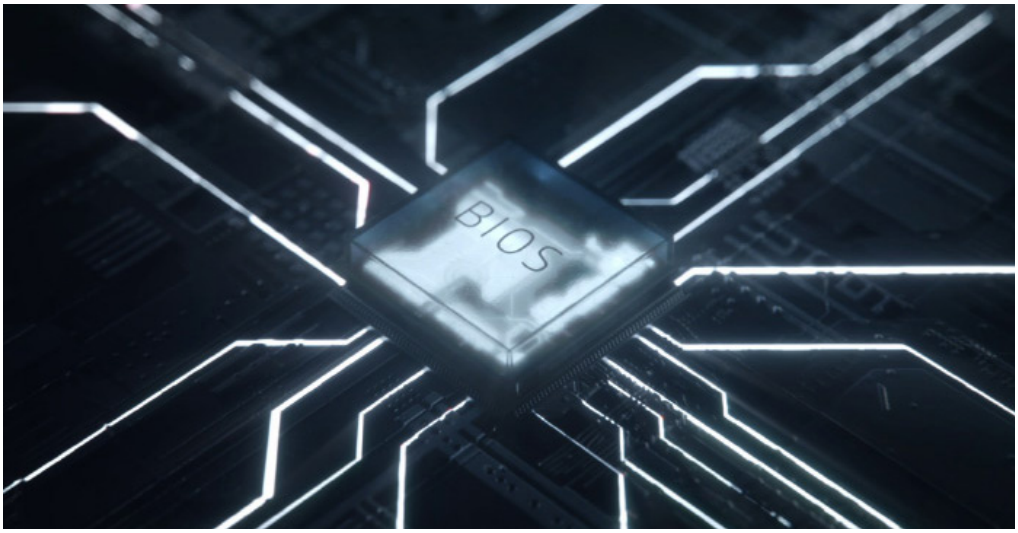
Waarom automatische beveiliging uw bedrijfsapparaten redt

Meer Info



Hoe bestrijdt u een dreiging die door uw beveiliging heen glipt? Met automatisering.

£338 miljard per jaar. Dat zijn de huidige kosten van cybercriminaliteit over de hele wereld[1]. Dat bedrag wordt hoger en hoger omdat hackers verfijnder te werk gaan en tot meer in staat zijn. Een van de nieuwste aanvalsmethoden, die een nachtmerrie wordt voor IT-managers, is de BIOS-aanval.

Miljoenen machines hebben standaard BIOS-tekortkomingen, waarmee ze kunnen worden gehackt door iemand met zelfs maar gemiddelde hackvaardigheden. Onderzoekers Xeno Kovah en Corey Kallenberg presenteerden een aantal jaren geleden een nieuw soort aanval op een conferentie, waarmee ze lieten zien dat ze in een paar uur op afstand de BIOS van meerdere systemen konden hacken en infecteren[2]. Omdat de meeste BIOS'en dezelfde code gebruiken was het, nadat de eerste gekraakt was, een kwestie van tijd voordat met dezelfde vaardigheden veel meer machines konden worden gekraakt.

Dit type aanval is zo gevaarlijk, omdat het zich richt op iets dat niet beveiligd is. Er is een onontgonnen gebied tussen het besturingssysteem en de hardware dat tot nu toe geen aandacht kreeg. En hoewel uw netwerk waterdicht lijkt en uw apparaat beschermd is achter de beste beveiligingssystemen ter wereld, is er nog steeds een kwetsbaar moment tijdens het opstarten en voordat uw verdedigingssystemen actief zijn. Op dat moment kan een vijandige BIOS-aanval zijn vernietigende werk doen.

Omdat de meeste software voor cyberbeveiliging op het niveau van het besturingssysteem werkt, is malware in de BIOS (vóór opstarten en de fase voor systeembeheer) niet te detecteren voor cyberbeveiligingssoftware voor endpoints. Daarvandaan vervangen hackers uw BIOS met hun eigen aangepaste versie, die op afstand en onbeperkt kan worden beheerd. En het ergste is dat het bijna onmogelijk is om te ontdekken dat de BIOS is gehackt of geïnfecteerd.

De beste manier om uw bedrijfsapparaten te beveiligen is door gebruik te maken van meerlaagse beveiliging. Uw IT-team moet niet alleen maar bezig zijn met scannen en handmatig oplossen. HP biedt een geautomatiseerde respons – als onderdeel van een reeks beveiligingsoplossingen – HP Sure Start.

"Dit is onderdeel van een samenwerking met HP Labs om bedrijven te helpen hun risico beter te beheren en gebruikers en IT-productiviteit te beschermen tegen kwaadwillende aanvallen, een mislukte update of andere ongelukkige of onbekende omstandigheden"

- Vali Ali, Chief Technologist for Security and Privacy in de HP PC Business Unit.

HP Sure Start is een zelfherstellende BIOS-beveiliging. Wij noemen deze benadering cyber-veerkracht. Het systeem werkt het een 'gouden master' van de BIOS, die direct op het apparaat versleuteld is. Dus als iemand de BIOS probeert te hacken, herstart deze automatisch en wordt vervolgens de 'gouden master' geladen, het wist de geïnfecteerde bestanden en brengt uw team op de hoogte. In feite herstelt de machine zichzelf.

Waarom automatische beveiliging uw bedrijfsapparaten redt

Dat betekent ononderbroken productiviteit en lagere kosten. Dat betekent ook meer veilige apparaten. En bovenal is het een eenvoudigere manier van werken.

Als u zich afvraagt wat de eenvoudigste manier is om moderne apparaten met HP Sure Start voor uw gebruikers aan te schaffen, overweeg dan HP Device as a Service. Het is een modern pc-gebruikersmodel dat het commerciële bedrijven eenvoudiger maakt om hun medewerkers uit te rusten met de juiste hardware en accessoires, netwerken met meerdere besturingssystemen te beheren en aanvullende diensten voor de gebruiksduur af te sluiten. HP DaaS biedt eenvoudige, maar flexibele plannen, tegen een vergoeding per apparaat om alles soepel en efficiënt te laten verlopen.

Endpoints en accesspoints dienen op elk niveau in de gaten te worden gehouden. Het wordt tijd dat u de verborgen onderdelen van uw apparaten niet meer negeert. Elk(e) persoon, onderneming en organisatie op de wereld kan veiliger en veerkrachtiger worden met HP's portfolio van producten, waaronder de HP EliteBook 800 serie. Als onderdeel van de HP Elite-serie biedt dit device beveiligingstechnologie dankzij ingebouwde beveiligingsfuncties als HP Sure Start.

Voor meer informatie over de bescherming van de apparaten binnen uw bedrijf, kunt u onze actuele HP Sure Start White Paper lezen en de voordelen ontdekken van HP beveiligingsoplossingen voor uw bedrijf.

Bronnen:

1. https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf
2. https://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/
3. verschillende generaties van HP Sure Start zijn beschikbaar op bepaalde configuraties van HP Elite en HP Pro-systemen.

4AA7-3219NLNL, Mei 2018