Esimerkkitapaus

Penetraatiotestaus osoittaa, että ”The Wolfin” Torvik Industriesiin kohdistama tietomurto olisi voitu estää HP:n tulostimilla

Tietomurron virallinen kokoomaraportti

Ala
Kuljetusala

Tehtävä
Verkon haavoittuvuusalueiden analysointi ja selvittäminen

Lähestymistapa
Penetraatiotesti, jolla paikannetaan hyökkäykseen johtaneet haavoittuvuudet

Tulokset ja suositukset
- Käyttäjien kouluttaminen epäilyttäviltä sähköposteilta ja liitteiltä suojautumiseen
- Uhkien tunnistuksella varustettujen HP-tulostimien ja -monitoimilaitteiden käyttöönotto
- Kaikkien päätelaitteiden tietoturvatoimintojen konfigurointi, johon sisältyy siirrettyjen tai väliaikaisissa sijainneissa olevien laitteiden infrastruktuuri

Yritystoimintaan liittyvät toimet
Vahvempien tietoturvatoimien käyttöönotto, millä estetään käyttökatkot ja parannetaan brändin luotettavuutta. Valvontakäytäntöjen kehittäminen väliaikaisissa sijainneissa sijaitseville verkon päätelaitteille.

Katsaus

Torvik Industries* kuljettaa 8 miljoonaa konttia joka vuosi. 22 000 valmistajalle ja jälleenmyyjälle Torvik on maailmanlaajuisesti elintärkeä linkki tuotteiden ja ihmisten välillä. Yhtiö omistaa konttisatamia, laivoja, varastoja ja kaiken verkoston ylläpitoa tukevan tekniikan.

Yhtiön tekninen infrastruktuuri on jäänyt jälkeen muusta kasvusta. IT-turvallisuushenkilöstö on konfiguroinut yhtiön palvelimet, mutta joidenkin satelliittitoimistojen tai väliaikaisten sijaintien tulostimia ja monitoimilaitteita ei ole suojattu.

23. huhtikuuta 2018 nimellä ”The Wolf” tunnettu kyberterroristi murtautui suojaamattomalle tulostimelle ja pystyi näin sabotoimaan Torvik Industriesin toimintoja tietokoneista nostureihin ja rahtilaivoihin asti. Yhtiön tietoturvaneuvonantaja analysoi tapahtumaa penetraatiotestauksen avulla ja antoi suosituksia tietoturvan parantamiseen ja henkilöstön kouluttamiseen.

Mitä tapahtui

Torvik Industriesin johtajisto oli tottunut olemaan itse johdossa vaativissa tilanteissa, joten he eivät odottaneet, että hakkeri pääsisi murtautumaan heidän verkkoonsa niin kattavasti, että tälle tarjoutuisi mahdollisuus sammuttaa yhtiön siltanostureita tai muuttaa avomerellä seilaavien laivojen reittejä.

Tätä varten The Wolfin täytyi ainoastaan murtautua rakennustyömaalla olevaan suurkokotulostimeen. Murtautumisen jälkeen hän pystyi liikkumaan yhtiön verkossa lateraalisesti ja siirtymään suuriin kohteisiin eli yhtiön toimintoihin. Hetkessä tämä johtava kuljetusalan yritys sai osakseen massiivisia toimintahäiriöitä, kansainvälistä huomiota ja tuhansia vihaisia asiakkaita.

Syy tapahtuneeseen

Yhtiön IT-turvallisuushenkilöstö luuli, että kaikki oleellinen on suojattu. Tekniikka- ja logistiikkatiimit valvoivat maailmanlaajuisia toimintoja jatkuvasti tietoturvaongelmien varalta. Yhtiöllä oli jopa käytössään tietoturvamenettelyitä tulostimien kaltaisille päätelaitteille. He kuitenkin unohtivat jotakin: rakennustyömaan konttiin väliaikaisesti sijoitetun suurkokotulostimen tietoturvakonfiguroinnin.

Hakkerin ei edes tarvinnut päästä suoraan käsiksi tulostimeen. Hänen tarvitsi ainoastaan lähettää PDF-liite suurkokotulostimen käytöstä vastaavalle Torvikin työntekijälle. PDF-tiedosto sisälsi piilotetun PostScript-tiedoston, joka alkoi toimia siinä vaiheessa, kun PDF lähetettiin tulostimeen. Kun työntekijä lähetti tulostustyön, haittaohjelma asentui tulostimeen ja levisi koko verkkoon. Hakkeri pääsi ohittamaan yhtiön haittaohjelmaohjelmistot piilottamalla haittaohjelman viattomalta näyttävään sähköpostiliitteeseen.

Murto oli mahdollinen, koska suurkokotulostimessa ei ollut sisäisiä tietoturvaominaisuuksia, kuten uhkien havaitsemistoimintoa. Lisäksi yhtiö ei pystynyt valvomaan ja hallinnoimaan kaikkia laitteiston tulostimia ja monitoimilaitteita, kuten sellaisia, jotka on asennettu väliaikaisesti satelliittitoimistoihin.

Murron jälkien korjaaminen

Torvik Industries palkkasi huipputason penetraatiotestausyrityksen analysoimaan organisaation kyberturvallisuutta kattavasti.

Penetraatiotestaustiimi suositteli sisäisillä tietoturvaominaisuuksilla varustettujen HP-tulostimien asentamista. Näihin lukeutuvat HP DesignJet -sarjan laitteet, joissa on suojattu käynnistys ja laiteohjelmiston tarkistus. Toimintojen avulla tulostin pystyy havaitsemaan haitallista koodia, sammumaan automaattisesti ja ilmoittamaan IT-osastolle aidon HP-laiteohjelmiston asennustarpeesta.

Asiantuntijat suosittelivat myös käyttämään HP JetAdvantage Security Manageria, koko laitteiston tietoturvahallintaan käytettävää ohjelmistoa, jonka avulla verkon tietoturvakäytännöt voi lisätä automaattisesti kaikille uusille verkkoon liitettäville laitteille. HP Security Managerilla voi myös luoda tietoturva-asetusten mukaisia raportteja, joihin sisällytetään kaikki
HP-tulostimet ja -monitoimilaitteet – myös ne, jotka ovat etäisissä tai väliaikaisissa toimipisteissä. Tämä helpottaa koko laitteiston tietoturvakonfiguroinnin yhtenäisyyden tarkistamista.

Lisäksi tietoturvaneuvonantaja suositteli ottamaan käyttöön koulutusohjelman, jonka avulla työntekijät voivat tunnistaa epäilyttävät sähköpostit ja välttää epäilyttävien liitteiden avaamisen.

Lopuksi

Torvik Industries ei ole vieläkään täysin palautunut toimintoihinsa kohdistuneesta kyberhyökkäyksestä sekä johtajansa epätavanomaisten näkemysten ja rikollisen toiminnan synnyttämästä negatiivisesta julkisuudesta. Organisaation johto pyrkii löytämään uuden suunnan, mutta lisäksi kyberturvallisuuden uusi ohjeistus on selvä: HP:n tulostimien ja monitoimilaitteiden sekä ratkaisujen puoleen kääntyminen auttaa estämään seuraavan Wolfin hyökkäyksen.

**Torvik Industries on kuvitteellinen yhtiö, joka joutuu kyberhyökkäyksen kohteeksi HP Studion elokuvassa "THE WOLF: TRUE ALPHA".*

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

Tilaa päivitysilmoitukset
hp.com/go/getupdated

Jaa kollegoiden kanssa

4AA7-3562FIE, elokuu 2018