ETLA Muistio | Brief | 93 14.12.2020

Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät?

Juri Mattila
Elinkeinoelämän tutkimuslaitos
juri.mattila@etla.fi

Jyrki Ali-Yrkkö
Elinkeinoelämän tutkimuslaitos
jyrki.ali-yrkko@etla.fi

Timo Seppälä
Elinkeinoelämän tutkimuslaitos
timo.seppala@etla.fi

Suositeltava lähdeviittaus:
Mattila, Juri, Ali-Yrkkö, Jyrki & Seppälä, Timo (14.12.2020). ”Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät?”.

ETLA Muistio No 93.
https://pub.etla.fi/ETLA-Muistio-Brief-93.pdf

Tiivistelmä

Kyberuhat yleistyvät erittäin nopeasti maailmalla. Suomessa esim. tietomurtojen määrä on kaksinkertaistunut parissa vuodessa. Kyberhyökkäysten taloudellisten kustannusten on arvioitu kasvavan sitäkin nopeammin. Tarkkaa käsitystä kyberuhkien taloudellisista vaikutuksista Suomen kansantalouteen ei kuitenkaan ole. Erityistesti mikroyritysten kyberturvasta tiedetään toistaiseksi tässä suhteessa hyvin vähän.

Vaikka Suomen yritysten kyberturva onkin Euroopan keskitasoa vahvempaa, on Suomi jäämässä kehityksen kärjestä useilla eri mittareilla arvioituna. Erityisesti tietovuodot vaikuttavat tuottavan kotimaisille yrityksille poikkeuksellisen paljon haasteita.

Myös kyberturvallisuustuotteiden ja -palvelujen kysyntä kasvaa maailmalla nopeasti. Suomessa alan kasvua rajoittaa kuitenkin akuutti kyberturvan osaamisvaje. Jopa 60 % kotimaisista kyberturva-alan yrityksistä kokee pulaa alan huippuosaajista. Suomen panostaessa digitaitojen kehittämiseen jopa eniten koko Euroopassa lienee syytä pohtia, kohdistuuko Suomessa tekeminen kyberturvan näkökulmasta oikeisiin asioihin.

Abstract

The New Cybersecurity Landscape – How Are Finnish Companies Faring?

Cyber threats are rapidly increasing around the world. In Finland, the amount of data breaches has doubled in a couple of years. The cost of being targeted for a cyber attack is estimated to increase even more rapidly. However, the economic effects of cyber threats on the Finnish economy are not comprehensively understood. Especially, very little is known about the state of microenterprises in this regard.

While the level of cybersecurity in Finnish companies is above the European average, Finland is falling behind the top countries according to many different indicators. Especially data leaks appear to be particularly challenging for Finnish companies.

The global demand of cybersecurity products and services is growing quickly. In Finland, however, this growth is restricted by a shortage of skilled cybersecurity professionals. As Finland invests heavily in the improvement of digital skills, the question arises whether these efforts are focused correctly in regards to competences in cybersecurity.

KTM **Juri Mattila** on Elinkeinoelämän tutkimuslaitoksen tutkija ja Aalto-yliopiston väitöskirjatutkija.

KTT **Jyrki Ali-Yrkkö** on Elinkeinoelämän tutkimuslaitoksen tutkimusjohtaja ja Etlatieto Oy:n toimitusjohtaja.

TkT **Timo Seppälä** on Elinkeinoelämän tutkimuslaitoksen johtava tutkija ja Aalto-yliopiston työelämäprofessori.

M.Sc. (Econ. & B.A.) **Juri Mattila** is a Researcher at ETLA Economic Research and a Doctoral Candidate at Aalto University.

D.Sc. (Econ.) **Jyrki Ali-Yrkkö** is a Research Director at ETLA Economic Research and the CEO at Etlatieto Oy, ETLA's subsidiary.

D.Sc. (Tech.) **Timo Seppälä** is a Researcher at ETLA Economic Research and a Professor of Practice at Aalto University.

Kiitokset: Tämä muistio pohjautuu aiempaan julkaisuun Mattila, J., Mäkäräinen, K., Pajarinen, M., Seppälä, T., Ali-Yrkkö, J. & Tervo, E. (2020). Digibarometri 2020: Kyberturvan tilannekuva Suomessa. Taloustieto Oy, Helsinki. Kiitämme hanketta rahoittaneita seuraavia tahoja: Business Finland, liikenne- ja viestintäministeriö, Elinkeinoelämän keskusliitto EK sekä Suomen Yrittäjät.

Acknowledgements: This brief is based on the earlier publication Mattila, J., Mäkäräinen, K., Pajarinen, M., Seppälä, T., Ali-Yrkkö, J. & Tervo, E. (2020). Digibarometer 2020: The status of cybersecurity in Finland Taloustieto Oy, Helsinki. The authors would like to thank the following funders: Business Finland, the Ministry of Transport and Communications, the Confederation of Finnish Industries, and Suomen Yrittäjät.

Avainsanat: Kyberturvallisuus, Digitalisaatio, Mikroyritys, Kansainvälinen kilpailukyky

Key words: Cybersecurity, Digitalization, Microenterprise, International competitiveness

JEL: L86, M15, O33

Kyberuhkien tilannekuva on mullistunut lyhyessä ajassa

Kyberuhat aiheuttavat nykyisellään maailmassa vuosittain satojen miljardien eurojen menetykset yksilöille, yrityksille ja julkisille sektoreille. Vuonna 2018 tietoturvayhtiö McAfee ja ajatushautomo CSIS arvioivat kyberrikollisuuden maailmanlaajuisiksi kustannuksiksi 600 miljardia euroa – eli karkeasti noin 0,8 % koko maailman vuotuisesta bruttokansantuotteesta (Lewis, 2018).

Pari vuotta sitten pelkästään Yhdysvalloissa kyberhyökkäysten aiheuttamiksi kustannuksissa arvioitiin 57–109 miljardia dollaria (The Council of Economic Advisers, 2018). Samassa raportissa nostettiin esiin myös se, että terveydenhoito, rahoitusala ja koulutus ovat houkuttelevia kohteita tietoturvahyökkäyksille.

Kyberuhkien kasvu ei ole sittemmin ainakaan hidastunut. Esimerkiksi F-Securen hunajapurkkiverkosto havaitsi vuonna 2019 yhteensä 5,7 miljardia kyberhyökkäystä maailmanlaajuisesti. Edellisvuonna vastaava lukema jäi noin miljardiin, ja vuonna 2017 järjestelmä havaitsi kyberhyökkäyksiä noin 800 miljoonaa (F-Secure, 2020).

Kyberrikollisuus kasvaa myös Suomessa

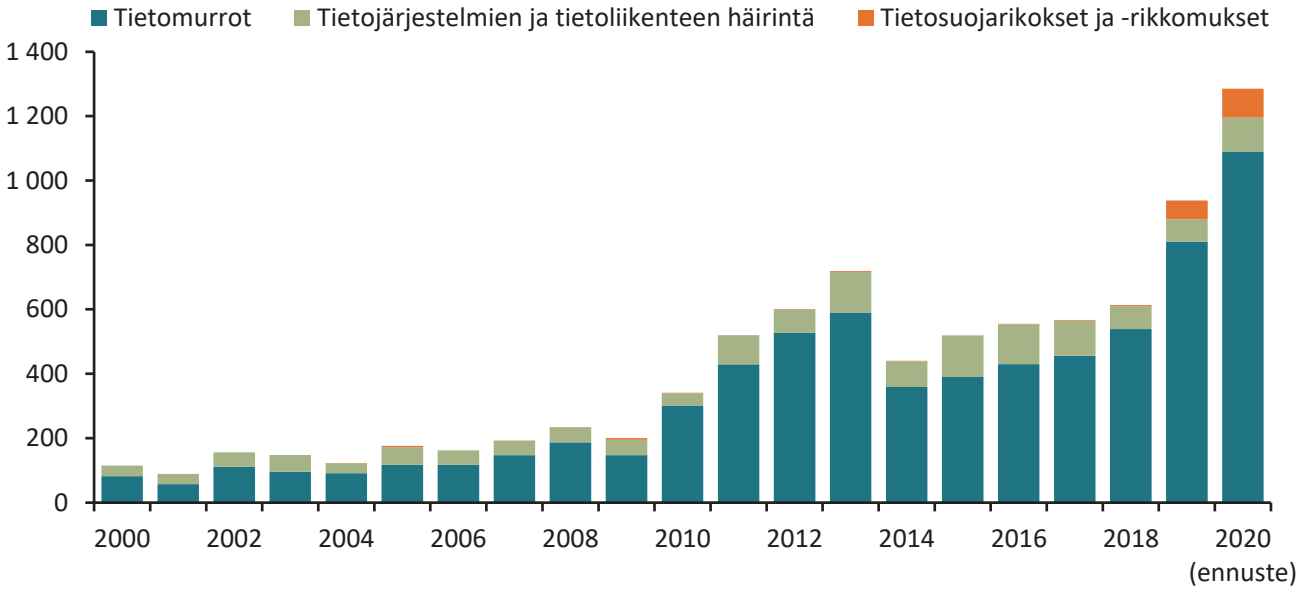
Mobiilin internetin syntymisen ja finanssikriisin jälkeen Suomessa poliisin tietoon tullut kyberrikollisuus on kasvanut selvästi (kuvio 1). Pienen tasaantuman jälkeen rikollisuus on tänä ja viime vuonna lähtenyt erittäin voimakkaaseen kasvuun. Erityisesti tämä näkyy tietomurroissa, joiden määrä on yli tuplaantunut kahdessa vuodessa. Tietomurtojen ennakoitu lukumäärä vuonna 2020 onkin jo suunnilleen sama kuin koko vuosituhannen ensimmäisen vuosikymmenen aikana yhteensä.

Myös tietojen kalastelu ja verkkohuijaukset ovat yleistyneet

Viimeisen vuoden aikana kyberhyökkäykset ja verkkohuijaukset ovat Suomessa lisääntyneet merkittävästi myös laajemmin. Esimerkiksi Kyberturvallisuuskeskukselle vuonna 2020 ilmoitettujen verkkohuijausten ennakoitu lukumäärä on yli viisinkertainen viime vuoteen verrattuna (kuvio 2).

Verkkoon kytkettyjen laitteiden (engl. Internet of Things, IoT) tietoturvaongelmien yleistyminen on ollut tahdiltaan sitäkin hurjempaa. Vaikkakin lukumäärältään edel-

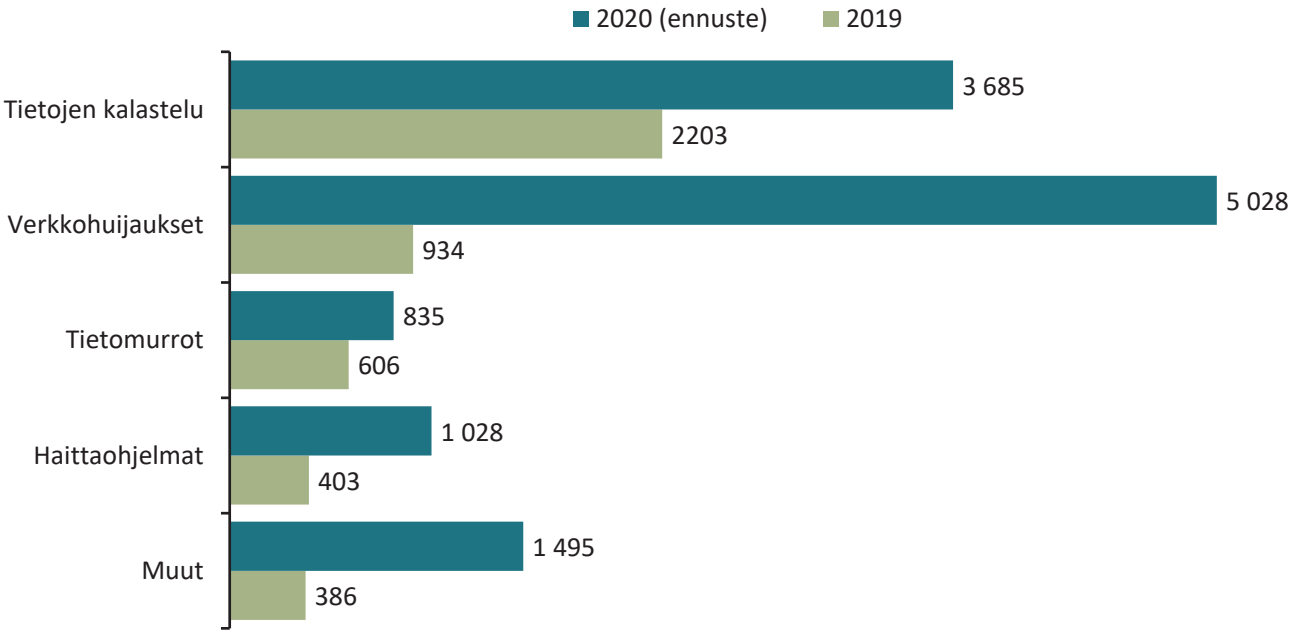
Kuvio 1 **Poliisin tietoon tullut kyberrikollisuuden määrä Suomessa vuosina 2000–2020, kpl**



Kuvion luvut sisältävät kaikki rikosten törkeysasteet sekä yritykset.

Aineistolähde: Poliisihallitus (soveltaen).

Kuvio 2 **Kyberturvallisuuskeskuksen käsittelemät tapaukset vuosina 2019–2020, kpl**



Aineistolähde: Kyberturvallisuuskeskus (soveltaen).

leen pieni joukko, ovat niihin liittyvät havainnot tämän vuoden ennusteessa yli kymmenkertaiset vuoteen 2019 verrattuna.

Kokonaisuutena Kyberturvallisuuskeskuksen käsittelemät kyberturvallisuuspoikkeamat ovat lähes kolminkertaistumassa kuluvan vuoden aikana. Kasvu on ollut hurjaa.

Hyökkäyksillä on myös hintansa

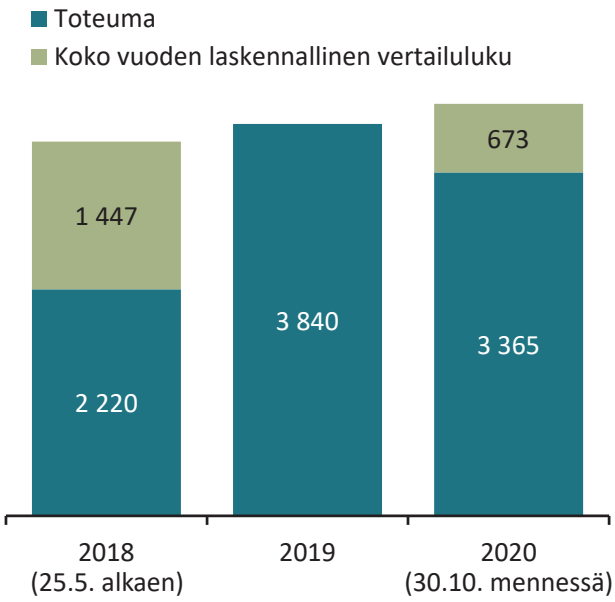
Parhaan tietomme mukaan Suomessa ei ole käsitystä siitä, millaisia kustannuksia kyberhyökkäykset ovat kaiken kaikkiaan aiheuttaneet. Muusta maailmasta tehdyt havainnot viittaavat kuitenkin siihen, että kyberhyökkäysten määrän lisäksi niiden aiheuttamat vahingot ovat yhä suurempia.

Esimerkiksi tietoturvayhtiö Radwaren selvityksen mukaan kyberhyökkäyksistä aiheutuvat taloudelliset kustannukset ovat viime vuosina kasvaneet hyökkäysten lukumäärää nopeammin. Kun vuonna 2018 kyberhyökkäyksen kohteeksi joutumisen keskimääräinen kustannus suuryrityksille oli noin 3 miljoonaa dollaria, oli hintalappu vuoteen 2019 tultaessa kohonnut 4,6 miljoonaan dollariin. Lisäksi yli 10 miljoonaa dollaria maksaneiden kyberhyökkäysten osuus oli kaksinkertaistunut edellisvuodesta, kohoten 13 %:iin tapauksista. (Radware, 2019).

Myös pienten yritysten kokoluokassa kyberuhkien merkitsevyys kasvaa. Vuonna 2018 Cisco raportoi kyberhyökkäyksen kohteeksi joutumisen maksavan pienyrityksille keskimäärin puoli miljoonaa dollaria (Cisco, 2018). Lisäksi muun muassa Euroopassa GDPR-lainsäädännön mahdollistamat sanktiot yrityksille tietoturvan laiminlyönneistä ovat lisänneet taloudellisten seuraamusten uhkaa niin suurten kuin myöskin pienten yritysten näkökulmasta. Yritysten GDPR-ilmoitukset tietoturvaloukkauksista tietosuojavaltuutetun toimistolle ovat niin ikään kasvamaan päin (katso kuvio 3).

On siis selvää, että kyberuhat aiheuttavat yhteiskunnalle mittavia ja kasvavia taloudellisia menetyksiä. Kyberuhkien kasvu vaikuttaa myös esimerkiksi digitaalista kulutuskysyntää laskevasti. Esimerkiksi vuonna 2015 eurooppalaisista 39 % ja suomalaisista 50 % jätti joitakin digitaalisia tuotteita tai palveluita käyttämättä niihin liittyvien turvallisuushuolien vuoksi. Vuoden 2019 vertai-

Kuvio 3 **Yritysten GDPR-ilmoitukset tietoturvaloukkauksista tietosuojavaltuutetun toimistolle, kpl**



Vuosien 2018 ja 2020 luvut sisältävät toteutuneet ilmoitukset (tumma) sekä projektiot koko vuoden ajalle suhteutettuna (vaalea).

Lähde: Tietosuojavaltuutetun toimisto (soveltaen).

lussa vastaava osuus oli Euroopassa jo 44 % ja Suomessa jopa 58 % (Mattila et al., 2020 perustuen Eurostatin (2020a) tietoihin).

Taloudellisten menetysten lisäksi kyberhyökkäykset voivat aiheuttaa erittäin suuria inhimillisiä kärsimyksiä. Terveystietojen tai muiden arkaluonteisten tietojen vuotaminen verkkoon saattaa aiheuttaa pysyviä pelkotiloja siitä, milloin ne mahdollisesti tulevat esiin. Syksyllä 2020 Suomessa koettu terveystietoja koskeva tietomurto antoi tästä äärimmäisen ikävän esimerkin.

Suomi kompuroi tietoturvassa

Kyberturvahaasteet kohdistuvat erilaisiin yrityksiin eri tavoin. Yleisesti ottaen kyberturvaongelmat ovat sitä yleisempiä, mitä suuremmasta yrityksestä on kyse.

Vuonna 2019 pienten, 10–49 henkilöä työllistävien yritysten kyberturvaongelmat olivat Suomessa jonkin verran muita EU-maita yleisempiä. Kun EU28-maissa kyberturvaongelmia oli kokenut 11 % pienyrityksistä, Suomessa vastaava lukema ylsi 16 %:iin. Kaikkein selvimmin pienyritysten kyberturvaongelmat liittyivät niin Suomessa kuin muuallakin Euroopassa palvelukatkoksiin esimerkiksi palvelunestohyökkäysten sekä kiristyshaittaohjelmien seurauksena. Toiseksi eniten ongelmia aiheutti tietojen tuhoutuminen esimerkiksi haittaohjelman takia tai ICT-laitteiden tuhoutumisesta tai varkaudesta johtuen (Mattila et al., 2020 perustuen Eurostatin (2020b) tietoihin).

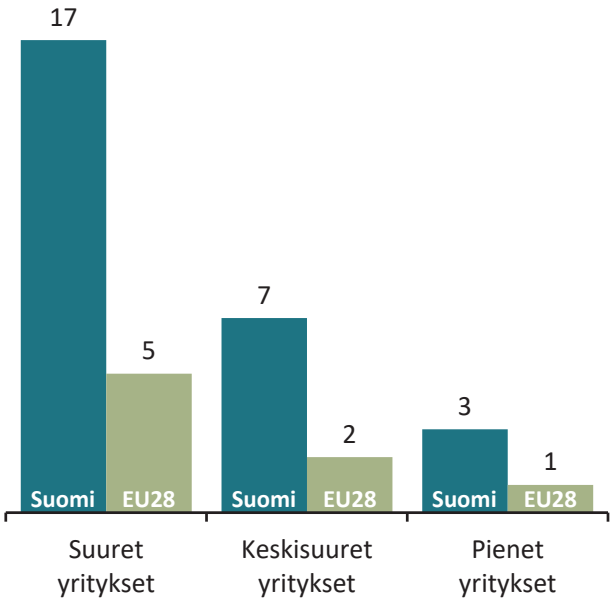
Mitä suurempi yritys, sen houkuttelevampi kohde

Keskisuurten yritysten tilanne oli Suomessa niin ikään selkeästi EU-maiden keskiarvoa hankalampi. Kun EU:ssa kyberturvaongelmia oli näistä yrityksistä kokenut keskimäärin 17 %, oli Suomessa vastaava määrä yli neljännes. Suomalaisten keskisuurten yritysten kokemissa kyberturvaongelmissa korostuvat erityisesti luottamuksellisten tietojen päätyminen vääriin käsiin esimerkiksi tietojärjestelmämurroista, tietojen kalastelusta sekä työntekijöiden virheellisestä menettelystä johtuen.

Kun vuonna 2019 Euroopassa keskimäärin 2 % keskikokoisista yrityksistä raportoi joutuneensa tietovuodon kohteeksi, oli vastaava luku Suomessa jopa 7 % (kuvio 4). Suomen osuus on varsin huomattava, sillä lukema oli selvästi EU28-maiden korkein.

Myös vähintään 250 henkilöä työllistävien suuryritysten kentässä Suomi sijoittui kyberturvallisuuteen liittyvien ongelmien esiintyvyydessä selkeästi EU:n keskitason yläpuolelle vuonna 2019. Suomessa kyberturvaongelmia kohdanneita suuryrityksiä oli 42 %, kun koko EU:n vastaava osuus oli 23 %. Suomessa suurten yritysten kyberturvallisuuden haasteissa korostuivat keskisuurten yritysten tavoin erityisesti tietovuodot jopa poikkeuksellisella tavalla. Kun esimerkiksi Ruotsissa tietovuotoihin liittyvien kyberturvallisuusongelmien esiintyvyys (8 %) oli lähellä EU-maiden keskitasoa (5 %), oli Suomen suuryrityksissä niiden esiintyvyys (17 %) yli kaksinkertainen Ruotsiin ja jopa yli kolminkertainen EU-maiden keskitasoon verrattuna (kuvio 4). Ainoa toinen yli kymmenen prosentin

Kuvio 4 **Tietovuodon kohteeksi joutuneet yritykset kokoluokittain (2019), %**



Lähde: Mattila et al. (2020), perustuen Eurostatin tietoihin.

osuuteen yltänyt EU28-maa tässä suhteessa oli Tanska. Siellä tietovuodon kohteeksi oli vuonna 2019 joutunut 12 % maan suuryrityksistä (Mattila et al., 2020 perustuen Eurostatin (2020b) tietoihin).

Toisin sanoen, tietovuodot vaikuttavat olevan suomalaisissa yrityksissä kautta linjan yli kolme kertaa yleisempiä kuin Euroopassa keskimäärin. Tilastojen valossa joka kuudes suomalainen suuryritys oli joutunut tietovuodon kohteeksi. Tietoturva näyttäytyykin siten Suomen yrityskentän aivan erityispiirteisenä haasteena.

Mikroyritysten kyberturva jää katveeseen

Kyberturvan tilastollinen tarkastelu keskittyy tyypillisesti pieniin – siis vähintään 10 henkeä työllistäviin – ja sitä suurempiin yrityksiin. Lähes 95 % suomalaisista yrityksistä on kuitenkin alle kymmenen henkilöä työllistäviä mikroyrityksiä. Kokonaisuutena arvioiden niiden rooli ei suinkaan ole kansantaloudellisesti vähäpätöinen. Yhteensä mikroyritykset työllistävät noin neljäsosan kotimaisen yrityskentän henkilöstöstä, ja muodostavat noin kuudesosan kotimaisten yritysten kokonaisliikevaihdosta (Tilastokeskus, 2018).

Mikroyritysten kyberturvallisuuden tilasta on kuitenkin tietoa saatavissa varsin niukasti. Onkin mahdollista, että merkittävä osuus kyberturvaongelmista jää Suomessa tilastointien ulkopuolelle. Jos vertailupohjaa haetaan Ruotsista, vuonna 2019 ruotsalaisista yhden hengen mikroyrityksistä 12 % oli kohdannut kyberturvaan liittyviä ongelmia. Kokoluokan kasvaessa myös kyberongelmat vaikuttavat lisääntyvän nopeasti: astetta suuremmista, 2–9 henkeä työllistävistä yrityksistä Ruotsissa ilmoitti ongelmia kokeneensa jo 27 % (Mattila et al., 2020 perustuen Eurostatin (2020b) tietoihin). Mikäli Ruotsin luvut oletetaan tässä suhteessa edustaviksi myös Suomen osalta, tarkoittaisi se vuositasolla vähintäänkin kymmeniä tuhansia kyberturvaongelmista kärsiviä kotimaisia yrityksiä, jotka eivät välttämättä näy nykyisissä tilastoissa.

Kuten aiemmin todettiin, pienten yritysten kyberturvaongelmissa korostuvat erityisesti palvelukatkokset sekä tietojen tuhoutuminen. Data onkin yksi pienten yritysten suurimpia ja yleisimpiä tunnistamattomia riskitekijöitä (Mattila et al., 2020). Vuonna 2018 Ciscon selvityksessä haastatelluista pienyrityksistä puolet arvioi ajautuvansa kuukauden sisällä tappiolliseksi, mikäli liiketoiminnan kriittisen datan käytettävyys katkeaisi kyberhyökkäyksen seurauksena (Cisco, 2018). Ei liene syytä olettaa, että mikroyritysten kestävyys olisi tässä suhteessa ainakaan pienyrityksiä parempi.

Suomi on jäämässä kehityksen kärjestä

Suomen yritysten varautuminen kyberuhkiin on viime vuosina monin tavoin parantunut aiemmista vuosista. Lähes kaikilla mittareilla arvioituna Suomi on kuitenkin jäämässä kehityksessä jälkeen erityisesti Tanskasta ja Ruotsista.

Esimerkiksi kyberturvavakuutusten yleisyydessä Suomi pärjää Euroopan unionin keskitasoa paremmin, mutta häviää selvästi pohjoismaisille kilpakumppaneilleen. Kun vuonna 2019 kyberturvavakuutus oli Suomessa käytössä 28 %:lla koko yrityskentästä, oli vastaava osuus Ruotsissa 39 % ja Tanskassa jopa 56 %. Myös Norja kiri vertailussa Suomen edelle 33 %:n osuudellaan.

Kun asiaa tarkastellaan yrityskokoluokittain, erityisesti suurten yritysten tilanne näytti Suomen kohdalla heikolta.

Niin Ruotsissa, Tanskassa kuin Norjassakin kyberturvavakuutusten hyödyntäminen suuryrityksissä oli vähintäänkin EU28-maiden keskitasolla (40 %). Suomessa sen sijaan suuryrityksistä kyberturvavakuutuksia toiminnassaan sovelsi ainoastaan noin kolmasosa. Suomen lukema jää siis selkeästi Euroopan unionin keskitason alapuolelle.

Pohjoismaiden välisessä mittelössä Suomi jää takamatkalle kaikissa yrityskokoluokissa. Vaikka pienten yritysten tarkastelussa Suomi pärjääkin koko Euroopan unionin keskitasoon (22 %) nähden hyvin, on Suomen takamatka tältäkin osin naapureihinsa verrattuna varsin huomattava. Kun kotimaisista pienyrityksistä hieman yli neljäsosalla (27 %) oli käytössään kyberturvavakuutus, löytyi vastaava vakuutus Norjassa kolmasosalta ja Ruotsissa 38 %:lta paikallisista pienyrityksistä. Pienyritysten osalta koko Euroopan paras tilanne oli kuitenkin Tanskassa, jossa jopa 57 % kyseisen kokoluokan yrityksistä sovelsi kyberturvavakuutusta toiminnassaan.

Vuoden 2019 tarkastelussa yritysten dokumentoitujen tietoturvakäytänteiden ajantasaisuus oli selvästi kohentunut muutaman vuoden takaisesta tilanteesta Euroopassa. Vaikka Tanskassa, Ruotsissa ja Suomessa taso oli parantunut kautta linjan, ottivat Tanska ja Ruotsi kehityksessä Suomea suuremman harppauksen. Vielä vuonna 2015 niin Suomessa, Ruotsissa kuin Tanskassakin niiden yritysten osuus, joiden dokumentoidut tietoturvakäytänteet oli päivitetty viimeisten 12 kuukauden aikana, oli yhtäläisellä tasolla (24–26 %). Vuonna 2019 sen sijaan Suomen osuus oli noussut 35 %:iin, mutta Ruotsissa osuus oli jo 39 % ja Tanskassa 42 % (Mattila et al., 2020 perustuen Eurostatin (2020b) tietoihin).

Vuonna 2019 säännöllistä tietojärjestelmien turvallisuustestausta harjoitti Euroopan unionissa reilu kolmasosa yrityksistä. Pohjoismaiden välisessä vertailussa toistuu Suomen kohdalla sama tarina kuin monilla muillakin mittareilla tarkasteltuna: Suomi (44 %) sijoittui EU28-maiden keskitason (36 %) paremmalle puolelle mutta jälleen kerran jäi jälkeen pohjoismaisista verrokeistaan Ruotsista (52 %) ja Tanskasta (49 %) (Mattila et al., 2020 perustuen Eurostatin (2020b) tietoihin).

Yrityskokoluokkakohtaisessa turvallisuustestauksen tarkastelussa parhaiten pohjoismaisiin kilpakumppaneihin nähden Suomessa suoriutuvat pienet yritykset. Kun Suomessa keskimäärin 40 % pienyrityksistä suoritti tietojärjestelmänsä säännöllisiä turvallisuustestauksia, oli vastaava lukema Ruotsissa 45 % ja Tanskassa 47 %. Keskikokoisten yritysten sarjassa Ruotsin ylivoima Suomeen nähden on murskaava. Kun Suomessa säännöllistä turvallisuustestausta harjoittavien keskisuurten yritysten osuus (57 %) heijasteli Euroopan unionin keskitasoa, oli Ruotsin keskisuurissa yrityksissä turvallisuustestaus jopa yhtä yleistä (74 %) kuin Euroopan unionin suuryrityksissä keskimäärin. Suuryritysten luokassa Suomi (79 %) sijoittui EU28-maiden keskitasoa paremmin, mutta jälleen kerran ei kuitenkaan Ruotsia (86 %) tai Tanskaa (84 %) paremmin (Mattila et al., 2020 perustuen Eurostatin (2020b) tietoihin).

Osaamispula jarruttaa Suomen kyberturvan kehitystä

Työn digitaalinen haastavuus lisääntyy kaikilla koulutustasoilla lähes kaikkialla Euroopassa. Kehitys näyttää kuitenkin tässä suhteessa olevan Pohjoismaissa muuta Eurooppaa nopeampaa, ja kaikkein nopeimmalta muutostahti näyttää Suomessa. Suomessa digitaalisen lisäkoulutuksen tarve näyttää myös jakautuvan muusta Euroopasta poikkeavasti, sillä vuonna 2018 tietoteknisen lisäkoulutuksen tarvetta kokivat Suomessa selvästi eniten kaikkein matalimmin koulutetut työntekijät (Mattila et al., 2020 perustuen Eurostatin (2020a) tietoihin).

Vaikka lisäkoulutuksen tarvetta koettiin Suomessa ylipäätään eurooppalaista keskiarvoa enemmän, toisaalta suomalaiset myös paransivat ICT-työtaitojaan muuta Eurooppaa selvästi hanakammin. Kun esimerkiksi Euroopan unionissa keskimäärin 9 % matalasti koulutetuista koki ajankäytön uusien tietoteknisten taitojen omaksumiseen lisääntyneen, Suomessa vastaava osuus oli jopa 33 %. Vaikkakin taitojen opetteluun käytettyjen lisäpanostusten vaikutukset näkynevät viiveellä, on syytä pohtia, kohdistuuko Suomessa tekeminen kyberturvan näkökulmasta oikeisiin asioihin.

Kyberturvan tulevia osaamistarpeita kartoittaneen tuoreen tutkimuksen mukaan kyberturvan huipputekijöiltä tullaan työmarkkinoilla lähitulevaisuudessa edellyttämään lähes 300 eri kyvykkyyttä, joissa yhdistyvät tekninen sekä laajempi liiketoiminnallinen ja strateginen osaaminen (Mattila et al., 2020 perustuen Concordian (2020) tietoihin). Suomen kyberturva-alan edunval-

vontajärjestö FISC:n tutkimuksen mukaan noin 60 % kotimaisista kyberturva-alan yrityksistä kokee pulaa alan osaajista. Osaamisvaje koettiin myös suurimmaksi haasteeksi suomalaisen kyberturvallisuusalan kasvun kannalta. Enimmäkseen suomalaiset kyberalan yritykset havittelevat osaajia Euroopan, Aasian ja Intian markkinoilta, sillä vain harvoin tarvittava henkilöresurssi löytyy kotimaan työmarkkinoilta (Mattila et al., 2020).

Johtopäätökset

Suomen yritysten kyberturvallisuuden tilanne on toistaiseksi edelleen eurooppalaista keskitasoa monin tavoin parempi. Useiden eri mittareiden valossa näyttää kuitenkin siltä, että Suomi on tältä osin hiljalleen jäämässä pohjoismaisten kärkimaiden kehityksen kelkasta. On ratkaisevaa Suomen digitalisaation kehityksen kannalta, saadaanko kyberturvallisuudessa nopea kurssikorjaus toteutettua, vai lipuuko Suomen yrityskanta hiljalleen kärjestä kyberturvan eurooppalaiseen keskikastiin.

Alle 10 henkilön yritysten tietoturvasta tarvitaan tietoa

Kotimaisten yritysten kyberturvallisuuden tilan kohentamiseksi voidaan hahmotella useita mahdollisia toimenpiteitä. Ensinnäkin mikroyritysten kyberturvasta kaivattaisiin parempaa tietoa. Mikroyritysten kyberturvan tilannetta ja sen roolia kansantalouden kehitykselle olisikin syytä kartoittaa Suomessa nykyistä tarkemmin. Talouden uudistumisen kannalta tärkeän potentiaalin omaavat korkean teknologian startup-mikroyritykset voivat olla houkuttelevia kohteita kyberrikollisille. Tuoreelle kasvuyritykselle kyberturvauhkien toteutuminen saattaakin tarkoittaa jopa koko yritystoiminnan päättymistä.

Suositeltavaa olisi, että esimerkiksi Tilastokeskus alkaisi kerätä kyberturvadataa myös alle 10 henkeä työllistävistä yrityksistä. Mikroyritysten kattavamman kyberturvanäkyvyyden pohjalta olisi paremmin arvioitavissa, tulisiko esimerkiksi korkean teknologian startupien kasvunhallintaa pyrkiä politiikkatoimenpitein tukemaan juuri kyberturvan näkökulmasta. Siirtymä mikroyrityksestä PK-luokkaan ja edelleen pienestä yrityksestä keskisuureksi on kyberturvallisuuden näkökulmasta usein haastava, sillä yrityksen houkuttelevuus kohteena kyberrikollisille ja yrityksen varautuminen kyberuhkiin eivät aina kehity samassa suhteessa liiketoiminnan ja yrityskoon kasvaessa.

Tietoturva-osaajista on pulaa – riittävätkö koulutuspanostukset?

Lähes kaksi kolmasosaa Suomen kyberturva-alan yrityksistä kärsii työvoimapulasta. Näiden lisäksi kyberturvaosaajia tarvitaan myös muissa yrityksissä julkista sektoria unohtamatta.

COVID-19-kriisi on varmasti lisännyt niin yritysten kuin yksityishenkilöidenkin digipalveluiden käyttöä, koskivat ne sitten etäpalavereja, verkkokauppaa tai muita digitalisaation muotoja.

Digitalisaatio etenee varmasti myös pidemmällä aikavälillä. Sen myötä tietoturvaosaajille on kasvavaa kysyntää. Voidaankin kysyä, ovatko Suomen nykyiset tietoturva-alan koulutuspanokset riittäviä. Koulutuspolitiikalla on syytä varmistaa, että tietoturva-asiantuntijoita valmistuu eri koulutusohjelmista riittävästi.

Yritysjohto on avainroolissa

Myös yritysten itsensä olisi syytä uudelleenarvioida, ovatko niiden panostukset kyberturvallisuuteen riittävällä ja ajanmukaisella tasolla. Ei riitä, että yrityksen kyberuhkiin varautumisen taso on tarkistettu lähivuosina, sillä kyberuhkien tilannekuva on muuttunut merkittävästi viimeisten kahden vuoden aikana. Operatiivisen johdon ja hallituksen tulisi ottaa kyberturvallisuus jatkuvan raportoinnin ja tarkastelun piiriin niin pienissä kuin suurissakin yrityksissä. Tähän liittyen Suomessa Kyberturvallisuuskeskus on laatinut muistion, joka keskittyy yrityksen hallituksen vastuuseen tietoturva-asioissa (Kyberturvallisuuskeskus, 2020).

Laajemmin ajateltuna verkottuva digitaalinen liiketoiminta vaatii yritysjohdolta ja yritysten hallituksilta systeemisempää kyberturvan ymmärrystä ja tietojärjestelmäkokonaisuuksien hallintaa. Yritysten tietojärjestelmäratkaisujen yhdenmukaistuessa yksittäisten hyökkäysmenetelmien potentiaalinen kohderyhmä kasvaa. Samalla laaja-alaistuvat myös jokaiseen yritykseen koh-

distuvat uhat, mikä on syytä tiedostaa myös pienten yritysten liiketoiminnan jatkuvuuden suunnittelussa.

Kyberturvallisuuden maailmassa eletään jatkuvaa kilpavarustelua hyökkääjien ja puolustajien välillä. Tämä lyhentää kyberturvallisuuteen liittyvien teknologioiden ja työkalujen elinkaarta. Kyberturvallisuuden hallitseminen vaatiikin toimijoilta jatkuvaa ja yhä nopeampaa reagointia sekä uuden oppimista.

Ylipäätään yritysten strategiassa tulisi siirtyä pois ajattelusta, jossa kyberturvallisuus nähdään vain pakollisena, tuottamattomana ja minimoitavana kulueränä.

Kyberturva on myös mahdollisuus

Kyberturvallisuus voi olla Suomelle myös mahdollisuus. Kyberturvallisuustuotteiden ja -palvelujen kysyntä kasvaa. Vuonna 2017 kyberturvayritysten liikevaihdoksi arvioitiin globaalisti jo yli 150 miljardia dollaria. Alan liikevaihdon on ennustettu kasvavan noin kymmenen prosentin vuosittaista vauhtia (Statista, 2018).

Mahdollisuus voi tulla myös toista kautta. Kyberturvallisuudella voi hyvinkin olla kasvava merkitys ostopäätöksissä. Mikäli esimerkiksi verkkokauppaa ei koeta turvallisena, potentiaalisten asiakkaiden ostot kohdistuvat muualle. Sama koskee myös yrityksiä, joilla on esimerkiksi henkilörekistereitä. Viimeistään syksyllä 2020 koettu mittava henkilötietojen vuotaminen ja niiden avulla kiristäminen nosti tietoturvallisuuden tärkeyden laajan yleisön tietoisuuteen.

Tarvitaan tarkempi tilannekuva

Käsityksemme mukaan tällä hetkellä ei ole tutkittua tietoa siitä, millaiset yritykset joutuvat tyypillisesti kyberhyökkäysten uhriksi. Tämän tietäminen auttaisi sekä yrityskenttää että julkisen sektorin toimijoita kohdistamaan omia toimenpiteitään.

Toinen keskeinen puute koskee tietoturvahyökkäysten aiheuttamia taloudellisia menetyksiä. Tietoturva-alan yritykset ovat tehneet omia arvioitaan, mutta ainakaan Suomessa asiaa ei ole tutkittu riippumattomien tahojen toimesta.

Lähteet

Cisco (2018). Small and Mighty. How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats. https://www.cisco.com/c/dam/global/hr_hr/solutions/small-business/pdf/small-mighty-threat.pdf (haettu 30.11.2020)

Concordia (2020). Participate in the definition of the European Cybersecurity Consultant profile. https://www.concordia-h2020.eu/news/participate-in-the-definition-of-the-european-cybersecurity-consultant-profile/ (haettu 9.12.2020)

The Council of Economic Advisers (2018). The Cost of Malicious Cyber Activity to the U.S. Economy. The Council of Economic Advisers, The United States. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf (haettu 30.11.2020)

Eurostat (2020a). Community survey on ICT usage in households and by individuals, https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Community_survey_on_ICT_usage_in_households_and_by_individuals (haettu 30.11.2020)

Eurostat (2020b). Digital economy and society statistics – enterprises https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_enterprises (haettu 30.11.2020)

F-Secure (2020). Attack Landscape H2 2019. F-Secure Blog. https://blog-assets.f-secure.com/wp-content/uploads/2020/03/04101313/attack-landscape-h22019-final.pdf (haettu 9.12.2020)

Kyberturvallisuuskeskus (2020). Kyberturvallisuus ja yrityksen hallituksen vastuu. Traficomin julkaisuja 2/2020, Traficom. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf (haettu 30.11.2020)

Lewis, J.A. (2018). Economic Impact of Cybercrime – No Slowing Down. McAfee & The Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/economic-impact-cybercrime (haettu 7.12.2020)

Mattila, J., Mäkäräinen, K., Pajarinen, M., Seppälä, T., Ali-Yrkkö, J. ja Tervo, E. (2020). Digibarometri 2020: Kyberturvan tilannekuva Suomessa. Helsinki: Taloustieto Oy.

Radaware (2019). C-Suite Perspectives: From Defense to Offense, Executives Turn Information Security into a Competitive Advantage; https://www.radware.com/c-suite-2019/ (haettu 30.11.2020)

Statista (2018). Size of the cybersecurity market worldwide, from 2017 to 2023. https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/ (haettu 10.12.2020)

Tilastokeskus (2018). Yritysten rakenne- ja tilinpäätöstilasto. Helsinki: Tilastokeskus. https://www.tilastokeskus.fi/tup/suoluk/suoluk_yritykset.html (haettu 10.12.2020)

Elinkeinoelämän tutkimuslaitos

ETLA Economic Research

ISSN-L 2323-2463
ISSN 2323-2463

Kustantaja: Taloustieto Oy

Puh. 09-609 900
www.etla.fi
etunimi.sukunimi@etla.fi

Arkadiankatu 23 B
00100 Helsinki