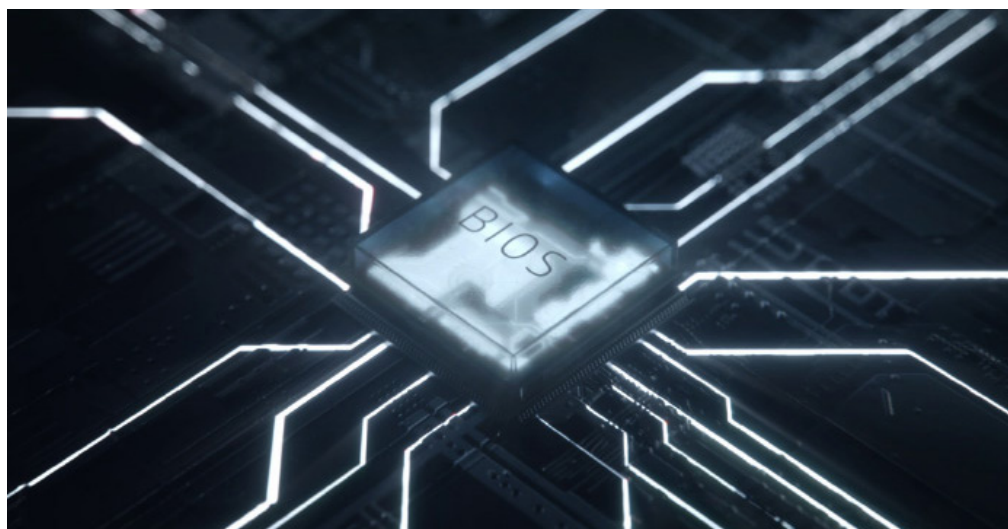




Derfor kan automatisk forsvar redde din virksomheds enheder



Flere oplysninger



Hvordan bekæmper du en trussel, som slipper gennem dit forsvar? Du automatiserer.

338 milliarder pund om året. Det er den aktuelle udgift til cyberkriminalitet over hele verden¹. Det tal bliver større og større, efterhånden som hackerne bliver dygtigere og mere sofistikerede. Et af de nyeste snigangreb, der kan blive et alvorligt problem for it-cheferne, er BIOS-angrebet.

Millioner af maskiner har grundlæggende BIOS-sårbarheder, hvilket betyder, at de kan hackes af nogen med blot moderate hackingfærdigheder. Forskerne Xeno Kovah og Corey Kallenberg præsenterede en ny type angreb på en konference for et par år siden, som viste, at de i løbet af et par timer kunne hacke og inficere BIOS på mange forskellige systemer² via fjernadgang. Fordi de fleste BIOS deler den samme kode, var det blot et spørgsmål om tid, når den første var blevet brudt, før de samme færdigheder kunne ødelægge forsvaret på mange flere maskiner.

Denne type angreb er så farlig, fordi den er rettet mod et sted, der ikke er blevet beskyttet. Der er et skjult område mellem operativsystemet og hardwaren, som tidligere blev ignoreret. Og selvom dit netværk lader til at være vandtæt, og din enhed er beskyttet med verdens bedste sikkerhedssystemer, er der stadig et kort øjeblik fra det tidspunkt, hvor enheden starter, til dit forsvar kommer op at køre. Det er i dette øjeblik, et fjendtligt BIOS-angreb kan skabe kaos.

Da det meste cybersikkerhedssoftware findes på operativsystemniveau, kan malware, der føjes til BIOS (inden opstart og sendes til systemadministrations tilstanden), være umulig at registrere for cybersikkerheds-software ved slutpunktet. Fra dette tidspunkt vil hackerne erstatte din BIOS med deres egen skræddersyede version, som kan administreres via fjernadgang på ubestemt tid. Det værste er, at det kan være næsten umuligt at opdage, at bruddet og infektionen er sket.

Den bedste måde at beskytte din virksomheds enheder på er at bruge flere lag af sikkerhed sikkerhed. Dit it-team bør ikke være optaget af konstant at scanne og løse problemer manuelt. HP tilbyder en automatisk reaktion – som en del af en række sikkerhedsløsninger – [HP Sure Start](#).

"Dette er en del af en samlet indsats fra HP Labs for at hjælpe virksomheder med bedre at administrere risici og beskytte bruger- og it-produktivitet mod ondsindede angreb, en mislykket opdatering eller en anden hændelig eller ukendt årsag."

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

Derfor kan automatisk forsvar redde din virksomheds enheder

[HP Sure Start](#) er en selvreparerende beskyttelse på BIOS-niveau. Vi kalder denne tilgang for cyberfleksibilitet. Systemet fungerer ved at oprette en "gold master" for BIOS, som er direkte krypteret på enheden. Så hvis nogen prøver at hacke BIOS, genstarter det automatisk sig selv og indlæser derefter "gold master", sletter den inficerede fil og orienterer dig og teamet om angrebet. I bund og grund reparerer maskinen sig selv.

Det betyder uforstyrret produktivitet. Det betyder færre omkostninger. Det betyder mere kompatible enheder. Først og fremmest er det en nemmere måde at arbejde på.

Hvis du overvejer, hvordan du nemmest kan få banebrydende enheder med HP Sure Start aktiveret til dine brugere, så skal du overveje [HP Device as a Service](#). Det er en moderne pc-forbrugsmodel, der gør det enklere for virksomheder at udstyre deres medarbejdere med den rigtige hardware og det rigtige tilbehør, administrere multi-OS-enhedsflåder og få yderligere livscyklusservices. HP DaaS tilbyder enkle, men alligevel fleksible planer, til én pris pr. enhed for at holde alt kørende effektivt og uden problemer.

Slutpunkter og adgangspunkter skal overvåges på alle niveauer. Det er på tide at holde op med at undgå de skjulte dele i vores enheder. Enhver person, virksomhed og organisation i hele verden kan blive sikrere og mere fleksibel med HP's portefølje af produkttilbud, herunder [HP EliteBook 800-serien](#), med mulighed for 8. generations Intel® Core™-processorer. Som en del af HP Elite-serien får du banebrydende sikkerhedsteknologi takket være indbyggede sikkerhedsfunktioner som HP Sure Start.

Hvis du vil vide mere om beskyttelse af dine virksomheds enheder, kan du læse vores nyeste [HP Sure Start-whitepaper](#) og opdage fordelene ved [HP's sikkerhedsløsninger](#) til din virksomhed.

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. Forskellige generationer af HP Sure Start fås på udvalgte konfigurationer af HP Elite- og HP Pro-systemer.

© Copyright 2018 HP Development Company, L.P. Oplysninger i dette dokument kan ændres uden varsel.

4AA7-3219DACI, Maj 2018

