Gestione continua delle vulnerabilità

Quando i punti deboli dell'infrastruttura IT vengono presi di mira, le conseguenze possono essere devastanti a livello di produttività, reputazione e costi. L'assenza di un approccio continuo alla sicurezza informatica lascia l'infrastruttura esposta, in quanto gli hacker possono trovare e sfruttare tali punti deboli più velocemente di quanto i tecnici non riescano ad applicarvi le patch. E se oggi i sistemi sono sicuri, non è detto che lo siano ancora tra una settimana, quando può essere scoperta e sfruttata una nuova vulnerabilità.

La gestione continua delle vulnerabilità è definita dal Center for Internet Security come la capacità di "acquisire e valutare le informazioni con continuità, intervenendo ove necessario, al fine di individuare le vulnerabilità, applicare le misure necessarie e ridurre al minimo la finestra di opportunità per gli attacchi".

La gestione continua delle vulnerabilità rappresenta un aspetto fondamentale delle pratiche di sicurezza di ogni organizzazione. Ma comporta un notevole impegno in termini di tempo e attività manuali dal momento in cui viene individuata una vulnerabilità, fino all'implementazione dell'aggiornamento software necessario per correggerla. Il processo dovrebbe iniziare con frequenti scansioni dell'ambiente alla ricerca di vulnerabilità, onde evitare punti ciechi tra un report e l'altro.

I team Security esaminano i dati sulle vulnerabilità raccolti dalle scansioni dell'ambiente, determinano le priorità, e li trasmettono al team IT, che dovrà quindi convertire tali CVE (Common Vulnerabilities and Exposures) in aggiornamenti software e determinare quali aggiornare per primi. Una vulnerabilità può essere identificata e corretta rapidamente. Ma se sono 10.000, o 100.000?

Una singola valutazione delle vulnerabilità può identificare le stesse vulnerabilità sui diversi sistemi dell'intero ambiente, e le stesse vulnerabilità possono esistere in numerosi software su ogni sistema. La deduplicazione e la ricerca necessarie per capire come risolvere ogni vulnerabilità possono richiedere ogni volta tra le 5 e le 8 ore. Una giornata... Che sarà mai? Se si considera che la maggior parte degli attacchi avviene entro i primi 14 - 28 giorni dalla disponibilità di un nuovo aggiornamento, allora ogni giorno che passa è un giorno di troppo.

Riducete il tempo tra vulnerabilità e applicazione delle patch

Le soluzioni Ivanti per la sicurezza offrono informazioni approfondite e consentono di rafforzare la sicurezza. Con l'applicazione automatica delle patch agli endpoint potrete restare al passo con le patch per tutte le applicazioni di terze parti e tutti i sistemi operativi presenti nell'azienda. Le nostre soluzioni per la gestione delle patch si integrano con le scansioni delle vulnerabilità e con gli strumenti per la gestione delle configurazioni e la reportistica, per ottimizzare il tempo dei team IT e Security.

Gestione continua delle vulnerabilità

Le nostra soluzioni per la sicurezza semplificano il processo di identificazione, classificazione e trattamento delle vulnerabilità per ridurre il gap tra la generazione dei report sulle vulnerabilità e gli interventi correttivi. I team IT possono importare i risultati delle scansioni delle vulnerabilità trasmessi dal team Security. Possono vedere rapidamente i CVE identificati e le relative patch, pubblicare o approvare eventuali patch mancanti da distribuire e risparmiare tempo prezioso.

Potete sfruttare le funzionalità "da CVE a patch" per applicare le patch sia agli endpoint con Ivanti Patch for SCCM e Ivanti Patch for Endpoint Manager, sia ai data center con le soluzioni Ivanti per la sicurezza.

I team IT potranno risparmiare ore di lavoro precedentemente dedicate alle attività manuali di ricerca, deduplicazione e

preparazione dei gruppi di patch di aggiornamento. È possibile importare gli elenchi rilasciati da fornitori per la gestione delle vulnerabilità, in qualsiasi formato: CSV, XML e file di testo. Quindi i CVE vengono associati in automatico agli aggiornamenti software appropriati per risolvere specifiche vulnerabilità e individuare le patch da applicare. Oltre a creare un gruppo di patch per gli elementi approvati nel vostro ambiente, potete anche visualizzare tutte le informazioni associate ad ogni patch.

Informazioni approfondite per migliorare lo stato di sicurezza

Quanti giorni servono al team IT per le attività di ricerca, test e implementazione delle patch, e come vengono definite le priorità? L'esame dei problemi noti da vari articoli di blog, documentazione dei fornitori e altre fonti per determinare l'affidabilità degli aggiornamenti patch è un'attività che richiede tempo. Inoltre, il livello di rischio può aumentare qualora nella definizione delle priorità non si tenga conto delle vulnerabilità effettivamente prese di mira.

Le decisioni in merito alle priorità, il testing e l'implementazione delle patch sono tutte attività che allungano i tempi di gestione delle vulnerabilità. Lo strumento Patch Intelligence di Ivanti combina i dati sulle patch dal catalogo Ivanti delle patch di terze parti con metriche sulla sicurezza e sull'affidabilità delle patch. Consente di ottimizzare l'implementazione di aggiornamenti importanti grazie a informazioni approfondite che potete acquisire in modo decisamente più rapido e semplice.

- Ottenete **visibilità** sui problemi segnalati dal fornitore di una patch o di un gruppo di patch, o identificati da Ivanti in base alle informazioni dei bollettini relativi a ad elenchi CVE e patch.
- Attingete alle **informazioni approfondite** sulle problematiche riscontrate da altri clienti Ivanti tramite dati raccolti in modalità anonima sull'eventuale ripristino delle patch implementate.
- Determinate l'**affidabilità** degli aggiornamenti e il livello di fiducia per un'implementazione rapida.
- Individuate le **patch** che richiedono ulteriori verifiche, applicate rapidamente quelle con un´alta probabilità di riuscita e determinate le priorità di test ed implementazione sulla base di valutazione delle minacce e punteggi di affidabilità, per ottimizzare i cicli di lavoro.

Giocate d'anticipo con le soluzioni Ivanti per la gestione continua delle vulnerabilità. **Per saperne di più, contattate sales@ivanti.com.**

Ulteriori informazioni

ivanti.it
+39 02 8734 3421
contact@ivanti.it