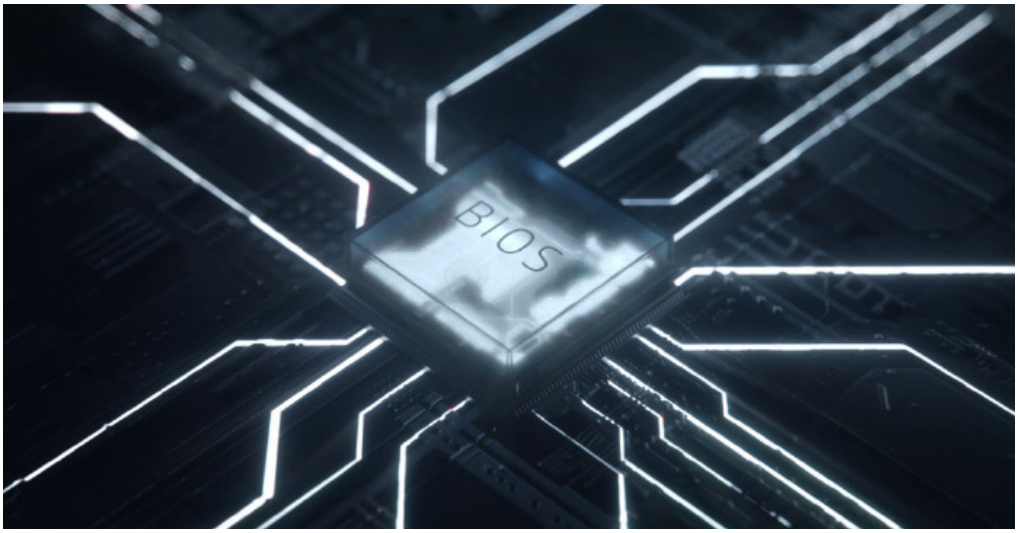
Hvorfor automatisk forsvar beskytter enhetene i virksomheten din

Finn ut mer



Hvordan slåss du mot en trussel som skjuler seg under forsvaret ditt? Du automatiserer.

338 milliarder pund i året. Det er de globale kostnadene som oppstår på grunn av cyberkriminalitet[1]. Dette tallet blir stadig større, i takt med at hackere blir flinkere og mer avanserte. Et av de siste snikangrepene som virkelig er blitt IT-lederes bane er BIOS-angrep.

Millioner av maskiner har iboende BIOS-sårbarheter, og det betyr at selv hackere med begrensede ferdigheter kan få tilgang til dem. På en konferanse for noen år siden presenterte forskerne Xeno Kovah og Corey Kallenberg en ny type angrep og viste at de, på få timer, kunne hacke seg inn i BIOS til flere systemer[2]. De fleste BIOS har den samme koden. Så når den første koden er knekket, tar det ikke lang tid før forsvaret til mange flere maskiner også brytes ned.

Denne typen angrep er så farlig fordi den er rettet mot mål som hittil ikke har vært beskyttet. Det er et skjult rom mellom operativsystemet og maskinvaren som ingen pleide å bry seg om. Så selv om nettverket ditt virker vanntett og enheten din er beskyttet av verdens beste sikkerhetssystemer, er det fremdeles et lite øyeblikk mellom oppstarting av systemet og iverksetting av forsvaret. Det er i dette lille øyeblikket et fiendtlig BIOS-angrep kan skape kaos.

Siden de fleste cybersikkerhetsprogramvarer er på/ved operativsystemnivå vil ikke skadelige programvare som føres inn i BIOS (før oppstart og før enheten går inn i systemadministrasjonmodus) bli oppdaget av cybersikkerhetsprogramvaren ved endepunktet.

Derfra erstatter hackere din BIOS med sin egendefinerte versjon som kan fjernadministreres, i det uendelige. Det verste er at det kan være nesten umulig å oppdage at inntrengningen og infiseringen er skjedd.

Den beste måten å beskytte enhetene i virksomheten din på er å bruke sikkerhet i flere lag. IT-teamet ditt skal ikke måtte bruke tiden sin til kontinuerlig kontroll og manuelle reparasjoner. HP tilbyr en automatisk respons – som del av et utvalg sikkerhetsløsninger – HP Sure Start.

"Dette er en del av et felles arbeid med HP Labs for å hjelpe virksomheter til å oppnå bedre risikoadministrasjon og beskytte brukere og IT-produktiviteten mot ondsinnede angrep, mislykkede oppdateringer eller andre utilsiktede eller ukjente årsaker"

- sier Vali Ali, Chief Technologist for Security and Privacy i HP PC Business Unit.

Hvorfor automatisk forsvar beskytter enhetene i virksomheten din

HP Sure Start er en selvreparerende beskyttelse på BIOS-nivå. Vi kaller denne tilnærmingen cybermotstand. Systemet fungerer ved å skape en "superhjelper" for BIOS som krypteres direkte på enheten. Så hvis noen prøver å hacke BIOS vil det automatisk starte på nytt og laste inn "superhjelperen", tømme den infiserte filen og informere deg og teamet ditt om angrepet. Maskinen reparerer egentlig seg selv.

Det betyr uavbrutt produktivitet. Det betyr lavere kostnader. Det betyr enheter som fungerer bedre. Fremfor alt er det en enklere måte å arbeide på.

Hvis du lurer på hva som er den enkleste måten å få banebrytende enheter aktivert med HP Sure Start for brukerne dine, skal du vurdere HP Device as a Service. Det er en moderne PC-forbruksmodell som gjør det enklere for kommersielle organisasjoner å utstyre sine medarbeidere med riktig maskinvare og tilbehør, administrere enhetssystemer med flere OS og få ytterligere livssyklus-tjenester. Med HP DaaS får du enkle, men likevel fleksible planer, til én pris per enhet, slik at alt går greit og effektivt.

Endepunkter og tilgangspunkter må overvåkes på alle nivåer. Det er på tide at vi retter oppmerksomheten mot de skjulte delene av enhetene våre. Alle personer, virksomheter og organisasjoner over hele verden kan bli tryggere og mer motstandsdyktige med HPs portefølje av produkttilbud, som blant annet inkluderer HP EliteBook 800-serien, med valgfrie 8. generasjons Intel® Core™-prosessorer. Som del av HP Elite-familien tilbyr denne enheten en forsterket sikkerhetsteknologi, takket være integrerte funksjoner som HP Sure Start.

For å finne ut mer om hvordan du kan beskytte enhetene i virksomheten din, kan du lese vårt siste HP Sure Start White Paper og se alle fordelene HPs sikkerhetsløsninger gir virksomheten din.

Kilder:

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. Ulike generasjoner av HP Sure Start er tilgjengelig på utvalgte konfigurasjoner av HP Elite- og HP Pro-systemer.

4AA7-3219NOE, Mai 2018