ivanti

DATASHEET

Le sfide da affrontare nella gestione delle patch

Risultati del sondaggio e approfondimenti sul passaggio delle organizzazioni a Everywhere Workplace

Introduzione

Gli ambienti di lavoro attuali non si limitano più a offrire spazi contenuti, in cui le postazioni PC controllate dall'IT costituiscono il centro della produttività. Oggigiorno, le organizzazioni sono più distribuite che mai e dispongono quindi di superfici di attacco più ampie. Con Everywhere Workplace, i dipendenti possono collegarsi da vari dispositivi per accedere a reti, dati e servizi aziendali mentre lavorano e collaborano da luoghi diversi; per questo motivo, il patching risulta davvero impegnativo.

Nel frattempo, i team IT e di sicurezza lottano per tenere sotto controllo il panorama del lavoro da remoto, in continua espansione. È necessario mantenere sicuro e aggiornato il nuovo spazio di lavoro online implementandolo con le ultime patch di sicurezza, ma questa operazione è diventata sempre più complessa.

Sfide

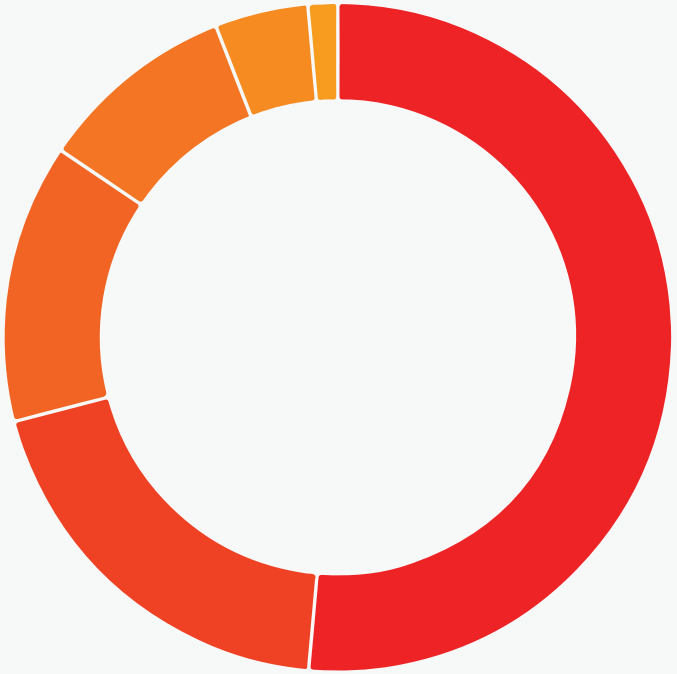
Un nuovo studio di Ivanti ha rivelato che il 71% dei professionisti IT e della sicurezza ritiene che l'applicazione di patch sia troppo complessa e dispendiosa in termini di tempo. Poiché i creatori di minacce rendono più sofisticate le proprie tattiche e sfruttano ogni eventuale vulnerabilità, in particolare quelle con l'esecuzione di un codice remoto, le organizzazioni sono alle prese con i rischi legati alla superficie di attacco e cercano modi per accelerare le azioni di correzione e patching.

I professionisti IT e della sicurezza non sono in grado di fornire sempre una risposta rapida; il 53% degli intervistati ha affermato che l'organizzazione e la definizione delle priorità legate alle vulnerabilità occupano la maggior parte del tempo. Questi dati risultano allarmanti poiché, più a lungo le vulnerabilità rimangono senza patch, più un'azienda è esposta al rischio di un attacco o ransomware. Tuttavia, nessuna organizzazione è in grado di correggere interamente tutti i punti di esposizione e la definizione delle priorità in base al rischio deve essere eseguita rapidamente per evitare attacchi avversari automatizzati. Attualmente le vulnerabilità prive di patch rimangono uno dei punti di infiltrazione più comuni per gli attacchi ransomware, che sono aumentati in termini di frequenza e impatto per le aziende di qualsiasi dimensione.

I team IT e di sicurezza trascorrono diverso tempo a offrire soluzioni per patch non riuscite (19%), testare patch (15%) e coordinarsi con altri reparti (10%). Le numerose sfide che i team IT e di sicurezza devono affrontare in materia di applicazione delle patch potrebbero essere il motivo per cui il 49% degli intervistati ritiene che gli attuali protocolli di gestione delle patch nella propria azienda non riescano a mitigare efficacemente il rischio.

I professionisti IT e della sicurezza hanno dichiarato che, ogni mese, dedicano la maggior parte del tempo alle seguenti attività:

- **53%** - Organizzazione e assegnazione priorità delle vulnerabilità
- **19%** - Risoluzione dei problemi per le patch non riuscite
- **15%** - Testing delle patch
- **10%** - Coordinamento con altri reparti
- **3%** - Conformità
- **1%** - Tenuta dei registri



Cause

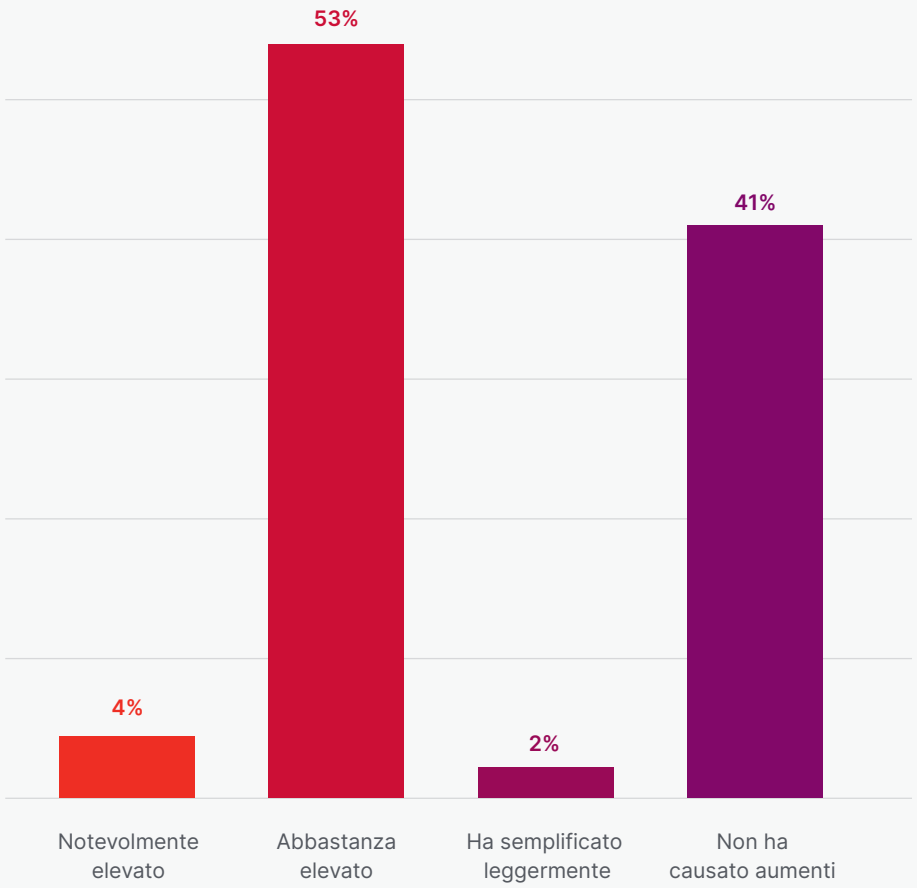
La maggioranza degli intervistati (il 57%) ritiene che la transizione globale verso uno spazio di lavoro decentralizzato abbia reso la gestione delle patch più complessa da affrontare. Anche la portata della stessa gestione delle patch è aumentata, con diversi endpoint disponibili per gli utenti e sistemi business critical che li supportano, da Windows a macOS, da Linux a Windows Server e molti altri.

In aggiunta, alcuni sistemi IT risultano difficili da correggere poiché devono essere sottoposti a interruzioni. Uno scoraggiante 61% composto da professionisti IT e della sicurezza ha affermato di ricevere richieste da parte di proprietari di linee di business per posticipare le finestre di manutenzione una volta ogni tre mesi. Un altro 28% ha dichiarato di ricevere questo tipo di richieste una volta al mese.

Allo stesso tempo, la velocità di attacco alle vulnerabilità continua ad aumentare, specialmente da parte di coloro che hanno la capacità di consentire l'esecuzione di un codice remoto (RCE). Tutto ciò conduce alla situazione ideale per approfittare di una scarsa visibilità, a causa del recente spostamento degli spazi di lavoro in diversi luoghi, nonché dell'aumento di autori di minacce che trovano e utilizzano rapidamente vulnerabilità sfruttabili.

Inoltre, molte organizzazioni non dispongono delle competenze di sicurezza, o del tempo necessario, per consentire alle proprie risorse di raccogliere informazioni sulle minacce e di mappare le minacce di exploit attive con vulnerabilità aperte nell'organizzazione allo scopo di ottenere un contesto basato sul rischio. La carenza di personale IT ha ridotto la capacità di mitigare prontamente i problemi relativi alla sicurezza per molte aziende. Dunque per queste organizzazioni, gli attacchi informatici e, in particolare, i ransomware si sono rivelati i più devastanti.

In che modo il lavoro a distanza ha aumentato la complessità e la portata della gestione di patch nella tua organizzazione?



Panorama delle minacce

Mentre i team IT lottano per far fronte a una maggiore superficie di attacco, gli hacker potenziano le proprie tattiche e monitorano i punti in cui le aziende riportano un rischio di esposizione alla vulnerabilità. Bilanciano tenacia e pazienza con un uso sofisticato di exploit, strumenti e tecnologie di ultimo livello. L'obiettivo principale è quello di distruggere, rubare e agire per ottenere guadagni monetari dai business aziendali.

Un altro sondaggio di Ivanti rivela che il 63% degli intervistati ha confermato di aver subito un attacco ransomware nell'ultimo anno, all'interno delle proprie organizzazioni. E l'89% ha identificato in laptop, desktop e dispositivi mobili gli strumenti che sono stati presi più di mira.

Gli hacker sono sempre alla ricerca di vulnerabilità, mentre i team IT e di sicurezza lottano per dare priorità agli sforzi di gestione delle patch, in modo da poter risolvere rapidamente l'esposizione al rischio di vulnerabilità.

L'attacco ransomware WannaCry, che si stima abbia criptato 200.000 computer in 150 paesi, rimane un ottimo esempio, persino dopo quattro anni, delle gravi ripercussioni che si possono riscontrare se le patch non vengono applicate tempestivamente. Una patch per lo sfruttamento di vulnerabilità esisteva già diversi mesi prima dell'attacco iniziale, ma molte organizzazioni non sono riuscite a implementarla. E ancora oggi, due terzi delle aziende non ha ancora applicato le patch di correzione ai propri sistemi. Eppure, molte organizzazioni in tutto il mondo sono ancora nel mirino degli attacchi causati dal ransomware WannaCry; da gennaio a marzo 2021, si è registrato un aumento del 53% nel numero di organizzazioni colpite proprio dal ransomware WannaCry.

Creazione di un contesto di fiducia per la sicurezza e la gestione dei rischi

L'espansione del panorama lavorativo e la trasformazione digitale non si fermeranno. Tuttavia, è necessario un modo per diffondere un contesto di fiducia relativo a sicurezza e gestione dei rischi.

L'implementazione di un framework Zero Trust è fondamentale per proteggere i dati aziendali sensibili da accessi non autorizzati e violazioni informatiche derivanti da attacchi. Zero Trust fornisce alle organizzazioni una valutazione continua di tutti i dispositivi, endpoint, risorse e reti dei dipendenti su cui si basa l'infrastruttura aziendale.

Il presidente americano Biden ha firmato un Ordine esecutivo nel maggio 2021, affermando che le agenzie federali sono tenute a sviluppare piani per implementare una strategia di sicurezza Zero Trust. La sicurezza Zero Trust costituisce anche una priorità assoluta per i professionisti IT e della sicurezza informatica: secondo uno studio recente condotto da Ivanti, il 98% dei professionisti IT e della sicurezza in Nordamerica ha affermato che le pratiche di sicurezza sono destinate ad allinearsi sempre di più con la strategia Zero Trust nel corso del prossimo anno.

Il contesto relativo a questa strategia esaminerà l'aspetto dei rischi legati a dispositivi, endpoint e risorse utilizzati in Everywhere Workplace. La comprensione del livello di rischio legato alle vulnerabilità che risulta accettabile e delle patch che devono essere implementate per soddisfare i requisiti di affidabilità stabiliti dall'azienda dovrebbe permettere di aumentare il valore della gestione delle patch basata sul rischio.

I leader più importanti del settore, i professionisti e le società di analisi consigliano un approccio basato sul rischio per identificare e assegnare una priorità ai punti deboli derivanti da vulnerabilità e per accelerare l'efficacia delle azioni correttive. La Casa Bianca ha recentemente pubblicato un promemoria che incoraggia le organizzazioni a utilizzare una strategia di valutazione basata sul rischio per guidare la gestione delle patch e rafforzare la sicurezza informatica contro gli attacchi ransomware. Inoltre, Gartner ha definito la gestione delle vulnerabilità basata sul rischio come uno dei migliori progetti di sicurezza su cui i professionisti della sicurezza e della gestione dei rischi dovrebbero concentrarsi nel 2021, per promuovere il valore aziendale e ridurre i rischi.

Conclusione

Il livello di produttività è sicuramente aumentato all'interno di Everywhere Workplace, ma anche le minacce sono aumentate a dismisura. In questo ecosistema distribuito, i dipendenti utilizzano diversi dispositivi per accedere a dati, reti e applicazioni aziendali e per continuare a lavorare da qualsiasi luogo e in qualsiasi momento. Queste postazioni di lavoro decentralizzate sono più soggette a minacce rilevanti da parte di malintenzionati, che sfruttano l'improvviso spostamento verso spazi di lavoro senza perimetri definiti come canale per infiltrarsi nelle organizzazioni.

Everywhere Workplace richiede un approccio alla sicurezza e alla gestione del rischio che valuti continuamente il contesto attuale, per stabilire una fiducia definita da un'analisi attiva basata sul rischio. Grazie all'accesso alla migliore intelligence per gestire vulnerabilità e patch, che include exploit di vulnerabilità attivi in circolazione, vulnerabilità legate a ransomware, dati sul sentiment relativo all'affidabilità delle patch, Ivanti sta espandendo gli strumenti che i team IT e di sicurezza possono distribuire senza problemi per migliorare l'efficacia della sicurezza e la gestione del rischio nella propria organizzazione.

Per ulteriori informazioni, dai un'occhiata al nostro blog e registrati alla serie di webinar Patch Tuesday di Ivanti. Ascolta il podcast Ivanti Insights "The Next Evolution of Patch Management: Don't Try to Patch Everything!"

For more information, check out our blog and register for the Ivanti Patch Tuesday webinar series. And listen to the Ivanti Insights podcast, "The Next Evolution of Patch Management: Don't Try to Patch Everything!"

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. i. Smarter with Gartner, Gartner Top 10 Security Projects for 2020-2021, February 22, 2021
2. ii. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.