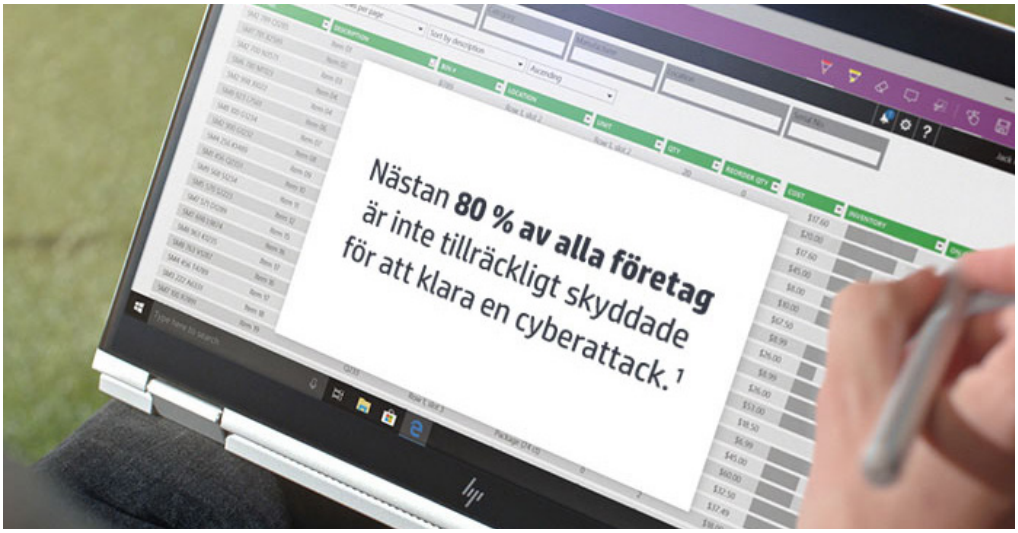
# Hur automatiska skydd kan rädda era företagsenheter

Läs mer




**Hur bekämpas ett hot som gömmer sig bakom ert försvar? Med automatisering.**

600 miljarder USD om året. Så mycket kostade cyberbrottsligheten i världen år 2017[2]. Beloppet ökar i takt med att hackare blir alltmer sofistikerade och kunniga. För inte så länge sedan rapporterades det att 20 % av alla små till mellanstora företag blev tvungna att avbryta sin verksamhet omedelbart, och 12 % förlorade intäkter efter en cyberattack[3]. Attacker mot hårdvara har på senare tid blivit en prioritet för IT-chefer. Dessa sker under en dators startprocess, och kallas för BIOS-attacker.

Miljontals enheter har enkla BIOS sårbarheter, vilket gör att de kan hackas av personer med måttliga hackarkunskaper. Forskarna Xeno Kovah och Corey Kallenberg presenterade en ny typ av attack på en konferens för några år sedan, och avslöjade att de kunde hacka och infektera BIOS i flera olika system på bara några timmar[4]. Eftersom de flesta BIOS delar samma kod är det bara en tidsfråga innan samma metoder som används för att knäcka den första även kan sätta andra enheters säkerhet på spel.

Den här typen av attacker är allvarliga då de angriper oskyddade punkter. Det finns ett dolt utrymme mellan operativsystemet och hårdvaran som man tidigare brukade bortse ifrån. Även om nätverket kan verka vattentätt och enheten är skyddad bakom de bästa virusskyddsprogrammen i världen, utgör det korta ögonblicket under uppstarten innan skyddet aktiveras en säkerhetsrisk som innebär att en fientlig BIOS-attack kan skapa kaos.

Eftersom de flesta antivirusprogramkörs på operativsystemnivå, är malware som förs in i BIOS före uppstart svår att upptäcka. Därifrån får hackare total kontroll över systemet. De kan stjäla alla data, göra dem oläsliga eller sprida ny malware i hela företagets nätverk. Det värsta av allt är att det kan vara näst intill omöjligt att upptäcka att det skett ett intrång och att systemet infekterats.

Det bästa sättet att skydda företaget är med hjälp av säkerhet i flera lager. IT-avdelningens kapacitet borde inte gå åt till att ständigt skanna och åtgärda problem manuellt. Därför erbjuder HP ett automatiskt försvar som ett led i våra säkerhetslösningar – HP Sure Start[5].

”Det här är en del i ett samarbete med HP Labs med syfte att hjälpa företag att hantera risker och skydda användare och IT-avdelningar mot skadliga attacker, misslyckade uppdateringar eller andra hot”,

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

## Varför automatiska skydd kan rädda era företagsenheter

HP Sure Start är ett skydd som går ut på att BIOS självläker. Vi kan kalla metoden cybermotståndskraft. Systemet skapar en gold master-version av BIOS som omedelbart krypteras på enheten. Om BIOS utsätts för hackningsförsök startar det om sig självt automatiskt och läser in gold master-versionen, eliminerar den infekterade filen och meddelar IT-avdelningen om attacken. I stort sett självläker enheten.

Det betyder oavbruten produktivitet. Det betyder lägre kostnader. Det betyder enheter som uppfyller regelverken. Och framförallt underlättar det arbetet.

Om ni undrar hur ni enklast kan få tillgång till avancerade enheter med HP Sure Start bör ni överväga HP Device as a Service (DaaS)[6]. Lösningen är en modern konsumtionsmodell som gör det enklare för företag att förse sina anställda med rätt hårdvara och tillbehör, hantera datorparker med flera olika operativsystem och få tillgång till ytterligare livscykeltjänster. HP DaaS erbjuder enkla men flexibla prisplaner där man betalar per enhet för att se till att allt fungerar smidigt och effektivt.

Klientenheter och accesspunkter måste övervakas på varje nivå. Det är dags att sluta bortse från enheternas dolda delar. Varje person, företag och organisation i världen kan bli säkrare och mer motståndskraftig med HPs produktportfölj, inklusive HP EliteBook x360 med 8:e generationens Intel® Core™ i7-processorer som tillval. Enheten är en del av HP Elite-serien och erbjuder säkerhetsteknik tack vare inbyggda säkerhetsfunktioner som HP Sure Start.

**Upptäck fördelarna med HPs säkerhetslösningar för ert företag.**

---

**Källor:**


1. Statista Survey ID 622857, “Small and medium sized enterprises in the U.S by Statista, October 2016
2. https://www.mcafee.com/enterprise/en-gb/solutions/lp/economics-cybercrime.html
3. Osterman Research, sponsrat av Malwarebytes “Second Annual State of Ransomware Report: US Survey Results” July 2017
4. https://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/
5. Flera generationer av HP Sure Start är tillgängliga för HP Elite- och HP Pro-system med utvalda konfigurationer.
6. Planer och/eller medföljande komponenter kan variera per region eller per auktoriserad HP DaaS Service Partner. Kontakta en lokal HP-representant eller auktoriserad DaaS-partner för specifika detaljer som gäller för aktuell plats. HP-tjänster styrs av HPs gällande användarvillkor för tjänster som tillhandahållits eller angivits till kunden vid inköpstillfället. Kunden kan ha ytterligare lagstadgade rättigheter enligt gällande lokala lagar, och sådana rättigheter påverkas inte på något sätt av HPs användarvillkor eller HPs begränsade garanti som medföljer HP-produkten.




4AA7-3219SVSE, april 2019