KAUPPAKAMARI

YRITYKSIIN KOHDISTUVAT KYBERUHAT 2019

Kolmas aiheesta tehty selvitys

Yritysten tietoverkkoon kohdistuvat tunkeutumiset.

SAATTEEKSI

Tämä Helsingin seudun kauppakamarin ”Yrityksiin kohdistuvat kyberuhat 2019” -selvitys on järjestyksessä kolmas aiheesta tehty selvitys ja painottuu yritysten tietoverkkoon kohdistuviin tunkeutumisiin. Helsingin seudun kauppakamari pitää tärkeänä synnyttää ja ylläpitää keskustelua tästä aiheesta yritysten kybertietoisuuden parantamiseksi.

Selvitys on osa Helsingin seudun kauppakamarin yritysturvallisuuteen liittyvää selvitystoimintaa. 600 johtohenkilöä suomalaisyrityksistä on antanut tähän selvitykseen luottamuksellisesti arvokkaita tietoja ja näkemyksiä yrityksiin kohdistuviin kyberuhkiin liittyvistä asioista. Olemme kiitollisia yritysjohdon merkittävästä panoksesta sekä siitä luottamuksesta, jota he ovat osoittaneet kauppakamarille antamalla tietoa selvityksen käyttöön.

Helsingissä 27.9.2019

Helsingin seudun kauppakamari

SISÄLLYS

*1 **JOHDANTO*** *4*

*2 **SELVITYKSEN TULOKSIA:***
YRITYKSIIN KOHDISTUVAT UHAT JA VARAUTUMISEN ESTEET *5*

Mitkä seuraavista vaihtoehdoista ovat suurimmat kyberturvallisuuden uhat suomalaisille yrityksille? *5*
Mitkä ovat kolme suurinta estettä tehokkaan kyberturvallisuuden toteuttamisessa? *7*
Onko yritys kohdistanut kyberturvallisuuteen jotain seuraavista toimenpiteistä viimeisen neljän vuoden aikana? *9*

*3 **SELVITYKSEN TULOKSIA:***
YRITYKSIIN KOHDISTUVAT TUNKEUTUMISET *11*

Mitkä seuraavista vaihtoehdoista ovat raskaimmat seuraukset kyberhyökkäyksistä? *11*
Miten organisaationne havaitsisi yrityksenne tietoverkossa käynnissä olevan tunkeutumisen? *12*
Minkälaista tietoa luulette tunkeutujien etsivän? *14*
Minkä tyyppistä tietoa olette menettäneet tietoverkkotunkeutumisten vuoksi? *16*
Tietääkö henkilökunta, miten toimia, jos he epäilevät tunkeutumista tietojärjestelmiinne? ... *17*

*4 **SELVITYKSEN TULOKSIA:***
VIRANOMAISTEN ROOLI JA TIEDON SAATAVUUS *18*

Miten hyvin tunnette suomalaisten viranomaisten roolia ja toimintaa kyberuhkiin liittyen? ... *18*
Oletteko saaneet jostakin käytännöllistä tietoa kyberuhkiin liittyen? *19*

*5 **SELVITYKSEN TULOKSIA:***
VARAUTUMINEN – VASTUUT, SUUNNITELMAT JA HARJOITUKSET *21*

Miten organisaationne on järjestänyt tietoturvallisuusvastuut johtotasolla? *21*
Kenelle tietoturvavastuullinen henkilö raportoi? *23*
Onko teillä käytössä käytännössä toimivia suunnitelmia tunkeutumisten varalle? *24*
Mitä asioita suunnitelmiin on sisällytetty? *25*
Oletteko koskaan harjoitelleet suunnitelmienne toimivuutta jollakin seuraavista tavoista? *26*
Onko teillä vahvistettua koulutus- ja harjoitusohjelmaa kyberturvallisuuteen liittyen? *27*
Ovatko kyberuhkiin liittyvät harjoitukset osa muihin liiketoimintaa uhkaaviin uhkiin liittyvää harjoittelua? *28*
Oletteko varautuneet kyberuhkiin seuraavin tavoin konkreettisesti tai suunnitelmilla? *29*

*6 **JOHTOPÄÄTÖKSET*** *30*

LIITE: SELVITYKSEN KYSYMYSLUETTELO *32*

1 JOHDANTO

Selvityksessä tutkitaan suomalaisten yritysten käsityksiä niihin kohdistuvista kyberuhista ja niihin varautumisesta. Selvitys perustuu 600 suomalaisen yrityksen antamiin vastauksiin. Taloustutkimus toteutti kyselyn Helsingin seudun kauppakamarin toimeksiannosta. Yritykset vastasivat kyselyyn toukokuussa 2019. Tutkimustulokset on esitetty taulukkoina ja kuvioina, joista yksittäisen vastaajan mielipide ei käy ilmi.

Alkuperäisen vuoden 2015 selvityksen ovat laatineet projektipäällikkö **Panu Vesterinen** Helsingin seudun kauppakamarista, **Chris Fogle** CyVantage Llc:stä ja Associate partner **Mika Laaksonen** KPMG:ltä.

Tähän selvitykseen on lisätty muutamia kohtia, mutta vanhoja kysymyksiä ei ole poistettu vertailtavuuden vuoksi. Selvitys on osa kauppakamarijärjestön yritysturvallisuustoimintaa.

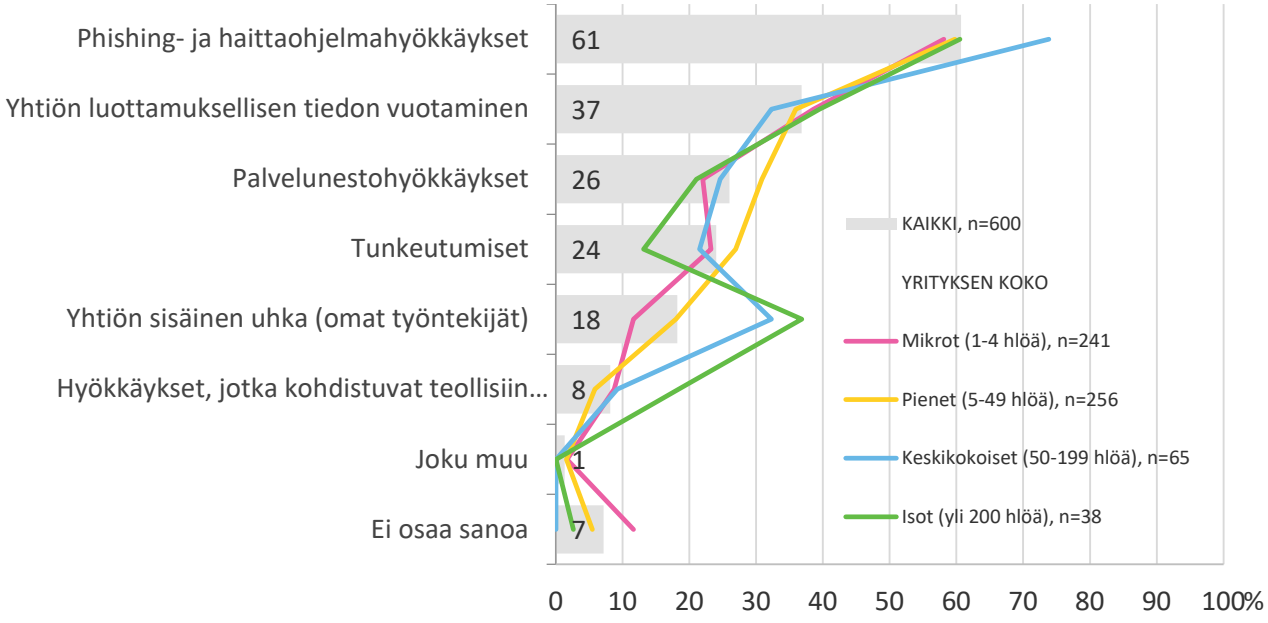
Kyselyyn vastanneista 600 yrityksestä 51 prosenttia edustaa palveluita, 21 prosenttia teollisuutta ja 14 prosenttia kauppaa. Rakennusalan yrityksistä on vastaajista 14 prosenttia.

Vastaajat olivat yritysten toimitusjohtajia (22 %), yrittäjiä tai omistajia (51 %), muita johtajia (8 %), asiantuntijoita (6 %) olevia. Päällikkötason tehtävissä vastaajista oli kymmenen prosenttia. Vastaajajoukon rakenne kertoo siitä että kysely on tavoittanut yritysten päätöksentekijät – turvallisuuden kehittämisen kannalta ratkaisevan ryhmän. Selvityksen kysymykset laadittiin tarkoituksella siten, etteivät ne ole ammattilaisia ja asiantuntijoita varten, vaan niihin voi vastata ilman teknistä asiantuntemusta.

Selvityksessä on kursiivilla lainauksia yritysten vapaamuotoisista vastauksista.

2 SELVITYKSEN TULOKSIA: YRITYKSIIN KOHDISTUVAT UHAT JA VARAUTUMISEN ESTEET

MITKÄ SEURAAVISTA VAIHTOEHDOISTA OVAT SUURIMMAT KYBERTURVALLISUUDEN UHAT SUOMALAISILLE YRITYKSILLE?



Tällä kysymyksellä pyrittiin kartoittamaan sitä, mitä elinkeinoelämä pitää uhkana toiminnalleen. Mikäli yrityksen johto ei tunnista uhkaa, on vaikea kehittää kyberturvallisuutta ja kohdistaa resursseja oikeisiin toimenpiteisiin.

Valtaosa yrityksistä, melkein kaksi kolmasosaa kaikista vastaajista (61 %), piti phishing- tai haittaohjelmahyökkäyksiä suurimpana uhkana suomalaisille yrityksille. Kyseiset hyökkäykset ovat saaneet paljon julkisuutta mediassa ja tämä on saattanut vaikuttaa vastaamisprosenttiin. Jos näin on, on se osoitus siitä, että johdon tietoisuutta turvallisuudesta voidaan kasvattaa mediassa julkaistujen artikkeleiden avulla.

Toiseksi suurimpana uhkana (37 %) vastaajayritykset pitivät tänä vuonna yrityksen luottamuksellisen tiedon vuotamista.

Selvästi yli puolet (61 %) suurista vastaajayrityksistä piti phishing- tai haittaohjelmahyökkäyksiä suurimpana ongelmana. Kaksi viidestä suuresta yrityksestä (40 %) piti yhtiön sisäistä uhkaa suurimpana uhkana.

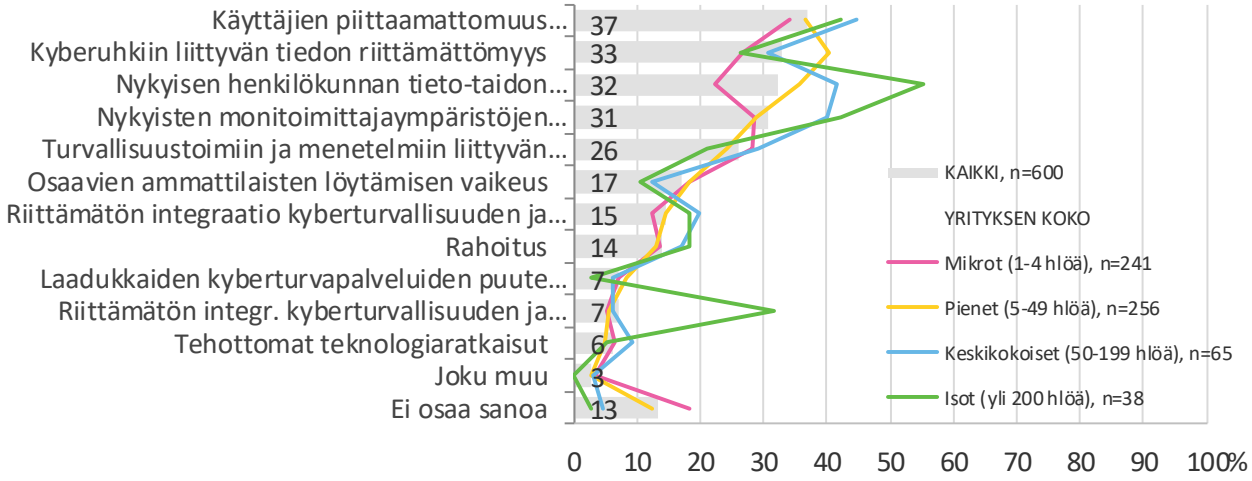
Kolmanneksi suurimpana uhkana vastaajayritykset (26 %) pitivät palvelunestohyökkäyksiä. Viidesosaa (22 %) suurista vastaajayrityksistä piti palvelunestohyökkäyksiä suurimpiin uhkin kuuluvana vaihtoehtona.

”Verkkokauppaamme kohdistunut palvelunestohyökkäysyritys saatiin estettyä.”

Neljänneksi yleisin vastaus oli tunkeutumiset. Joka neljäs (24 %) vastaaja nosti sen esille. Yllättävää on, että vain kymmenesosa (13 %) suurista vastaajista piti niitä mainittavana uhkana. Suuret yritykset ovat houkuttelevia kohteita hyökkäyksille. Saattaa olla, että ne ovat lisänneet valmiuttaan niiden tunnistamiseen tai sitten ne eivät ole havainneet tietoverkoissaan käynnissä olevia hyökkäyksiä. Niiden havainnointi on vaikeaa ja vaatii osaamista. Tunkeutumisten saama julkisuus on onneksi lisännyt yritysten tietoisuutta niiden luomasta uhasta.

Tuotantoprosesseihin kohdistuvia hyökkäyksiä piti uhkana hieman alle kymmenesosa (8 %) kaikista vastaajista. Suurista vastaajista joka viides (20 %) piti niitä merkittävänä uhkana.

MITKÄ OVAT KOLME SUURINTA ESTETTÄ TEHOKKAAN KYBERTURVALLISUUDEN TOTEUTTAMISESSA?



Suurimmat esteet kyberturvallisuuden toteuttamiselle ovat pysyneet kaikkien vastaajien osalta samoina kuin vuoden 2015 selvityksessä. Jopa niiden keskinäinen järjestys on pysynyt samana.

Tällä kysymyksellä oli tarkoitus selvittää elinkeinoelämän ajatuksia siitä, mitkä asiat ovat niitä, joihin tulee kiinnittää huomiota, kun yritys kohdistaa toimenpiteitä kyberturvallisuuden kehittämiseksi. Esteet ovat juuri niitä tekijöitä, jotka yrityksen tulee uhkien tunnistamisen jälkeen kehittää.

Kysyttäessä kolmea suurinta estettä tehokkaalle kyberturvallisuuden toteuttamiselle, nousi käyttäjien piittaamattomuus tietoturvallisuudesta ja kyberuhista suurimmaksi esteeksi. Lähes kaksi viidesosaa kaikista vastaajista (37 %) pitää sitä yhtenä suurimmista esteistä.

”Henkilökunta ei ole ymmärtänyt sähköpostiviestin olleen kalasteluviesti.”

Heti seuraavana esille nousi kyberuhkiin liittyvän tiedon riittämättömyys. Kolmasosa kaikista vastaajista (33 %) piti tätä suurimpien esteiden joukossa.

Kolmannelle sijalle (32 %) esteiden joukossa sijoittui henkilökunnan kyberuhkiin liittyvän tieto-taidon ylläpito. Neljänneksi suurin este on turvallisuustoimiin ja menetelmiin liittyvän tiedon riittämättömyys (26 %). Yrityksillä ei vieläkään ole riittävästi tietoa kyberuhista ja niihin varautumisesta. Tiedon jakamisessa on vielä paljon kehitettävää sillä pelkät juhlapuheet eivät ole tilannetta muuttaneet viimeisen neljän vuoden aikana.

“Huolimattomuus sähköpostin lähettämisessä.”

Yhä vai noin joka kahdeksas (14 %) yritys piti rahoitusta suurimpien esteiden joukossa. Tämä saattaa kertoa siitä, että kyberturvallisuus ei ole suuressa määrin

noussut yritysten investointilistalle, sillä rahoitus muodostuu usein esteeksi, kun puhutaan turvallisuuden kehittämisestä. Kun selvityksen tulokset huomioidaan, voi kyse olla juuri tästä.

Noin joka seitsemäs (15 %) vastaaja pitää riittämätöntä integraatiota liiketoiminnan ja kyberturvallisuuden välillä esteenä kehittämiselle. Integraatio on tärkeä osa tehokkaan kyberturvallisuuden kehittämiselle.

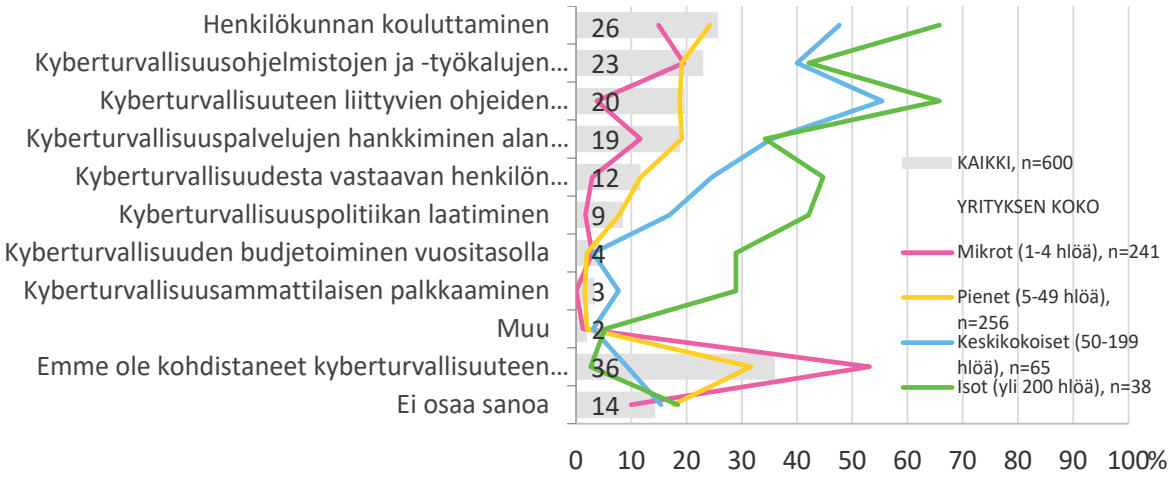
Suurten vastaajayritysten tilanne on hieman erilainen verrattuna kaikkiin vastaajiin. Rahoitus on este enää joka (18 %) viidennen suuren vastaajan mielestä kun se 2015 oli ongelma joka neljännelle (27 %), integraation puute liiketoiminnan kanssa esteenä joka viidennelle (18 %) kun se vuonna 2105 oli ongelma toiselle (47 %).

Suurten yritysten varautuminen kyberuhkiin on jatkunut ja se heijastuu vastauksissa. Erityisesti nykyisen henkilökunnan tietotaidon ylläpitäminen koetaan haastavana suurten joukossa, yli puolet (55 %) suurista kokee näin, kun vuonna 2015 luku oli 47 prosenttia. Integraation puute muun turvallisuuden kanssa taas koetaan esteeksi joka kolmannen (32 %) taholta ja vuonna 2015 se oli yhtä suuri ongelma (30 %).

Vastaajayritysten muut vastaukset olivat seuraavanlaisia:

- Aikapula
- Ei halua panostaa kyberturvallisuuteen
- Johdon tietämättömyys ja välinpitämätön suhtautuminen. Raha
- Kyberturvallisuus hoidetaan meidän emoyhtiön toimesta Ruotsissa
- Laaja yhteistyöverkosto pienten yritysten / toimijoiden kanssa
- Liian laaja kokonaisuus, hankala hahmottaa mitä pitäisi tehdä
- Liiketoimintajohdon ymmärtämättömyys tai haluttomuus reagoida uhkiin
- Päätöksiä tekevien henkilöiden asenteet ja ymmärrys kyberuhkia kohtaan ovat puutteelliset.
- Tehokas turva voi hankaloittaa toimintaa
- Uhkiin liittyvän viestinnän vaikeus: englantiin pohjaava terminologia, sanojen epätarkat ja osin päällekkäiset merkitykset, toimintaohjeiden vaikeus
- Vieläkään ei kyberuhkiin tule suhtauduttua tarpeeksi vakavasti.
- Yrittäjän tietämättömyys

ONKO YRITYS KOHDISTANUT KYBERTURVALLISUUTEEN JOTAIN SEURAAVISTA TOIMENPITEISTÄ VIIMEISEN NELJÄN VUODEN AIKANA?



Tämä kysymys kysyttiin ensimmäistä kertaa tämän vuoden selvityksessä. Tarkoituksena oli selvittää mihin yritykset kohdistavat resursseja kehittäessään kyberturvallisuutta. Vastaukset antavat myös mahdollisuuden arvioida sitä, ovatko yritykset kohdistaneet resursseja se mukaan, mitä ne pitävät uhkina ja esteinä.

"Henkilökunnan osaaminen kasvanut huimasti."

Yleisin vastaus (36 %) oli, ettei kyberturvallisuuteen ole kohdistettu mitään toimenpiteitä. Tässä vastaajien ryhmässä suurinta määrää edustivat mikro- ja pienet yritykset. Osa näistä saattaa kuitenkin toimittaa palveluja tai tavaroita myös suurille yrityksille. Jo vuosia sitten on ollut tapauksia, joissa tällaisten toimijoiden heikkoa turvallisuutta on hyödynnetty ja niiden kautta on hyökätty lopulliseen kohteeseen. Tämän vuoksi olisi tärkeää, että suuremmat yritykset vaatisivat alihankkijoiltaan varautumista kyberturvallisuuteen.

"Asiakkaiden digitaalisiin palveluihin kohdistuneiden hyökkäysten estäminen."

Neljäsosa (26 %) kaikista vastaajista oli panostanut henkilökunnan kouluttamiseen ja tämä osoittaa, että osa yrityksistä on ymmärtänyt henkilökunnan osaamisen ja tietoisuuden roolin kyberturvallisuuden osana. Monet hyökkäystavat hyödyntävät ihmisen luottamusta ja huolimattomuutta, joten kouluttaminen on tehokas tapa rakentaa toimivan kyberturvallisuuden perustaa.

"Henkilöstön kouluttaminen henkilökohtaisten päätelaitteiden kyberturvalliseen hallintaan."

"Käyttäjät tunnistavat phishing -yritykset."

Lähes yhtä suuri osa vastaajista (23 %) on sijoittanut rahaa kyberturvallisuusohjelmistojen ja -työkalujen hankkimiseen. Näillä on suuri merkitys kyberturvallisuuden kannalta, mutta niiden tehokas käyttö edellyttää henkilön, joka osaa käyttää niitä ja ennen kaikkea reagoida oikein hyökkäyksen tapahtuessa.

”Estetty salakirjoituksella laitevarkauden kautta tapahtuva tietojen paljastuminen.”

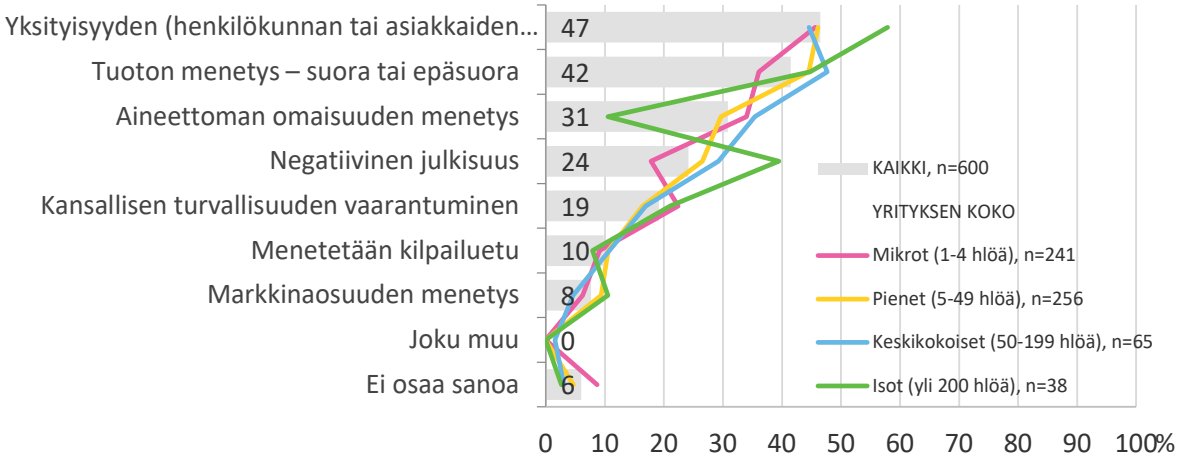
”Yrityksessämme käytetään laajasti sekä rauta- että ohjelmistotietoturvatuotteita, joita päivitetään säännöllisesti. Palomuurien ylläpito on ulkoistettu muutama vuosi sitten.”

Viidesosa vastaajista oli laatinut ohjeistuksia (20 %) ja hankkinut kyberturvallisuuspalveluja palveluntarjoajalta (19 %). Kymmenesosa oli palkannut kyberturvallisuusammattilaisen (12 %) ja laatinut kyberturvallisuuspolitiikan (9 %). Kaikki edellä mainitut ovat olennaisia kyberturvallisuuden kehittämisen kannalta, mutta valitettavan suuri määrä yrityksiä ei ole tehnyt mitään niistä.

”Tilien väärinkäytön estäminen, tunkeutumis- ja kevyiden DoS-yritysten estäminen ja havainnointi, ennaltaehkäisevät toimet salausten yms. kautta.”

3 SELVITYKSEN TULOKSIA: YRITYKSIIN KOHDISTUVAT TUNKEUTUMISET

MITKÄ SEURAAVISTA VAIHTOEHDOISTA OVAT RASKAIMMAT SEURAUKSET KYBERHYÖKKÄYKSISTÄ?



Kun yritys ymmärtää millaisia seurauksia kyberhyökkäyksestä voi seurata sille, on sen helpompi hyväksyä se, että kyberturvallisuuteen on sijoitettava resursseja. Kyberhyökkäykset ovat yleistyneet ja kehittyneet viimeisten vuosien aikana. Siksi myös yritysten tulisi panostaa kyberturvallisuuden kehittämiseen.

Puolet (47 %) kaikista vastaajista piti henkilökunnan tai asiakkaiden yksityisyyden loukkausta merkittävänä seurauksena kyberhyökkäyksestä. Yli puolet (57 %) suurista vastaajayrityksistä piti tätä raskaimpien seurausten joukossa. Euroopan unionin yksityisyyden suojaa koskevan lainsäädännön voimaan tulo viime vuonna on osaltaan nostanut yksityisyyden merkitystä yrityksille.

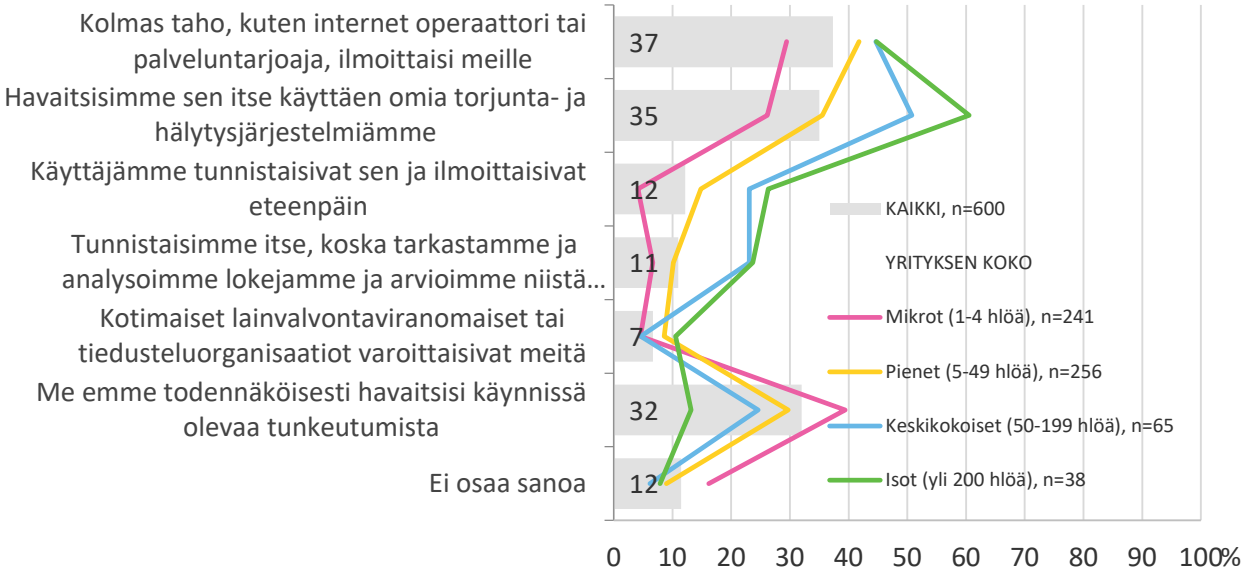
Neljä viidestä (42 %) piti suoraa tai epäsuoraa tuoton menetystä raskaimpana seurauksena kyberhyökkäyksistä.

Kolmasosa (31 %) kaikista vastaajista nosti esille aineettoman omaisuuden menetyksen. Yllättäen suurista vastaajista vain kymmenesosa (11 %) piti tätä raskaana seurauksena. Vuonna 2015 vastaava osuus oli kolmasosa (29 %). Tätä laskua on vaikea selittää.

”Yksi verkkoon tunkeutuminen, jonka yhteydessä menetettiin tiedostoja.”

Neljäsosa (24 %) vastaajista koki negatiivisen julkisuuden raskaana seurauksena ja viidesosa (19 %) piti kansallisen turvallisuuden vaarantumista raskaimpien seurauksien joukossa. Suurista vastaajista kaksi viidesosaa (39 %) tunnisti negatiivisen julkisuuden vakavaksi seuraukseksi tunkeutumisesta ja viidesosa (22 %) tunnisti kansallisen turvallisuuden vaarantumisen kyberhyökkäyksen seurauksena. Kansallisen turvallisuuden vaarantumisen tunnistaminen on tärkeää, sillä kyberhyökkäykset voivat olla osa hybriditoimintaa tai suoraa hyökkäystä kohdemaan infran ja elinkeinoelämän toiminnan estämiseksi ennen varsinaista hyökkäystä.

MITEN ORGANISAATIONNE HAVAITSISI YRITYKSENNE TIETOVERKOSSA KÄYNNISSÄ OLEVAN TUNKEUTUMISEN?



Mikäli yritys ei kykene tunnistamaan olevansa kyberhyökkäyksen kohteena, on sen vaikea suojata liiketoiminnan kriittistä tietoa. Tällöin jäljelle jää jälkijättöinen tapahtuneen selvittely, jos tunkeutumista edes koskaan havaitaan.

Yleisin oletus (37 %) sille miten vastaajayritys saisi tiedon käynnissä olevasta hyökkäyksestä oli ”Kolmas taho, kuten internet operaattori tai palveluntarjoaja, ilmoittaisi meille”. Melkein puolet (45 %) suurista vastaajista vastasi näin.

”Palveluntarjoaja on pyytänyt vaihtamaan salasanat epämääräisen liikenteen vuoksi.”

Toiseksi yleisin vastaus (35 %) oli ”Havaitsisimme sen itse käyttäen omia torjunta- ja hälytysjärjestelmiämme”. Melkein kolmasosa (60 %) suurista yrityksistä kokee kykenevänsä havaitsemaan tunkeutumisen itse ja tässä vastaajaryhmässä itse havaitseminen oli yleisin vastausvaihtoehto.

“Kalasteluyritysten ja toimitusjohtajahuijausten tunnistaminen onnistunut.”

Kolmasosa (32 %) kaikista vastaajayrityksistä tiedostaa sen, ettei heillä ole valmiuksia tunnistaa hyökkäystä ja vastasi siksi ”Me emme todennäköisesti havaitsisi käynnissä olevaa tunkeutumista”. Suurista yrityksistä joka kymmenes (13 %) vastasi tilanteen olevan näin. Vuonna 2015 viidesosa (22 %) suurista vastaajista vastasi tilanteen olevan tämä, joten näiden vastaajien keskuudessa on tapahtunut myönteistä kehitystä.

”Sähköposti-identiteetti varastettiin, onneksi pankki reagoi eikä rahoja voitu lähettää.”

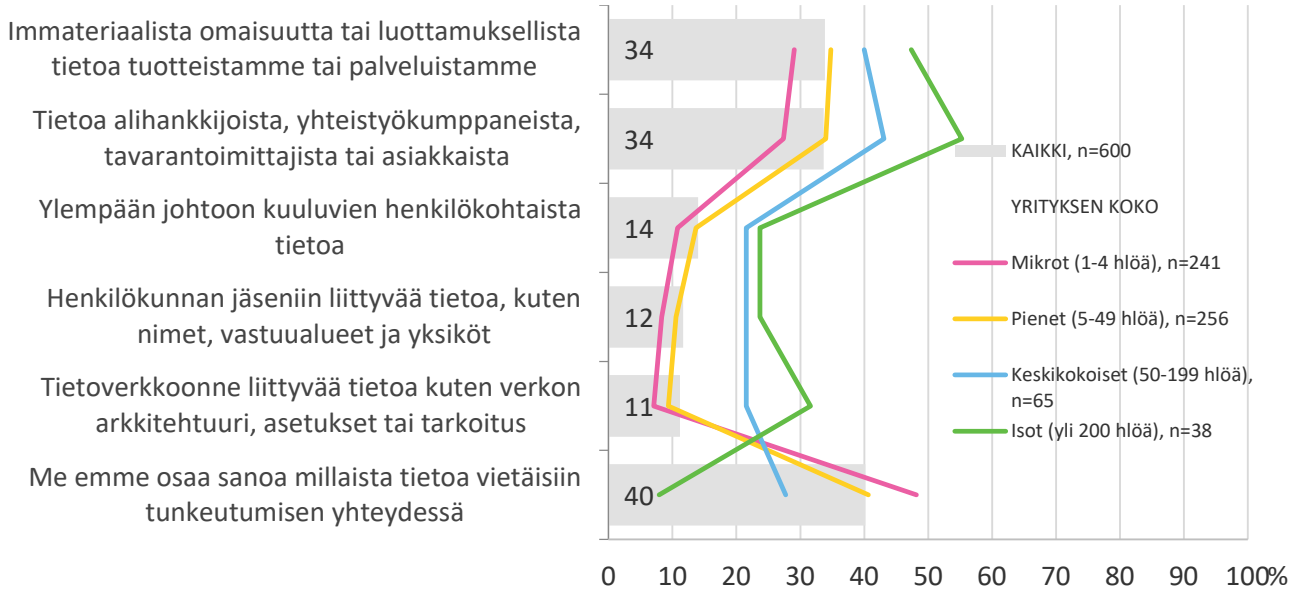
Käyttäjien kykyyn tunnistaa hyökkäys uskoi joka kymmenes (13 %). Suurien vastaajayritysten keskuudessa tilanne oli parempi, neljäsosa (26 %) uskoi käyttäjiinsä. Neljässä vuodessa on tapahtunut kehitystä, sillä 2015 vastaava luku oli 16 prosenttia. Työntekijöiden kouluttamisen lisääminen saattaa selittää positiivisen kehityksen.

”Estetty phishing-viestien läpimeno.
Henkilöstön koulutuksen tuloksena henkilöstö ottaa
oma-aloitteisesti yhteyttä nimettyyn palveluntarjoajaan.”

”Jokunen vuosi sitten kalastelija pääsi työntekijän sähköpostitiliin kiinni
huomaamatta ja pääsi seuraamaan henkilön sähköpostiliikennettä.
Tämän jälkeiset investoinnit lisäturvaan estävät ko. tilanteet.”

Kymmenesosa kaikista vastaajista (11 %) kertoi tarkastavansa ja analysoivansa lokeja sekä arvioivansa tilannetta ja havaitsevansa käynnissä olevan hyökkäyksen tällä tavalla. Käytännössä tämä tarkoittaa, ettei yhdeksän kymmenestä yrityksestä analysoi omia lokejaan. Suurista vastaajayrityksistä taas neljäsosa (23 %) seuraa ja analysoi lokejaan.

MINKÄLAISTA TIETOA LUULETTE TUNKEUTUJIEN ETSIVÄN?



Varauduttaessa kyberuhan varalta on ensin tunnistettava mitä pitää ja halutaan suojata ja suhteuttaa toimenpiteet riskeihin nähden. Tunkeutujan haluamien tietojen tunnistaminen on ensisijaisen tärkeää suunnattaessa usein rajallisia resursseja oikeaan tekemiseen.

”Ennen nykyisen tietoturvapalveluntarjoajamme sopimusta meidän serverimme kaapattiin ja tiedot salattiin. Sen jälkeen niistä vaadittiin lunnaita, jotta ne olisi taas avattu. Saimme kuitenkin ne pelastettua varmuuskopiosta ja lisäsimme tietoturvalaitteistoamme ja -ohjelmistoamme sen jälkeen.”

Suuriin osa vastaajista (40 %) ei osannut sanoa millaista tietoa tunkeutumisen yhteydessä vietäisiin. Tämä prosentti ei ole parantunut lainkaan vuoden 2015 (38 %) tilanteesta. On huolestuttavaa, jos yritykset eivät osaa arvioida, mikä tieto olisi kriittistä tai arvokasta. Jos ei tunne mikä tieto on yritykselle tärkeää, miten voi suojata sitä?

Kolmasosa kaikista vastaajista (34 %) Yhtä suuri osa kaikista vastaajista (34 %) olettaa tunkeutujan etsivän tietoa alihankkijoista, yhteistyökumppaneista, tavarantoimittajista tai asiakkaista. Näitä ryhmiä yhdistää se, että yleensä molemmat sisältävät toiminnan kannalta kriittistä ja luottamuksellista tietoa.

”Sähköposti kaapattu, josta onnistuneesti lähetetty laskuja tilitoimistolle, jotka menivät maksuun asti. Onneksi maksutapahtuma ehdittiin perua.”

Suurista vastaajista (47 %) olettaa tunkeutujan etsivän tietoa immateriaalisesta omaisuudesta tai luottamuksellista tuotteisiin- tai palveluihin liittyvää tietoa. Kaksi kolmasosaa (65 %) olettaa tunkeutujan etsivän tietoa alihankkijoista, yhteistyökumppaneista, tavarantoimittajista tai asiakkaista.

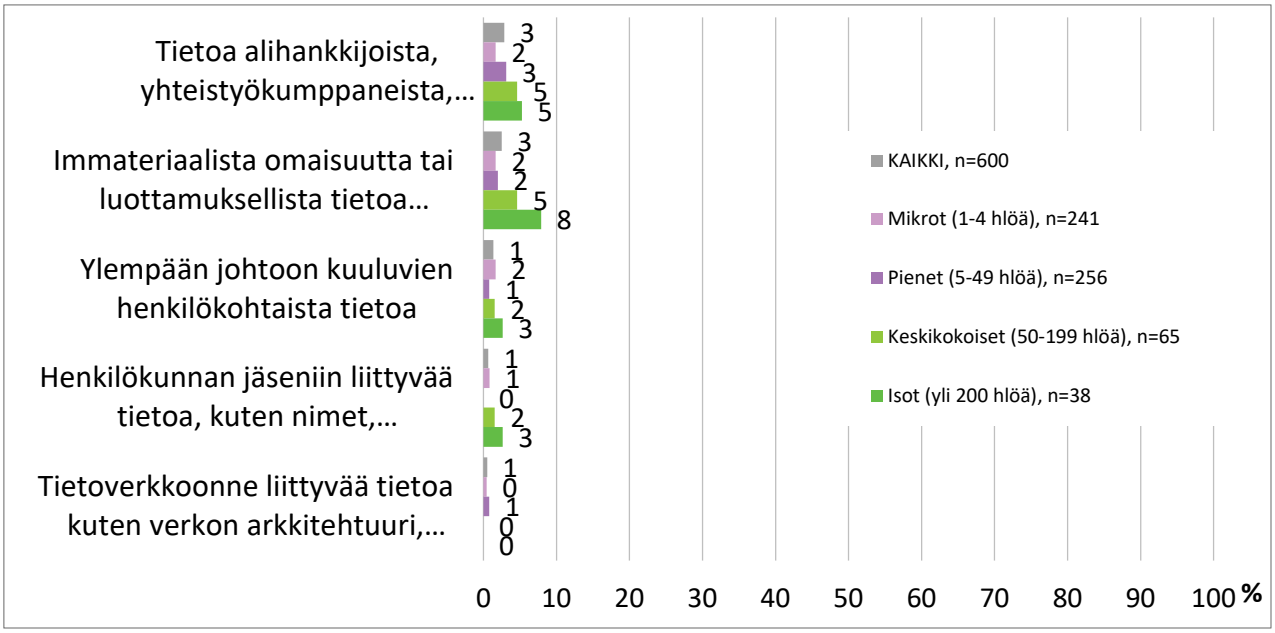
Kymmenesosa kaikista vastaajista (11 %) uskoi tunkeutujan etsivän tietoa verkon arkkitehtuurista, asetuksista tai tarkoituksesta. Nämä ovat kriittisiä tietoja, joita voidaan käyttää hyväksi myöhemmin tehtävissä hyökkäyksissä.

Tänä vuoden selvityksessä yli kymmenesosa (14 %) vastaajista uskoi tunkeutujan etsivän ylemmän johdon tietoja. Myös yli kymmenesosa (12 %) vastaajista uskoi tunkeutujan etsivän henkilökuntaan liittyvää tietoa. Vuonna 2015 alle kymmenesosa vastaajista uskoi tunkeutujan etsivän ylemmän johdon tietoja (8 %) tai henkilökuntaan liittyvää tietoa (9 %). Kasvun selityksenä voi olla toimitusjohtaja- ja phishing -hyökkäysten saama julkisuus. Yritykset ovat ymmärtäneet että tällaisia tietoja voidaan käyttää yrityksiin kohdistuvissa hyökkäyksissä.

”Palvelinmurto,
jossa emme tiedä mitä kaikkea on vuotanut tai varastettu.”

”Yksittäisiin työasemiin on onnistuttu murtautumaan. Ohjelmistojen ajantasaisuus on ollut puutteellista ja siten aiheuttanut kasvanutta uhkaa.”

MINKÄ TYYPPISTÄ TIETOA OLETTE MENETTÄNEET TIETOVERKKOTUNKEUTUMISTEN VUOKSI?



Tämän kysymyksen vastauksissa käy ilmi se, että yritykset havaitsemat tiedon menetykset ovat harvassa. Kyse ei kuitenkaan automaattisesti ole, että onnistuneet hyökkäykset olisivat harvinaisia, niitä ei vain ole kyetty tunnistamaan.

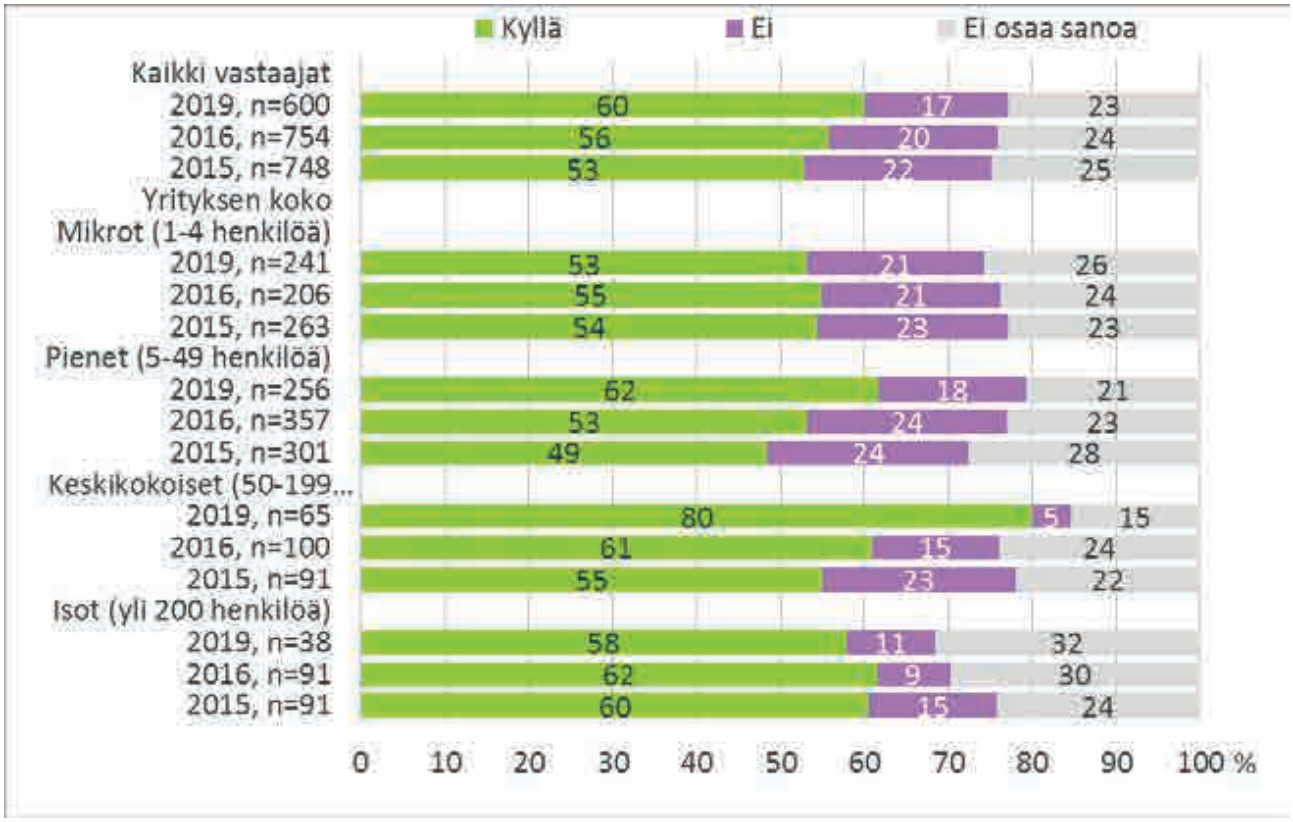
Suurin osa vastanneista (3 %) kertoi tunkeutujan vieneen tietoa immateriaalisesta omaisuudesta tai luottamuksellista tuotteisiin- tai palveluihin liittyvää tietoa.

Sama määrä vastaajista (3 %) kertoi tunkeutujan vieneen tietoa alihankkijoista, yhteistyökumppaneista, tavarantoimittajista tai asiakkaista.

Vastaajista (1 %) kertoi tunkeutujan vieneen tietoa verkon arkkitehtuurista, asetuksista tai tarkoituksesta.

Vastaajista yksi prosentti kertoi tunkeutujan vieneen ylemmän johdon tietoja (1 %) tai henkilökuntaan liittyvää tietoa (1 %).

TIETÄÄKÖ HENKILÖKUNTA, MITEN TOIMIA, JOS HE EPÄILEVÄT TUNKEUTUMISTA TIETOJÄRJESTELMIINNE?



Lähes kahdessa kolmasosassa (60 %) vastaajayrityksessä henkilökunta osaisi toimia, jos he epäilisivät tunkeutumista. Kehitystä vuodesta 2015 on tapahtunut seitsemän prosenttiyksikköä. Suurten yritysten keskuudessa kehitystä ei yllättäen ole tapahtunut, vaan henkilökunnan osaamiseen uskovien määrä on vähentynyt kaksi prosenttiyksikköä. Muutos ei ole merkittävä, mutta kehityksen puuttuminen on huomionarvoinen seikka.

”Tietohallinnollinen suojausluokittelu toimii erinomaisesti, henkilökunta osaa hyvin käyttää ja luokitella materiaalia.”

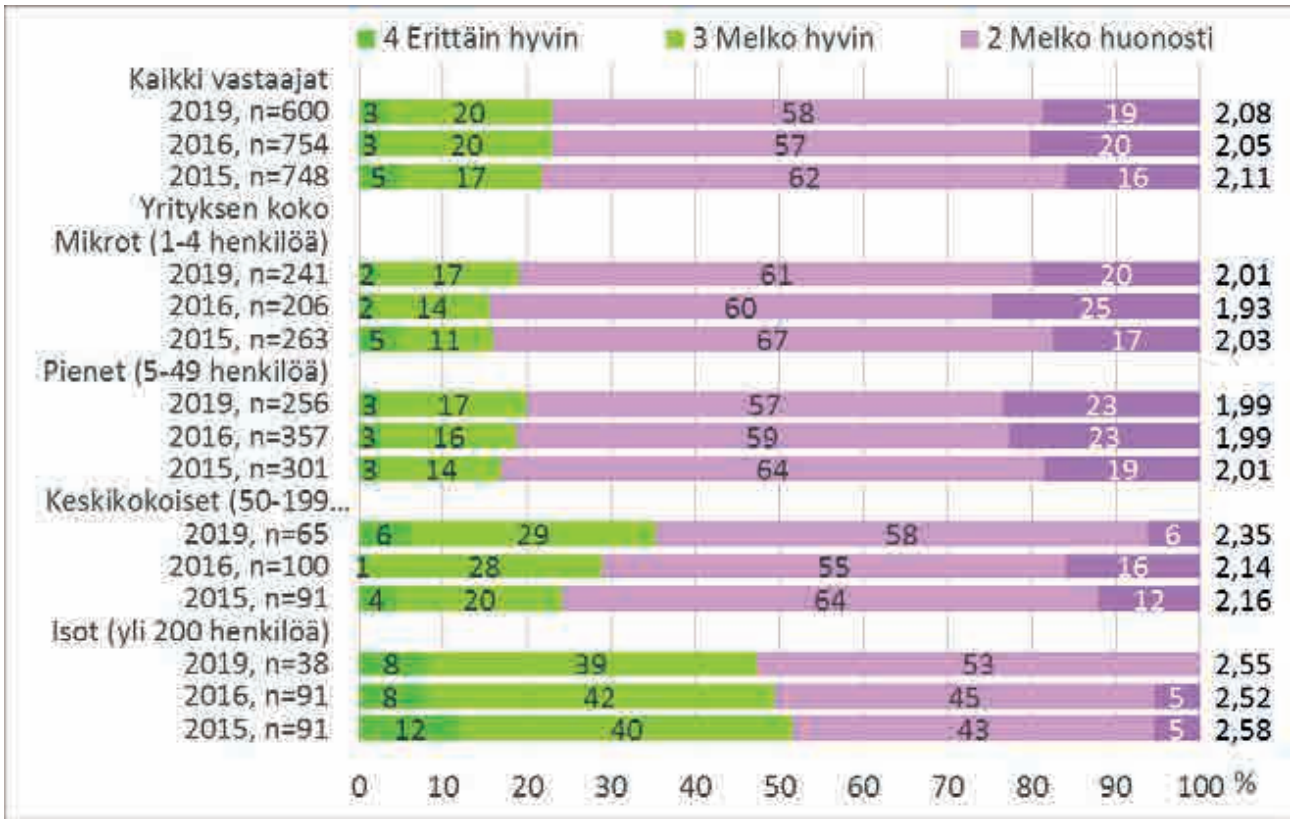
Hieman alle viidesosa (17 %) vastasi suoraan, ettei henkilökunta osaisi toimia, vaikka epäilisi tunkeutumista.Tässäkin ryhmässä on tapahtunut positiivista kehitystä, sillä vastausprosentti oli aiemmin viisi prosenttiyksikköä (22 %) suurempi.

”Kalasteluviesti mennyt henkilöltä läpi ja sähköpostin salasana saatu --> tili kaapattu ja käytetty edelleen levittämiseen sekä sisäiseen ns. toimitusjohtajahuijausyritykseen.”

Lähes neljäsosa (23 %) vastaajista ei osannut sanoa osaisiko henkilökunta toimia tilanteessa.

4 SELVITYKSEN TULOKSIA: VIRANOMAISTEN ROOLI JA TIEDON SAATAVUUS

MITEN HYVIN TUNNETTE SUOMALAISTEN VIRANOMAISTEN ROOLIA JA TOIMINTAA KYBERUHKIIN LIITTYEN?



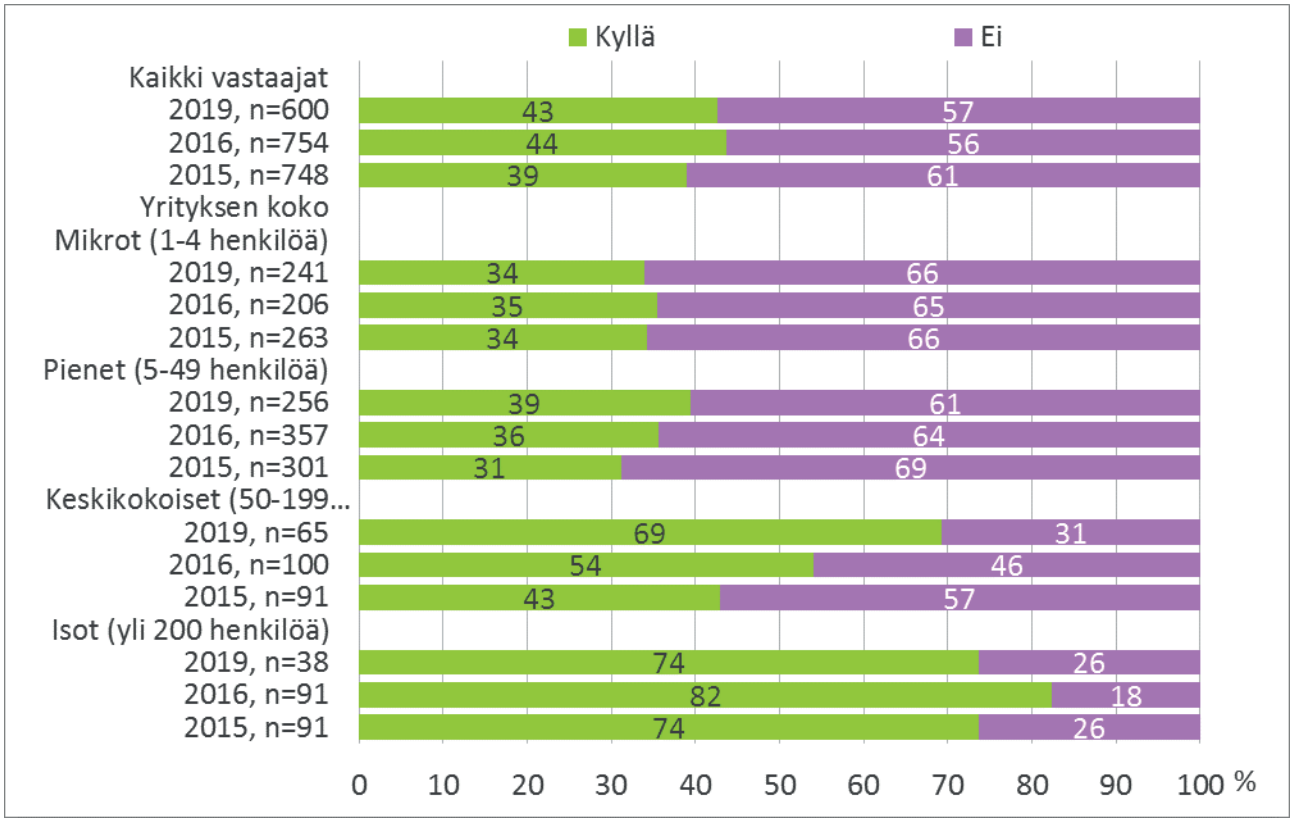
Kyberuhkilla on pahimmillaan yhteiskunnallisia ja kansatalouteen vaikuttavia seurauksia. Viranomaisilla on merkittävä rooli myös yritysten varautumisen kannalta. Kansallisen turvallisuuden ulottuvuuden vuoksi viranomaisten tulisi ottaa aktiivinen rooli myös elinkeinoelämän suuntaan. Yleisellä tasolla voidaan todeta, että tämän selvityksen valossa viranomaiset eivät ole onnistuneet yritysten tietoisuuden kehittämisessä neljän vuoden aikana.

Lähes joka viides vastaajayritys (19 %) ei tuntenut lankaan suomalaisten viranomaisten roolia ja toimintaa kyberuhkiin liittyen. Vuodesta 2015 on syntynyt negatiivista kehitystä kolmen prosenttiyksikön (16 %) verran. Määrä ei ole merkittävä, mutta huolestuttavaa on, ettei minkäänlaista parannusta ole tapahtunut. neljän vuoden aikana. Melko huonosti niitä tunsi miltei kaksi kolmesta (58 %) yrityksestä. Viranomaisten kannalta tilannetta voidaan pitää huonona. Aiheesta puhutaan julkisuudessa, mutta viranomaisten roolit kyberuhkiin liittyen eivät ole selvinneet elinkeinoelämälle.

Kaikista vastaajista siis yhä kahdeksan kymmenestä (77 %) tunsi vähintään melko huonosti viranomaisten roolia ja toimintaa.

Suurista yrityksistä vain alle kymmenesosa (8 %) tunsi viranomaisten roolit ja toiminnan erittäin hyvin, kun sama luku neljä vuotta sitten oli kaksitoista prosenttia. Yli puolet (53 %) suurista yrityksistä tunsi viranomaisten roolit melko huonosti.

OLETTEKO SAANEET JOSTAKIN KÄYTÄNNÖLLISTÄ TIETOA KYBERUHKIIN LIITTYEN?



Kaksi viidesosaa (43 %) kaikista vastaajayrityksistä on saanut käytännöllistä tietoa kyberuhkiin liittyen. Vuodesta 2015 on tapahtunut positiivista kehitystä neljän prosenttiyksikön verran.

Lukuun ottamatta keskikokoisia vastaajayrityksiä, ei tiedonsaannissa ole juurikaan tapahtunut kehitystä. Tiedonsaanti on avainasemassa niille yrityksille, jotka yrittävät kehittää kyberturvallisuuttaan ja pysyä ajan tasalla uhkien suhteen.

Mistä on saanut tietoa:

Isot yritykset (yli 200 henkilöä)

- CERT-FI tiedotteet, viranomaisyhteistyön kautta (KRP, poliisi...)
- Ficora
- Huoltovarmuuskeskus
- Traficom
- Kyberturvakeskuksen tiedotteet
- NCSC-FI, KRP, PV, SuPo
- Funet
- Internet
- Kaupalliset toimijat/palveluntarjoajat
- Sisäiset asiantuntijat
- Kurssit
- Yhteistyökumppanit

Keskikokoiset yritykset (50–99 henkilöä)

- Seminaarit, koulutukset
- F-Secure
- Ficora
- It-kumppanit, it-toimittajat, yhteistyökumppanit
- Kyberturvallisuuskeskus
- Media, lehdet, netti
- Oma organisaatio
- Tietosuojatoimisto
- Traficom
- Viestintävirasto

Pienet yritykset (5–49 henkilöä)

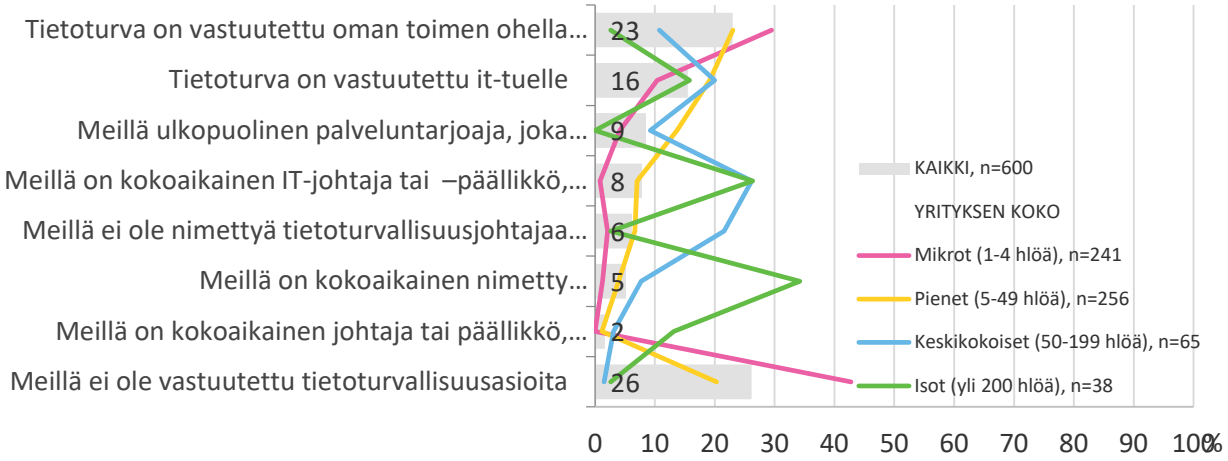
- Emoyhtiö, omat asiantuntijat
- Internet
- Järjestelmätoimittajat, ohjelmistotoimittajat
- Koulutukset, koulutusmateriaalit
- Kumppanit
- Kyberturvallisuuskeskus
- Poliisi, Traficom, Puolutusvoimat, Suomen Yrittäjät, viranomaiset
- Tiedotusvälineet
- Vakuutusyhtiöt

Mikroyritykset (1–4 henkilöä)

- Yhteistyökumppanit
- Asiakkaat
- F-Secure
- Ficora
- Internet, lehdet, media, uutiset
- Koulutukset
- Laitteistotoimittajat
- Seminaarit
- Suomen Yrittäjät, yrittäjäjärjestöt
- Viestintävirasto/kyberturvallisuuskeskus

5 SELVITYKSEN TULOKSIA: VARAUTUMINEN – VASTUUT, SUUNNITELMAT JA HARJOITUKSET

MITEN ORGANISAATIONNE ON JÄRJESTÄNYT TIETOTURVALLISUUSVASTUUT JOHTOTASOLLA?



Jos jotain toimintaa yrityksessä ei ole selkeästi vastuutettu jollekulle eikä resurssejakaan ole osoitettu, on mahdotonta kehittää järkevää tai toimivaa kyberturvallisuutta. Kyberuhat voivat pahimmillaan keskeyttää yrityksen toiminnan ja siksi on tärkeää nimetä joku vastaamaan tästä yrityksen toiminnan kannalta kriittisestä suojautumisen osa-alueesta.

Neljäsosassa (26 %) vastaajayrityksistä tietoturvallisuutta ei ollut vastuutettu miten-kään. Näiden vastaajien osuus on kasvanut vuodesta 2015 viiden prosenttiyksikön verran. Käytännössä nämä yritykset edustavat avointa hyökkäyspinta-alaa rikollisille.

Toiseksi yleisintä (23 %) kaikkien vastaajayritysten keskuudessa oli se että vastuu tietoturvallisuudesta oli nimetty oman toimen ohella päällikkötason henkilölle tai toimitusjohtajalle.

Kolmanneksi yleisin vaihtoehto (16 %) oli se että tietoturvallisuus oli vastuutettu IT-tuelle.

Alle kymmenesosassa (8 %) vastaajayrityksistä oli kokopäivätoiminen IT-johtaja tai –päällikkö, joka vastasi oman toimen ohella.

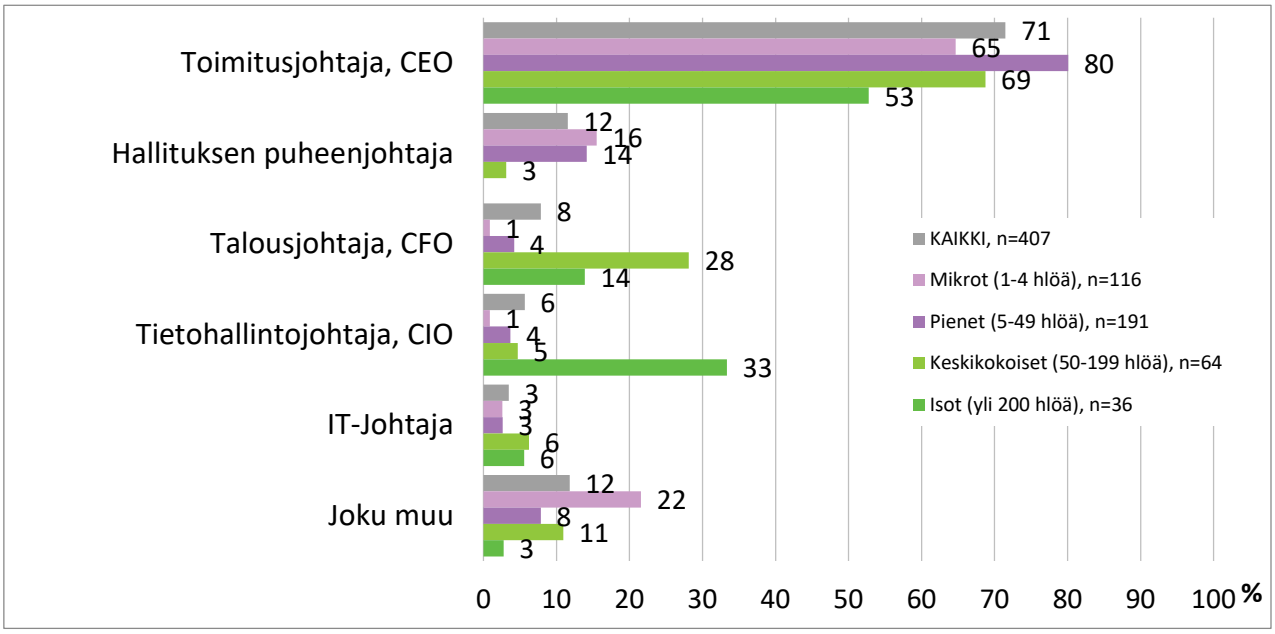
Kymmenesosa (9 %) kertoi heillä olevan ulkopuolisen palveluntarjoajan joka tarjoaa tietoturvallisuusjohtajan tai päällikön. Tämä on huomioonotettava vaihtoehto jos ei ole mahdollisuutta asiantuntevaan kokopäiväresurssiin.

”It -puolelle on otettu ulkopuolinen henkilö/toimittaja hoitamaan servereitä, domainit ja tietoturvallisuusasioiden ylläpito.”

Vain joka kahdeskymmenes (5 %) vastaajista oli palkannut kokoaikaisen tietoturvallisuusjohtajan tai –päällikön.

”Kyberturvallisuushenkilö on kerran pyytänyt vaihtamaan salasanat, kun on epäilty niiden vuotaneen. Toimenpiteet tehty alle tunnin, ei vahinkoa.”

KENELLE TIETOTURVAVASTUULLINEN HENKILÖ RAPORTOI?



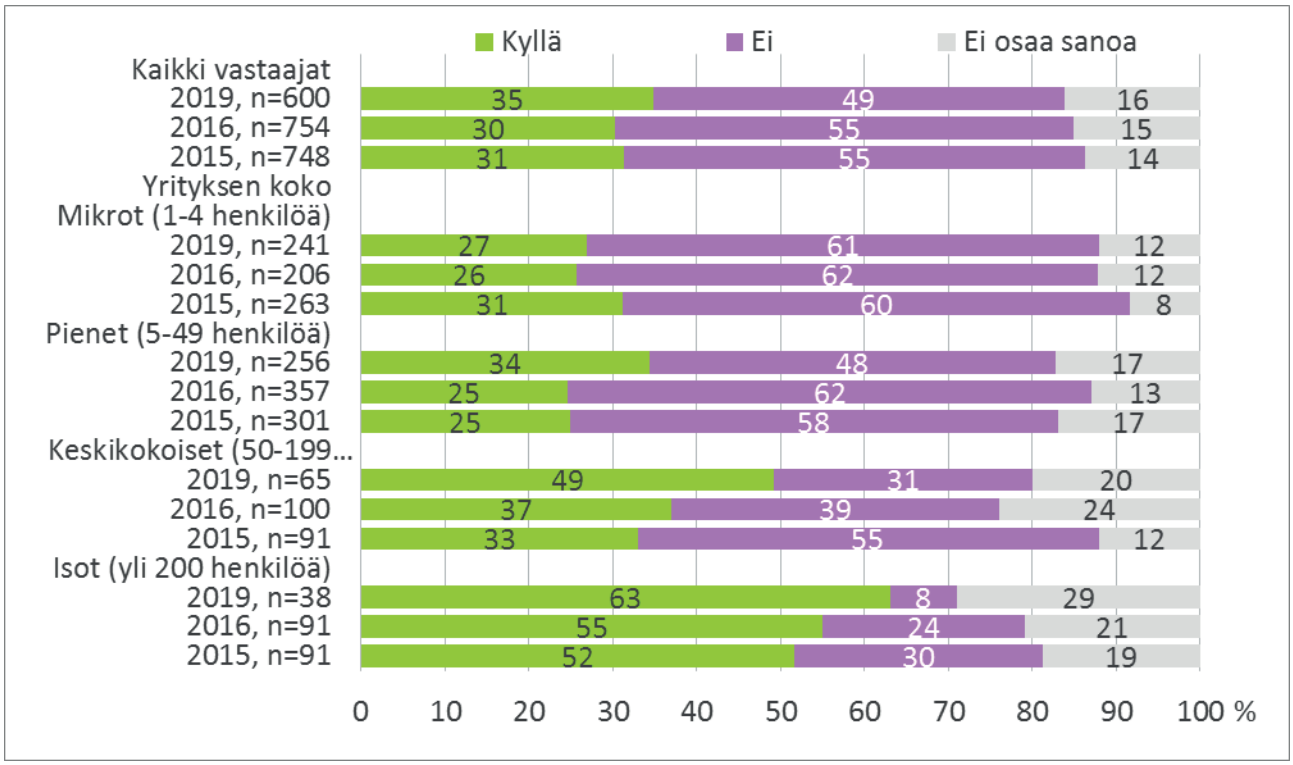
Yleisin raportointitaho oli toimitusjohtaja (71 %). Puolet suurista (53 %) oli järjestänyt asian näin. Toiseksi yleisin taho oli hallituksen puheenjohtaja (12 %). Näiden tahojen etuna on se, että kyseessä on päätösvaltainen henkilö, jolloin varsinkaan akuutit asiat eivät jää helposti hautumaan.

”Yrityksemme johto antaa toimivaltuuksia, tukea sekä rahoitusta kyberturvallisuuden asianmukaiseen hoitamiseen.”

Kaksi seuraavaksi yleisintä tahoa olivat talousjohtaja (8 %) ja tietohallintojohtaja. Näiden osalta huomionarvoista on se, että suurista vastaajayrityksissä neljäsosassa (28 %) raportoidaan talousjohtajalle ja kolmasosassa (33 %) tietohallintojohtajalle.

Kyberuhkien luonteen vuoksi ne voivat uhata lyhyessä ajassa liiketoiminnan jatkuvuutta ja siksi on tärkeää, että kyberturvallisuudesta raportoidaan organisaatiossa sellaiselle henkilölle, jolla on riittävä päätösvalta tai joka saa asian nopeasti sellaisen henkilön käsiteltäväksi. Liiketoiminnan jatkuvuutta uhkaava tekijään varautuminen kuuluu aina yrityksen toimintaa johtavien henkilöiden vastuulle.

ONKO TEILLÄ KÄYTÖSSÄ KÄYTÄNNÖSSÄ TOIMIVIA SUUNNITELMIA TUNKEUTUMISTEN VARALLE?

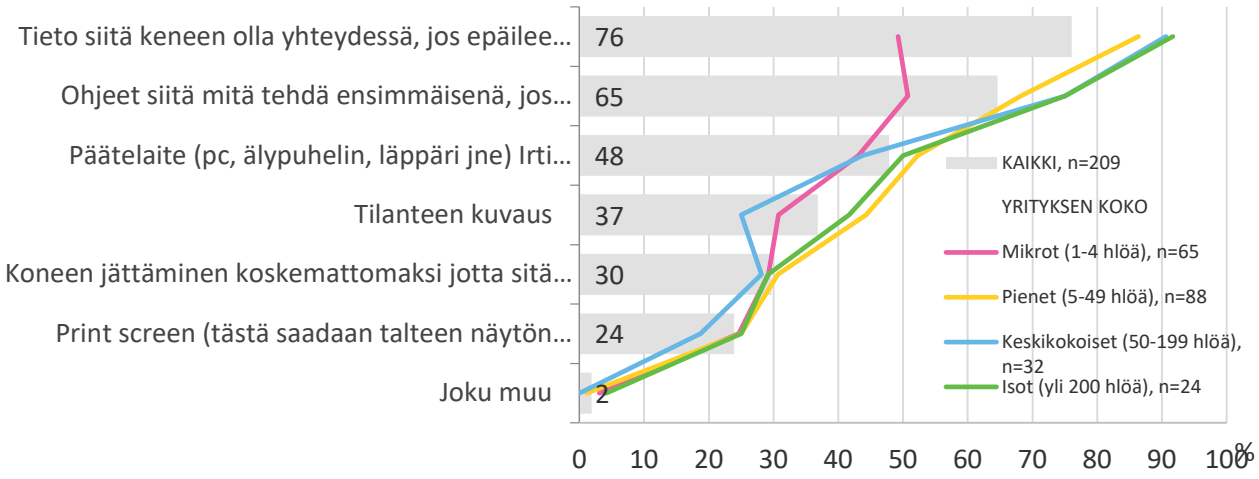


Kyberhyökkäysten luonteeseen kuuluu, että ne tapahtuvat mihin vuorokauden aikaan tahansa ja ne voivat pysäyttää liiketoiminnan. Jos yritys ei pysty laskuttamaan tai toimittamaan tavaroita tai palveluja, ollaan nopeasti yrityksen jatkuvuutta uhkaavassa tilanteessa. Siksi yrityksen on hyvä tehdä suunnitelmat kyberhyökkäyksien varalta. Parhaimmillaan toimivilla suunnitelmilla vältetään liiketoiminnan jatkuvuutta uhkaava tilanne.

Kolmasosa kaikista vastaajista (35 %) kertoi heillä olevan käytännössä toimivia suunnitelmia tunkeutumisten varalle. Suurista yrityksistä kahdella kolmasosalla (63 %) oli suunnitelma.

Puolet kaikista vastaajayrityksistä (49 %) kertoi ettei heillä ollut toimivia suunnitelmia tunkeutumisten varalle.

MITÄ ASIOITA SUUNNITELMIIN ON SISÄLLYTETTY?



Tämä jatkokysymys oli osoitettu niille vastaajayrityksille, jotka vastasivat heillä olevan käytännössä toimivan suunnitelman. Sen tarkoitus on esitellä asioita, joita suunnitelmaan voisi kirjata.

Vastaajista kolme neljäsosaa (76 %) kertoi suunnitelmissa olevan tiedon siitä keneen olla yhteydessä, jos epäilee tunkeutumista.

Toiseksi yleisin (65 %) oli ohje siitä mitä tehdä ensimmäisenä, jos epäilee tunkeutumista.

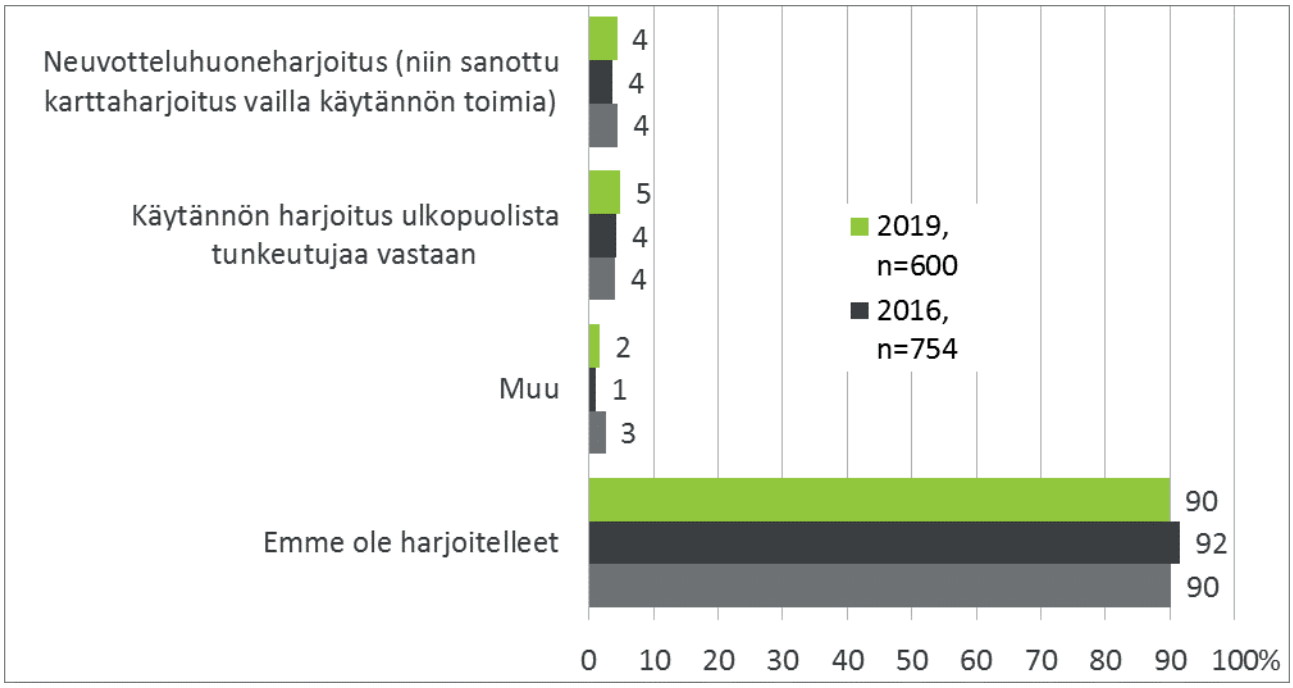
Kolmanneksi yleisin (48 %) oli ohje irrottaa päätelaite verkosta.

Neljäntenä ohjeena (37 %) oli tilanteen kuvaaminen.

Viidentenä (30 %) tuli ohje jättää kone koskemattomaksi tutkimista varten.

Kuudentena (24 %) oli ohje toteuttaa print screen –komento, jotta näytön kuva saadaan varmasti tallennettua.

OLETTEKO KOSKAAN HARJOITELLEET SUUNNITELMIENNE TOIMIVUUTTA JOLLAKIN SEURAAVISTA TAVOISTA?



Vain joka kymmenes (10 %) yritys on harjoitellut ja testannut tällä tavalla suunnitelmiensa toimivuutta. Suunnitelmia oli vain kolmasosalla kaikista vastaajista. Yhdeksän kymmenestä yrityksestä, joka on sijoittanut resursseja suunnitelmien tekemiseen, ei ole testannut niiden toimivuutta harjoittelemalla. Tämä tarkoittaa sitä, että vain noin kolme prosenttia kaikista vastaajayrityksistä on harjoitellut kyberhyökkäyksen varalta.

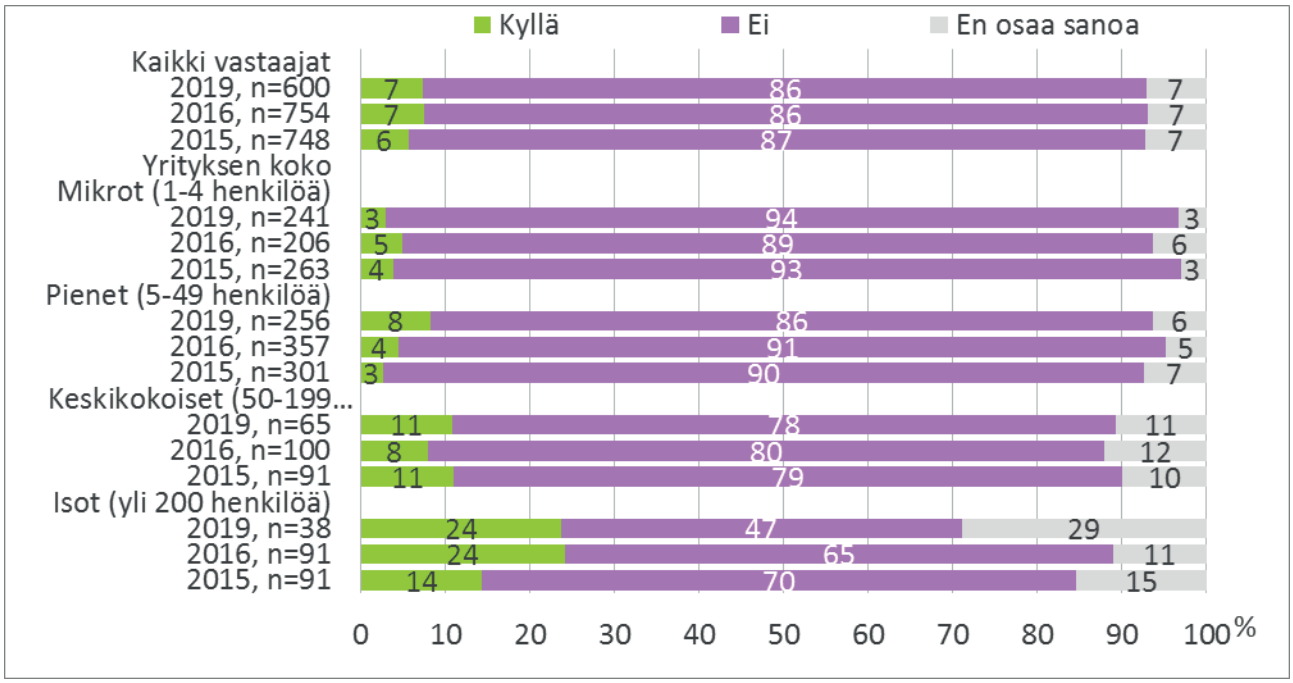
”Henkilöstö on suhtautunut uhkaharjoituksiin positiivisesti, harjoituksessa on saatu paranevia tuloksia. Phishing -testi ja koulutus on parantanut erityisesti vanhemman henkilöstön osaamista.”

Neljä prosenttia kaikista vastaajista on toteuttanut neuvotteluhuoneharjoituksen. Hieman useampi (5 %) on harjoitellut ulkopuolista hyökkääjää vastaan.

Muita yleisimpiä harjoittelutapoja olivat:

- palautustestaus
- sisäinen hakkerointiharjoittelu yritysjärjestelmiämme vastaan
- tiedottaminen ja yhteinen keskustelu kuinka toimittu ja olisiko muuta pitänyt huomioida
- tietoturvallisuutta seurataan johtoryhmässä systemaattisesti
- tuotannon kyberriskien simulointi
- yritys tunkeutua käytännössä

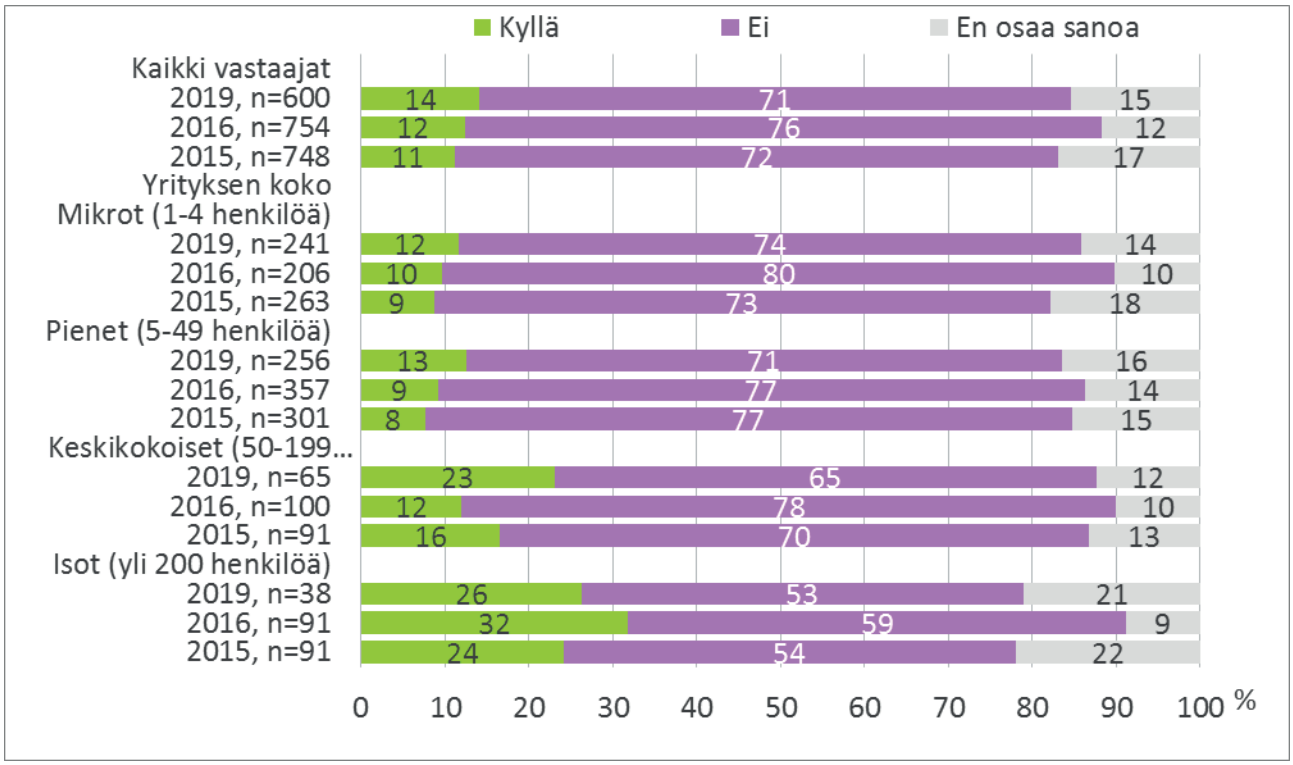
ONKO TEILLÄ VAHVISTETTUA KOULUTUS- JA HARJOITUSOHJELMAA KYBERTURVALLISUUTEEN LIITTYEN?



Ohjelman olemassaolo kertoo yrityksen varautuneen jo varsin hyvin uhkaan ja sen torjumiseen. Kovin yleisiä nämä eivät vielä ole, kuten tuloksista on nähtävissä. Vahvistettu suunnitelma osoittaa yritysjohdon sitoutuneen koulutukseen hyväksymällä sen osaksi muuta koulutusta. Samalla yritysjohto sitoutuu osoittamaan resursseja koulutukseen.

Hyvin harva (7 %) vastaajayritys kertoi heillä olevan vahvistetun koulutus- ja harjoitusohjelman kyberturvallisuuden varalle. Vuodesta 2015 minkäänlaista kehitystä ei käytännössä ole tapahtunut.

OVATKO KYBERUHKIIN LIITTYVÄT HARJOITUKSET OSA MUIHIN LIIKETOIMINTAA UHKAAVIIN UHKIIN LIITTYVÄÄ HARJOITTELUA?

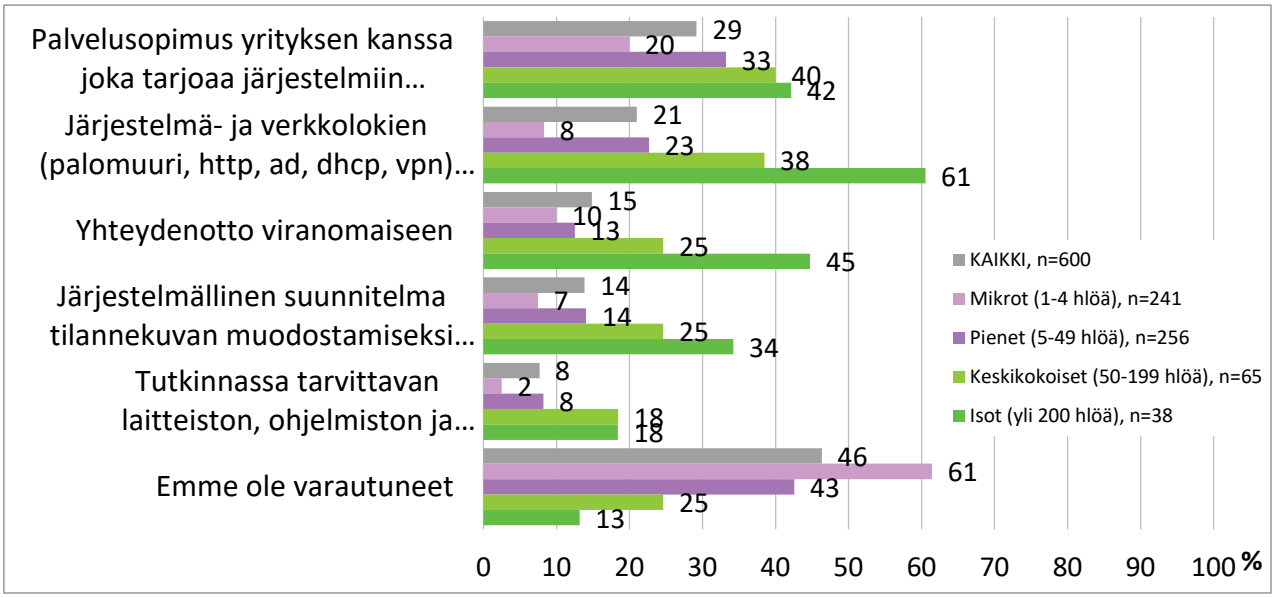


Tänä päivänä kyberuhat ovat osa normaaleita yritysten toimintaan kohdistuvia uhkia. Yrityksen kytkiessä kyberuhkiin liittyvät harjoitukset osaksi muihin liiketoimintaa uhkien harjoitteluun, on yritys ymmärtänyt kyberuhkaan varautumisen olevan osan normaalia riskienhallintaan liittyvää harjoittelua.

Yli kymmenesosa (14 %) kaikista vastaajista kertoi, että harjoitukset ovat osana muihin uhkiin varautumisen harjoittelua.

Joka seitsemäs (71 %) niitä ei ollut otettu osaksi muita harjoituksia. Tämä kuvaa sitä, että kyberuhkien ymmärtämisessä osaksi normaaleja uhkia on paljon kehittämisen varaa.

OLETTEKO VARAUTUNEET KYBERUHKIIN SEURAAVIN TAVOIN KONKREETTISESTI TAI SUUNNITELMILLA?



Yritysten on tärkeää varautua siihen, miten tunkeutumista selvitetään sen tapahduttua ja miten mahdollista viranomaisten tai omaa tutkintaa voidaan edesauttaa. Vuoden 2015 selvityksen jälkeen ei näissä toimissa ole tapahtunut käytännössä minkäänlaista kehitystä.

Lähes puolet (46 %) vastaajista ei ollut varautunut millään kysymyksessä esitetyllä vaihtoehdolla.

Miltei kolmasosalla kaikista vastaajayrityksistä (29 %) oli palvelusopimus tunkeutumisiin ja haittaohjelmiin liittyvää tutkintaa tarjoavan tahon kanssa

Viidesosa (21 %) kerää eri järjestelmä- ja verkkolokien tietoa selvittelyä varten.

Joka seitsemäs (15 %) oli ollut yhteydessä viranomaisiin varautumisen tiimoilta.

Seitsemäsosalla vastaajista (14 %) oli suunnitelma tilannekuvan luomiseksi tutkintaa, puhdistustoimenpiteitä ja loppuraportointia varten.

Lähes kymmenesosa kaikista vastaajayrityksistä (8 %) oli hankkinut tutkinnassa tarvittavaa laitteistoa, ohjelmistoa ja tutkintakykyä.

6 JOHTOPÄÄTÖKSET

Neljän viimeisen vuoden aikana varautumisen tilanne ei juurikaan muuttunut – uhat samana aikana kehittyneet merkittävästi

Kauppakamarin ensimmäinen valtakunnallinen kyberuhkien selitys tehtiin vuonna 2015. Sen jälkeen suurien yritysten kohdalla on tapahtunut jonkin verran kehitystä, mutta kaikissa muissa kokoluokissa tilanne ei juurikaan ole parantunut uhkien ja kehittämisen esteiden tunnistamisesta huolimatta. Esimerkiksi yrityksillä on yhä hyvin harvoin nimettyjä täysipäiväisiä tietoturvallisuusvastaavia, päinvastoin niiden osuus, jotka eivät ole vastuuttaneet tietoturvaa lainkaan, on kasvanut. Suuri osa yrityksistä ei myöskään tiedä mitä tunkeutuja haluaisi viedä heiltä ja tämä kertoo, ettei suojattavia arvoja tunneta. Tällöin on lähes mahdotonta kehittää kyberturvallisuutta järkevällä tavalla. Kyberturvallisuuden kannalta tärkeä hyökkäysten tunnistamiskyky ei ole parantunut ollenkaan.

Yleisellä tasolla yritysten kyberturvallisuuden tilanne ei siis ole muuttunut neljässä vuodessa. Yritysten joukossa on suuri määrä helppoja kyberturvattomia kohteita, jotka eivät ole pitäneet huolta digitaalisesta yritysvastuustaan osana tietoverkkojen yhdistämää yhteiskuntaa. Tämä avaa mahdollisuuden erilaisille elinkeinoelämään kohdistuville hyökkäyksille.

Viranomaisilla paljon tekemistä elinkeinoelämän tukemisessa

Viimeisen neljän vuoden aikana kyberturvallisuuteen liittyvien viranomaisten tunnettavuus elinkeinoelämän keskuudessa ei ole lisääntynyt lainkaan ja on yhä huonolla tasolla. Kyberuhat ovat pahimmillaan kansallisen turvallisuuden uhka ja siksi viranomaisten on otettava näkyvämpi rooli elinkeinoelämän keskuudessa. Viranomaiset tarvitsevat lisää resursseja kyetäkseen palvelemaan elinkeinoelämää vastaavalla tavalla kuin monessa muussa maassa toimitaan.

Elinkeinoelämä on keskeisessä asemassa yhteiskunnassa ja sen lamaantuessa alkaa kansantalous kärsiä lyhyessä ajassa. Viranomaisten on tiedostettava roolinsa kansallisessa kyberturvallisuudessa ja elinkeinoelämän keskeinen rooli osana sitä. Sen vuoksi tukea elinkeinoelämälle kyberturvallisuuden saralla on lisättävä voimallisesti.

Suuri määrä yrityksiä ei ole tehnyt neljän viimeisen vuoden aikana mitään kyberturvallisuuden kehittämiseksi

Kysyttäessä erikseen mitä yritykset ovat tehneet kyberturvallisuuden edistämiseksi viimeisen neljän vuoden aikana, yleisin vastaus oli, ettei mitään ole tehty. Näin vastanneiden painopiste oli pienissä yrityksissä, mutta verkottuneessa tietoyhteiskunnassa yrityksen koolla ei ole väliä. Alihankintaketjut ovat tunnettu ja käytetty hyökkäysvektori lopulliseen kohteeseen pääsemiseksi.

Hyökkäykset ovat yleistyneet ja kehittyneet, niitä tutkittaessa on kuitenkin käynyt selväksi, että vanha totuus että rosvo menee siitä mistä on helpointa mennä, koskee myös digitaalista maailmaa. Helppo, nopea ja tehokas tapa houkuttelee rikollisia vaikean ja monimutkaisen hyökkäyksen käyttäminen. Tuloksen saavuttaminen pienellä ponnistuksella houkuttaa aivan kuten yritystoiminnassa. Suomessa on suuri määrä kyberturvattomia yrityksiä, jotka muodostavat suuren ja helpon hyökkäyspinta-alan kenelle tahansa pahoissa aikeissa olevalle taholle. Loppujen lopuksi kyse on kansallisesta turvallisuudesta.

Henkilökunnan kouluttaminen yleisin tapa parantaa kyberturvallisuutta – suunnitelmat hyökkäysten varalta uupuvat yhä suurelta osalta yrityksiä

Yritykset ovat kouluttaneet henkilökuntaa, hankkineet kyberturvallisuusohjelmia, laatineet ohjeita ja ostaneet palveluita kyberpalveluyrityksiltä. Valitettavasti suuri määrä yrityksiä ei kuitenkaan ole tehnyt näitä toimenpiteitä. Hyökkäyksen varalta tehdyt suunnitelmat uupuvat yhä joka toiselta yritykseltä. Kun hyökkäys tapahtuu, nämä suunnitelmat ovat toiminnan selkäranka. Niiden tärkeyden ymmärtää viimeistään kun hyökkäyksen hetkellä tajutaan ettei niitä ole ja yrityksen tuloksen tekeminen keskeytyy.

Kyberturvallisuuteen liittyvän tiedon saamisessa hieman kehitystä – kuitenkin yhä haasteena

Luotettavan tiedon saaminen kyberuhista ja niihin varautumisesta on olennaista yritysten varautumisessa. Tämä tieto kilpailee kaiken muun informaatiotulvan kanssa huomatuksi tulemisesta. Se kuka tämän tiedon tuottaa, ei ole samantekevää. Viranomaiset tuottavat erilaista tietoa, mutta jostain syystä se ei tavoita juurikaan sen suurempaa määrää yrityksistä kuin neljä vuotta sitten. Kehitystä on tapahtunut pienten ja keskisuurten yritysten keskuudessa, mutta lähteet ovat yhä moninaiset.

Viranomaisten tulisi sisäistää roolinsa ja toimivan tiedonjakamisen merkitys. Sen jälkeen tulisi pyrkiä keskitettyyn viestintään, sillä muutoin on olemassa riski kilpalaulannasta sekä ristiriitaisesta ja painotukseltaan erilaisesta kyberturvallisuusviestinnästä. Aina tulee olemaan useita tiedonlähteitä, mutta on tärkeää nostaa luotettava ja markkinaneutraali viranomaisten viestintäkanava paremmin elinkeinoelämän tietoisuuteen.

LIITE: SELVITYKSEN KYSYMYSLUETTELO

Yritysten kyberturvallisuus 2015

T1 Aloitamme tutkimuksen kysymällä ensin muutamia taustatietoja. Asemanne yrityksessä?
1. Toimitusjohtaja
2. Yrittäjä/omistaja
3. Muu johtaja
4. Päällikkötaso
5. Asiantuntija
6. Jokin muu, mikä?_____

T2 Yrityksenne liikevaihto vuonna 2014?
1. Alle 0,2 milj. euroa
2. 0,2–1 milj. euroa
3. 1,1–2 milj. euroa
4. 2,1–10 milj. euroa
5. 10,1–20 milj. euroa
6. 20,1–100 milj. euroa
7. Yli 100 milj. euroa

T3 Yrityksenne toimipaikkojen määrä?
kpl: _____

T4 Henkilöstön määrä?
1. 1–4
2. 5–9
3. 10–19
4. 20–49
5. 50–99
6. 100–199
7. 200–499
8. 500+

T5 Millaista kaupankäyntiä yrityksenne harjoittaa? Voitte valita useita.
1. Business-to-business (b2b) eli yritysten välinen kauppa
2. Business-to-consumer (b2c) eli kuluttajille suunnattu kauppa
3. Business-to-government (b2g) eli julkishallinnolle suunnattu kauppa

T6 Yrityksellänne on liiketoimintaa? Voitte valita useita.
1. Suomessa
2. Muissa EU-maissa
3. EU:n ulkopuolella

T7 Yrityksenne päätoimiala?
1. Teollisuus
2. Rakentaminen
3. Kauppa
4. Palvelut

Kysymykset

1. Mitkä seuraavista vaihtoehdoista ovat suurimmat kyberturvallisuuden uhat suomalaisille yrityksille? *Valitkaa kaksi mielestänne suurinta uhkaa.*
a. Yhtiön sisäinen uhka (omat työntekijät)
b. Phishing- ja haittaohjelmahyökkäykset
c. Tunkeutumiset
d. Palvelunestohyökkäykset
e. Hyökkäykset jotka kohdistuvat teollisiin tuotantoprosesseihin
f. Muu, mikä?_____

2. Mitkä ovat kolme suurinta estettä tehokkaan kyberturvallisuuden toteuttamisessa?
a. Rahoitus
b. Osaavien ammattilaisten löytämisen vaikeus
c. Nykyisen henkilökunnan tietotaidon ylläpitäminen kyberuhkien suhteen
d. Käyttäjien piittaamattomuus tietoturvallisuudesta ja kyberuhista
e. Kyberuhkiin liittyvän tiedon riittämättömyys
f. Turvallisuustoimiin ja menetelmiin liittyvän tiedon riittämättömyys
g. Tehottomat teknologiaratkaisut
h. Riittämätön integraatio kyberturvallisuuden ja liiketoiminnan välillä
i. Riittämätön integraatio kyberturvallisuuden ja muiden turvallisuuden osa-alueiden välillä (jatkuvuussuunnittelu, kriisienhallinta jne.)
j. Jokin muu, mikä? _____

3. Mitkä seuraavista vaihtoehdoista ovat raskaimmat seuraukset kyberhyökkäyksistä?
Valitkaa kaksi mielestänne suurinta uhkaa.
a. Aineettoman omaisuuden menetys
b. Negatiivinen julkisuus
c. Markkinaosuuden menetys
d. Kansallisen turvallisuuden vaarantuminen
e. Yksityisyyden (henkilökunnan tai asiakkaiden tiedot) loukkaus
f. Tuoton menetys – suora tai epäsuora
g. Muu, mikä?_____

4. Miten hyvin tunnette suomalaisten viranomaisten roolia ja toimintaa kyberuhkiin liittyen?
a. Erittäin hyvin
b. Melko hyvin
c. Melko huonosti
d. En tunne lainkaan

5. Oletteko saaneet jostakin käytännöllistä tietoa kyberuhkiin liittyen?
a. Kyllä
b. En

6. (OHJELMOINTI: Jos vastannut KYLLÄ edellisessä kysymyksessä, kysytään)
Mistä saitte tällaista tietoa? AVOIN

7. Miten organisaationne havaitsisi yrityksenne tietoverkossa käynnissä olevan tunkeutumisen?
a. Havaitsisimme sen itse käyttäen omia torjunta- ja hälytysjärjestelmiämme
b. Käyttäjämme tunnistaisivat sen ja ilmoittaisivat eteenpäin
c. Tunnistaisimme itse, koska tarkastamme ja analysoimme lokejamme ja arvioimme niistä ilmenevää uhkaan olemassaoloon liittyvää tietoa
d. Kotimaiset lainvalvontaviranomaiset tai tiedusteluorganisaatiot varoittaisivat meitä
e. Kolmas taho, kuten internet operaattori tai palveluntarjoaja, ilmoittaisi meille
f. Me emme todennäköisesti havaitsisi käynnissä olevaa tunkeutumista

8. Minkälaista tietoa luulette tunkeutujien etsivän?
a. Ylempään johtoon kuuluvien henkilökohtaista tietoa
b. Henkilökunnan jäseniin liittyvää tietoa, kuten nimet, vastuualueet ja yksiköt
c. Tietoa alihankkijoista, yhteistyökumppaneista, tavarantoimittajista tai asiakkaista
d. Immateriaalista omaisuutta tai luottamuksellista tietoa tuotteistamme tai palveluistamme
e. Tietoverkkoonne liittyvää tietoa kuten verkon arkkitehtuuri, asetukset tai tarkoitus
f. Me emme osaa sanoa millaista tietoa vietäisiin tunkeutumisen yhteydessä

9. Minkä tyyppistä tietoa olette menettäneet tietoverkkotunkeutumisten vuoksi?
a. Ylempään johtoon kuuluvien henkilökohtaista tietoa
b. Henkilökunnan jäseniin liittyvää tietoa, kuten nimet, vastuualueet ja yksiköt
c.Tietoa alihankkijoista, yhteistyökumppaneista, tavarantoimittajista tai asiakkaista
d. Immateriaalista omaisuutta tai luottamuksellista tietoa tuotteistamme tai palveluistamme
e. Tietoverkkoonne liittyvää tietoa kuten verkon arkkitehtuuri, asetukset tai tarkoitus
f. Me emme osaa sanoa millaista tietoa on viety

10. Miten organisaationne on järjestänyt tietoturvallisuusvastuut johtotasolla?
a. Meillä on kokoaikainen nimetty tietoturvallisuusjohtaja tai -päällikkö
b. Meillä on kokoaikainen IT-johtaja tai -päällikkö, joka vastaa tietoturvasta varsinaisen tehtävän ohella
c. Meillä on kokoaikainen johtaja tai päällikkö, joka vastaa tietoturvasta riskienhallinen tai yritysturvallisuuden osana
d. Meillä ei ole nimettyä tietoturvallisuusjohtajaa tai –päällikköä, vaan tietoturva on yleisesti IT-osaston vastuulla
e. Meillä ulkopuolinen palveluntarjoaja, joka tarjoaa tietoturvallisuusjohtajan tai -päällikön
f. Tietoturva on vastuutettu it-tuelle
g. Tietoturva on vastuutettu oman toimen ohella päällikkötason henkilölle tai toimitusjohtajalle
h. Meillä ei ole vastuutettu tietoturvallisuusasioita

11. Tietääkö henkilökuntanne miten toimia, jos he epäilevät tunkeutumista tietojärjestelmiinne?
a. Kyllä
b. Ei

12. Onko teillä käytössä käytännössä toimivia suunnitelmia tunkeutumisten varalle?
a. Kyllä
b. Ei

13. (Jos vastannut KYLLÄ edelliseen kysymykseen, kysytään)
Mitä asioita suunnitelmiin on sisällytetty?
a. Tieto siitä keneen olla yhteydessä, jos epäilee tunkeutumista
b. Ohjeet siitä mitä tehdä ensimmäisenä, jos epäilee tunkeutumista
c. Päätelaite (pc, älypuhelin, läppäri jne) Irti verkosta (otetaan yhteyskaapeli irti tai katkaistaan langaton yhteys)
d. Print screen (tästä saadaan talteen näytön näkymä myöhempää selvittelyä varten)
e. Koneen jättäminen koskemattomaksi, jotta sitä voidaan tutkia
f. Tilanteen kuvaus
g. Muuta, mitä_____

14. Oletteko koskaan harjoitelleet suunnitelmienne toimivuutta jollakin seuraavista tavoista?
a. Neuvotteluhuoneharjoitus (niin sanottu karttaharjoitus vailla käytännön toimia)
b. Käytännön harjoitus ulkopuolista tunkeutujaa vastaan
c. Muu, mikä? _____
d. Emme ole harjoitelleet

15. Oletteko varautuneet kyberuhkiin seuraavin tavoin konkreettisesti tai suunnitelmilla?
a. Järjestelmällinen suunnitelma tilannekuvan muodostamiseksi (datan kopiointi) tutkintaa ja puhdistustoimenpiteitä sekä loppuraportointia varten
b. Järjestelmä- ja verkkolokien (palomuuri, http, ad, dhcp, vpn) kerääminen kaikista järjestelmistä mahdollisimman pitkältä ajalta
c. Tutkinnassa tarvittavan laitteiston, ohjelmiston ja tutkintakyvyn ennakkoon hankinta
d. Yhteydenotto viranomaiseen
e. Palvelusopimus yrityksen kanssa, joka tarjoaa järjestelmiin tunkeutumisen ja haittaohjelmien tutkintaa
f. Emme ole varautuneet

16. Onko teillä vahvistettua koulutus- ja harjoitusohjelmaa kyberturvallisuuteen liittyen?
a. Kyllä
b. Ei

17. Ovatko kyberuhkiin liittyvät harjoitukset osa muihin liiketoimintaa uhkaaviin uhkiin liittyvää harjoittelua?
a. Kyllä
b. Ei

18. Oletteko viimeisen neljän vuoden aikana kohdistaneet kyberturvallisuuteenne jotain seuraavista toimenpiteistä?
henkilökunnan kouluttaminen
a. kyberturvallisuuteen liittyvien ohjeiden laatiminen henkilökunnalle
b. kyberturvallisuusammattilaisen palkkaaminen
c. kyberturvallisuuspalvelujen hankkiminen alan palveluntarjoajalta
d. kyberturvallisuusohjelmistojen ja -työkalujen hankkiminen
e. kyberturvallisuuden budjetoiminen vuositasolla
f. kyberturvallisuudesta vastaavan henkilön nimeäminen
g. kyberturvallisuuspolitiikan laatiminen
h. jotain muuta, mitä_____?

19. Mainitkaa tilanteita, joissa kyberturvallisuutenne on onnistunut? AVOIN

20. Mainitkaa tilanteita, joissa kyberturvallisuutenne on pettänyt? AVOIN

YRITYKSIIN KOHDISTUVAT KYBERUHAT 2019

Helsingin seudun kauppakamari
Kalevankatu 12, 00100 HELSINKI
puh. 09 228 601, www.helsinki.chamber.fi