White paper Business

La sicurezza inizia dall'endpoint

Perché è fondamentale assegnare la massima priorità alla sicurezza degli endpoint

Brought to you by

Sintesi del documento

L'82% delle organizzazioni ha subito una minaccia o una violazione in termini di sicurezza informatica negli ultimi 12 mesi.[1] La criminalità informatica sta crescendo in termini di frequenza, gravità e costi che le aziende devono sostenere a seguito degli attacchi.

Il paradigma della sicurezza basato sulla prevenzione e sulla protezione è ormai superato. Ad oggi il rilevamento precoce e la risposta immediata agli attacchi rappresentano sicuramente una strategia più efficace.

Sfortunatamente, i budget IT non riescono a tenere il passo con i continui mutamenti di scenario in tema di sicurezza informatica: il 77% delle spese viene ancora destinato a sistemi di prevenzione e protezione,[2] mentre solo il 36% dei responsabili della sicurezza IT ritiene di avere a disposizione un budget adeguato per un'efficace sicurezza degli endpoint.[3]

Una solida protezione dei dati è possibile grazie all'uso della giusta tecnologia, unitamente a soluzioni di sicurezza basate sul rilevamento e sulla risposta agli attacchi e a una strategia appropriata con un numero adeguato di risorse impiegate.

In un futuro imminente, il fatto di non aver incrementato gli investimenti in sicurezza informatica e di non averli reindirizzati su sistemi difensivi davvero efficaci determinerà un aumento della frequenza delle violazioni alla sicurezza, facendo lievitare i costi per le organizzazioni.

Introduzione

La sicurezza informatica nell'epoca delle reti amorfe
Il 60% dei responsabili IT ritiene che l'aumento della portata e della complessità della criminalità informatica stiano sovrastando i sistemi di sicurezza nelle aziende. L'80% dei responsabili della sicurezza si rende conto della crescita della minaccia derivante da attacchi APT (Advanced Persistent Threat), da società criminali, da hacker sostenuti dai governi e dagli hacktivisti, e ritiene che la sfida maggiore, oggi, risieda nel garantire la sicurezza dell'IT.[4]

Non hanno torto. Nel Regno Unito, il governo ha stimato un costo pari a 27 miliardi di sterline per affrontare la criminalità informatica, una cifra "significativa che è destinata a salire", con una perdita per le aziende di 21 miliardi di sterline.[5] Nel Ponemon 2016 State of the Endpoint Report, il 78% delle aziende ha segnalato un incremento nella gravità degli attacchi malware, in crescita del 47% nel 2011.

Ma l'attenzione nei confronti delle minacce provenienti dall'esterno può condurre a un'eccessiva concentrazione di risorse nel sistema di difesa, improntando la sua costruzione esclusivamente sulla prevenzione e sulla protezione.

Sebbene gli attacchi esterni (virus, malware, phishing) prevalgano, gli attacchi provenienti da utenti interni risultano più onerosi.[6] Inoltre, molti degli attacchi esterni vengono originati da vulnerabilità interne, come dipendenti negligenti che ignorano i protocolli di sicurezza, o dispositivi non protetti che si connettono alla rete, tutti aspetti che l'81% degli intervistati nel sondaggio Ponemon ha identificato come la minaccia più grave alla sicurezza IT.

Questa situazione diventerà sempre più rilevante nel prossimo futuro. Gli endpoint si stanno rivelando gli anelli più deboli di una rete anche a causa dell'aumento del BYOD, del lavoro da remoto e dell'Internet delle cose.

Ben lontane dalle precedenti reti controllate dei PC desktop collegati mediante Ethernet, le reti aziendali sono diventate elementi amorfi, un insieme di dispositivi aziendali e personali, che accedono ai dati tramite differenti nodi Wi-Fi sia dall'interno che dall'esterno dell'organizzazione.

Lo scenario descritto non è incontrovertibile, ma implica l'adozione di un nuovo approccio alla sicurezza informatica caratterizzato da strategie in grado di rispondere alla continua evoluzione della criminalità informatica.

In questo white paper, esamineremo la natura e la portata delle minacce (per conoscere meglio il nostro nemico) prima di affrontare la questione di come fronteggiare la sicurezza informatica nell'epoca della molteplicità dei dispositivi, delle reti non protette e del cloud.

[1] HPI Printer Security Research 2016 (Spiceworks)
[2] PAC Incident Response Management 2015: https://www.pac-online.com/download/19443/155514
[3] Ponemon 2016 State of the Endpoint Report
[4] IBM CISO Assessment 2014
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic

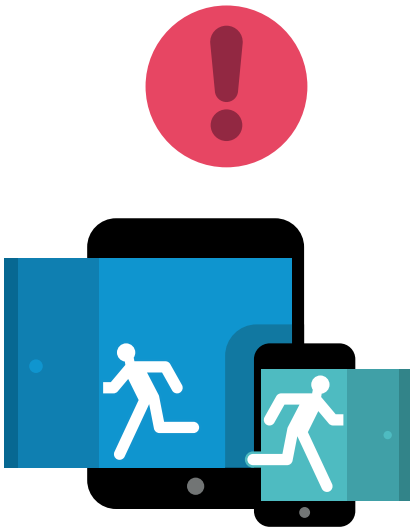
La portata delle minacce

Risollevarsi da una violazione delle informazioni costa alle aziende circa 907.053 dollari, con un ulteriore 13% di perdita in ricavi. Senza considerare che in media, un'organizzazione, per riprendersi, ha bisogno di impiegare almeno nove settimane lavorative.[7]

Circa l'85% delle aziende esaminate nell'HP Printer Security Report 2015 ha affermato di aver subito una minaccia o violazione in termini di sicurezza informatica nei precedenti 12 mesi. L'80% dei professionisti IT coinvolti nell'indagine prevede una tendenza in crescita delle minacce nei prossimi tre anni.[8]

La criminalità informatica ha un costo effettivo che possiamo riassumere in: perdita di valore a seguito della sottrazione o del danneggiamento di contenuti, perdita di ricavi a seguito del danno alla reputazione e perdita di produttività, perdita di risorse impiegate nel recupero, tempo impiegato dal servizio clienti, implementazione delle nuove politiche di sicurezza, perdite di personale e altre risposte interne, sanzioni e penali imposte da parte di enti normativi, diminuzione delle quotazioni in borsa.

Le minacce sono solo destinate a crescere parallelamente al numero dei dispositivi connessi alla rete. Grazie all'Internet delle cose, Gartner prevede che ci saranno 11,4 miliardi di dispositivi connessi entro il 2018 a partire dai 6,4 miliardi registrati nel 2016. Entro il 2020, oltre il 25% degli attacchi identificati nelle aziende sarà correlato all'Internet delle cose, che, tuttavia, sarà oggetto di meno del 10% dei budget riservati alla sicurezza.[9]



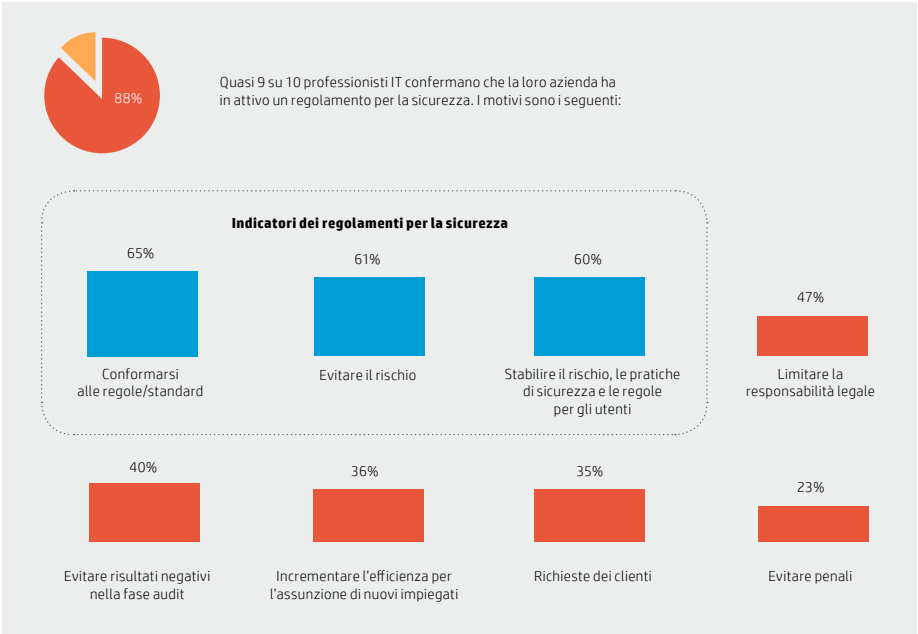
La forma delle minacce

Le aziende sono preda ogni giorno di innumerevoli attacchi informatici, di cui la maggior parte sferrati tramite virus e malware di basso livello. Il 99% delle organizzazioni esaminate nel sondaggio Ponemon del 2016 ha subito un attacco malware nei precedenti 12 mesi. Attacchi esterni basati sul Web simili a questi casi sono relativamente benigni, poiché costano alle organizzazioni, in media, circa 4639 dollari.[10]

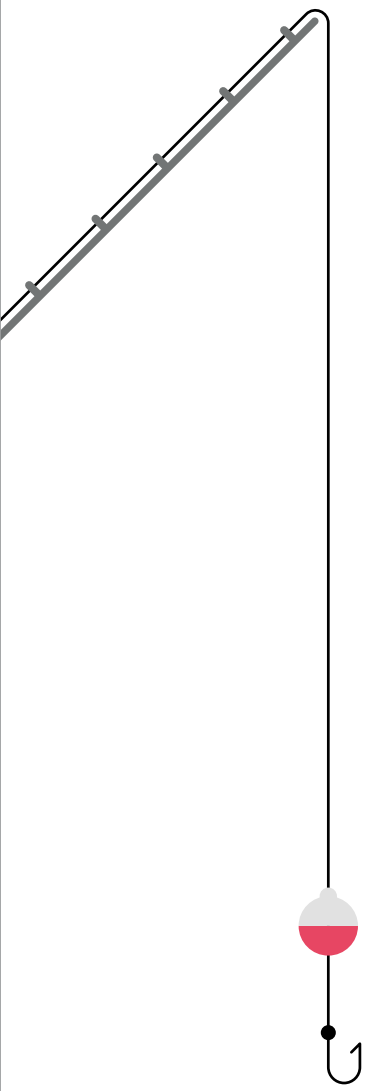
Tuttavia, gli attacchi più seri sono sempre più frequenti. Il 51% delle organizzazioni esaminate nel 2015 ha subito attacchi di tipo DDoS (Direct Denial of Service), che possono anche diventare insostenibili, arrivando a costare, in media, 127.000 dollari. Ancor più allarmante è il fatto che il 35% di esse abbia subito attacchi da parte di utenti interni malintenzionati, per un costo medio di 145.000 dollari.[9]

Il quadro emergente è rappresentato da implacabili attacchi minori provenienti dall'esterno e da attacchi gravi infrequenti ma sorprendentemente probabili, causati da atti di negligenza, se non di mala fede, da parte di utenti interni. Il 62% delle organizzazioni ha subito attacchi di phishing o ingegneria sociale, sfruttando le debolezze dei dipendenti, per un costo medio di 86.000 dollari.[11]

Un sondaggio separato condotto da Spiceworks, per conto di HP, ha riportato gli attacchi subiti negli anni 2014 e 2015 da parte di 90 organizzazioni britanniche.[12]



[7] NTT Security Risk:Value Report 2016
[8] HP 2Printer Security Report 2015
[9] http://www.gartner.com/newsroom/id/3291817
[10] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf
[11] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic
[12] HPI Printer Security Research, Spiceworks 2016



Come si verificano le violazioni

I mass media ritraggono gli hacker aziendali come capaci di oltrepassare sofisticate reti protette di governi e aziende, Tuttavia la realtà è, di solito, meno complessa.

I virus possono trarre vantaggio da reti compromesse, ma i malware, di solito, richiedono una qualche forma di errore da parte dell'utente. Da questi errori dipendono anche gli attacchi di phishing o ingegneria sociale. Anche i grandi attacchi di tipo DDoS e di furto di informazioni sono spesso il risultato di un atto di negligenza da parte degli utenti.

L'ormai famigerato hacker di Dropbox ebbe la strada spianata probabilmente da un incauto dipendente Dropbox che usò la stessa password per i sistemi interni e per il suo account LinkedIn.[13] Il presunto attacco hacker russo ai danni del DNC avvenne apparentemente grazie a John Podesta, ex consigliere di Hillary Clinton, a seguito di un clic su un collegamento presente in un'email di phishing che era stata contrassegnata erroneamente come attendibile da un assistente.[14]

Gli hacker, per la buona riuscita degli attacchi, non hanno bisogno di un'assistenza attiva. Altrettanto pericolosa è la scarsa conoscenza o l'inosservanza dei protocolli di sicurezza. Una minaccia crescente è rappresentata dal fatto che i dipendenti portano i propri dispositivi sul posto di lavoro e usano programmi software commerciali sul cloud: entrambi gli aspetti introducono elementi non protetti in una rete altrimenti sicura, al di fuori del controllo del reparto IT aziendale, creando una vulnerabilità non controllabile.

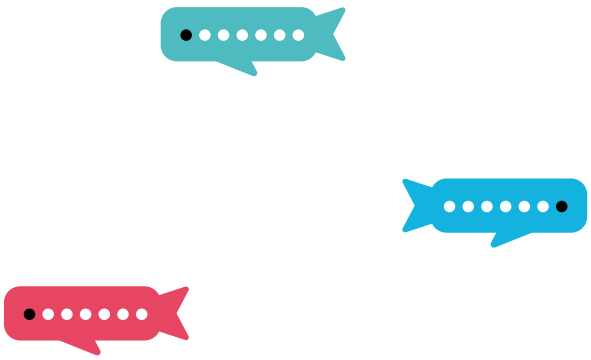
Quasi sempre, gli hacker non hanno la necessità di impiegare algoritmi sofisticati o tecnologie all'avanguardia, quando basta loro soltanto una piccola distrazione da parte di un utente.

Niente più firewall

Una strategia corretta volta a proteggere i sistemi informativi aziendali era fondata, fino a poco tempo fa, sull'applicazione di programmi antivirus e software di firewall. Il dictat condiviso era "prevenire e proteggere". Nell'odierno ambiente lavorativo, questa strategia non è più credibile.

L'81% degli intervistati nel sondaggio Ponemon ha affermato che i dispositivi mobili della loro rete sono stati oggetto di attacchi malware. Fra gli altri aspetti che aumentano i rischi alla sicurezza, figurano l'uso da parte dei dipendenti di applicazioni commerciali sul cloud (aspetto citato dal 72% degli intervistati), il BYOD (69%) e il lavoro di alcuni dipendenti da casa e fuori sede (62%).[15]

In breve, un firewall aveva senso quando gli amministratori di rete potevano controllare i dispositivi connessi. Ma in un'epoca in cui i dipendenti portano i propri dispositivi sul posto di lavoro (spesso anche più dispositivi e senza notificarlo al reparto IT) e in cui aumenta il numero di lavoratori che si connettono da remoto, è praticamente impossibile proteggere la rete aziendale. Ogni dispositivo non controllato è un endpoint vulnerabile che può essere sfruttato dagli hacker.



[13] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach
[14] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0
[15] Ponemon 2016 State of the Endpoint Report

La visione di HP: andare oltre la sicurezza della rete

Michael Howard, responsabile delle pratiche di sicurezza globali di HP, in riferimento ai temi legati alla sicurezza degli endpoint ha affermato che:

Una delle principali preoccupazioni correnti consiste nel fatto che le aziende si sforzano di proteggere ogni endpoint a causa della mancanza di consapevolezza e di conoscenze su alcuni dispositivi e sui rischi correlati. La sicurezza sembra possa essere garantita da un firewall che, tuttavia, non è più sufficiente per proteggersi da un attacco. I team addetti alla sicurezza devono conoscere ogni endpoint all'interno dell'infrastruttura e garantire che ciascuno sia messo al riparo da attacchi sempre più sofisticati tramite diversi livelli di protezione.

È fondamentale per i team addetti alla sicurezza esaminare ogni angolo dell'infrastruttura IT dell'azienda e creare un livello di protezione aggiuntivo oltre ai controlli di rete standard. I firewall da soli non possono resistere ad attacchi sofisticati, pertanto diventa imprescindibile disporre di una politica di difesa costituita da più livelli di protezione su ogni endpoint per garantire alle aziende di poter soddisfare i requisiti normativi ed evitare di incorrere in sanzioni cospicue.

La politica di HP prevede che, per ogni nuova soluzione, nuovo servizio o nuovo prodotto sviluppato dall'azienda, la sicurezza sia la priorità assoluta. I team addetti allo sviluppo sanno che devono rispondere alle criticità poste dalla sicurezza e che devono sapere come mettere in atto sulla rete, in modo sicuro, le strategie adeguate.

Ora come non mai, la sicurezza deve essere una priorità assoluta, non una clausola aggiuntiva.

La sicurezza a più livelli

Un nuovo approccio alla sicurezza informatica deve essere stratificato.
La sicurezza della rete è ancora importante, ma deve fondarsi su un approccio diversificato. Molte violazioni si basano su un ingresso iniziale che garantisce l'accesso a tutti i componenti del sistema. Pensiamo ad esempio al passo falso compiuto nel caso di phishing di John Podesta. Diventa di fondamentale importanza sottoporre le informazioni sensibili a più livelli di accesso.

I dispositivi devono essere tenuti sotto controllo. Una questione fondamentale per i responsabili IT consiste nel garantire che ciascun dispositivo connesso alla rete sia protetto da software di sicurezza aggiornati regolarmente e sia esaminato abitualmente per rilevare eventuali anomalie. Ancora meglio, si dovrebbero usare gli stessi dispositivi come sensori per raccogliere informazioni in tempo reale al fine di allertare su eventuali violazioni sulla totalità della rete di cui fanno parte.

È necessario mettere in atto sistemi di gestione della sicurezza il più possibile completi, che includano la formazione di ogni dipendente sui protocolli di sicurezza informatica. L'errore umano rappresenta la minaccia numero uno per la sicurezza della rete.

La sicurezza dei dispositivi

Forse, la questione principale relativa alla gestione dell'odierna sicurezza informatica riguarda il controllo sui dispositivi che possono accedere alla rete.
La prima, semplice soluzione spesso adottata in prima battuta consiste nel tenere separate le reti Wi-Fi per utenti ospiti e dipendenti, in modo che dispositivi esterni non protetti non possano accedere alla rete principale. Questo approccio procede di pari passo con la formazione dei dipendenti sull'uso della rete dai loro dispositivi personali.

La seconda soluzione consiste nel tenere sotto controllo i dispositivi dei dipendenti. Questa precauzione deve passare attraverso le politiche aziendali in materia di BYOD o CYOD, e sono molti i sostenitori del CYOD poiché fornisce un maggior controllo sui dispositivi utilizzati, offrendo la possibilità di scegliere quelli con funzioni di sicurezza migliori.

L'utilizzo di uno dei nostri PC della gamma HP Elite, ad esempio, è preferibile rispetto a un laptop economico. Ogni PC HP Elite è dotato della tecnologia HP SureStart che controlla il BIOS ogni 15 minuti e ripristina il computer al suo stato originale quando rileva un'anomalia, bloccando eventuali accessi indesiderati. Per questa funzione (e per molte altre), i computer della nostra serie HP Elite 800 sono stati recentemente dichiarati come i "PC più sicuri al mondo".[16] Tuttavia, i dipendenti difficilmente posseggono un proprio PC HP Elite.

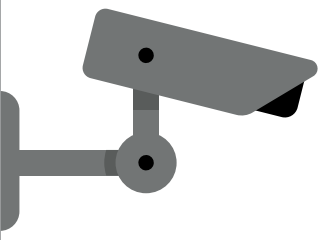
I dipendenti, spesso, preferiscono usare i propri dispositivi per due ragioni:
1. La tecnologia destinata ai consumatori è spesso migliore di quella fornita dall'ufficio
2. Ai dipendenti piace usare la tecnologia che conoscono meglio.

Proponendo una politica del CYOD ben assortita, che offra gli ultimi dispositivi con un ciclo di aggiornamento regolare, le organizzazioni possono fornire dispositivi migliori rispetto a quelli dei dipendenti e mantenere un maggior controllo sulla sicurezza di tali dispositivi. Ecco su cosa basiamo la vendita della nostra soluzione HP Device as a Service (DaaS).

È essenziale includere tutti i dispositivi nella strategia di sicurezza, anche quelli spesso dimenticati. In un sondaggio condotto da IDC, l'80% degli intervistati ha affermato che la sicurezza IT è importante per le proprie aziende, ma solo il 59% ha riconosciuto l'importanza della sicurezza di stampa, sebbene più della metà di tali aziende abbia subito una violazione di questo tipo nei precedenti 12 mesi.

Il numero medio di violazioni alla sicurezza prima dell'implementazione di una politica per la sicurezza di stampa era pari a 9,9 all'anno con un costo medio di 521.400 dollari (sanzioni incluse). A seguito dell'implementazione di politiche per la sicurezza di stampa, il numero medio di violazioni è sceso fino a 1,5. Il risparmio così ottenuto è pari a 200 ore all'anno per i dipendenti e a 250.000 dollari in costi correlati, inclusi controlli e conformità.[17]

[16] http://www8.hp.com/us/en/campaign/computersecurity/
[17] IDC The Business Value of Printer Security 2015



Rilevamento e risposta in modo proattivo

Secondo una ricerca condotta da PAC, il 77% della spesa per la sicurezza IT viene impiegato in tecnologie di prevenzione e protezione come software antivirus e firewall. Tuttavia, questo approccio si è rivelato nel tempo poco efficace. La ricerca ha evidenziato, inoltre, che il 67% delle aziende esaminate ha subito una violazione informatica nei precedenti 12 mesi e il 100% di esse almeno una volta nel passato.[18]

Un software antivirus, in modo particolare, è sorprendentemente inefficace. Damballa ha condotto dei test in cui è stata deliberatamente attaccata una rete per misurare la risposta del software antivirus. Ci sono voluti più di sei mesi prima di riuscire a identificare tutti i file dannosi.[19] Questo risultato è coerente con un'altra ricerca PAC in cui è emerso che le aziende hanno impiegato da uno a sei mesi per rilevare gli attacchi subiti.

Mantenere gli endpoint al sicuro non può più basarsi sulla prevenzione. Il crescente numero di incidenti causati da virus e malware, oltre all'intrinseca insicurezza del lavoro condotto sui dispositivi BYOD mobili, porta all'inevitabilità delle violazioni. Nessuno suggerisce di abbandonare del tutto i sistemi di prevenzione e protezione, ma la capacità di rilevare e rispondere chiaramente agli attacchi deve diventare una delle massime priorità di un'azienda.

Il monitoraggio continuo in tempo reale è necessario, idealmente mediante l'uso degli stessi endpoint come sensori, per allertare il resto della rete in caso di violazioni. Ciò consente risposte remote da parte del team di sicurezza IT, che includono processi quali:

- Arresto di un dispositivo da remoto
- Eliminazione di un processo infetto o che sta diffondendo malware
- Messa in quarantena di un file specifico o di un gruppo di file
- Interruzione delle comunicazioni di rete per isolare i dispositivi infettati[20]

Accettare che le violazioni siano inevitabili e attuare appropriati protocolli per rispondervi, nonché implementare la tecnologia necessaria per metterli in pratica: sono queste le condizioni per garantire la sicurezza informatica quando non si può più fare affidamento sui sistemi di prevenzione.

"Nessuna tecnologia può garantire la sicurezza se gli utenti la mettono a rischio."

– Joseph Steinberg [21]

La sicurezza dei dipendenti

Altrettanto importante, se non di più, è garantire che il dispositivo stesso protegga il suo utente. Tutti i dipendenti devono ricevere un'adeguata formazione sulla sicurezza informatica, per essere messi al corrente dei rischi derivanti dal phishing, dal visitare siti Web sospetti, dal procedere con download di allegati sospetti. I dipendenti devono conoscere le politiche per la sicurezza delle password, che prevedono l'uso di password complesse e univoche per ogni accesso sensibile e dell'appropriato sistema per la gestione delle password in cui conservarle.

Devono essere resi consapevoli dell'importanza di mantenere regolarmente aggiornato il software di sicurezza sui loro dispositivi, per alleggerire il carico di lavoro per il monitoraggio da parte del reparto IT. Devono stare attenti a usare solo dispositivi protetti per accedere alle reti dell'organizzazione, evitando di usare i dispositivi personali su reti esterne non protette quando accedono a dati sensibili.

Molti esperti in sicurezza informatica di alto livello consigliano di eseguire simulazioni di attacchi di phishing, creando addirittura siti Web fittizi di phishing per addestrare i dipendenti, e di fornire una formazione regolare sulla sicurezza informatica. Perché la maggior parte degli attacchi sfrutta le debolezze umane, tramite un atto di negligenza o di mala fede.

[18] PAC Incident Response Management 2015
[19] https://www.damballa.com/time-to-fix-malware-strategies-2/
[20] The Essential Endpoint Detection Checklist – HP Now
[21] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Conclusione

La spesa per la sicurezza IT deve spostarsi dai sistemi di prevenzione e protezione alle soluzioni di rilevamento e risposta agli attacchi all'endpoint
La difesa dei dati di un'organizzazione nell'attuale ambiente IT, che si trova ad affrontare minacce crescenti e allo stesso tempo una perdita di controllo sui confini della rete, prevede due aspetti: un cambiamento concettuale e un maggior numero di risorse impiegate per la sicurezza.

Il concetto della rete deve cambiare. La concezione della rete come di un recinto che circonda una serie di dispositivi non è più applicabile in quanto le reti attuali non sono altro che singoli dispositivi connessi, ognuno dei quali costituisce un endpoint. Proteggere la rete significa proteggere gli endpoint. Ogni endpoint è costituito da due elementi: il dispositivo e il suo utente. Entrambi questi elementi vanno tenuti in considerazione.

Tuttavia, garantire la sicurezza in questo nuovo paradigma è molto più complicato rispetto all'ambiente dei semplici PC desktop connessi tramite Ethernet del passato. Richiede un maggior numero di risorse, che è necessario sostenere. Circa il 61% degli intervistati nel sondaggio Ponemon lo riconosce.

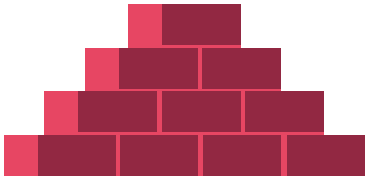
Il difficile è convincere il resto dell'organizzazione. Solo il 36% degli intervistati ritiene di avere a disposizione un budget adeguato e personale sufficiente per garantire la sicurezza degli endpoint. Il 69% afferma che il reparto IT non riesce a tenere il passo con la domanda da parte dei dipendenti di ricevere una maggiore assistenza. Il 71% afferma che le politiche di sicurezza degli endpoint sono difficili da applicare.[22]

L'80% dei responsabili della sicurezza IT considera la conformità normativa il modo migliore per giustificare il finanziamento dei propri programmi di sicurezza, ma anche la ragione meno importante per effettuare una spesa. La conformità implica soddisfare i minimi requisiti.[23]

I responsabili decisionali IT devono collaborare con gli alti dirigenti per sottolineare l'importanza della sicurezza, chiarendo quali sono i costi legati a un sistema di sicurezza permissivo (spese di recupero, perdita di ricavi, valore delle azioni deprezzato) e sottolineare l'importanza dei risparmi nel lungo termine. Molte soluzioni di sicurezza generano miglioramenti anche in altri ambiti. Pensiamo alla migliore produttività derivante dall'implementazione di politiche per la sicurezza di stampa e i vantaggi in termini di produttività derivanti dal fornire regolarmente tecnologie aggiornate in un programma CYOD flessibile, fornito da terze parti tramite sottoscrizione (come HP DaaS).

La sfida è formidabile: con il tempo, con l'esplosione dei dispositivi nell'era dell'Internet delle cose e con l'aumento della complessità della criminalità informatica, la situazione diventerà sempre più complessa, ma non insormontabile. Con la giusta tecnologia, una strategia appropriata e un numero adeguato di risorse, possiamo difendere i nostri endpoint mantenendo al sicuro i nostri dati.

Per saperne di più sulla soluzione HP Device as a Service e su come sia d'aiuto nel realizzare un programma CYOD completo, flessibile e sicuro, visitate **questa** pagina.



Registratevi per ricevere gli aggiornamenti
hp.com/go/getupdated

Condividete con i colleghi

Valutate questo documento

[22] Ponemon 2016 State of the Endpoint Report
[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697