire i pacchetti di aggiornamenti software, nonché ad applicare le patch più urgenti.

Che i sistemi siano online o offline, è importante ridurre i tempi e dedicare le risorse disponibili alle azioni che producono risultati immediati e di elevato valore.

È possibile ridurre i tempi e i rischi in diversi modi. Ad esempio, utilizzando dei modelli di patching si risparmia tempo e si riducono i rischi ogni volta che viene creato un

nuovo server. La possibilità di trovare rapidamente tutte le macchine virtuali offline e di applicare le patch alle VM offline può far risparmiare fino a un'ora per sistema. Se le immagini offline vengono mantenute sempre aggiornate e pronte ad essere distribuite, sarà possibile implementare una macchina virtuale senza preoccuparsi del suo stato di aggiornamento.

Il modo più efficace per risparmiare tempo consiste nell'automatizzare ogni parte del processo di gestione delle patch dei server. Considerate il metodo che usate attualmente per gestire le valutazioni delle vulnerabilità pubblicate dai vari fornitori. Con la possibilità di trovare tutte le patch relative agli elenchi CVE (Common Vulnerabilities and Exposures) e creare automaticamente i gruppi di patch per gli aggiornamenti potreste risparmiare molto tempo.

Infine, potete semplificare la gestione della conformità mediante funzioni di reporting che consentano di estrarre dall'enorme mole di informazioni sull'intero ambiente, in qualsiasi momento, proprio i dati che servono. Rendendo disponibili specifici dati ai dirigenti, ai manager e ai responsabili delle varie applicazioni potrete offrire loro la visibilità necessaria per supportare gli audit. Inoltre sarà possibile accedere a informazioni sempre aggiornate sullo stato di sicurezza e prendere decisioni efficaci basate su dati accurati.

Lista di controllo per la gestione delle patch

L'automazione del processo di gestione delle patch, dal rilevamento alla valutazione fino all'implementazione per tutte le workstation e tutti i server fisici e virtuali sia online che offline, consente di ridurre i tempi necessari per applicare le patch di sicurezza più importanti. La tabella di seguito vi aiuterà a trovare la soluzione migliore per le vostre esigenze.

Ivanti può aiutarvi

Con le nostre soluzioni affidabili e semplici per la gestione delle patch che rispondono a tutti i vostri requisiti, Ivanti può aiutarvi sia a proteggere il data server, sia a risparmiare tempo e denaro da reinvestire nel supporto delle iniziative di business principali. Bastano pochi minuti per rendere gli strumenti Ivanti operativi, per aiutarvi a rilevare, valutare e correggere i sistemi del data center in automatico, in base ai criteri che definite. I nostri strumenti semplificano la gestione delle patch negli ambienti fisici e virtuali. Potete rilevare workstation e server sia online che offline, analizzare i sistemi, individuare le patch mancanti ed implementarle. Quindi potete gestire le patch di ogni elemento: sistema operativo e applicazioni, VM, modelli virtuali e persino l'hypervisor ESXi, grazie alla stretta integrazione con VMware.

Funzionalità	Descrizione
Amministrazione	Punto di gestione singolo basato sui ruoli
Automazione delle operazioni di rilevamento, inventario e patching	Protezione dei computer client, dei server fisici e virtuali, degli hypervisor e dei modelli
Aggiornamenti dei sistemi operativi	Sistemi operativi Windows e Linux
Patch delle applicazioni	Applicazioni di terze parti e personalizzate
Automazione della generazione di elenchi CVE-patch	Importazione degli elenchi di valutazione delle vulnerabilità di qualsiasi fornitore
Contenuti delle patch	Accesso a un ampio catalogo di patch
Distribuzione delle patch	Funzionamento senza agent, con agent e con agent basato su cloud
Supporto del rollback	Possibilità di salvare istantanee dello stato pre-patch
Supporto dell'automazione	API per automazione e orchestrazione
Collaborazione	Verifica della compliance delle patch e condivisione dello stato corrente con altri
Reportistica	Cruscotti in tempo reale e report personalizzabili

Per saperne di più www.ivanti.it +39 02 8734 34 21 contact@ivanti.it