Check Point testasi, miten helposti ultraäänilaite hakkeroidaan

*Verkkoyhteydellä varustetut laitteet helpottavat elämää niin kotona kuin työpaikollakin. Tietoturvayhtiö Check Point varoittaa kuitenkin IoT-laitteisiin liittyvistä tietoturvariskeistä. Havainnollistaakseen sanomaansa tietoturvatutkijat hakkeroivat ultraäänilaitteen.*

**Espoo – 8. maaliskuuta 2019 –** Check point nimesi [tuoreessa tietoturvaraportissaan](https://pages.checkpoint.com/cyber-security-report-2019-cloud-mobile-iot.html?utm_source=blog&utm_medium=cp-website&utm_campaign=cm_wr_19q1_ww_security_report_vol_3_cloud_mobile_iot_ww9) IoT-laitteet, pilvipalvelut ja mobiililaitteet tietoturvan heikoimmiksi linkeiksi. Nettiyhteyttä hyödyntävät laitteet pääsivät listalle vähintään kolmesta syystä.

IoT-laitteet on usein rakennettu vanhentuneiden käyttöjärjestelmien varaan, ja tietoturvaominaisuudet saattavat puuttua niistä täysin. Toiseksi laitteille kerääntyy yhä useammin suuria määriä dataa, joka kiinnostaa kyberrikollisia. Kolmanneksi niiden kautta pääsee usein helposti sisään organisaation tietoverkkoon ja sen vielä kiinnostavampien data-aarteiden äärelle. Jo pelkkä laitteen kaappaaminen ja sen toiminnan pysäyttäminen voi aiheuttaa suurta tuhoa esimerkiksi sairaalassa.

Kyberhyökkäyksistä terveydenhuollossa on raportoitu viime vuosina tasaiseen tahtiin. Esimerkiksi helmikuussa hakkerit jäädyttivät [australialaisen sydänklinikan](https://www.theguardian.com/technology/2019/feb/21/hackers-scramble-patient-files-in-melbourne-heart-clinic-cyber-attack) potilastiedot. Viime vuonna tuli [Singaporessa](https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html) ilmi iso tietomurto, jossa muun muassa pääministerin terveystiedot joutuivat hakkereiden haltuun. [USA:n](https://www.healthcareitnews.com/news/14-million-patient-records-breached-unitypoint-health-phishing-attack) viime vuoden laajin terveydenhuollon tietoturvavälikohtaus vaaransi 1,4 miljoonan potilaan tiedot. Suomessa sairaalan tietoturva on ollut uhattuna viime vuosina ainakin [Lahdessa](https://yle.fi/uutiset/3-10066289) ja [Pohjois-Karjalan sairaanhoitopiirissä](https://yle.fi/uutiset/3-8343829). Läheltä piti -tilanteista ei yleensä tiedoteta.

Vanha laite voi olla helppo murrettava

Terveydenhuollon laitteiden valmistajat ovat alkaneet varustaa laitteitaan tietoturvaominaisuuksilla. Esimerkiksi uudessa ultraäänilaitteissa voi olla palomuuri, haittaohjelmasuojaus ja potilastietojen salaus. Vanhemmat laitteet muodostavat kuitenkin isomman riskin. Niinpä Check Pointin tutkijat päättivät katsoa, mitä hieman ikääntyneempi IoT-ultraäänilaite pitää sisällään.

”Laitteen käyttöjärjestelmäksi paljastui Windows 2000, jolle ei enää julkaista ohjelmistopäivityksiä. Käyttöjärjestelmässä on useita hyvin tunnettuja haavoittuvuuksia, joita hyödyntämällä pääsimme helposti käsiksi laitteen koko tietokantaan ja sen sisältämiin potilaiden ultraäänikuviin”, Check Pointin tutkijat kertovat yhtiön blogissa.

Potilastietojen segmentointi pienentää riskiä

Check Point muistuttaa, että isossa terveydenhuollon organisaatiossa voi olla satoja laitteita, joiden raudassa tai ohjelmistossa voi olla haavoittuvuuksia. Niiden kaikkien paikkaaminen ja pitäminen päivitettyinä jatkuvasti on käytännössä mahdotonta. Kun henkilöstöllä lisäksi on tarve käyttää potilastietoja jatkuvasti, päivityksille sopivia hetkiä on harvoin. Siksi tarvitaan nykyaikainen, monitasoinen uhkientorjuntaratkaisu, joka pysäyttää väistämättömät hyökkäykset alkuunsa. Lisäksi Check Point suosittelee laitoksen sisäisen verkon segmentointia.

”Potilastietojen erottaminen muusta IT-verkosta helpottaa verkon liikenteen seuraamista, jolloin epätavallinen toiminta paljastuu nopeammin. Lisäksi segmentointi estää mahdollisen kiristyshaittaohjelmasta johtuvan tietojen salaamisen leviämisen laitteelta toiselle. Segmentointia tulisi harjoittaa myös siinä mielessä, että kullakin henkilöllä olisi pääsy vain työnsä kannalta tarpeellisille laitteille ja tietoihin”, Check Point neuvoo.

**Lue Check Pointin blogi ja katso siihen liittyvä video täältä:** **<https://blog.checkpoint.com/2019/03/07/ultrahack-the-security-risks-of-medical-iot/>**

**Lisätiedot ja haastattelupyynnöt:**

OSG Viestintä, Maija Rauha, [maija.rauha@osg.fi](mailto:maija.rauha@osg.fi), p. 0400 630 065

Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, [ramira@checkpoint.com](mailto:ramira@checkpoint.com)

**Seuraa Check Pointia:**

Twitter: <http://www.twitter.com/checkpointsw>

Facebook: <https://www.facebook.com/checkpointsoftware>

Blog: <http://blog.checkpoint.com>

YouTube: <http://www.youtube.com/user/CPGlobal>

LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

**Check Point Software Technologies Ltd.**

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on johtava yritysten ja valtionhallinnon kyberturvallisuusratkaisujen tarjoaja globaalisti. Sen ratkaisut suojaavat 5. sukupolven kyberhyökkäyksiltä alan johtavalla haittaohjelmien, kiristysohjelmien ja muiden kohdistettujen hyökkäysten kiinnijäämisprosentilla. Check Pointin monitasoinen tietoturva-arkkitehtuuri käsittää uuden 5. sukupolven (Gen V) edistyneen uhkientorjunnan, joka suojaa yrityksen kaikkia verkko-, pilvi- ja mobiilitoimintoja kaikilta tunnetuilta hyökkäyksiltä, ja sitä hallitaan alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän kautta. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.