Check Pointin tietoturvaennuste 2017: Pilvestä tulossa turvaton

*Check Point ennustaa, että kiristyshaittaohjelmista tulee yhtä iso tietoturvan uhka kuin palvelunestohyökkäykset ovat nyt, ja hyökkäysten kohteeksi joutuvat myös pilvipalveluiden käyttäjät.*

**Espoo, 27. lokakuuta 2016 –** Tietoturvayhtiö Check Point Software Technologiesin tietoturvaennuste vuodeksi 2016 osui valitettavan hyvin kohdalleen.

Tunnistamattomiksi muunnellut ja tarkasti räätälöidyt haittaohjelmat yleistyivät - Check Pointin laskujen mukaan yritysverkkoihin ladattiin 971 uutta haittaohjelmatyyppiä tunnissa.

Mobiililaitteiden tietoturvariskit kasvoivat ja nousivat otsikoihin. [Quadrooter](http://blog.checkpoint.com/2016/08/07/quadrooter/) oli havaituista haavoittuvuuksista vain yksi.

Kriittinen infrastruktuuri joutui hyökkäyksen kohteeksi esimerkiksi Ukrainassa, jossa [voimalaitokseen](https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01) iskeneelle haittaohjelmalle annettiin nimeksi Black Energy. Varsovassa pommitettiin [lentokentän tietojärjestelmää](http://uk.reuters.com/article/us-poland-lot-cybercrime-idUKKBN0P21DC20150622) palvelunestohyökkäyksellä ja Yhdysvalloissa hyökättiin [Bowmanin padon SCADA-järjestelmään](https://securityledger.com/2016/03/hacker-charged-in-breach-of-new-york-dam/).

Kyberrikolliset käyttivät hyväkseen myös IoT:tä eli verkkoyhteyttä hyödyntävän kodin elektroniikan ja pienlaitteiden yleistymistä. Miljoonat turvakamerat ja muut laitteet valjastettiin erittäin laajoihin palvelunestohyökkäyksiin tänä syksynä.

Olisi parempi, jos ennusteet eivät toteutuisi

– Tietoturvan ammattilaisina me Check Pointilla tietenkin näkisimme mieluummin, että ennustaisimme väärin. Olisi paljon parempi, jos tietoverkot ja laitteet säilyisivät puhtaina eikä lamauttavia hyökkäyksiä jouduttaisi kokemaan. Julkistamme silti tänäkin vuonna ennusteet, jotta varautuminen riskeihin helpottuisi edes hieman. Tavoitteena tulisi olla, että pysymme aina askeleen edellä rikollisia, kommentoi Check Point Software Technologiesin Suomen maajohtaja **Petri Sonkeri.**

Check Pointin tietoturvatutkijoiden ennusteet vuodeksi 2017 ovat seuraavat:

**1. Hyökkäykset mobiililaitteita kohtaan yleistyvät edelleen**

Älypuhelimien ja tablet-laitteiden kautta pyritään ensi vuonna entistä useammin pääsemään käsiksi yritysverkkojen sisältämään tietoon. Juuri äskettäin löydettiin iPhone-puhelinten Apple iOS -käyttöjärjestelmästä [kolme uutta haavoittuvuutta](http://www.bbc.com/news/technology-37185544), joiden kautta yritettiin murtaa ihmisoikeusaktivistin puhelin. Tapaus todistaa kyberrikollisten etsivän jatkuvasti uusia aseita ja alleviivaa tarvetta ottaa riskit vakavasti myös yrityksissä.

**2. Teollisuuden ja tuotannon ohjausjärjestelmät ovat riskialttiita**

Teollisia prosesseja valvovat tuotannonohjausjärjestelmät (SCADA) ovat usein haavoittuvia, koska niihin ei ole tarjolla tietoturvaa parantavia päivityksiä tai päivitykset on jätetty tekemättä. Monet järjestelmät ovat yhteydessä internetiin. Tuore [raportti](https://www.us-council.com/news/us-industrial-systems-the-most-exposed.php) kertoi, että yli 188 000 tuotannonohjausjärjestelmää 170 maassa oli ovet avoinna verkossa. Myös tuotantolaitosten tulee jatkossa kiinnittää enemmän huomiota tietoturvan uhkien torjuntaan.

**3. Yhteiskunnan peruspalvelut vaarantuvat**

Kriittisen infrastruktuurin tietoturvariskien toteutumista ei valitettavasti voi tänäkään vuonna jättää pois ennusteesta. Melkein kaikki yhteiskunnan peruspalvelut, kuten voimalaitokset, sähkö- ja televiestintäverkot on rakennettu aikana, jolloin tietoturvariskejä ei tunnettu eikä niiltä ollut tarvetta suojautua. Riskitilanne on maailmanlaajuinen. Maailman ensimmäinen tahallinen, verkon kautta aiheutettu sähkökatkos on jo koettu. Peruspalveluista huolehtivien laitosten on syytä varautua hyökkäyksiin, joiden tekijät voivat olla niin rikollisia, terroristeja kuin valtiollisiakin toimijoita.

**4. Kiristyksen torjunta edellyttää uusia lähestymistapoja**

Ennustamme, että yrityksissä kiristyshaittaohjelmista tulee yhtä yleisiä ja pelättyjä kuin palvelunestohyökkäyksistä. Aivan kuten palvelunestohyökkäykset, myös kiristyshaittaohjelman tartunta voi pysäyttää yrityksen toiminnan. Kiristyksen torjuminen edellyttää monikerroksista tietoturvastrategiaa, jossa on mukana myös hiekkalaatikointi ja epäilyttävän aineksen poistaminen. On myös syytä harkita uusia keinoja hyökkäysten suitsimiseksi: yhteistyö yritysten kesken ja viranomaisten kanssa on tässä tärkeää. Lunnaiden maksamista ei koskaan suositella, mutta joskus se on ainoa keino, kun toimintaa halutaan jatkaa. Yhä useammat yritykset varautuvat tähän taloudellisesti.

Ennustamme myös, että toimijan hiljentämiseen pyrkivät ja vaikuttamistarkoituksessa tehdyt hyökkäykset yleistyvät. Tästä on saatu merkkejä Yhdysvaltain presidentinvaalikampanjassa.

**5. Pilvipalveluiden käytön riskit kasvavat**

Kun yritykset varastoivat yhä enemmän tietoa pilvipalveluihin, kyberrikollisten isku palveluntarjoajan järjestelmään vaikeuttaa useiden yritysten toimintaa kerralla. Juuri näin kävi äskettäisessä voimakkaassa ja tehokkaassa palvelunestohyökkäyksessä, jossa oli [kohteena DynDNS](https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/). Tämän tyyppistä hyökkäystä voi käyttää esimerkiksi kilpailijan tai tietyn organisaation häiritsemiseen. Kun moni muukin kärsii samasta iskusta, kohteen ja tekijän selvittäminen vaikeutuu.

Ennustamme myös, että kiristyshaittaohjelmia tullaan jatkossa kohdistamaan myös pilvipalveluita hoitaviin konesaleihin ja pilvipalveluiden käyttäjiin.

--

**Check Pointin kansainvälisten asiantuntijoiden haastattelupyynnöt:**

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

**Haastattelupyynnöt myös:**

Check Point Software Technologies Finland, maajohtaja Petri Sonkeri, [petris.@checkpoint.com](mailto:petris.@checkpoint.com), p. 040 5047843

Seuraa Check Pointia:

Check Pointin blogi: <http://blog.checkpoint.com/>

Twitter: [www.twitter.com/checkpointsw](http://www.twitter.com/checkpointsw)

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

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

**Check Point Software Technologies Ltd.**  
Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on maailman suurin yksinomaan kyberturvallisuustuotteisiin keskittynyt yhtiö. Se on alan edelläkävijä ratkaisuillaan, joiden kyky havaita haittaohjelmat ja muut tunkeutujat sekä suojata asiakkaat kyberhyökkäyksiltä on ainutlaatuisen tehokas. Check Pointin täydellisen kattava tietoturva-arkkitehtuuri suojaa niin yritysverkot kuin mobiililaitteetkin, ja myös sen hallintajärjestelmä on kattava sekä intuitiivinen. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta. At Check Point, we secure the future.