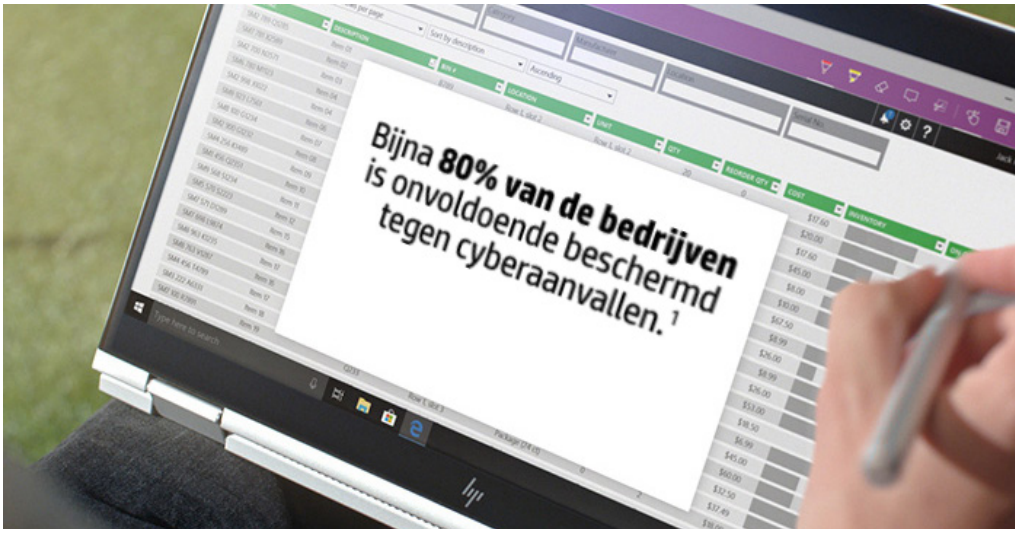
Automatische beveiliging kan uw bedrijfsapparaten redden

Meer informatie



Hoe bestrijdt u een dreiging die onder de radar blijft? Met automatisering.

$ 600 miljard per jaar. Dat waren de kosten voor cybercriminaliteit over de hele wereld in 2017[2]. Dat bedrag wordt hoger en hoger omdat hackers geraffineerder te werk gaan en tot meer in staat zijn. Recentelijk is gemeld dat 20% van de MKB-bedrijven direct heeft moeten stoppen met de bedrijfsactiviteiten, en dat 12% inkomsten heeft verloren na een cyberaanval[3]. Een van de nieuwste aanvalsmethoden, die een nachtmerrie wordt voor IT-managers, zijn aanvallen op de firmware van pc's tijdens het opstartproces: BIOS-aanvallen.

Miljoenen apparaten hebben standaard BIOS-tekortkomingen, waarmee ze zelfs kunnen worden gehackt door iemand met gemiddelde hackvaardigheden. Onderzoekers Xeno Kovah en Corey Kallenberg presenteerden een aantal jaren geleden op een conferentie een nieuw soort aanval, waarmee ze lieten zien dat ze in een paar uur op afstand het BIOS van meerdere systemen konden hacken en infecteren[4]. Omdat de meeste BIOS'en dezelfde code gebruiken was het, nadat het 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 met de beste antivirusbeveiligingssoftware ter wereld, is er nog steeds een kwetsbaar moment tijdens het opstarten en voordat uw verdedigingssystemen actief zijn, waardoor een vijandige BIOS-aanval grote schade kan aanrichten.

Omdat de meeste software voor cyberbeveiliging op het niveau van het besturingssysteem werkt, is malware in het BIOS (vóór opstarten en de fase voor systeembeheer) niet te detecteren voor cyberbeveiligingssoftware voor endpoints. Daarvandaan krijgen hackers volledige controle over uw systeem. Ze kunnen uw gegevens stelen, het onleesbaar maken of nieuwe malware binnen het netwerk van uw bedrijf verspreiden. En het ergste is dat het bijna onmogelijk is om te ontdekken dat het 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[5].

"Dit is onderdeel van een samenwerking met HP Labs om bedrijven te helpen hun risico beter in te schatten 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.

Automatische beveiliging kan uw bedrijfsapparaten redden

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

Dat betekent ononderbroken productiviteit. Dat betekent lagere kosten. Dat betekent veiligere 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 (DaaS)[6]. Het is een modern pc-servicemodel dat het voor commerciële bedrijven eenvoudiger maakt om hun medewerkers uit te rusten met de juiste hardware en accessoires, netwerken met meerdere besturingssystemen te beheren en aanvullende lifecycle-services af te sluiten. HP DaaS biedt eenvoudige, maar flexibele plannen, tegen één vergoeding per apparaat om alles soepel en efficiënt te laten verlopen.

Endpoints en toegangspunten 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 de producten van HP, waaronder de HP EliteBook x360, met optionele 8e generatie Intel® Core™ i7-processoren. Als onderdeel van de HP Elite-serie beschikt dit device over beveiligingstechnologie dankzij ingebouwde beveiligingsfuncties zoals HP Sure Start.

Ontdek de voordelen van HP beveiligingsoplossingen voor uw bedrijf.

Bronnen:

1. Statista Survey ID 622857, "Small and medium sized enterprises in the U.S by Statista, oktober 2016
2. https://www.mcafee.com/enterprise/en-gb/solutions/lp/economics-cybercrime.html
3. Osterman Research, gesponsord door Malwarebytes "Second Annual State of Ransomware Report: US Survey Results" juli 2017
4. https://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/
5. Verschillende generaties van HP Sure Start zijn beschikbaar op bepaalde configuraties van HP Elite en HP Pro-systemen.
6. HP DaaS-plannen en/of bijgeleverde onderdelen kunnen per regio of per geautoriseerde HP DaaS Servicepartner verschillen. Neem contact op met uw HP vertegenwoordiger of geautoriseerde DaaS-partner voor specifieke details op uw locatie. Voor HP services gelden de van toepassing zijnde HP servicevoorwaarden, die bij aankoop aan de klant worden verstrekt of getoond. Mogelijk heeft de klant volgens de geldende lokale wetgeving nog andere rechten. De Algemene Servicevoorwaarden van HP en de HP garantie op uw HP product maken geen inbreuk op deze wettelijk vastgelegde rechten.

4AA7-3219NLE, april 2019