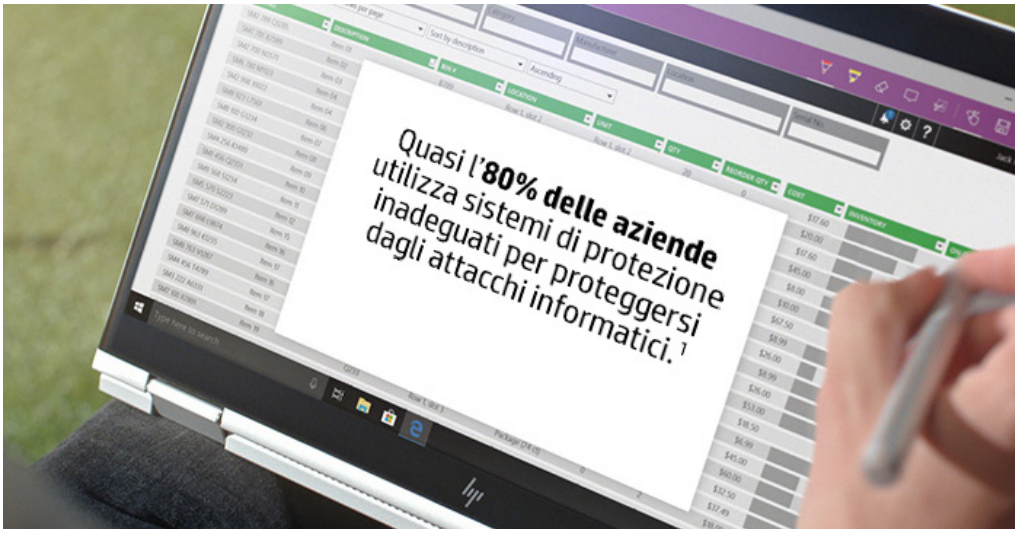
I sistemi automatici di difesa possono salvare i tuoi dispositivi aziendali

Scopri di più



Come combatti una minaccia che è invisibile alle tue difese? Con l'automazione.

600 miliardi di sterline l'anno. Questo è stato il costo della criminalità informatica nel mondo nel 2017[2]. E la cifra cresce di continuo, grazie ad hacker sempre più sofisticati e abili. Recentemente è stato riferito che il 20% delle piccole e medie imprese vittime di un attacco informatico ha dovuto cessare le attività aziendali con effetto immediato, e il 12% ha subito una perdita di ricavi[3]. Uno degli ultimi subdoli attacchi a diventare la rovina dei responsabili IT è quello che ha come bersaglio il firmware durante il processo di avvio del PC: l'attacco al BIOS.

Milioni di macchine hanno una serie di punti deboli di base legati al BIOS, e potrebbero quindi essere violate anche da hacker non molto competenti. Qualche anno fa, i ricercatori Xeno Kovah e Corey Kallenberg hanno presentato a una conferenza un nuovo tipo di attacco, svelando che in poche ore sarebbero stati in grado di attaccare da remoto e infettare il BIOS di vari sistemi[4]. Poiché la maggior parte dei BIOS condivide lo stesso codice, dopo aver violato il primo, è solo una questione di tempo abbattere le difese di molte altre macchine con le stesse competenze.

Questo tipo di attacco è particolarmente pericoloso perché il suo obiettivo è qualcosa di non protetto. Tra il sistema operativo e l'hardware esiste uno spazio nascosto che è sempre stato ignorato. E anche se la tua rete può sembrare a tenuta stagna e il tuo dispositivo è protetto dai migliori software di sicurezza antivirus al mondo, c'è sempre un breve momento all'avvio in cui le tue difese si stanno preparando: è in quel momento che un attacco ostile al BIOS può creare seri danni.

Dato che la maggior parte dei software di sicurezza informatica è installata a livello del sistema operativo, il malware inserito nel BIOS (prima dell'avvio e quindi trasferito alla Modalità di gestione del sistema) non sarà individuabile dal software di sicurezza informatica dell'endpoint. Da lì, gli hacker otterranno il controllo totale del sistema. Saranno in grado di rubare i tuoi dati, renderli illeggibili oppure diffondere nuovi malware all'interno della rete aziendale. Cosa ancora peggiore: può rivelarsi quasi impossibile scoprire che si è verificata una violazione o infezione.

Il modo migliore per proteggere i tuoi dispositivi aziendali è usare una sicurezza multi-livello. Tuttavia, le competenze del tuo personale IT sono troppo importanti per essere sprecate in una scansione continua e nella riparazione manuale di reti e dispositivi. HP offre una risposta automatica, inclusa nella sua gamma di soluzioni per la sicurezza: HP Sure Start[5].

"Questa misura fa parte di uno sforzo congiunto con gli HP Lab per assistere le aziende nel gestire al meglio i rischi e proteggere gli utenti e la produttività dell'IT contro attacchi dannosi, un aggiornamento non andato a buon fine o qualsiasi altra ragione casuale o sconosciuta".

- Vali Ali, Chief Technologist for Security & Privacy nella Business Unit PC di HP.

I sistemi automatici di difesa possono salvare i tuoi dispositivi aziendali

HP Sure Start è una protezione con riparazione automatica a livello di BIOS. Chiamiamo questo approccio "resilienza informatica". Il sistema funziona creando un'immagine "golden master" del BIOS, crittografata direttamente sul dispositivo. Pertanto, se qualcuno cerca di violare il BIOS, questo si riavvia automaticamente caricando la versione "golden master", cancellando il file infetto e informando te e il tuo team dell'attacco. In pratica, la macchina si auto-ripara.

Tradotto: la produttività non si interrompe. I costi sono inferiori. I dispositivi sono più conformi ai requisiti sulla protezione dei dati. E, soprattutto, è un modo di lavorare più semplice.

Se ti chiedi quale sia il modo più semplice di avere dispositivi all'avanguardia dotati di HP Sure Start, considera HP Device as a Service (DaaS)[6]. Si tratta di un moderno modello di approvvigionamento informatico che semplifica il modo in cui le organizzazioni commerciali possono fornire ai dipendenti l'hardware e gli accessori giusti, gestire flotte di dispositivi con diversi sistemi operativi e ricevere servizi aggiuntivi per il ciclo di vita. HP DaaS offre piani semplici ma flessibili, a una tariffa singola per dispositivo per consentirti di lavorare con la massima sicurezza ed efficienza.

Gli endpoint e gli access point devono essere monitorati a tutti i livelli. È ora di prestare la dovuta attenzione alle parti nascoste dei nostri dispositivi. Ogni persona, azienda e organizzazione al mondo può diventare più sicura e resiliente con il portafoglio di prodotti HP, compreso HP EliteBook x360, con processori opzionali Intel® Core™ i7 di ottava generazione. Come tutti i componenti della linea HP Elite, questo dispositivo offre una tecnologia di sicurezza avanzata, grazie alle funzioni integrate come HP Sure Start.

Scopri i vantaggi delle soluzioni per la sicurezza HP per la tua azienda.

Fonti:

1. ID Statista Survey 622857, "Small and medium sized enterprises in the U.S", Statista, ottobre 2016
2. https://www.mcafee.com/enterprise/en-gb/solutions/lp/economics-cybercrime.html
3. Osterman Research, sponsorizzata da Malwarebytes "Second Annual State of Ransomware Report: US Survey Results", luglio 2017
4. https://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems
5. Varie generazioni di HP Sure Start sono disponibili su configurazioni selezionate dei sistemi HP Elite e HP Pro.
6. I piani HP DaaS e/o i componenti inclusi possono variare per regione o in base al partner di servizio HP DaaS autorizzato. Per informazioni specifiche sulla vostra zona, contattate il rappresentante HP locale o un partner DaaS autorizzato. I servizi HP sono regolati dai termini e dalle condizioni di servizio applicabili di HP, forniti o indicati al Cliente al momento dell'acquisto. Il cliente può disporre di ulteriori diritti legali in base alle leggi vigenti nel Paese in cui risiede e tali diritti non sono in alcun modo influenzati dai termini e dalle condizioni del servizio o dalla garanzia limitata HP fornita con il prodotto HP acquistato.

4AA7-3219ITIT, aprile 2019