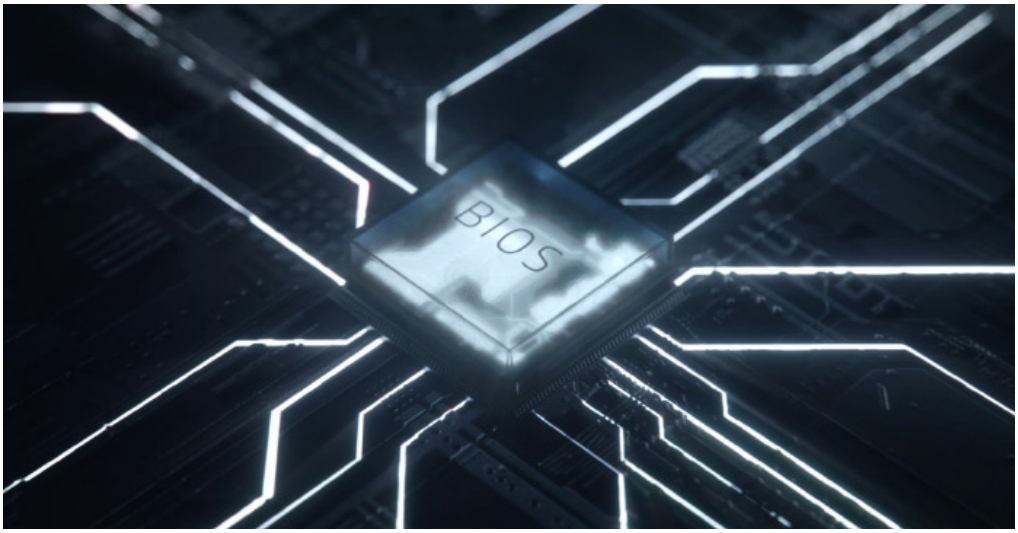
Kuinka automaattinen suojaus pitää yrityksesi laitteet turvassa

Lisätietoja



Kuinka torjua kyberuhka, joka piiloutuu suojauksen alle? Suojaudu automaattisesti.

385 miljardia puntaa vuodessa on kustannus, minkä maailmanlaajuinen kyberrikollisuus aiheuttaa vuodessa[1]. Summa kasvaa, koska hakkereista tulee entistä huomaamattomampia ja taitavempia. BIOS-hyökkäykset ovat olleet yksi IT-päällikköjen viimeisimmistä riesoista.

Miljoonissa laitteissa on perustason BIOS-haavoittuvuuksia, joten ne ovat hakkeroitavissa kohtalaisillakin taidoilla. Tutkijat Xeno Kovah ja Corey Kallenberg esittelivät uuden hyökkäystyypin muutama vuosi sitten järjestetyssä konferenssissa. He paljastivat, kuinka he pystyisivät hakkeroimaan ja tartuttamaan useiden eri järjestelmien BIOSit etänä muutamassa tunnissa[2]. Useimmissa BIOSeissa käytetään samaa koodia, joten ensimmäisten murtamisen jälkeen oli vain ajan kysymys, kun samoilla keinoilla saataisiin murrettua suojaus monista muista laitteista.

Tällaiset hyökkäykset ovat vaarallisia, koska ne kohdistuvat järjestelmän suojaamattomaan osaan. Käyttöjärjestelmän ja laitteiston välissä on piilotettu tila, joka on jätetty aiemmin huomiotta. Vaikka verkko vaikuttaisi tiiviiltä ja vaikka laitteet olisi suojattu maailman parhailla tietoturvajärjestelmillä, laitteen ja suojauksen käynnistymisen välissä on pieni viive. Tuon hetken aikana BIOS-hyökkäys voi aiheuttaa mittavaa tuhoa.

Suurin osa suojauksesta toimii käyttöjärjestelmän tasolla, joten BIOSiin ennen käynnistystä lisätty ja System Management Mode -tilaan siirtyvä haittaohjelma jää tunnistamatta. Tällöin hakkerit voivat korvata BIOSin omalla, rajoituksetta etänä hallittavalla versiollaan. Kaikkein pahinta on, että murron ja tartunnan havaitseminen on lähes mahdotonta.

Monikerroksinen tietoturva on paras tapa yrityksesi laitteiden suojaamiseen. IT-tiimisi aikaa tällöin ei tarvitse käyttää jatkuviin tarkistuksiin ja manuaalisiin korjauksiin. HP tarjoaa tietoturvaratkaisujensa osana automaattisesti toimivan sovelluksen – HP Sure Startin.

”Ratkaisulla HP Labs pyrkii tukemaan yritysten riskinhallintaa ja auttamaan niitä suojaamaan käyttäjiä sekä IT-osaston tuottavuutta tapauksissa, jotka johtuvat hyökkäyksistä, epäonnistuneesta päivityksestä, muusta vahingosta tai tuntemattomasta syystä.”

Vali Ali, tietoturvan ja tietosuojan chief technologist, HP PC -liiketoimintayksikkö.

Kuinka automaattinen suojaus pitää yrityksesi laitteet turvassa

HP Sure Start on itseään korjaava BIOS-tason suojaus. Me kutsumme sen lähestymistapaa kybersietokyvyksi. Järjestelmä luo BIOSista pääversion, joka salataan suoraan laitteelle. BIOSin hakkeroinnin tapahtuessa laite käynnistää itsensä automaattisesti, lataa pääversion, poistaa tartunnan sisältävän tiedoston ja ilmoittaa asiasta sinulle ja tiimillesi. Laite siis käytännössä korjaa itse itsensä.

Tämä merkitsee tuottavuuden säilymistä, pienempiä kustannuksia, useampia yhteensopivia laitteita ja ennenkaikkea helpompaa työskentelyä.

Jos mietit helpointa tapaa HP Sure Startilla varustettujen laitteiden hankkimiseen, harkitse HP:n laite palveluna -mallia. Kyseessä on nykyaikainen tietokoneiden kulutusmalli, joka yksinkertaistaa liikeyritysten laitteiston ja lisävarusteiden hankintaa, erilaisilla käyttöjärjestelmillä varustettujen laitekantojen hallintaa ja ylimääräisten elinkaaripalvelujen tilaamista. HP DaaS tarjoaa laitekohtaisilla hinnoilla varustetut yksinkertaiset mutta joustavat sopimukset, jotka takaavat laitteiston tasaisen ja tehokkaan toiminnan.

Päätelaitteita ja -pisteitä täytyy valvoa joka tasolla. On aika alkaa valvoa laitteidemme piilossa olevia kohtia. Jokainen henkilö, yritys ja organisaatio voi lisätä tietoturvaansa ja sen vastustuskykyä HP:n laitteilla, kuten HP EliteBook 800 -sarjalla, jonka laitteet ovat saatavana varustettuna 8. sukupolven Intel® Core™ -suorittimilla. HP Elite -tuoteperheelle ominaisesti laitteet tarjoavat sisäänrakennettua tietoturvatekniikkaa, kuten HP Sure Startin.

Lue lisää yrityslaitteille tarjoamastamme suojauksesta viimeisimmästä HP Sure Start -selvityksestä ja katso, mitä hyötyä HP:n tietoturvaratkaisuista voi olla yrityksellesi.

Lähteet:

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. Eri sukupolven HP Sure Start -ratkaisut ovat saatavilla valittuihin HP Elite ja HP Pro -järjestelmiin.

© Copyright 2018 HP Development Company, L.P. Tässä esitetyt tiedot voivat muuttua ilman ennakkoilmoitusta.

4AA7-3219FICI, Toukokuu 2018