TeamViewer
Remote Management

INFORMATIVA

Non perderti più una patch: riduci i rischi per la sicurezza e mantieni al sicuro la tua infrastruttura IT con la Patch Management automatizzata

Sommario

Introduzione:
Cos’è una soluzione di Patch Management?

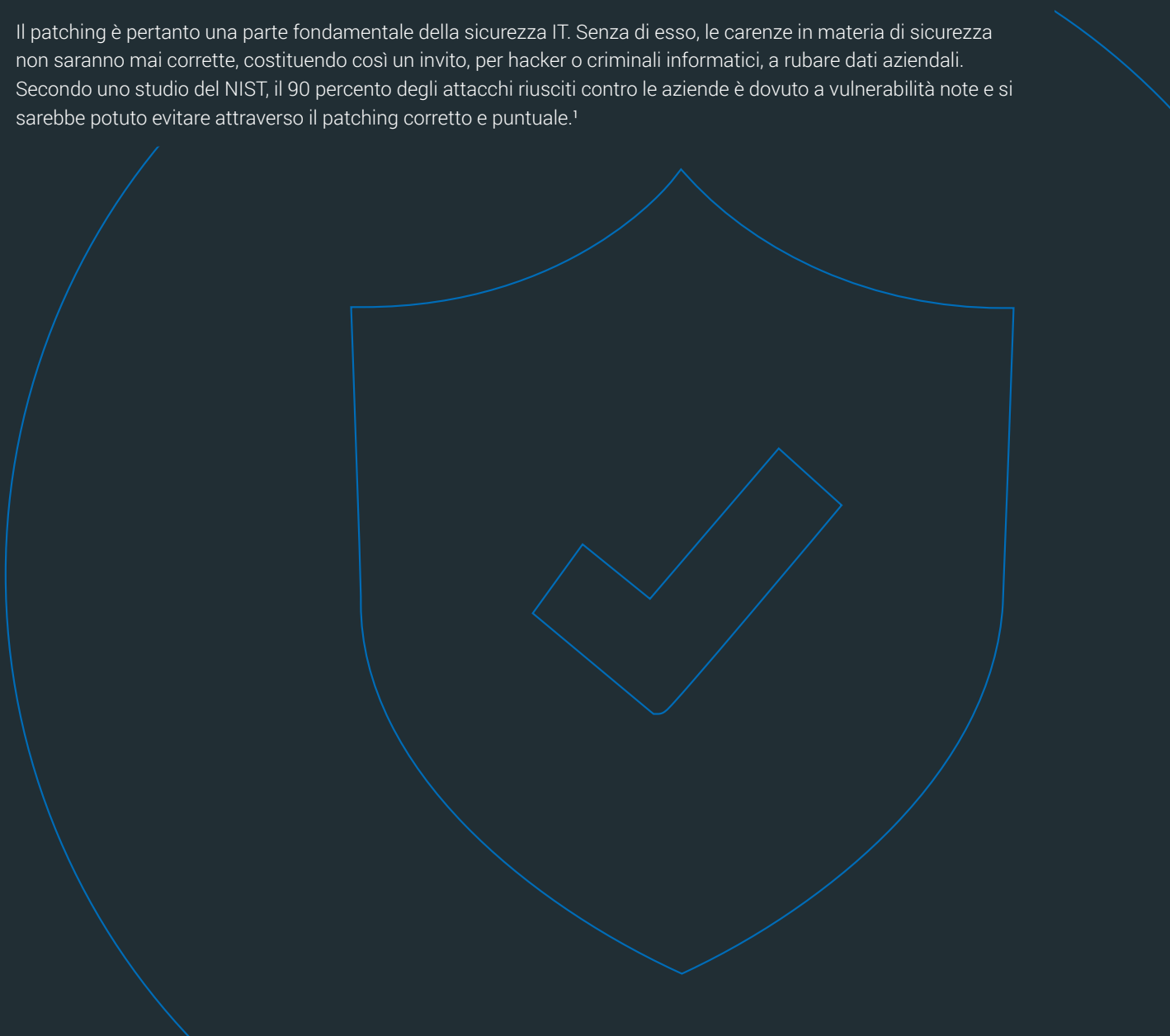
Per mantenere la tua infrastruttura IT stabile e sicura servono una manutenzione regolare e aggiornamenti puntuali per tutti i computer e i dispositivi. Il mancato aggiornamento dei tuoi computer e dispositivi può condurre a notevoli vulnerabilità di sicurezza dovute a software datato.

Le organizzazioni IT si trovano ad affrontare nuove sfide per garantire che i dispositivi siano sempre aggiornati o "patchati" per via del numero sempre più elevato di vulnerabilità informatiche, applicazioni e dispositivi aziendali.

Nel mondo IT, una "patch" è un elenco di modifiche apportate a un programma informatico, appositamente progettate per aggiornarlo, ottimizzarlo o correggerlo. Le patch, rese disponibili agli utenti tramite aggiornamenti software, sono applicabili per correggere vulnerabilità dei software e altri bug. Il monitoraggio della disponibilità delle patch e l’installazione delle patch mancanti richiedono una soluzione di gestione delle patch automatizzata.

Con una soluzione di gestione delle patch, puoi rilevare e applicare patch a software vulnerabile e datato.

Il patching è pertanto una parte fondamentale della sicurezza IT. Senza di esso, le carenze in materia di sicurezza non saranno mai corrette, costituendo così un invito, per hacker o criminali informatici, a rubare dati aziendali. Secondo uno studio del NIST, il 90 percento degli attacchi riusciti contro le aziende è dovuto a vulnerabilità note e si sarebbe potuto evitare attraverso il patching corretto e puntuale.[1]



Importanza
della Patch Management per le aziende

Gli attacchi informatici tramite malware possono causare danni notevoli alle aziende. Perdita di dati, danno d'immagine, o interruzione della produzione possono costare milioni alle organizzazioni. Il numero di varianti di malware aumenta quasi quotidianamente, e ciò significa che la tua infrastruttura IT necessita di una gestione efficiente della sicurezza.

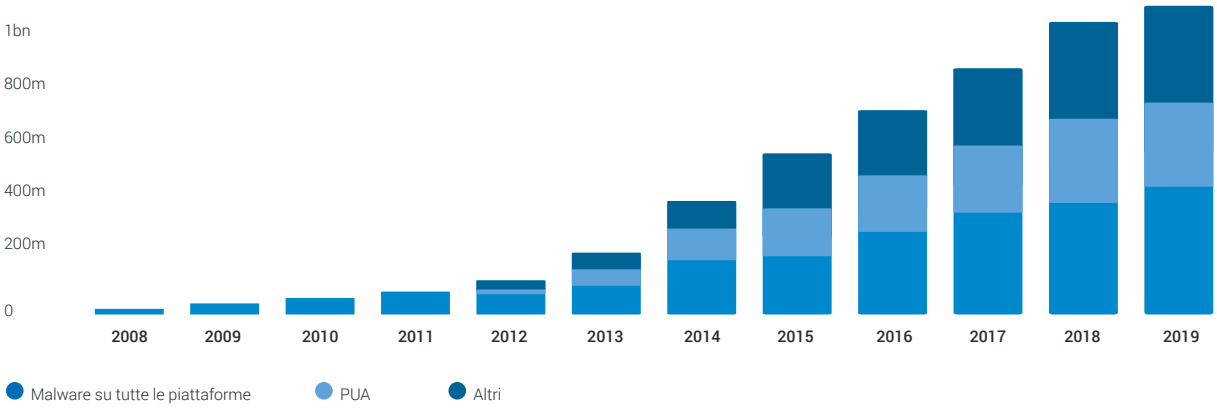


Immagine 1: Totale delle varianti di malware note *PUA - potentially unwanted application²(applicazione potenzialmente indesiderata)

Attacchi informatici, quali l'attacco ransomware WannaCry nel 2017, hanno dimostrato ancora una volta l'importanza di proteggere il proprio hardware e software dagli attacchi. Ora, alla maggior parte dei sistemi e delle applicazioni delle grandi aziende si accede attraverso internet, il che facilita l'accesso da parte dei criminali. Il software antivirus da solo non è sufficiente per proteggere in modo completo le infrastrutture IT. A causa dell'elevata complessità del software, vengono commessi più errori durante lo sviluppo, che lasciano vulnerabilità all'interno dello stesso.

Il German Federal Office for Information Security - BSI (agenzia governativa della Repubblica federale di Germania responsabile per la sicurezza informatica) ha annunciato che "gli attacchi riusciti sono spesso dovuti ad attacchi eseguiti tramite vulnerabilità sconosciute e carenza di gestione delle patch."[3] Ciò accade a causa del notevole incremento del numero delle vulnerabilità critiche all'interno dei prodotti IT standard avvenuto negli ultimi anni.

Solo nel 2017 vi erano più di 450 vulnerabilità note nelle 10 applicazioni più conosciute. Secondo BSI, non vi è alcun segno che indichi la situazione possa cambiare nei prossimi anni. Nel 2019 sono state verificate 12.174 vulnerabilità all'interno dei 50 prodotti software più utilizzati.4

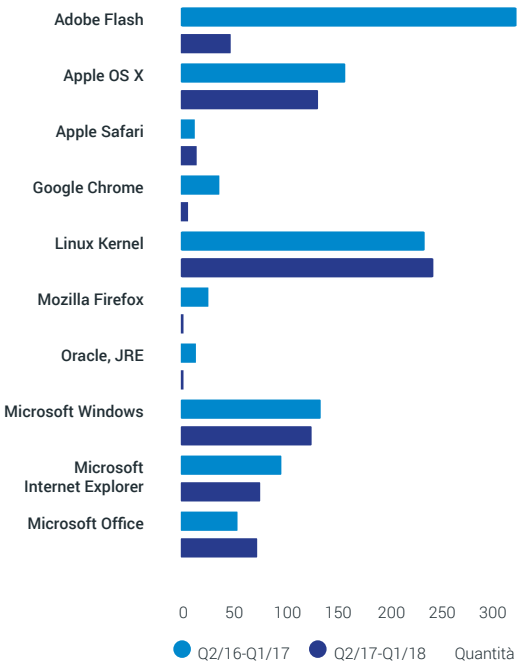


Immagine 2: Inserimenti CVE critici, dal 31.03.20185

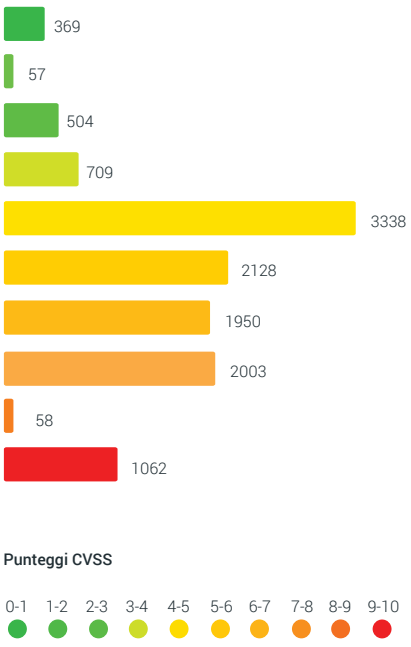


Immagine 3: Distribuzione delle vulnerabilità nel 2019 a partire dal 30.10.19. Da non critico (verde) a critico (rosso) dei primi 504

Il 90 percento delle vulnerabilità software è sfruttato entro i primi 40 – 60 giorni dal rilascio. Dato che gli amministratori IT sono ritenuti responsabili, devono agire rapidamente. Le patch devono essere implementate, testate e distribuite. Ciò, per gli amministratori IT, non solo richiede moltissimo tempo, ma rappresenta anche un fattore di costo significativo.

Con l'aumento del volume delle vulnerabilità, il patching manuale è divenuto più tedioso e meno pratico da eseguire su base regolare con la garanzia che tutti i dispositivi abbiano effettivamente ricevuto le patch. I processi di patching manuale necessitano anche di processi manuali di follow-up, che aumentano lo stress su risorse e tempo degli amministratori IT.

Quando si tratta di processi di patching manuali, a seconda della complessità del sistema, per l'implementazione delle patch potrebbe essere necessario fare affidamento sugli utenti finali. In genere, ciò influisce sul successo dell'implementazione delle patch.

Il patching lato server è relativamente semplice grazie al controllo totale dell'IT su di esso, ma il lato cliente è dove si verifica la maggior parte delle vulnerabilità (~95 percento) e mantenere i clienti aggiornati è difficile. I problemi logistici sono d'intralcio, così come il fattore umano; le persone ritardano il patching in quanto non vogliono interrompere il proprio lavoro. Per questi motivi, il patching è spesso trascurato. Sebbene le patch siano spesso disponibili per molto tempo, non sono mai implementate per motivi di tempo e costi. Tuttavia, se le patch non sono applicate correttamente, i criminali informatici possono sfruttare tali vulnerabilità in modo sistematico.

Queste vulnerabilità software possono condurre a serie vulnerabilità di sicurezza in un'applicazione o in una rete IT. È per questo motivo che le aziende affrontano oggi la grande sfida di organizzare e gestire in modo migliore la loro infrastruttura IT. Patch Management è la soluzione ottimale per alleggerire gli amministratori IT e aumentare prestazioni, efficienza ed efficacia dell'infrastruttura IT. Una soluzione di gestione delle patch efficiente verifica quali patch siano più adatte ai sistemi, ne automatizza la distribuzione e le classifica in base all'urgenza. Di conseguenza, la gestione delle patch non solo ne migliora l'implementazione, ma riduce anche al minimo i passaggi manuali e il rischio di errore umano.

Rischi di una cattiva Patch Management

Costosa inattività del sistema

Credibilità persa nei confronti dei clienti

Lunghi tempi di riparazione

Integrità dei dati discutibile

PR negativo

Ambiente IT non sicuro

Vantaggi della Patch Management

Il patching regolare e automatizzato aumenta notevolmente la sicurezza dei sistemi IT e l'integrità delle reti. Questo è il vantaggio più ovvio della gestione delle patch. Tuttavia, una soluzione di gestione delle patch automatizzata presenta altri importanti vantaggi per le aziende.

Aumenta la produttività IT e riduci le interruzioni delle attività non previste

Per gli amministratori IT, il patching manuale è molto dispendioso in termini di tempo. L'individuazione delle vulnerabilità, la definizione degli endpoint che necessitano di patch, e infine la loro distribuzione e la garanzia che le patch siano state applicate in maniera corretta ai computer e laptop interessati richiedono molto tempo e risorse.

Inoltre, ciò causa interruzioni delle attività non previste per i dipendenti che devono accedere ai loro dispositivi. Una soluzione di gestione delle patch automatizzata, di conseguenza, non solo aiuta il personale IT ad aumentare la propria efficienza, ma riduce anche al minimo le interruzioni delle attività non previste per i dipendenti.

Abilita la sicurezza e la conformità dei dati per mitigare i rischi

Le linee guida della conformità in materia di sicurezza nei reparti IT sono fondamentali e non devono essere trascurate. La conformità IT protegge le aziende da sanzioni o potenziali danni al loro marchio. Per esempio, le vulnerabilità dei software rappresentano un grande rischio di sicurezza che può condurre a gravi violazioni dei dati.

Se i dati sensibili di un cliente o di un dipendente sono esposti, le aziende possono incorrere in sanzioni per la violazione delle normative in materia di protezione dei dati. Ciò può causare l'abbandono dei clienti o pubblicità negativa. Una soluzione di gestione delle patch efficace rileva vulnerabilità di sicurezza e può contribuire a mitigare tali rischi.

Vantaggi **principali**

Risparmia tempo con aggiornamenti del sistema IT completi e rapidi

Applica patch in modo automatico per correggere le vulnerabilità del software

Gestisci i computer a livello centrale

Aumenta la produttività dei dipendenti

Sfrutta le informazioni provenienti da rapporti cross-network dettagliati

Comprendi la tua infrastruttura con le panoramiche degli stati del sistema

Riduci le interruzioni impreviste del dispositivo

Mitiga i rischi di conformità e sicurezza

Funzionalità **principali**

Individua vulnerabilità

Ottieni visibilità totale attraverso la tua rete rilevando automaticamente vulnerabilità dovute a software obsoleto.

Distribuzione rapida, integrata con TeamViewer

Implementa la Patch Management nella tua intera rete con pochi clic.

Implementazione patch automatica

Rileva e implementa automaticamente patch basate sulle policy per applicazioni di terze parti e sistemi operativi con software vulnerabili obsoleti al fine di mantenere la tua infrastruttura IT sicura e aggiornata.

Soluzione di Patch Management di TeamViewer

Gli endpoint di patching possono proteggere la tua intera rete dai criminali informatici. Lo sapevi che un solo dispositivo privo di patch costituisce un rischio per la tua intera infrastruttura IT?

Con la soluzione Patch Management di TeamViewer Remote Management, **le vulnerabilità sono rilevate automaticamente**, semplificando così il mantenimento di ogni dispositivo aggiornato e sicuro.

Proteggi le tue reti IT con Patch Management by TeamViewer

Rimani al passo con le patch critiche grazie alla gestione automatizzata delle patch. Verifica subito la presenza di aggiornamenti e implementali in massa da una piattaforma centralizzata.

Gestisci e implementa gli aggiornamenti di Windows da una dashboard centralizzata, garantendo l'aggiornamento di tutti i tuoi dispositivi Windows.

Riduci i rischi, monitora e implementa automaticamente le patch per gli aggiornamenti di sistemi operativi e applicazioni di terze parti.

Visualizza lo stato delle patch dei tuoi dispositivi e di tutte le patch disponibili da un'unica dashboard.

Definisci le singole policy per diversi reparti e clienti per personalizzare e automatizzare le attività di patching.

Privilegia le patch, vedi quali di esse sono critiche, urgenti, o possono essere posposte riordinandole in base alla priorità.

Gestisci e verifica le tue patch da remoto, ovunque ti trovi. L'integrazione perfetta tra TeamViewer Remote Management e TeamViewer Remote Access ti consente di accedere ai dispositivi secondo necessità con pochi clic.

Conclusione

Le organizzazioni IT sanno che devono proteggere continuamente le loro aziende dai criminali informatici e che una soluzione di gestione delle patch automatizzata è fondamentale per migliorare la sicurezza endpoint. La gestione delle patch è fondamentale ma non deve necessariamente essere complicata.

Con funzionalità facili da utilizzare, Patch Management by TeamViewer ti consente di proteggere in maniera proattiva la tua infrastruttura IT, e di eliminare tediose attività di patching manuale, aumentando al contempo sicurezza, stabilità e integrità della tua rete.

Risorse

Richiedi una dimostrazione gratuita di TeamViewer Remote Management (include Patch Management)

Maggiori informazioni all'indirizzo teamviewer.com/patchmanagement

Inizia con una prova gratuita della gestione delle patch

Referenze

1. National Institute of Standards and Technology (novembre 2019): Automation Support for Security Control Assessments: Software Vulnerability Management, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8011-4-draft.pdf
2. Bundesamt für Sicherheit in der Informationstechnik (2018): Die Lage der IT-Sicherheit in Deutschland 2018, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf
3. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf;jsessionid=F64FE0EE50A281C976D952B395DCD531.2_cid369?__blob=publicationFile&v=5 S.11
4. Dettagli CVE (2019): Current CVSS Score Distribution for all Vulnerabilities, https://www.cvedetails.com/cvss-score-distribution.php
5. Bundesamt für Sicherheit in der Informationstechnik (2018): Die Lage der IT-Sicherheit in Deutschland 2018. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf?__blob=publicationFile&v=3 page. 43
6. Dettagli CVE (2019): Vulnerabilità a oggi, https://www.cvedetails.com/browse-by-date.php

A proposito di TeamViewer

In quanto piattaforma leader di connettività remota globale, TeamViewer consente agli utenti di connettere chiunque, qualunque oggetto, ovunque, in qualsiasi momento. TeamViewer offre accesso remoto sicuro, supporto, controllo e abilità di collaborazione per endpoint online di qualsiasi tipo e aiuta le aziende di tutte le dimensioni ad attingere pienamente al loro potenziale digitale. TeamViewer è stato attivato approssimativamente su 2 miliardi di dispositivi; fino a 45 milioni di dispositivi sono online contemporaneamente. Fondata nel 2005 a Göppingen, Germania, TeamViewer è un'azienda pubblica quotata alla borsa valori di Francoforte, che impiega circa 800 collaboratori in uffici situati in Europa, Stati Uniti e Asia Pacifico.

www.teamviewer.com