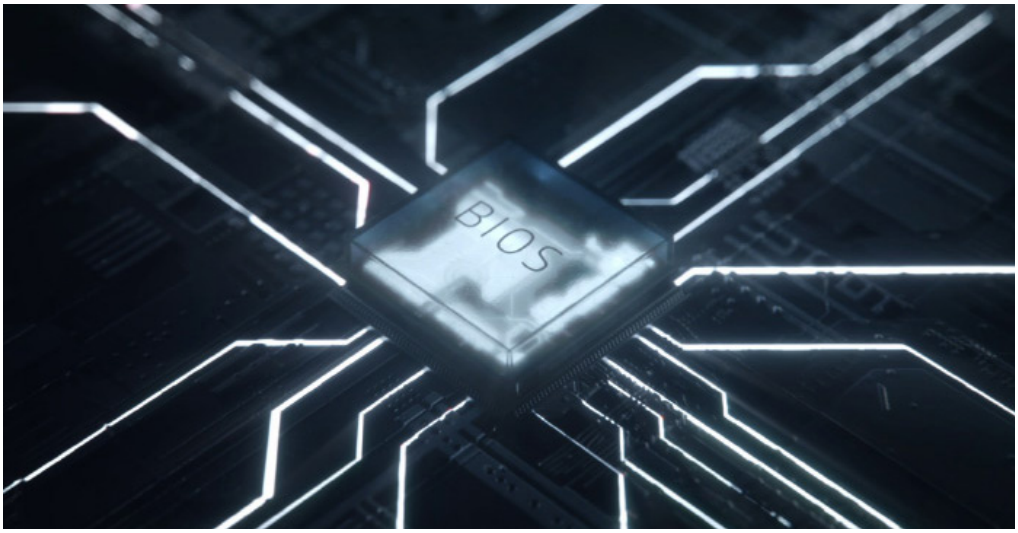
Perché i sistemi automatici di difesa salveranno i tuoi dispositivi aziendali

Scorpi di più



Come combatti una minaccia che si nasconde tra le tue difese? Con l'automazione.

338 miliardi di sterline all'anno. È l'attuale costo della criminalità informatica nel mondo[1]. E la cifra cresce di continuo grazie ad hacker sempre più sofisticati ed esperti. Uno degli ultimi subdoli attacchi a diventare la rovina dei responsabili IT è 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 potevano attaccare da remoto e infettare il BIOS di vari sistemi[2]. 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 moltre 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 sistemi di sicurezza al mondo, c'è sempre un breve momento all'avvio in cui le tue difese si stanno preparando. È proprio 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 trasferito nella Modalità di gestione del sistema) non sarà individuabile dal software di sicurezza informatica dell'endpoint. Da lì, gli hacker sostituiranno il tuo BIOS con la loro versione personalizzata, che potranno gestire da remoto per un tempo indefinito. 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. Le competenze del tuo personale IT non dovrebbero essere sprecate per una scansione costante e per riparazioni manuali. HP offre una risposta automatica, compresa nella sua gamma di soluzioni per la sicurezza: HP Sure Start.

"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.

Perché i sistemi automatici di difesa salveranno 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. E, soprattutto, è un modo di lavorare più semplice.

Se ti chiedi quale sia il modo più semplice di avere dispositivi all'avanguardia con l'abilitazione di HP Sure Start, considera HP Device as a Service. Si tratta di un moderno modello di fruizione di PC che semplifica il modo in cui le organizzazioni commerciali forniscono ai dipendenti l'hardware e gli accessori giusti, gestiscono flotte di dispositivi con vari sistemi operativi e ricevono servizi aggiuntivi per il ciclo di vita. HP DaaS offre piani semplici ma flessibili, a una tariffa per dispositivo perché tutto funzioni senza intoppi ed efficientemente.

Gli endpoint e gli access point devono essere monitorati a tutti i livelli. È ora di smettere di evitare le 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 l'HP EliteBook Serie 800, con processori Intel® Core™ di ottava generazione opzionali. Come tutti i componenti della linea HP Elite, questo dispositivo offre una tecnologia di sicurezza grazie alle funzioni di sicurezza integrate come HP Sure Start.

Per saperne di più su come proteggere i tuoi dispositivi aziendali, leggi il nostro ultimo White Paper HP Sure Start e scopri i vantaggi delle soluzioni per la sicurezza HP per la tua azienda.

Fonti:

1. https://www.mcafee.com/error-pages/404.aspx?url=https://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf
2. https://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/
3. Varie generazioni di HP Sure Start sono disponibili su configurazioni selezionate dei sistemi HP Elite e HP Pro.

4AA7-3219ITE, Maggio 2018