Esimerkkitapaus

HP:n tulostimet havaitsivat Lontoon lentoasemaan kohdistuneen kyberuhkan

Tietomurron virallinen kokoomaraportti

Ala
Ilmailu

Tehtävä
Kyberturvallisuuskäytäntöjen heikkojen kohtien tunnistaminen ja niiden korjaaminen

Lähestymistapa
Laadittiin kattava tietoturvasuunnitelma yhteistyössä HP:n tietoturva-asiantuntijoiden kanssa

Tietotekniikkaan liittyvät toimet
- IoT-päätelaitteisiin lisättiin suojaustoimintoja
- Otettiin käyttöön sisäiset tietoturvatoiminnot HP:n tulostimissa ja monitoimilaitteissa
- Parannettiin tietoturvallisuuden valvontaa koko verkon tasolla

Yritystoimintaan liittyvät toimet
Parannettiin kyberturvallisuutta niin, että pystytään suojaamaan kriittistä kansainvälistä infrastruktuuria ja ylläpitämään matkustajien turvallisuutta

Katsaus

Lontoon lentoasema* palvelee päivittäin yli 300 000:ta matkustajaa, jotka lentävät yli 94 maahan eri puolille maailmaa. Lentoasemalla työskentelee lähes 50 000 ihmistä 300 yrityksestä, mikä tekee siitä käytännössä tiiviin kaupungin.

Kasvun myötä lentoaseman infrastruktuuri on verkottunut ja automatisoitunut. Sisäiset järjestelmät LVI:stä valaistukseen ja tulostimiin on nykyään yhdistetty lentoaseman verkkoon. Tulostamisesta, skannaamisesta ja kopioinnista vastaa yli 60 HP:n monitoimilaitteen kalusto, joka on sijoitettu ympäri lentoasemaa.

23. huhtikuuta 2018 nimellä ”The Wolf” tunnettu kyberterroristi murtautui lentoaseman verkkoon valaistusjärjestelmän kautta ja pääsi levittämään haittaohjelmaa. Koska hyökkääjä on tunnettu alisuojattujen päätelaitteiden hyödyntämisestä, tietoturva-asiantuntijat alkoivat välittömästi käydä läpi HP Enterprise -tulostimien uhkalokeja hyökkäyksen eristämiseksi ja pysäyttämiseksi. Yllättäen lokeista löytyi viitteitä The Wolfin iskun alkukohdasta. Jälkikäteen Lontoon lentoasema vahvisti päätelaitteidensa tietoturvaa HP:n avustuksella.

Mitä tapahtui

The Wolf paikansi haavoittuvuuden todennäköisesti kalastelemalla tietoja verkossa olevien käyttäjien sähköposteista, minkä jälkeen hän pystyi levittämään haittaohjelman IoT-valaistusjärjestelmään. Hän pystyi jakamaan haittaohjelmaa verkon välityksellä ja luomaan sille piilopaikkoja muihin suojaamattomiin päätelaitteisiin.

Piiloutumalla valvomattomiin IoT-laitteisiin The Wolfin tiimi pystyi verkon valvontajärjestelmien huomaamatta kehittämään useita lähtöpisteitä massiiviselle ja tuhoisalle hyökkäykselle.

Lentoaseman valvontahenkilöstö yritti epätoivoisesti sulkea useita järjestelmiä ja pitää samalla yllä lentokoneiden ja matkustajien kaltaista kriittistä infrastruktuuria.

Hyökkäykseen vastaaminen

The Wolf oli palkattu hyökkäämään lentoaseman verkkoon. Lentoaseman tietoturvahenkilöstö *ajatteli*, että aseman verkko on suojattu hyvin hakkereilta, mutta he eivät olleet huomioineet IoT-laitteisiin piiloutumisen muodostamaa uhkaa.

Onneksi lentoaseman HP Enterprise -tulostimien HP Connection Inspector -toiminto pystyi pysäyttämään haittaohjelman siinä vaiheessa, kun se yritti ottaa yhteyttä hakkereiden komento- ja ohjauspalvelimiin.

Kyseiset toimet tallentuivat tulostimien järjestelmälokeihin. Kun IT-henkilöstö tajusi jonkin olevan pielessä, he etsivät hyökkäykseen viittaavia tietoja järjestelmälokeista. Aika on kortilla, kun haittaohjelma leviää verkossa. Jos tietoturvahenkilöstö olisi yhdistänyt tulostimien järjestelmälokit tietoturva- ja tapahtumavalvontajärjestelmään (SIEM), he olisivat saaneet tiedon hyökkäyksestä välittömästi.

Entistä vahvempaa tietoturvaa

Murron jälkeen IT-henkilöstö tarkisti käytössä olevat tietoturvakäytännöt hallinnoidun tulostuspalvelun tarjoajan ja HP:n tietoturvaneuvojien kanssa.

HP Enterprise -tulostimien ansiosta Lontoon lentoasema oli jo valmiiksi oikealla tiellä. Ainoastaan HP Enterprise -tulostimet ja -monitoimilaitteet tarjoavat käytönaikaisen hyökkäysten havaitsemisen ja HP Connection Inspector -toiminnon, joka havaitsee ja pysäyttää haittaohjelmien leviämisen toiminnan aikana ja pakottaa uudelleenkäynnistyksen. Käynnistyksen yhteydessä HP Sure Start tarkistaa BIOSin ja voi korjata muokattua koodia, minkä lisäksi laiteohjelmisto tarkistetaan.

Hallinnoidun tulostuspalvelun tarjoaja otti käyttöön HP JetAdvantage Security Managerin, joka tarkistaa tulostimen tietoturva-asetukset automaattisesti jokaisen uudelleenkäynnistyksen yhteydessä ja palauttaa mahdolliset luvatta muutetut asetukset.

Lisäksi lentoaseman IT-henkilöstö yhdisti tulostimien järjestelmälokit SIEM-työkaluun. Muiden valmistajien tulostimista poiketen HP:n laitteet voivat lähettää uhkakohtaisia lokeja useille SIEM-työkaluille, joten IT-henkilöstö saa reaaliaikaiset hälytykset kaikista tietoturvaongelmista. Tämä tekee HP:n tulostimista korvaamattoman arvokkaita verkon valvontalaitteita.

Lopuksi

HP Enterprise -tulostimien ja The Wolfin jättämien jälkien avulla tietoturvatiimi sai eristettyä uhkan ennen kuin se pääsi pysäyttämään lentoaseman toiminnan. Lisäksi se pystyi välttämään negatiivisen julkisuuden, sakkomaksut ja brändin vahingoittumisen.

Vahvojen tietoturvakäytäntöjen ja HP-tulostimien sisäisten tietoturvaominaisuuksien ansiosta lentoaseman tietoturva on eheä koko verkon laajuudelta.

**Lontoon lentoasema on kuvitteellinen organisaatio, joka joutuu kyberhyökkäyksen kohteeksi HP Studion elokuvassa "THE WOLF: TRUE ALPHA".*

Lisätietoja HP:n ratkaisuista:
Tulostuksen tietoturva: hp.com/go/reinventsecurity
Tietokoneiden tietoturva: hp.com/go/ComputerSecurity
Katso "The Wolf" -elokuvat osoitteessa
hp.com/thewolf

Tilaa päivitysilmoitukset
hp.com/go/getupdated

Jaa kollegoiden kanssa

4AA7-3560FIE, elokuu 2018