Check Point tutki: Kyberrikolliset pommittavat suomalaisyrityksiä, mutta kaikki eivät tunnista syöttejä eivätkä tiedä, minne osui

*Suomea pidetään usein tietoturvan lintukotona. Check Pointin teettämä tietoturvakysely paljastaa, ettei se ole koko totuus. Valtaosaa (71 %) yrityksistä on vuoden aikana pommitettu vähintään haitallisen linkin sisältävillä sähköpostiviesteillä. On kuitenkin syytä olettaa, etteivät kaikki tunnista niitä hyökkäyksiksi. Noin viidesosa yrityksistä ei tiedä, mitä kautta haittaohjelma pääsi heidän verkkoonsa.*

**Espoossa 29. kesäkuuta 2017** – Suomalaisyrityksissä yleisimmin tavattu tietoturvaloukkaus on haitallisen linkin tai liitteen sisältävä sähköpostiviesti. Niitä on havaittu 71 prosentissa yrityksistä. Yleistä (46 %) on myös kohdistettu kalastelu, jossa haittasisältöä sisältävä syöttiviesti näyttää tulevan tutulta lähettäjältä. Tätä oli liikkeellä etenkin isommissa, yli 100 henkilön yrityksissä (59 %).

Yleisiä ovat myös troijalaiset (32 %) ja madot (25 %). Tälläkin viikolla paljon julkisuutta saaneet kiristyshaittaohjelmat ovat viidenneksi yleisin hyökkäystyyppi. Niitä on havaittu joka viidennessä (21 %) yrityksessä; isoissa yrityksissä enemmän (27 %) kuin pienissä (14 %).

Suomalaisvastaajista 17 prosenttia kertoi, ettei yrityksessä ole tavattu mitään tietoturvan uhkia 12 viime kuukauden aikana. Pienistä yrityksistä niin vastasi joka neljäs (25 %) ja isoista yrityksistä kahdeksan prosenttia.

– Pidän mahdollisena, ettei etenkään pienissä yrityksissä raportoida jokaista tietoturvaongelmaa. Esimerkiksi haitallisia linkkejä sisältävä sähköposteja on voitu pitää harmittomina. Kiristyshaittaohjelmat leviävät kuitenkin tyypillisesti juuri tällaisten linkkien kautta, kommentoi Check Point Software Technologiesin Suomen maajohtaja **Robert Lindqvist**.

**Perustason tietoturva on käytössä, mutta se ei pysäytä kalastelua**

Lähes kaikissa yrityksissä on kyselyn tulosten mukaan käytössä palomuuri (98 %), virustorjuntaohjelmisto (97 %) ja roskapostin suodatus (97 %). Edistyneempään tietoturvaan kuuluva ennakoiva uhkientorjunta on kuitenkin käytössä vain 41 prosentissa yrityksistä ja neljännen sukupolven palomuuri 39 prosentissa yrityksistä.

– On myönteistä, että monella on perustason tietoturva kunnossa. Melkein 60 prosenttia yritysverkoista on kuitenkin yhä alttiina uusille, sofistikoiduille hyökkäystavoille, kuten kohdistetulle kalastelulle. Tämä on yrityksille riski.

– Riskin hallitsemiseen tarvitaan tehokas ennakoiva uhkientorjuntaratkaisu, joka pystyy käymään nopeasti läpi suuria määriä aineistoa ja pysäyttämään haitalliset elementit ilman, että yrityksen toiminta häiriintyy. Check Pointin ennakoiva uhkientorjunta yhdistää useita eri lähestymistapoja, jotta kaikki uudet, vanhat ja muunnellut hyökkäykset havaitaan ennen kuin ne ehtivät aiheuttaa tuhoa, Lindqvist sanoo.

**Aina löytyy joku, joka klikkaa vahingossa haitallista linkkiä**

Ylivoimaisesti yleisin tie suomalaisyrityksen tietoverkkoon kulkee juuri sähköpostilinkin kautta. Kun tietoturvavastaavilta kysyttiin, miten hyökkääjä pääsi yrityksen tietoverkkoon, yli puolet (55 %) valitsi vaihtoehdon ”Selaimen kautta sähköpostilinkkiä klikattaessa”. Esimerkiksi ohjelmistojen haavoittuvuudet tai tartunnan sisältäneet muistitikut mainitsi vain viisi prosenttia vastaajista. Kysymys kysyttiin niiltä, jotka kertoivat, että heidän yritysverkossaan oli vuoden sisällä tavattu tietoturvan loukkauksia.

– Tarvitaan vain yksi huolimaton klikkaus, ja organisaation tärkeät järjestelmät vaarantuvat. Aina löytyy joku, joka klikkaa vahingossa haitallista linkkiä. Tietoturva on vasta silloin hyvin hoidettu, kun se kestää myös erehdyksiä, kommentoi Lindqvist.

Vastaajista 19 prosenttia ei osannut sanoa, mistä hyökkääjä pääsi yritysverkkoon. Isoissa yrityksissä luku oli 17 prosenttia, pienissä 20. Ruotsissa tehdyssä vastaavassa kyselyssä luku oli vain 8 prosenttia.

– Tämä vahvistaa tulkintaa, että kaikki ei ole niin hyvin kuin päältä näyttää. On tärkeää tietää, mistä aita on rikki, jotta sen voi korjata. Läpinäkyvyys ja helppo tulkittavuus ovat hyvän tietoturvaratkaisun ominaisuuksia. Yrityksen tarpeisiin räätälöity, keskitetysti hallittava tietoturva on siksi parempi ratkaisu kuin yksittäiset ohjelmistot, Lindqvist arvioi.

Check Pointin uusi tietoturva-arkkitehtuuri Infinity kattaa sekä verkot, pilven että mobiilin, hyödyntää globaalia reaaliaikaista tietoa ja sisältää Check Pointin ennakoivan uhkientorjunnan. Se on yhtenäinen, konsolidoitu tietoturvajärjestelmä, jota voi hallita yhden ikkunan kautta. Käyttäjä näkee koko tilanteen yhdellä silmäyksellä.

Tutkimusyhtiö NSS on juuri testannut Infinityn neljännen sukupolven palomuurin ja myöntänyt sille ”Suosittelemme”-leiman. NSS kiitti [raportissaan](http://pages.checkpoint.com/nss-ngfw-test-2017.html) erityisesti palomuurin tehokkuutta.

**Mobiilitietoturva on yhä iso haaste**

Valtaosassa (93 %) kyselyyn osallistuneista yrityksistä henkilöstö saa käyttää yrityksen sähköpostia puhelimillaan. Mobiililaitteiden tietoturvaan liittyvät riskit on yrityksissä tiedostettu, mutta niiden torjunta on tuloksista päätellen jäänyt puolitiehen.

Vain alle joka toisessa yrityspuhelimessa (46 %) on mobiilitietoturvaratkaisu. 67 % suomalaisyrityksistä aikoo kuitenkin parantaa mobiilia tietoturvaansa lähitulevaisuudessa, 12–18 kuukauden aikana. Mobiilihaittaohjelma oli jo saatu kiinni 17 prosentissa yrityksistä. Check Pointin Dimensional Researchilla teettämässä [globaalissa mobiilitietoturvakyselyssä](http://blog.checkpoint.com/2017/04/12/survey-enterprise-security-pros-doubtful-can-prevent-mobile-breaches/) vastaava prosentti oli 20.

– Mobiilitietoturvaan panostavat yritykset ovat oikeilla jäljillä. Kyberrikolliset pyrkivät mobiililaitteisiin useasta ovesta: tartunnan saaneiden sovellusten avulla, verkon kautta, hyödyntämällä laitteiden haavoittuvuuksia sekä kalastelemalla tekstiviestien avulla. Hyvä tietoturvaratkaisu tukkii kaikki nämä väylät ja luo laitteelle turvallisen työympäristön, Lindqvist sanoo.

**Valtaosa yrityksistä aikoo panostaa tietoturvan kehittämiseen**

Valtaosa yrityksistä aikookin parantaa tietoturvaansa seuraavien puolentoista vuoden aikana. Isoista yrityksistä 88 % ja pienistä 65 % aikoo kiinnittää huomiota riskienhallintaan ja säännöstenmukaisuuteen, käytännössä uuden eurooppalaisen tietosuojalainsäädännön vaatimusten täyttämiseen (yhteensä 78 % yrityksistä). Isot yritykset ovat pieniä innokkaampia kehittämään myös tietovuodoilta (76 %) ja kiristyshaittaohjelmilta (74 %) suojautumista, IoT:n tietoturvaa (66 %) ja omien virtuaalisten ympäristöjen tietoturvaa (77 %). Pienemmät yritykset aikovat keskittyä perinteiseen tietoturvaan ja pilvipalvelujen tietoturvaan, jotka olivat alle 100 hengen yritysten suosituimmat kehityskohteet (78 % ja 79 % yrityksistä)

Vain kaksi prosenttia alle 100 hengen yrityksistä ei aio parantaa tietoturvaansa millään kyselyssä mainituista tavoista. Isommista yrityksistä kaikki aikovat panostaa tietoturvaansa tavalla tai toisella.

– Check Point on tunnetuin palomuureistaan, mutta tosiasiassa tietoturvatuotteiden ja ohjelmistojen valikoimamme on erittäin laaja. Yritys voi valita tarvitsemansa osat, jotka Infinity-arkkitehtuuri yhdistää helppokäyttöiseksi kokonaisuudeksi. Järjestelmä on skaalattava ja helposti täydennettävä, Lindqvist summaa.

**Check Pointin suositukset yrityksille, jotka haluavat paremman tietoturvan:**

1. Tietoturva kannattaa nähdä yrityksen strategisena voimavarana digitalisoituneessa maailmassa.
2. Tietoturva ei kohene riittävästi pelkästään ostamalla laitteita. Tietoturvakäytännöt on vietävä koulutuksen avulla henkilöstön arkeen kaikilla tasoilla.
3. On järkevää pysyä rikollisten edellä käyttämällä neljännen sukupolven palomuureja, ennakoivaa uhkientorjuntaa ja muita moderneja ratkaisuja. Yhtenäinen arkkitehtuuri tekee järjestelmästä helposti hallittavan.
4. Erehdyksiä sattuu aina. Tietoturvan tulee olla niin hyvällä tolalla, että se kestää, vaikka joku klikkaisi vahingossa väärää linkkiä.
5. Kumppanuus kokeneen tietoturvan asiantuntijan kanssa on hyvä investointi, joka vapauttaa yrityksen voimia sen ydinosaamisalueelle.

Tutkimuksen toteutti tutkimusyritys Norstat puhelinhaastatteluina, joihin osallistui 200 yritysten tietoturvasta päättävää henkilöä. Vastaajana oli IT- tai tietoturvavastaava tai sellaisen puuttuessa toimitusjohtaja. 100 vastaajaa oli 50–99 hengen yrityksistä ja 100 yli sadan hengen yrityksestä. Haastattelut tehtiin pääosin helmikuussa 2017. Ruotsissa Norstat toteutti vastaavan kyselyn syyskuussa 2016.

--

Oheinen kuvatiedosto on vapaasti käytettävissänne. Maajohtaja Robert Lindqvistin taustalla on kuvassa Check Pointin ThreatCloud-kartta, josta meneillään olevat tietoturvahyökkäykset näkyvät reaaliaikaisesti. Kuva: Juha Saastamoinen.

Kartta löytyy myös täältä: <https://threatmap.checkpoint.com/ThreatPortal/livemap.html>

--

**Lisätiedot, tulosraportti ja haastattelupyynnöt:**

Maajohtaja Robert Lindqvist, Check Point Software Technologies, robertl@checkpoint.com, p. 050 368 4912

OSG Viestintä, Maija Rauha, maija.rauha@osg.fi, p. 0400 630 065

**Petyan opetukset: Näin suojaudut seuraavalta kiristyshaittaohjelmahyökkäykseltä** (Check Pointin blogi):

<http://blog.checkpoint.com/2017/06/28/preventing-petya-stopping-next-ransomware-attack/>

**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.