Jyväskylän koulutuskuntayhtymä

Keski-Suomen liitto
Regional Council of Central Finland

Keskisuomalaisten yritysten kyberturvallisuus

Selvitys toisen asteen koulutuksen roolista keskisuomalaisessa kyberturvallisuusosaamisessa

Tekijät
Jarmo Nevala
Jouni Aho

Päivitetty 29.08.2016

Sisältö

Kuviot

Taulukot

1 Johdanto

Suomen tavoite on olla kyberturvallisuuden kärkimaa. Keski-Suomen maakunta on keskeinen toimija tämän strategisen tavoitteen toteuttamisessa, sillä Jyväskylällä on/oli kansallinen koordinaatiorooli kyberturvallisuuden Innovatiiviset kaupungit 2014-2017 (INKA) -ohjelmassa. Keväällä 2016 Työ- ja Elinkeinoministeriö päätti uusista kärkihankkeista ja kyberturvallisuus ei mahtunut näiden joukkoon. Keski-Suomen suunnalla ehdittiin kuitenkin saamaan paljon uutta aikaiseksi, joten oli luontevaa jatkaa jo tehtyä hyvää työtä.

Ajankohtaisten kirjoitusten mukaan Suomessa ei tällä hetkellä ole kokonaiskuvaa kyberosaamisen nykytilasta ja tietotarpeesta. Kyberturvallisuuteen liittyvät toiminnot yrityksille ja yritysten työntekijöille kantautuvat lähinnä varoituksina ja ikävinä uutisina. Kybertietämyksen tarve on kasvava, se koskettaa jokaista meistä ja ulottuu osaksi kaikkea toimintaa. Kyberturvallisuus on jokaisen kansalaisen asia! Parhaana keinona kyberturvallisuuden omaksumiseen ja ylläpitämiseen pidetään sivistystä ja koulutusta. Kyberturvallisuus pitää nostaa kansalaistaidoksi.

Keski-Suomen maakuntastrategian (2014) mukaan kyberturvallisuus on keskeinen kilpailukykytekijä digitaloudessa, jossa bitit ja tietoverkot arkipäiväistyvät yhä enenevässä määrin ja tulevat olennaiseksi osaksi tuotteita, palveluita ja toimintatapoja. Tämä mahdollistaa uusia asiakkuuksia, ansaintamalleja ja markkinoita. Jyväskylällä kyberturvallisuuden kansallisena keskittymänä on avainasema kilpailuetujen hyödyntämiseen. Myös digitalouden edelläkävijyys vaatii uudenlaista orientaatiota palveluiden ja sisältöjen kehittämiseen. Menestyäkseen Keski-Suomen tulee olla sekä digitaalisten palveluiden ja sisältöjen vahva tuottaja, että niiden käytön vahva hyödyntäjä. Hyödyntäminen vaatii osaamista ja ymmärrystä kansalaisilta sekä tavallisilta mikro- ja pienyrityksiltä.

Tietoteknisten laitteiden ja järjestelmien toimimattomuus, tahattomina tai kyberhyökkäyksen kautta, aiheuttavat kielteisiä vaikutuksia liike-elämään, julkisiin palveluihin ja hallintoon ja siten koko yhteiskunnan elintärkeisiin toimintoihin. Kuitenkin keskeinen toimija kyberturvallisuuden ylläpitäjänä on yksittäinen henkilö. Vähäiselläkin ajattelemattomuudella, tietämättömyydellä tai välinpitämättömyydellä voi syntyä mittavat

vahingot, joita vakuutuksetkaan eivät korvaa. Syynä vahinkoihin useimmiten on ohjeistuksen, tiedotuksen, välinevalinnan ja/tai kouluttautumisen puute.

Toisen asteen kyber -hankkeen selvityksen avulla kartoitetaan opettajien käsityksiä kyberturvallisuudesta. Opetetaanko opiskelijoille kyberturvallisuuteen liittyviä suosituksia ja millaisia uhkia opettajat ovat kohdanneet työssä tai vapaa-ajallaan. Selvityksen avulla pyritään löytämään ne kriittiset osa-alueet, joihin tarvitaan lisäkoulutusta opettajille.

Osana hanketta selvitetään tyypillisten mikro- ja pk-yritysten kyberosaamisen koulutustarpeita. Tähän mennessä Keski-Suomessa osaamistarpeita on selvitetty korkeakoulujen ja kyberturvallisuuteen asiantuntijayritysten kanssa, mutta Toisen asteen kyber –hankkeen tavoitteena on laajentaa näkökulmaa yritysten suuntaan. Kyberturvallisuuden edelläkävijän rooliin tarvitaan korkeakoulujen kehittämisyhtiöiden, asiantuntijayritysten lisäksi myös toisen asteen koulutusta ja tavallisia yrityksiä.

Molemmat kyselytutkimukset toteutettiin keväällä 2016. Jyväskylän koulutuskuntayhtymän henkilöstölle suunnattuun kyselyyn vastasi 254 henkilöä. Keskisuomalaisille yrityksille toteutettuun kyselyyn vastasi 201 yritystä.

Selvityksen ovat laatineet Jarmo Nevala Jyväskylän ammattiopistosta sekä Jouni Aho Jyväskylän aikuisopistosta. Selvitys on osa hankkeen "Toisen asteen kyber" toimintaa. Hankkeen rahoittajana toimi Keski-Suomen Liitto.

2 Tutkimuksen taustat

Keski-Suomen Liitto hyväksyi syksyllä 2015 Jyväskylän koulutuskuntayhtymän Toisen asteen kyber -hankkeen. Hankkeen tavoitteena on luoda kokonaiskuva toisen asteen koulutuksen roolista ja merkityksestä Keski-Suomen kyberturvallisuusstrategian toteuttamisessa.

Hankkeen selvitys jakautuu kahteen eri osaan. Opetushenkilöstölle tehty kyselytutkimus, sekä Keski-Suomalaisille yrityksille tehty kyselytutkimus. Molempien tutkimusten pohjalta tehdään toimenpidesuunnitelma, miten kyberturvallisuutta pitäisi kehittää koulutuksessa.

Selvityksessä tutkitaan Jyväskylän koulutuskuntayhtymän opettajien käsityksiä kyberturvallisuudesta. Selvityksen tavoitteena on tukea ja kehittää opettajien omaa työtä. Tutkimustuloksista opettajat saavat paremman kokonaiskuvan kyberuhista ja siitä, miten uhkiin on osattu varautua.

Yrityskyselyyn on valittu satunnaisesti pieniä ja keskisuuria yrityksiä Keski-Suomen alueelta. Kyselyn avulla selvitetään miten yritykset ovat varautuneet kyberuhkiin ja onko yrityksiin kohdistunut näitä uhkia.

Hankkeen tavoitteet:

- Luoda kokonaiskuva toisen asteen koulutuksen roolista ja merkityksestä Keski-Suomen kyberturvallisuuden verkostoissa ja kyberturvallisuusstrategian toteuttamisessa.
- Selvittää Keski-Suomen pk- ja mikroyritysten kyberturvallisuusosaamisen koulutustarpeet toisen asteen koulutuksen näkökulmasta.
- Valmistella toisen asteen koulutukselle toimenpideohjelma kyberturvallisuuden edistämiseksi sekä yksilötasolla että Keski-Suomen pk- ja mikroyrityksissä

Toimenpiteet:

- Rakennetaan toisen asteen toimijoille osallistumisväylät maakunnan kyberturvallisuuden verkostoihin.

- Toteutetaan kysely ja haastatteluita Keski-Suomen tyypillisten pk- ja mikroyritysten kyberturvallisuuden osaamisen koulutustarpeista.
- Selvitetään kyberturvallisuuden tarpeet toisen asteen koulutuksessa:
    - tutkinnot, joita asia koskettaa
    - tutkinnon opettajien osaaminen ja linkittyminen verkostoon
    - opiskelijoiden osaamistavoitteet tutkinnon perusteissa
    - tulosten esittely työryhmissä ja tapahtumissa

Tulokset:

- Kokonaiskuva toisen asteen roolista ja merkityksestä Keski-Suomen kyberturvallisuuden verkostoissa
- Tilanneselvitys toisen asteen koulutuksen yhteistyöyritysverkoston kyberturvallisuusosaamisesta ja –koulutustarpeista
- Tilanneselvitys kyberturvallisuuden kouluttamisvalmiuksista ja opetushenkilöstön osaamisesta toisella asteella
- Toisen asteen koulutuksen toimenpidesuunnitelma kyberturvallisuuden edistämiseksi Keski-Suomen pk- ja mikroyrityksissä

Hyödyt:

- Eri koulutusorganisaatioiden keskinäinen työnjako selkiytyy
- Tulokset ovat suoraan alueen kyberturvallisuusyritysten hyödynnettävissä
- Selvityksessä paljastuvat maakunnan kyberturvallisuuden toisen asteen koulutustarpeet
- Herättävät tavallisten pienyritysten mielenkiinnon ja huolen suojautumisintresseistä (liiketoiminta, tuotannon/toiminnanhallinta) ja johtaa parempaan tietoturvauhkien ennakointiin.
- Keski-Suomen asema kyberturvallisuuden edelläkävijänä vahvistuu.

Tämän selvityksen aineiston hankintaan käytettiin Digium Enterprise kyselynhallintaohjelmistoa. Kysely suunnattiin toisen asteen koulutuksen opettajille, tarkempana kohderyhmänä Jyväskylän koulutuskuntayhtymään kuuluvien Jyväskylän

ammattiopiston, Jämsän ammattiopiston ja Jyväskylän aikuisopiston kaikki opettajat ja kouluttajat.

Oppilaitoskyselyyn vastasi yhteensä 254 henkilöä, joista 64 % (161) oli ammattiopiston henkilökuntaa ja 36 % (93) aikuisopiston henkilökuntaa. Kutsu kyselyyn lähetettiin sähköpostitse kaikkiaan 931 vastaajalle, jolloin vastausaktiivisuus oli noin 27 %.

Yrityskyselyyn vastasi yhteensä 201 yritystä, joista alle 10 henkilön yrityksiä oli 74 % (148) ja yli 10 henkilön yrityksiä 26 % (53). Tarkempi jaottelu löytyy kappaleesta 4. Tutkimus: Vastaajien taustatiedot. Kutsu lähetettiin sähköpostitse kaikkiaan 2276 keskisuomalaiselle yritykselle, jolloin vastausaktiivisuus oli noin 9 %.

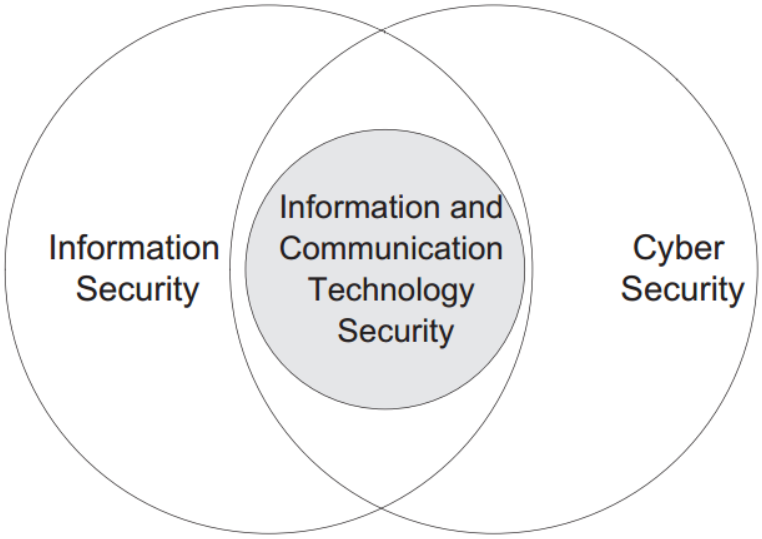
3 Mitä tietoturvallisuus ja kyberturvallisuus on

Kyberturvallisuus on nykypäivänä läsnä ihmisten arjessa ja sen merkitys kasvaa jatkuvasti. Yksi merkittävä tekijä tässä kohdalla on esineiden internet (Internet of Things, IoT) aikakauden kasvu ja tekniikan kehitys. Kymmenen vuotta sitten vain harvalla oli internetyhteys käytössä jatkuvasti, kun nykypäivänä se on melkein jokaisella ja useimmat kantavat sitä myös mukanaan.

Tietoturvallisuus on laaja käsite. Tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja saatavuuden takaamista. Luottamuksellisuudella tarkoitetaan sitä, että esimerkiksi jos tieto on luokiteltua tai muuten salassa pidettävää, sen voivat saada käyttöönsä vain sellaiset tahot, jolla on tiedonsaanti- ja käyttöoikeus siihen. Tietojärjestelmissä luottamuksellisuus toteutetaan normaalisti käyttöoikeuksien hallinnalla, käyttäjälle annetaan sekä vapaa-ajalla käytettäviin, että työtehtävissä käytössä oleviin järjestelmiin sellaiset oikeudet, jotka ovat tarpeen tehtävien hoitamisen kannalta. Tiedon eheydellä tarkoitetaan, että tieto ei saa muuttua hallitsemattomasti. Työtehtävissä tämä tarkoittaa, että tietoa saavat muuttaa vain sellaiset käyttäjät, joilla on siihen tarvittava käyttöoikeus, ja vain sallituilla keinoilla. Kyberturvallisuuden näkökulmasta esimerkiksi henkilö- ja väestötiedot, kansalaisten terveydenhoitoon liittyvät tiedot, julkishallinnon johtamisessa tarvittavat järjestelmät, pankkijärjestelmät, verotus, maanomistus- ja kiinteistötiedot sekä vakuutustiedot ovat sellaisia järjestelmiä ja tietoja, jotka eivät saa muuttua hallitsemattomasti ja joiden pitää kaikissa olosuhteissa olla palautettavissa. Tiedon saatavuudella tarkoitetaan, että tietojen pitää olla saatavilla niitä tarvitseville käyttäjille palvelussa. Rousku, 2014

Kyberturvallisuus keskittyy vahvasti ICT-järjestelmien turvaamiseen niiden toimintaa uhkaavia riskejä vastaan. Pääpaino on niissä ympäristöissä, jotka ovat yhteyksissä tietoverkkoihin ja ennen kaikkea internetverkkoon. Useimmat toteutuneet kyberturvallisuuden pettämiseen liittyvät uutiset koskevatkin internetverkon kautta tehtyjä kyberhyökkäyksiä. Hyökkäysten avulla on heikennetty tietoturvallisuutta (esim. päästy muuttamaan tietojen sisältöä), yksityisyyden suojaa (vuodettu henkilötietoja) sekä heikennetty toimintojen käytettävyyttä (tehty palvelunestohyökkäys ja estetty palveluiden toiminta). Rousku, 2014

Hyvään kyberturvallisuuteen ja tietoturvaan voidaan pyrkiä tiedostamalla yrityksen tai organisaation digitaalinen maailma ja havainnoimalla siihen liittyvät riskit. Tämän tiedon perusteella on mahdollista ennakoida ja ennen kaikkea estää tulevia tietoon ja digitaaliseen omaisuuteen kohdistuvia uhkia.



Kuvio 1. The relationship between information and communication security, information security, and cyber security (von Solms & van Niekerk 2013).

Tietoturvallisuuden (Information security), ICT:n (Information and communication technology security) ja kyberturvallisuuden (Cyber security) suhdetta toisiinsa voidaan esittää myös kuvion 1 pohjalta, jonka ovat laatineet von Solms & Van Niekerk (2013). Tietoturvallisuudella voidaan ajatella datainformaatiota ja kyberturvallisuudella niiden yhteyttä verkkoon. ICT voidaan sijoittaa näiden väliin esimerkiksi fyysisenä laitteena kuten tietokone. Esimerkiksi Datainformaatio – Tietokone – Internet.

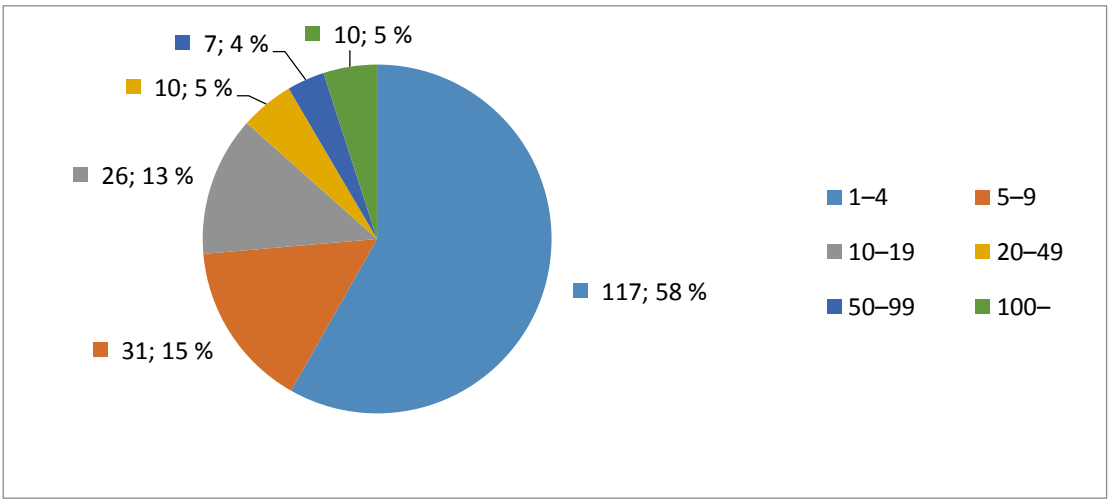
4 Tutkimus: Vastaajien taustatiedot

Tutkimukseen vastasi 201 keskisuomalaista yritystä/yrittäjää. Vastaajista 68 % kuului Suomen yrittäjien keskusjärjestöön ja 13 % Kauppakamariin. Yritysten järjestäytyneisyys (81 %) on melko aktiivista ja näin ollen myös yksi kanava mahdolliselle tukiverkostolle.

Taulukko 1. Vastaajien asema yrityksessä

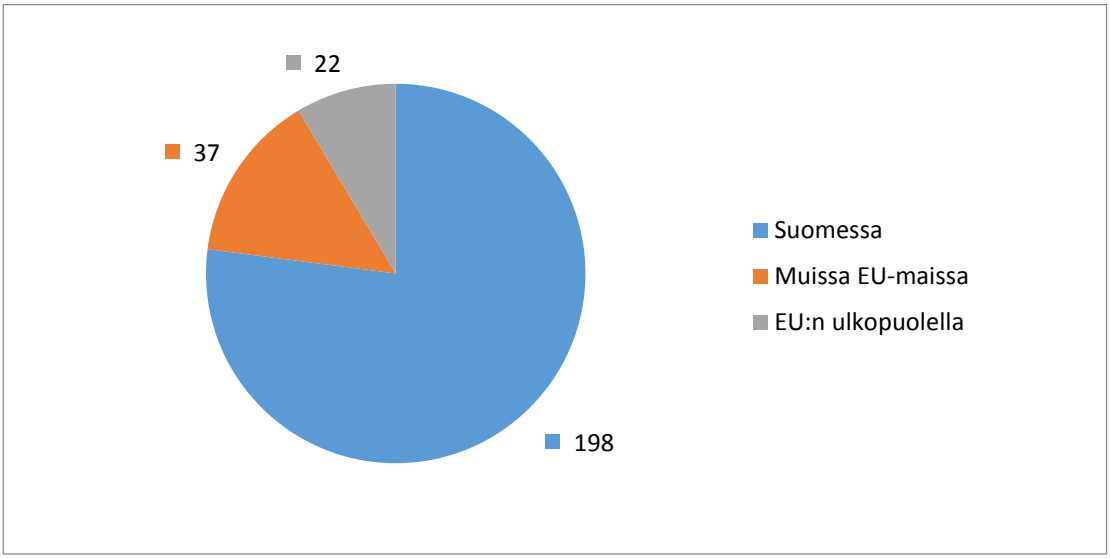
	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Toimitusjohtaja	43	21,39 %					
2.	Yrittäjä/omistaja	112	55,72 %					
3.	Muu johtaja	12	5,97 %					
4.	Muu työntekijä	24	11,94 %					
5.	Tietoturva-asioista vastaava henkilö	5	2,49 %					
6.	Tietohallinto-päällikkö	1	0,50 %					
7.	Jokin muu, mikä	4	1,99 %					
	Yhteensä	201	100 %					

Taulukossa 1 on kuvattuna vastaajien asema yrityksessä. Yli puolet vastaajista oli yrityksen omistajia (56 %). Tämä selittyy sillä, että yli puolet vastanneista yrityksistä oli kooltaan 1 - 4 hengen yrityksiä (58 %). Kokonaisuudessaan kyselyyn vastanneista 77 % on yrityksen johtajia (Toimitusjohtaja, Yrittäjä, Omistaja). Yrityksen tietoturvasta vastaavia henkilöitä oli vain kolme prosentti vastanneista.



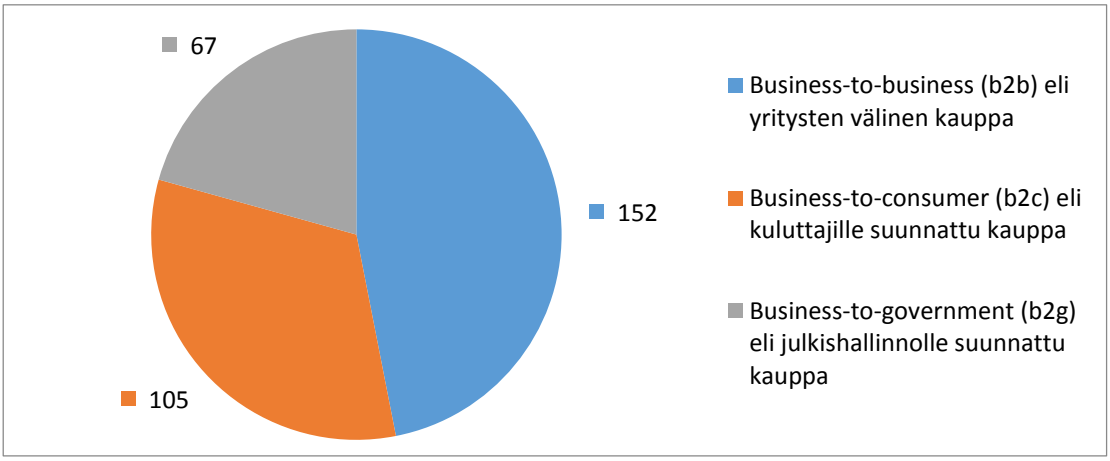
Kuvio 2. Yrityksen koko (montako työntekijää), N=201

Pääosa vastanneista yrityksistä oli 1 - 4 henkilön yrityksiä. Kuviossa 2 on esitettynä yritysten koot (määrä; prosenttiosuus). Pienien yrityksien (1-4 hlö) osuus oli 58 % (117) vastanneista. Tutkimuksen kannalta tämä on hyvä otos, koska lähtökohtana oli selvittää millaisia haasteita pienet yritykset kohtaavat tietoturvan parissa.



Kuvio 3. Yrityksen liiketoiminta-alue, N=201

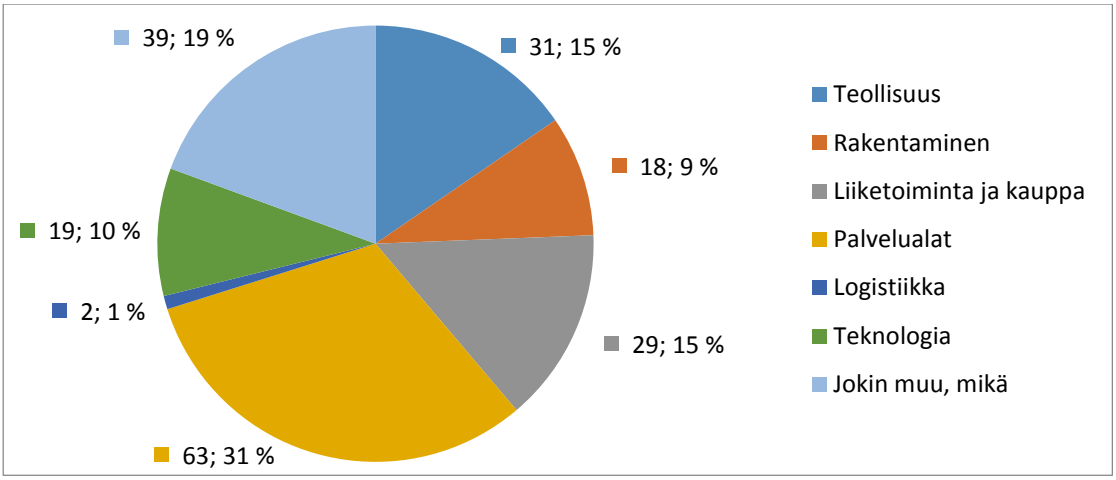
Pääosa vastaajista (kuvio 3) toimii Suomen markkinoilla (98 %). Osalla vastaajia on myös liiketoimintaa muissa EU-maissa (18 %) sekä EU:n ulkopuolella (11 %). Suluissa olevat prosenttiluvut ovat verrattuna kokonaisvastaajamäärään (N = 201). Osalla yrityksistä on liiketoimintaa jokaisella yllä mainitulla osa-alueella.



Kuvio 4. Millaista kaupankäyntiä yrityksenne harjoittaa? N=201

Vastaajien liiketoiminta jakaantuu melko tasaisesti jokaiselle osa-alueelle (kuvio 4). Suurimpana nousee esiin yritysten välinen kaupankäynti (76 %). Kuluttajille suunnattu kaupankäynti (52 %) on hieman pienempi ja viimeisenä tulee julkishallinnolle suun-

nattu kaupankäynti (33 %). Suluissa olevat prosenttiluvut on verrattuna kokonaisvastaajamäärään (N = 201). Osa yrityksistä tekee kaupankäyntiä jokaiselle osa-alueelle, minkä vuoksi kokonaisvastaajamäärä menee yli otosmäärän.



Kuvio 5. Yrityksen päätoimiala, N=201

Vastaajien päätoimiala jakautuu tasaisesti (kuvio 5) jokaiselle osa-alueelle. Suurimpana nousee esiin palvelualat (31 %). Jokin muu toimiala kohtaan vastattiin muun muassa metsäteollisuus, taloushallinto, asiantuntijapalvelut, konsultointi, turvallisuus ja majoitus.

5 Tutkimus: Tietoturvan huomioiminen

Keväällä 2016 hyväksyttiin EU-tietosuoja-asetus ja se tulee voimaan kahden vuoden siirtymäajan jälkeen. EU:n tietosuoja-asetus koskee lähtökohtaisesti kaikkea henkilötietojen käsittelyä EU:n jäsenvaltioissa. Asetus koskee sekä asiakkailta kerättäviä, että oman henkilöstön tietoja. Kun kyseessä on EU-asetus, sanktiot ovat myös samaa tasoa. Asetukseen on määritelty sanktioksi 4 % yrityksen globaalista liikevaihdosta. Valtiovarainministeriö, 2016.

Taulukko 2. Oletko tietoinen EU-lainsäädännöstä kyberturvallisuuteen liittyen?

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Kyllä	33	16,42 %					
2.	En	168	83,58 %					
	Yhteensä	201	100 %					

Vastaajista ainoastaan 16 % oli tietoinen EU-tietosuoja-asetuksesta (taulukko 2). Kysymys asettelu saattaa tässä kohdalla johtaa vastaajaa harhaan, sillä kaikki eivät osanneet yhdistää tätä tietosuoja-asetukseen.

Ristiintaulukoinnissa halusimme saada tarkennusta keitä nämä 33 vastaajaa ovat, jotka vastasivat EU-lainsäädäntö kysymykseen kyllä. Vastanneista 24 henkilöä oli yrityksen omistajia/yrittäjiä/toimitusjohtajia. Yrityksen kokoon verrattaessa, näistä 18 (55 %) vastausta tuli 1 - 4 hengen yrityksistä. Yli 20 henkilön yrityksistä vain 8 (30 %) oli tietoisia EU-lainsäädännöstä.

Taulukko 3. Millä laitteilla yrityksessänne on pääsy tietoverkkoon (internet)? N=201

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Pöytätietokoneilla	144	71,64 %					
2.	Kannettavilla tietokoneilla	164	81,59 %					
3.	Tablet-laitteilla	117	58,21 %					
4.	Älypuhelimilla	168	83,58 %					
5.	Yrityksen tuotantoon liittyvillä koneilla/laitteilla	24	11,94 %					
6.	Jokin muu, mikä	2	1,00 %					

Aikaisemmin internetyhteyttä käytettiin vain pöytätietokoneella, mutta tekniikan kehittyessä laitekanta on monipuolistunut. Taulukon 3 perusteella nykypäivänä yritykset käyttävät aktiivisesti älypuhelimia (84 %) työssään. Myös tablet laitteiden osuus on peräti 58 %. Nämä kaksi edellä mainittua muodostavat yhden suurimmista tietoturvariskeistä yrityksille, koska näitä laitteita ei useimmiten suojata tai osata suojata. Tabletti otetaan työmatkalle mukaan ja kytketään kiinni ensimmäiseen avoimeen langattomaan verkkoon miettimättä sen turvallisuutta. Kuinka monen eri järjestelmän tunnukset taas on tallennettu älypuhelimen apuohjelmiin tai itse laitteeseen?

Vastauksien perusteella voidaan myös tulkita, että pöytäkoneet ja kannettavat tietokoneet ovat vähentyneet yrityksissä. Ovatko älypuhelimet ja tablet-laitteet syrjäyttämässä tietokoneen? Jokin muu kohtaan tuli kaksi vastausta, jotka olivat maksupääte ja kassajärjestelmä.

Taulukko 4. Käytätkö työasioiden hoitamiseen muita kuin yrityksen laitteita?

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Kyllä	63	31,34 %					
2.	Ei	138	68,66 %					
	Yhteensä	201	100 %					

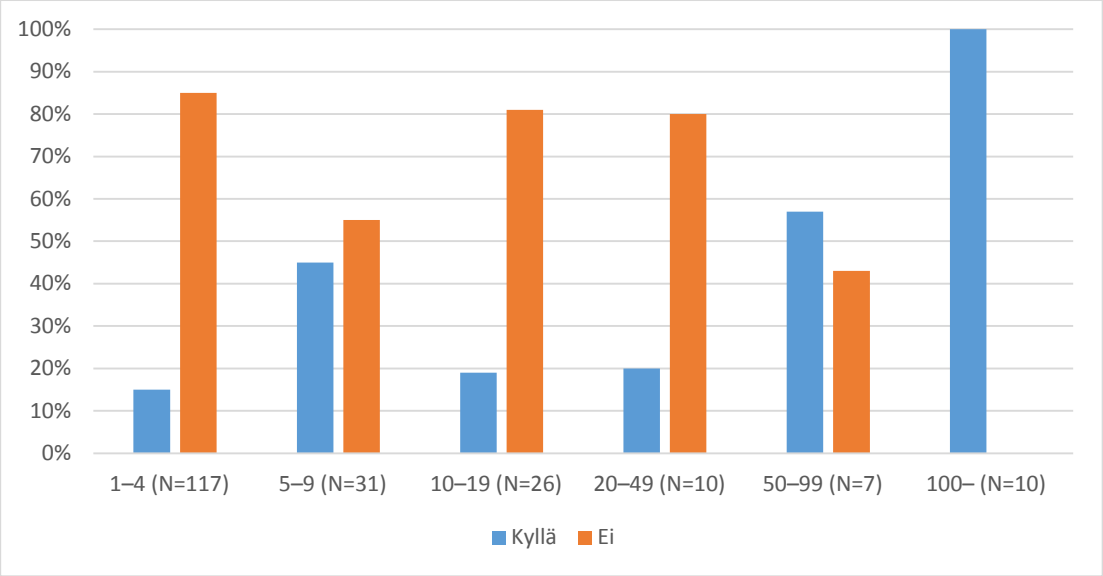
Peräti 31 % vastaajista käyttää työasioiden hoitamiseen omia laitteita. Tämä voi tarkoittaa esimerkiksi oman henkilökohtaisen puhelimen tai tablet-tietokoneen käyttämistä sähköpostin lukemiseen.

Henkilökohtainen laite aiheuttaa aina yritykselle riskitilanteen, koska se on uusi laite yrityksen järjestelmissä. Riskien näkökulmasta katsottuna henkilökohtaista laitetta voi käyttää myös perheenjäsen. Mikäli jokaisella käyttäjällä ei ole omaa käyttäjäprofiilia, niin on riskinä, että perheenjäsenet saavat eteensä salassa pidettävää materiaalia.

Taulukko 5. Onko yrityksessänne laadittu tietoturvaohje?

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Kyllä	52	25,87 %					
2.	Ei	149	74,13 %					
	Yhteensä	201	100 %					

Tietoturvaohjeistus (taulukko 5) on useimmiten yrityksen toimintamalli, missä määritellään esimerkiksi ohjeistukset mitä laitteita verkkoon saa kytkeä tai miten toimia, jos epäilee tietomurtoa. Ainoastaan 26 % yrityksistä oli laadittuna tietoturvaohjeistus.



Kuvio 6. Onko yritykselle laadittu tietoturvaohje

Kuviossa 6 on esitettynä tietoturvaohjeistuksen jakautuminen yrityskoon mukaan. Tulosten perusteella ainoastaan suuret yritykset ovat tehneet tietoturvaohjeistuksen. Pienissä yrityksissä on harvemmin tietohallintoa tai henkilöä joka vastaa tietoturva-asioista, mikä selittää vastausten jakaantumisen.

Taulukko 6. Valvotaanko yrityksessänne henkilöstön tietoturvaohjeen noudattamista?

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Kyllä	38	69,09 %					
2.	Ei	11	20,00 %					
3.	En osaa sanoa	6	10,91 %					
	Yhteensä	55	100 %					

Tutkimuksessa kysyttiin myös, että valvotaanko tietoturvaohjeistuksen (taulukko 6) noudattamista. Suurin osa valvoo, mutta silti 20 % vastaajista ilmoitti, että ohjeen noudattamista ei valvota. Taustalla saattaa olla tietämättömyys, mutta useimmiten ohjeistus voi olla epäselvä työntekijälle. Vaihtoehtoisesti saatetaan myös ajatella, että tietoturvaohje on tehty vaikeuttamaan normaalia työskentelyä. Dokumentin merkitystä ei välttämättä ymmärretä.

Taulukko 7. Mitä seuraavia asioita yrityksenne tietoturvaohjeessa käsitellään? N=52

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Päätelaitteiden ja työvälineiden käyttö	47	90,38 %					
2.	Käyttöoikeudet, tunnukset ja salasanat	51	98,08 %					
3.	Internetin ja sähköpostin käyttö	47	90,38 %					
4.	Toimitilojen turvallisuus	36	69,23 %					
5.	Sosiaalisen median käyttö	30	57,69 %					
6.	Tietojen salassa-pito (vaitiolo)	45	86,54 %					
7.	Etätyö ja etäkäyttö	29	55,77 %					
8.	Vastuualueet ja organisointi	28	53,85 %					
9.	Ongelmatilanteet ja seuraamukset	30	57,69 %					
10.	Jokin muu, mikä	1	1,92 %					

Taulukossa 7 on esitettynä osa-alueet, joita yrityksen tietoturva-ohjeessa käsitellään. Tämä kysymys oli ainoastaan niille vastaajille, jotka vastasivat, että yrityksellä on tietoturvaohjeistus määriteltynä. Tulosten perusteella yritykset noudattavat perinteisen tietoturvaohjeistuksen laatimisen oppaita. Vastauksissa jokainen osa-alue sai vastausprosentiksi yli 50 %. Jokin muu kohdassa tuli esiin varmuuskopiot ja ohjelmistolisenssien säilyttäminen.

Taulukko 8. onko henkilökunta perehdytetty tunnistamaan liiketoiminnan kannalta luottamukselliset tiedot?

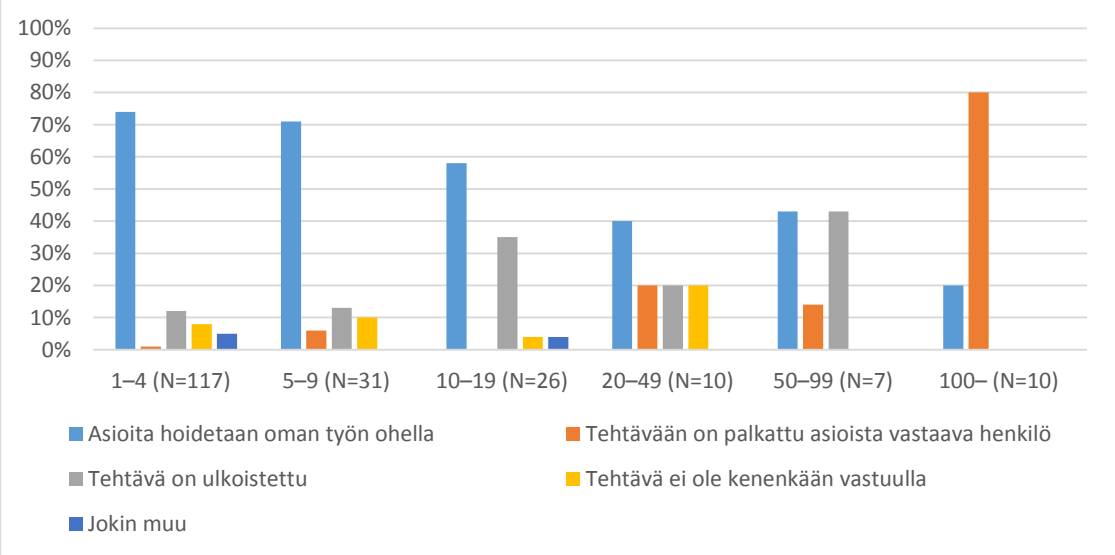
	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Kyllä	148	73,63 %					
2.	Ei	41	20,40 %					
3.	En tiedä	12	5,97 %					
	Yhteensä	201	100 %					

Tutkimusta tehdessä olettamus oli, että pienillä yrityksillä ei ole tietoturvaohjeistusta määriteltynä. Sen takia halusimme selvittää, onko henkilökunta perehdytetty tunnistamaan luottamukselliset asiat. Suurin osa on perehdytetty työhön, mutta silti 20 % vastaajista ei tiennyt mitkä asiat ovat luottamuksellisia.

Taulukko 9. Miten yrityksen tietoturva-asiat on resursoitu?

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Asioita hoidetaan oman työn ohella	132	66,00 %					
2.	Tehtävään on palkattu asioista vastaava henkilö	14	7,00 %					
3.	Tehtävä on ulkoistettu	32	16,00 %					
4.	Tehtävä ei ole kenenkään vastuulla	15	7,50 %					
5.	Jokin muu, mikä	7	3,50 %					
	Yhteensä	200	100 %					

Taulukon 9 perusteella vastanneista peräti 66 % ilmoitti, että asioita hoidetaan oman työn ohella. Vastaajista suurin osa on pieniä yrityksiä/yrittäjiä, jolloin yrityksellä ei ole mahdollisuutta palkata erillistä henkilöä hoitamaan tietoturva-asioita. Jokin muu kohtaan vastattiin yhteistyökumppaneitten apu, sekä laitteiden hankinta ja suojaus ulkopuoliselta palveluntarjoajalta.



Kuvio 7. Miten yrityksen tietoturva-asiat on resursoitu?

Pienissä yrityksissä tietoturva-asioita hoidetaan pääasiassa oman työn ohella (kuvio 7) ja sitä mukaan, kun yrityksen koko kasvaa, myös tietoturva asioiden hoitoon varataan enemmän resurssia. Isoissa yrityksissä on palkattu henkilö hoitamaan näitä asioita. Asia voidaan myös tulkita niin, että isoissa yrityksissä on tietohallinto, joka vastaa laitteiden ja järjestelmien toimivuudesta.

Taulukko 10. Mihin häiriötilanteisiin yrityksessänne on varauduttu? N=201

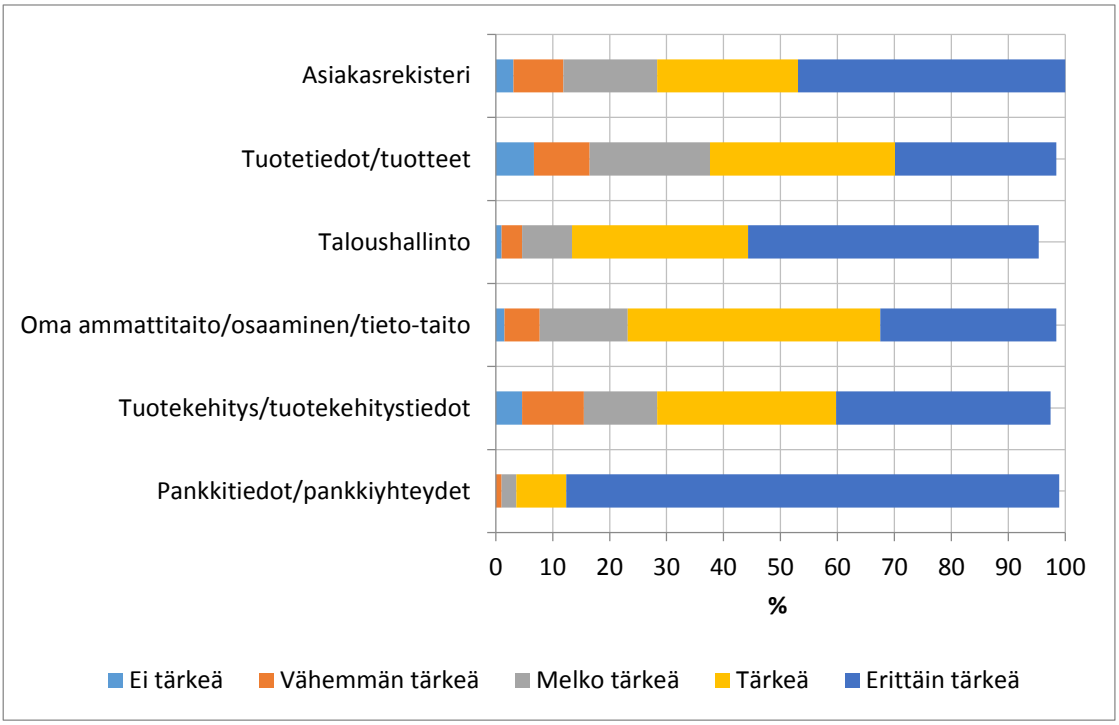
	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Väärinkäytöksiin	79	39,30 %					
2.	Järjestelmien toimimattomuuteen	125	62,19 %					
3.	Sähkökatkoihin	122	60,70 %					
4.	Tietovuotoihin	50	24,88 %					
5.	Yritys ei ole varautunut häiriötilanteisiin	47	23,38 %					
6.	Jokin muu, mikä	8	3,98 %					

Taulukon 10 vastausten perusteella yritykset ovat varautuneet järjestelmien toimimattomuuteen sekä sähkökatkoihin. Nämä edellä mainitut ovat perinteisiä häiriötilanteita, joita useimmiten sattuu, mutta silti tietoturvallisuus on unohdettu. Peräti 23 % vastanneista ei ole varautunut häiriötilanteisiin.

Jokin muu, mikä -kohtaan vastattiin seuraavaa: tietojen häviämiseen, poikkeusolot, sosiaalisen median juttuihin, fyysinen murtautuminen, tietokoneen kaatumiseen, reagoidaan jos huomataan, ennalta ehkäisevää valvontaa ei tehdä ja palvelunestohyökkäyksiin.

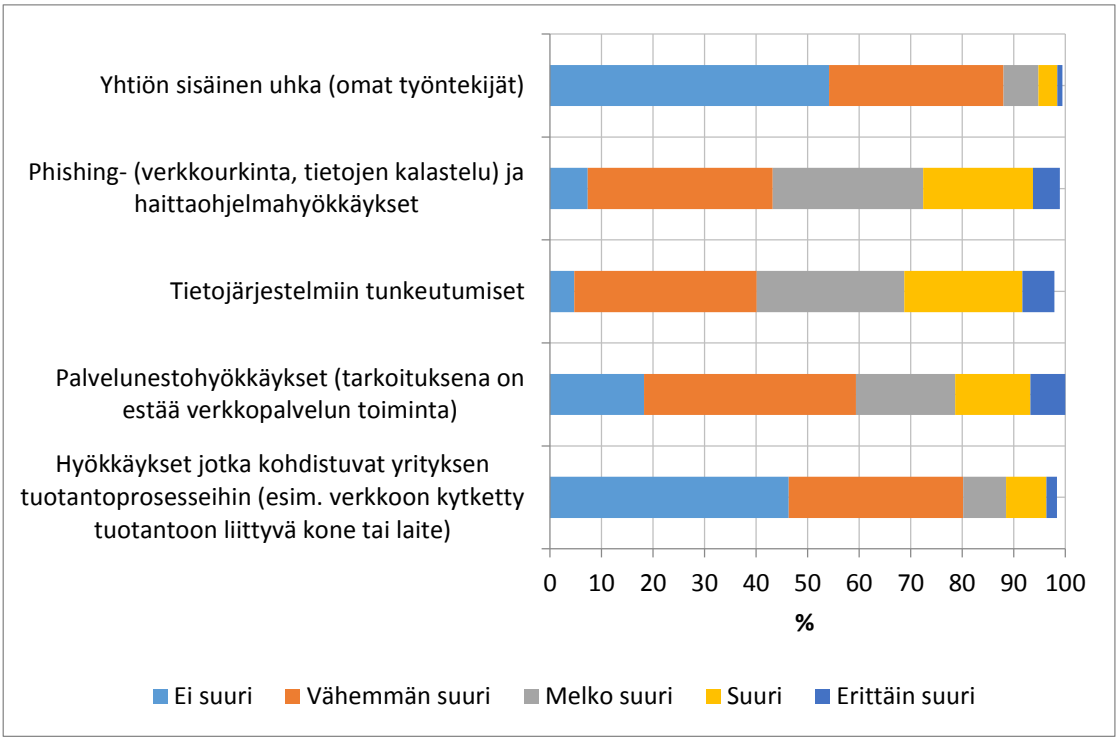
6 Tutkimus: Asenteet

Oikeastaan kaikki lähtee asenteesta. Halutaanko asioihin reagoida ja koetaanko ne tärkeiksi. Miten yritykset kokevat työntekijänsä. Ovatko he uhkia vai mahdollisuuksia? Murtautumiset yritysten verkkoon alkavat usein työntekijöiden toiminnan hyödyntämisellä. Työntekijöiden pitäisi ymmärtää, että hyökkäys ei ole vain internetin kautta tulevaa haittaohjelmaa, vaan se voi tulla, vaikka puhelinkeskustelun tai vähäpätöisen sähköpostiviestin kautta. Usein on puhuttu esimerkiksi sähköpostien linkeistä ja liitetiedostoista, jotka sisältävät haittaohjelman. Silti näitä viestejä avataan.



Kuvio 8. Miten tärkeänä pidät seuraavien asioiden turvaamista? N=194

Suurin osa vastaajista koki kuvion 8 mukaan, että tärkeimmät turvattavat asiat ovat pankkitiedot, taloushallinto ja asiakasrekisteri. Perinteisesti fyysinen omaisuus koetaan tärkeäksi, mutta eikö yritys tuotteet muodosta yhtä tärkeän osa-alueen? Jos tuotteita ei ole, niin onko silloin myöskään myyntiä.

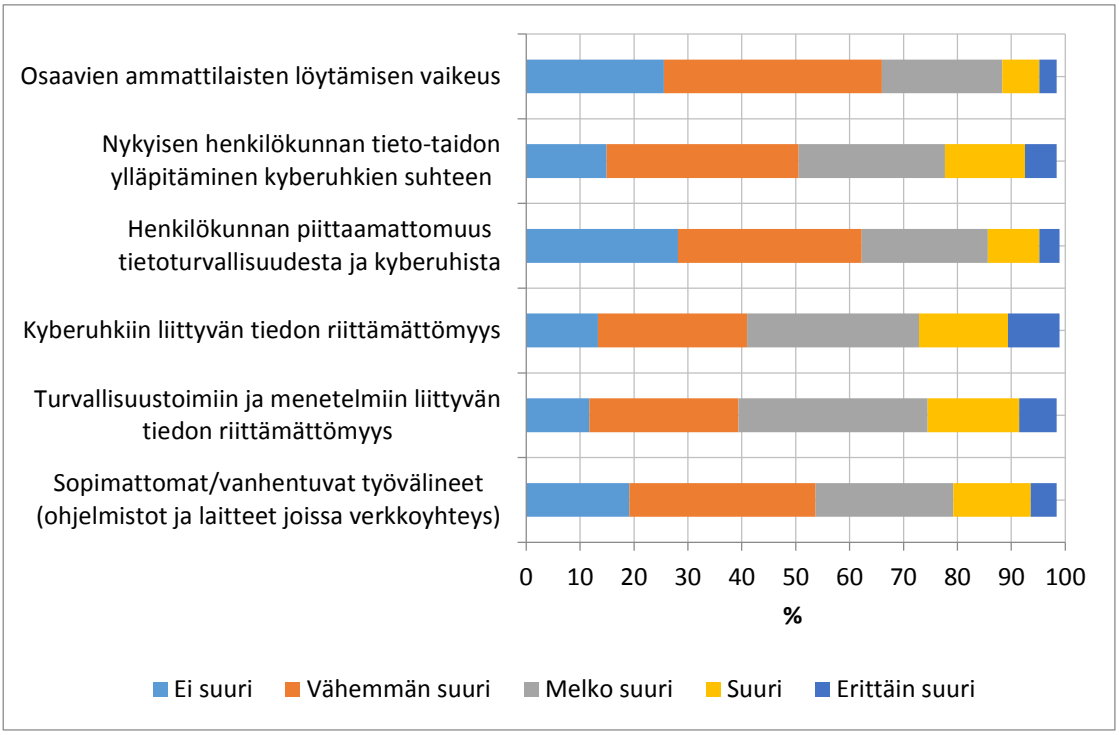


Kuvio 9. Miten suurina kyberturvallisuusuhkina pidätte seuraavia asioita yrityksessänne? N=192

Vuosi sitten Helsingin kauppakamari (2015) julkaisi tutkimuksen ”Yrityksiin kohdistuvat kyberuhat 2015”. Kyseisessä tutkimuksessa yrityksen omia työntekijöitä pidettiin suurena sisäisenä uhkana. Kuvion 9 pohjalta yrityksen omia työntekijöitä ei enää pidetty suurena uhkana. Joko asenteissa on tapahtunut muutos, tai tutkimuksen kysymystä ei ole ymmärretty oikein.

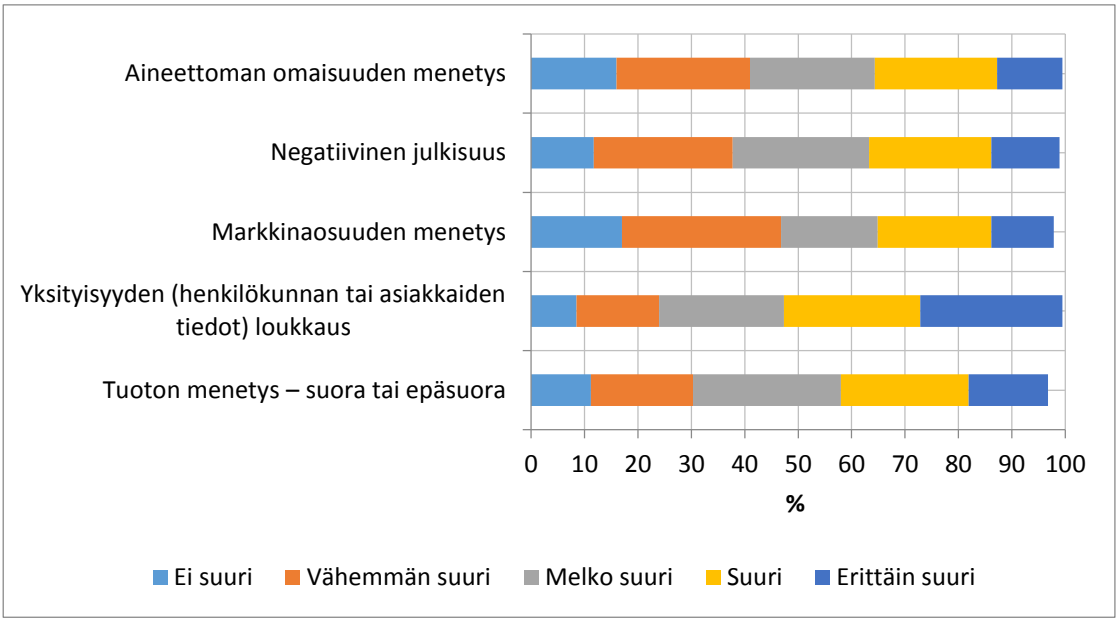
Kysyttäessä mielipiteitä uhkakuvista, verkkourkinta ja tietojärjestelmiin tunkeutumiset koettiin suurimmiksi uhkakuviksi. Toisaalta kohta, hyökkäykset yrityksen tuotantoprosesseihin, on ristiriidassa edellä mainitun kanssa.

Jos kuviosta 10. katsotaan ainoastaan kohtia *ei suuri* ja *vähemmän suuri* yritykset eivät koe uhkakuviksi oikeastaan mitään kuvion 10 kohdista. Herää kysymys, että tiedostetaanko yrityksissä näitä riskejä ja mitä nämä voivat pahimmillaan aiheuttaa yritykselle?



Kuvio 10. Miten suurena esteenä pidätte seuraavia asioita tehokkaan kyberturvallisuuden toteuttamiseksi yrityksessänne? N=188

Yritykset eivät koe kuvion 10 perusteella esteitä yrityksen kyberturvallisuuden kehitykselle. Pieni osuus oli vastannut, että tiedon riittämättömyys on suurin este yrityksen kyberturvallisuuden kehityksessä. Tämä on kuitenkin ristiriidassa taulukon 11 kanssa, missä kysyttiin, tärkeimmät kehittämiskohteet yrityksen kyberturvallisuudessa. Peräti 71 % (143) vastasi tärkeimmäksi kehittämiskohteeksi yrityksen tietoturvaosaamisen.



Kuvio 11. Miten merkittävinä pidätte seuraavia kyberhyökkäyksestä aiheutuvia seurauksia? N=188

Kysyttäessä kyberhyökkäyksestä aiheutuneita seurauksia (kuvio 11), yritykset kokevat suurimmaksi yksityisyyden loukkauksen. Joko henkilökunnan tai asiakkaiden tietoja päätyy vääriin käsiin. Asenteet ovat muuttuneet negatiivisen julkisuuden näkökulmasta. Aikaisemmin tietovuoto koettiin negatiiviseksi, mutta nykypäivänä siihen suhtaudutaan paremmin. Ehkä tähän vaikuttaa myös se, että nykyään melkein joka viikko saadaan lukea mediasta, kun johonkin yritykseen on tehty tietomurto.

Taulukko 11. Tärkeimmät kehittämiskohteet yrityksenne kyberturvallisuudessa? N=201

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Oma/yrittäjän tietoturva-osaaminen	143	71,14 %					
2.	Henkilökunnan/ käyttäjien osaaminen	92	45,77 %					
3.	Varmuuskopiointi/ varmistukset	102	50,75 %					
4.	Koulutuksen/tiedon lisääminen	74	36,82 %					
5.	Laitteet/laitteisto/ koneet	72	35,82 %					
6.	Varajärjestelmät	68	33,83 %					
7.	Ohjelmistojen päivittäminen	72	35,82 %					
8.	Kulunvalvonta	19	9,45 %					
9.	Jokin muu, mikä	4	1,99 %					

Tärkeimmäksi kehittämiskohteiksi (taulukko 11) yritykset kokivat tietoturvaosaamisen kehittämisen (71 %) sekä varmuuskopiointien tekemisen (51 %). Myös henkilökunnan osaamista (46 %) haluttaisiin kehittää yrityksissä. Jokin muu, mikä kohtaan vastattiin maalaisjärjen käyttö eli toisin sanoen mieti mitä olet tekemässä.

7 Tutkimus: Toteutuneet uhat

Vaikka asenteet ovat muuttuneet, silti tämä osa-alue on arka paikka monelle yrittäjälle. Varsinkin suuret yritykset, jotka toimivat B2B tai B2G toimialueella ja ovat tehneet esimerkiksi KATAKRI akkerdoinnin eivät voi/halua myöntää julkisuuteen tietomurtoa, ellei ole aivan pakko.

Aikaisemmissa tutkimuksissa (Kivikoski & Kauppinen, Kauppakamari) alle 10 % yrityksiin on kohdistunut tietoturvahöykkäys.

Taulukko 12. Mitkä seuraavista tietoturvauhkista ovat toteutuneet yrityksessänne? N=201

	Vastaus	**Lukumäärä**	**Prosentti**
1.	Käyttäjätunnuksia ja salasanoja on varastettu ja niitä on väärinkäytetty	6	2,99 %
2.	On yritetty urkkia tai vakoilla työtehtäviin liittyviä tietoja	18	8,96 %
3.	Identiteetti on varastettu ja sitä on väärinkäytetty	4	1,99 %
4.	Organisaatio on menettänyt rahaa nettihuijauksen takia	6	2,99 %
5.	Yrityksen tietoja on vuotanut	1	0,50 %
6.	Yritys on menettänyt tärkeitä tietoja laiterikon tai vastaavan takia	26	12,94 %
7.	Päätelaite on varastettu tai hävinnyt	9	4,48 %
8.	Työntekijä on saanut näkyville tai tietoonsa salassa pidettäviä tietoja, joihin hänellä ei ole ollut oikeutta	7	3,48 %
9.	Työpaikan luottokorttia on käytetty väärin	7	3,48 %
10.	Yritykseen on tehty tietoturvahyökkäys	15	7,46 %
11.	Yritykseen ei ole kohdistunut tietoturvauhkaa	118	58,71 %
12.	Jokin muu, mikä	21	10,45 %

Peräti 59 % (118) yritystä ilmoittaa taulukon 12 mukaan, että yritykseen ei ole tehty tietoturvahyökkäystä. Näin ollen voidaan tulkita, että 41 % (83) yrityksistä on joutunut jonkinlaisen tietoturvamurron tai vastaavan kohteeksi.

Kohtaan yritykseen on tehty tietoturvahyökkäys, vastasi 15 yritystä. Kyselyjärjestelmän avulla teimme suodatuksen näiden yrityksien kohdalle ja vertasimme tuloksia normaaliotokseen. Yleisinä havaintoina voidaan esittää, että yrityksien koot olivat alle 50 henkilön yrityksiä ja toimialat jakautuivat tasaisesti. Laitekannan suhteen ei ollut eroavaisuuksia normaaliotokseen.

Taulukko 13. Vertailulukuja tietoturvahyökkäys vs. normaaliotos

	Normaaliotos, N=201	Suodatettu, N=15
Millä laitteilla yrityksessänne on pääsy tietoverkkoon (internet)? Älypuhelin	84 %	93 %
Käytätkö omia laitteita työasioiden hoitamiseen, Kyllä	31 %	47 %
Oletko tietoinen EU-lainsäädännöstä kyberturvallisuuteen liittyen?, Kyllä	16 %	47 %
Onko yrityksessänne laadittu tietoturvaohje?, Kyllä	26 %	40 %
Miten yrityksen tietoturva-asiat on resurssoitu? Tehtävä on ulkoistettu	16 %	36 %
Mihin häiriöitilanteisiin yrityksessänne on varauduttu? Järjestelmien toimimattomuuteen	62 %	93 %
Mihin häiriöitilanteisiin yrityksessänne on varauduttu? Tietovuotoihin	25 %	67 %
Tärkeimmät kehittämiskohteet yrityksenne kyber-turvallisuudessa? Koulutuksen/tiedon lisääminen	37 %	80 %
Onko yrityksenne henkilöstö ollut viimeisen vuoden aikana tietoturvaan liittyvässä koulutuksessa?, Kyllä	13 %	46 %
Olisiko yrityksenne kiinnostunut osallistumaan tietoturvaseminaariin/työpajaan?, Kyllä	54 %	73 %

Jokin muu, mikä -kohtaan oli vastattu seuraavaa: tiedonkalastus, palvelunestohyökkäys, vakoiluepäilyt, viruksen aiheuttama laitteiston toimimattomuus, laiterikko, työntekijän kotoa varastetut muistitikut ja huijaussähköpostit. Yksi yritys vastasi myös, että ”*kysymykseen vastaaminen ei ole mahdollista, koska virallisesti/julkisesti ei ole tiedotettu mitään aiheesta”.* Oikeastaan on hyvä merkki, että yritykset kertovat olevansa tietomurron kohteena, sillä silloin yrityksen havainnointikyky on toiminut ja poikkeamat huomattu.

Taulukko 14. Miten havaitsitte edellisessä kysymyksessä tarkoitetun tietoturvauhkan? N=91

	Vastaus	**Lukumäärä**	**Prosentti**
1.	Havaitsimme sen itse käyttäen omia torjunta- ja hälytysjärjestelmiämme	38	41,76 %
2.	Käyttäjämme tunnistivat sen ja ilmoittivat eteenpäin	22	24,18 %
3.	Tunnistimme itse, koska tarkastamme ja analysoimme lokejamme	13	14,29 %
4.	Kotimaiset lainvalvontaviranomaiset tai tiedusteluorganisaatiot varoittivat meitä	4	4,40 %
5.	Kolmas taho, kuten internet operaattori tai palveluntarjoaja, ilmoitti meille	14	15,38 %
6.	Jokin muu, mikä	17	18,68 %

Taulukon 14 jokin muu, mikä -kohtaan oli vastattu seuraavaa: muun muassa verkkoyhteyden katkeaminen ja laitteen rikkoontuminen.

Taulukko 15. Minkälaista tietoa luulette tunkeutujien etsivän? N=91

	Vastaus	Lukumäärä	Prosentti
1.	Ylempään johtoon kuuluvien henkilökohtaista tietoa	8	8,79 %
2.	Henkilökuntaan liittyvää tietoa, kuten nimet, vastuualueet ja yksiköt	5	5,49 %
3.	Tietoa alihankkijoista, yhteistyökumppaneista, tavarantoimittajista tai asiakkaista	13	14,29 %
4.	Luottamuksellista tietoa tuotteistamme tai palveluistamme	18	19,78 %
5.	Tietoverkkoonne liittyvää tietoa, kuten verkon rakennetta ja muita laitteita yrityksen verkossa	9	9,89 %
6.	Emme osaa sanoa	49	53,85 %
7.	Jokin muu, mikä	14	15,38 %

Kysyttäessä millaista tietoa luulette tunkeutujan etsivän (taulukko 15), niin jakautumista vastauksissa tulee melko paljon. Peräti 54 % vastasi *Emme osaa sanoa*, mikä on sinänsä hyvä vastaus, koska harvemmin pystytään tarkasti sanomaan miksi järjestelmään murtaudutaan. Useimmiten tavoitteena on saada järjestelmä haltuun, jotta sitä voi käyttää eteenpäin seuraavan paikan murtamiseen. Vastaajista 20 % oli sitä mieltä, että tunkeutuja etsi luottamuksellista tietoa tuotteista tai palveluistamme.

Jokin muu, mikä -kohtaan oli vastattu seuraavaa: nettisivun tietoja, rekisterit, pankkitietoja, innovaatioiden informaatiota ja häirintä.

8 Tutkimus: Yrityksen koulutusnäkökulma

Tekniikan kehittyessä on välillä vaikea pysyä aallonharjalla, sillä niin nopeasti se etenee. Toisaalta, jos pienen yrittäjän päätoimiala on, vaikka traktoreiden korjaus, kuinka paljon hänellä on aikaa käydä tietotekniikkakoulutuksissa.

Taulukko 16. Onko yrityksenne henkilöstö ollut viimeisen vuoden aikana tietoturvaan liittyvässä koulutuksessa?

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Ei	174	86,57 %					
2.	Kyllä, missä?	27	13,43 %					
	Yhteensä	201	100 %					

Taulukon 16 vastausten perusteella harva yritys osallistunut aiheeseen liittyvään koulutukseen. Vain 13 % yrityksistä ilmoitti olleensa koulutuksessa. Paikoiksi yritykset ilmoittivat verkkokursseja ja webinaareja. Peräti viisi henkilöä ilmoitti olleensa F-Securen järjestämässä koulutuksessa.

Taulukko 17. Mistä tietoturva osa-alueista haluaisit saada koulutusta? N=200

	Vastaus	Lukumäärä	Prosentti
1.	Hallinnollinen tietoturva - Tietoturvan johtaminen ja hallinnointi	40	20,00 %
2.	Fyysinen tietoturva - Toimitilojen ja laitteiden fyysinen suojaaminen	32	16,00 %
3.	Laitteistoturvallisuus - Esimerkiksi tietokoneiden yleinen suojaaminen	94	47,00 %
4.	Ohjelmistoturvallisuus - Ohjelmistojen tietoturvaan liittyvät asiat	87	43,50 %
5.	Tietoaineiston turvallisuus - Sähköisten ja paperisten dokumenttien käsittely ja suojaaminen	54	27,00 %
6.	Tietoliikenneturvallisuus - Esimerkiksi tiedonsiirtoon liittyvät tietoturvamekanismit	72	36,00 %
7.	Henkilöstöturvallisuus - Rooleihin, vastuihin ja tietoturvaohjeistuksiin liittyvät asiat	36	18,00 %
8.	Käyttöturvallisuus - Esimerkiksi salasanoihin liittyvät asiat	69	34,50 %
9.	Jokin muu, mikä	16	8,00 %

Taulukon 17 perusteella vastaajat ovat kiinnostuneet eniten laitteistoturvallisuudesta (47 %) ja ohjelmistoturvallisuudesta (44 %). Melko lähellä näitä tulee myös tietoliikenneturvallisuus (36 %) ja käyttöturvallisuus (35 %). Nämä kaikki ovat oikeastaan yleisimpiä osa-alueita joissa on eniten haasteita.

Jokin muu, mikä -kohtaan vastattiin pääosin, että ei tiedä tai osaa määritellä millaista koulutusta pitäisi saada. Yksi henkilö vastasi: *Ei haluta koulutusta - ei voi olla kaiken asiantuntija - vastaukset löytyy netistä, myös asiantuntijoilla.* Vastaaja on oikeassa, sillä ei pidäkään olla kaiken asiantuntija vaan keskittyä omaan vahvuusalueeseen.

Taulukko 18. Mikä olisi mielestäsi sopiva pituus koulutukselle?

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	4 tuntia	114	57,00 %					
2.	Koko päivä	56	28,00 %					
3.	Kaksi päivää	8	4,00 %					
4.	Jokin muu, mikä	22	11,00 %					
	Yhteensä	200	100 %					

Taulukon 18 perusteella sopivin koulutus olisi puoli päivää. Harvalla pienellä yrittäjällä on mahdollisuutta olla useampaa päivää koulutuksessa, sillä tämä kaikki on pois yrittäjän tuloista. Jokin muu -kohdan vastaukset vaihtelivat yhdestä tunnista jatkuvaan koulutukseen ja osa korosti webinaareja, koska ei yrityksellä ole resursseja lähettää henkilöä pitkiin kouluksiin.

Webinaareilla tarkoitetaan internetin kautta katsottavia luentoja, joiden pituus vaihtelee puolesta tunnista pariin tuntiin. Useimmiten nämä ovat tehokkaita, koska ne pystytään katsomaan jälkikäteen silloin kun on aikaa. Reaaliajassa osallistumisen etu on mahdollisuudessa esittää kysymyksiä webinaarin pitäjille.

Taulukko 19. Olisiko yrityksenne kiinnostunut osallistumaan tietoturvaseminaariin/työpajaan?

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Kyllä	108	53,73 %					
2.	Ei	93	46,27 %					
	Yhteensä	201	100 %					

9 Tutkimus: Yrityksen koulutusnäkökulma

Koulutuksen pitäisi vastata yritysmaailman tarpeeseen ja kyselyyn otettiin mukaan myös koulutusnäkökulma. Mitä yrityksien mielestä pitäisi koulussa opettaa tulevaisuuden työntekijöille.

Taulukko 20. Kun olette palkanneet/palkkaamassa uutta henkilöstä, he ovat pääasiassa? N=201

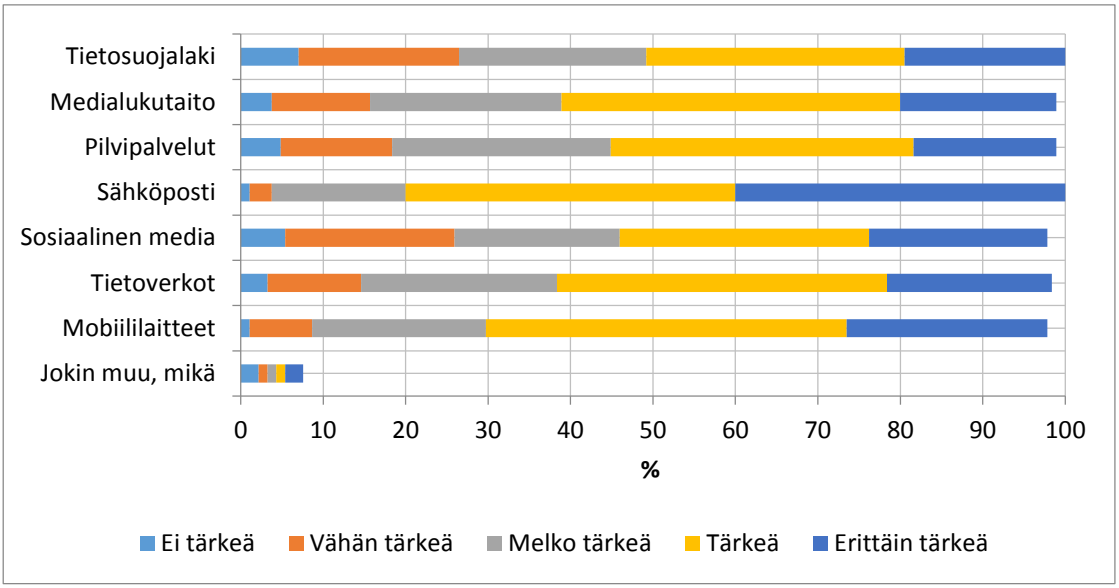
	Vastaus	Lukumäärä	Prosentti
1.	Ammatillisen tutkinnon	111	55,22 %
2.	Alemman korkeakoulututkinnon	62	30,85 %
3.	Ylemmän korkeakoulututkinnon suorittaneita henkilöitä	40	19,90 %
4.	Jokin muu, mikä	28	13,93 %

Taulukon 20 perusteella vastaukset jakaantuvat melko tasaisesti jokaiselle koulutusasteelle. Suurin kohderyhmä on ammatillisen koulutuksen (55 %) osuus. Todennäköisesti taustalla on suuri pienien yrittäjien osuus vastauksissa ja he tarvitsevat perustyön osaajia. Jokin muu, mikä -kohdassa tuli paljon erilaisia vastauksia kuten: työn kautta hankittu osaaminen, oppisopimus, yrittäjähenkisiä, koulutusasteella ei ole merkitystä. Moni vastasi myös niin, että uutta henkilöstöä ei olla palkkaamassa.

Taulukko 21. Arvioi uusien työntekijöiden tietotekninen osaamistaso.

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Heikko	12	5,97 %					
2.	Keskitaso	102	50,75 %					
3.	Hyvä	87	43,28 %					
	Yhteensä	201	100 %					

Kysyimme vastaajilta arvioita uusien työntekijöiden tietoteknisestä osaamistasosta (taulukko 21). Vastaukset jakautuivat hyvän ja keskitason kesken. Vain muutama prosentti oli sitä mieltä, että osaamistaso on heikko. Usein työttömät työnhakijat käyvät tietotekniikan käyttökoulutuksia, jolloin työllistyessä osaaminen saattaa olla parempaa tasoa.



Kuvio 12. Miten tärkeänä pidät ammatillisen perustutkinnon suorittaneen työntekijän seuraaviin asioihin liittyviä yleisiä tietoturvataitoja? N=185

Kuvion 12 perusteella kaikki osa-alueet koetaan tärkeäksi työllistymisen näkökulmasta. Erityisesti sähköposti ja mobiililaitteet pitävät kärkiasemaa vastaajien keskuudessa. Mielenkiintoisinta on kuitenkin, että sosiaalisen median taitoja ei koeta niin tärkeäksi kuin muita. Nykypäivänä sosiaalinen media on kuitenkin se tärkein kanava, joiden viesteihin pitää reagoida. Jokin muu -kohtaan vastattiin asenne – henkilökohtaisen vastuun ymmärtäminen sekä esineiden internet (IoT).

Kysymyksessä 33. kysyttiin millaisia asioita ammatillisen perustutkinnon opiskelijoille pitäisi opettaa tietoturvasta? Vastaukset olivat monipuolisia ja alapuolelta löytyy suoraan lainauksia käyttäjien vastauksista (kursivointi).

Oikeat asenteet ja käytännönläheiset toimenpiteet. Mitä tietoja sinä saat katsoa!

Perusymmärrys ja valmius tietoturva-asioiden jatkuvan kehittymisen seuraamiseen.

Omille laitteille ei saa tallentaa tietoja työnantajan tuotteista, tuotannosta ja asiakkaista. Muuten saa olla omissa mobiileissa vapaasti tietoa, mutta työnantajalle kuuluvaa tietoa niissä ei saa olla.

Internetin käytön riskit. Yleiset työelämän tietosuoja asiat. Ammatti/ alakohtaiset tietosuoja asiat syvennetysti.

Uhat ja perusasiat suojautumisesta

Erilaisten haitallisten ohjelmistojen, www-sivustojen, huijausten yms. tunnistaminen ja niiden ehkäisy

Yleiset käytännöt, yleisimmät riskit. Standardit, perustiedot lainsäädännöstä. Kokonaiskuva: esineiden Internet ja laitteiden muodostama kokonaisuus yrityksessä.

Medialukutaito ja some-sinisilmäisyyden poisto, huolellisuus ja tarkkaavaisuus,

Mitä työpaikasta saa ja mitä ei saa kirjoittaa sosiaaliseen mediaan ns. omina mielipiteinään.

Tiedettävä, mitä saa ja mitä ei saa julkaista mm. sosiaalisessa mediassa (luottamuksellinen tieto). Yleisimmät tietovuodon aiheuttajat.

TCP/IP protokollan kommervinkit, porttitietous, tiedon yksityisyys, binäärialgebra.

Nettimaailma muuttuu niin nopeaan tahtiin ja vasta väärinkäyttäjät luovat tarpeen siirtyä eteenpäin/ylemmälle tasolle että tulevaisuutta heille ei voi opettaa mutta heille voi antaa hyvän pohjan selvittää tulevia ongelmia tietämällä suurin osa nykyisistä väärinkäytön keinoista.

Kyberturvallisuuden perusteet ja kybermaailma toimintaympäristönä. Perustaidot turvallisesta toiminnassa internetissä Oman ammatillisen suuntautumisvaihtoehdon mukaisen toimintaympäristön kyberturvallisuusuhat, -riskit ja turvaamisratkaisut

Kaikkien työntekijöiden pitäisi sisäistää se, että urkkijoita on jokapuolella. Urkkija ei välttämättä ole verkossa vaaniva nörtti, vaan se voi olla myös roskiksi kollaava dyykkari tai ovia satunnaisesti kokeileva "remonttimies"..

Pilvipalvelut ja niihin liittyvä tietoturva. Varmistusratkaisujen ja palveluiden tietoturva.

Perusasiat internet-turvallisuudesta, palomuureista ja erilaisista tietojenkalastelukeinoista.

Tietokonetta käytettäessä pitäisi aina varmistaa, että virustorjuntaohjelma on toiminnassa

Tietoverkkojen käyttäämiseen liittyvät turvallisuusriskit.

Salasanat - välimuisti - lataukset netistä - haittaohjelmat - suojausohjelmat - Fishing

Medialukutaito, miten tunnistaa tietojen kalastelun, perustiedot viruksista, yhteyksien suojaamisesta ym.

Yksityisyyden suoja, eettinen toiminta ja epäeettisen seuraamukset, tekninen tietotaito

Salassa pitovelvollisuus, potilasasia pitovelvollisuus,

Perusteet eri asioista, osaamista voi syventää työtehtävien vaatimusten mukaisesti.

Tietoturvan suojausmenetelmät ja vaihtoehdot

Kohdan 32 asioista perusteet jotka työelämässä on käytettävä. Tietoteknisen kehityksen mukanaan tuomat ohjelmien ja medioiden ominaispiirteet, käyttö yritysmaailmassa ja tietoturvaan liittyvät asiat niiden suhteen. Ammatillisen peruskoulutuksen saaneella pitäisi olla ajantasainen tieto niistä mennessään työelämään.

Opetuksen pitää sisällään tieto, että turvallisuus on kokonaisuus.

Kuluttajasuojalaki (perusteet), vaitiolovelvollisuus, medialukutaito, somen käyttö

Paljon mielenkiintoisia ja täysin paikkansa pitäviä vastauksia. Erityisesti korostaisin lausetta ”Mitä tietoja sinä saat katsoa!” sekä ”Urkkija ei välttämättä ole verkossa vaaniva nörtti, vaan se voi olla myös roskiksi kollaava dyykkari tai ovia satunnaisesti kokeileva remonttimies”. Vaikka sinulla olisi mahdollisuus, se ei tarkoita silti sitä, että sinulla olisi oikeus!

Taulukko 22. Pitäisikö kehittää tietoturvakortti, jolla taataan tietty tietämys tietoturvasta?

	Vastaus	Lukumäärä	Prosentti	20 %	40 %	60 %	80 %	100 %
1.	Kyllä	59	29,35 %					
2.	Ei	64	31,84 %					
3.	En osaa sanoa	78	38,81 %					
	Yhteensä	201	100 %					

Välillä on käyty keskustelua uudesta korttikoulutuksesta, joka painottuisi tietoturvaan. Taulukon 22 perusteella tämä jakaa vastaajien mielipiteet hyvin tasaisesti. Puolesta puhujien ja vastustajien määrä on melkein yhtä suuri. Todennäköisesti tässä kohdalla saattaa olla pelko, että kyseeseen tuli taas yksi pakollinen korttikoulutus, joita on muutenkin entuudestaan paljon. Joillain aloilla on pakko suorittaa korttikoulutuksia, ennen kuin työtehtäviä voi suorittaa.

Kysymyksessä 35. kysyttiin mitä osaamista tietoturvakorttikoulutuksen pitäisi pitää sisällään? Vastaukset olivat monipuolisia ja alapuolelta löytyy suoraan lainauksia käyttäjien vastauksista (kursivointi).

Erillistä tietoturvakorttia ei tarvita (5kpl)

Kysymyksessä 32 ja/tai 33 oleviin asioihin liittyvät kysymykset (3kpl)

Perusteet tässä kyselyssä olevista asioista (3kpl)

Ei korttia - kortti annetaan liian hepposin perustein,
eri syistä ja ajan myötä kortti on syrjivä.

Ihmisille olisi syytä kertoa että kerran verkkoon laitettu tieto ei häviä sieltä koskaan. On käsittämätöntä ja valitettavaa useiden ihmisten kannalta että esimerkiksi työnantajaa

Toisen asteen kyber (25274)

haukutaan julkisesti verkossa - oli siihen syytä tai ei. Nämä tiedot ja kirjoitukset saavat tulevaisuudessa vielä uusia merkityksiä, esim. kun facebook alkaa myydä ihmisten käyttäjähistorioita yrityksille ja vakuutusyhtiöille. No, korttikoulutuksessa sitten lisää aiheesta.

Perusteet kyberturvallisuusuhkista ja -riskeistä. Turvallinen toiminta verkkoympäristössä

Tietoturva rakentuu hyvin yksinkertaisista ja helpoista arjen toimenpiteistä. Ongelma on vain niiden tärkeyden sisäistämisessä. Muista ettet kerro tai vuoda salasanaasi.. älä kerro sensitiivistä tietoa puhelimessa tai sähköpostissa sitä kysyvälle.. älä leuhki asiakkaista baarissa.. muista silputa kaikki tekniset piirrustukset ja asiakasdokumentaatio.. jne.. jne.. helppoja ja intuitiivisia juttuja, mutta niin monesti unohtuu tai ei pidetä tärkeänä.

Meidän alalla (mielenterveyskuntoutus) tärkein olisi, että tietoturvakortti olisi viranomaisten vaatima kuten hygieniapassi, lääkelupa, ensiapukoulutus, vastaavahoitajan kelputus ja mielenterveys- ja päihdeongelma erikoistuminen.

Taloudellinen näkökulma tietoturvallisuuteen, raha on usein este järjestelmien ohjelmien päivittämiseen

Kohdan 32 asioista perusteet joita työelämässä on käytettävä. Tietoteknisen kehityksen mukanaan tuomat ohjelmien ja medioiden ominaispiirteet, käyttö yritysmaailmassa ja tietoturvaan liittyvät asiat niiden suhteen. Ammatillisen peruskoulutuksen saaneella pitäisi olla ajantasainen tieto niistä mennessään työelämään.

Tieto-, fyysinen-, tietotekninenturvallisuus ja turvallisuusjohtaminen

Tietoturvakortin omistamattomuus ei saa olla este, muuten kortti olis hyvä jopa perusopetuksen puolella. Voisi olla yhtenä kurssina

---

Kysymys 36. oli vapaa sana kyselyn tekijöille. Vastaukset olivat monipuolisia ja alapuolelta löytyy suoraan lainauksia käyttäjien vastauksista (kursivointi).

Tietoturva-asiat riippuvat tietysti alasta. Hyvin tietointensiiviset ja aineettomien palvelujen kanssa tekemisissä olevat yritykset ovat haavoittuvaisempia, kuin esimerkiksi meidän yritys. Teollinen internet kuitenkin lisääntyy jatkuvasti ja tiedonsiirron sekä tiedon säilyttämisen riskit kasvavat jatkuvasti.

Kaikkein parasta on, kun hankitaan työntekijälle omat puhelimet työpaikalle. Jussilassa on kertakaikkisen yksinkertaiset puhelimet joka osastolla, mutta ei niillä nettiin pääse.

Esineiden Internetin laitteet ovat usein erittäin heikosti suojattuja, tietoturvassa pitäisi oppia tunnistamaan heikoin lenkki. Myös laitteiden turvallista hävitystä ei käsitelty tässä kyselyssä,

mikä on iso osa tietoturvaa. Laitteita pitäisi käsitellä elinkaaritasolla: päivitykset, asetukset, käytöstä poisto ja hävitys.

Suomessa on hyvin vähän yrityksiä mitkä ovat kiinnostavia varkaille (oli sitten patentti, prosessi tai muun) tietonsa takia joten suurimmat huolet, suurimmalla osalla, Suomalaisilla yrityksillä ovat tietokoneiden kaappaajat ja muut "kiusaajat" jotka käyttävät konetta omiin tarpeisiin ei olemassa olevien tietojen varastamiseksi. Usein pienillä (nykyisin mikro-) yrityksillä on niin "pienet" ja hitaat koneet että eivät kiinnosta ketään. Tietoturva ja kyber on ok mutta ei kannata tehdä siitä liian suurta numeroa.

Tietoturvakortista tulee mieleen tietokoneenajokortti, joka oli vähän turhankin kevyt suoritettava. Ei sillä voinut taata, että henkilö osaisi kunnolla perusteitakaan.

Meillä on osuuskunta, johon onpalkattu tietoturva /ATk Vastaava, eli sitä kautta saan apuja

Hyvä tutkimus. Tutkimustiedon kannalta olisi ehkä voinut päätoimialaluokituksen lisäksi olla seuraavan tason luokitustieto. Näin voitaisiin tarkemmin analysoida vastauksia eri tyyppisten esim. teknologiayritysten näkökulmasta. Kysymys 23 on hieman epäselvä. Nimittäin jokainen verkkoon kytketty laite ja sen IP-portti ovat jatkuvan porttiskannakuksen ja tunkeutumisyritysten kohteena eli kaikkiin kohdistuu hyökkäyksiä. Tämän lisäksi lähes kaikki saavat sähköposteihin kalasteluviestejä. Ts. kaikki olemme kyberuhkien kohteita. Kaikki hyökkäykset eivät onnistu ts. riski ei toteudu, koska henkilöstön toiminta, yrityksen turvallisuusprosesit ja suojaustekniikat ovat olleet kunnossa.

Varmaan yksinkertainen koulutus perusriskeihin varautumisen olisi paikallaan ja sen päivitys tietyin väliajoin eli pysyttäisiin (kartalla) kiitos !

Ei ainakaan yhtään uutta korttikoulutusta, niitä on jo liiankin kanssa

Kun opiskelija tulee esim. työssäoppimaan, pitää olla selvillä mitä salassapito tarkoittaa. Meillä yrityksessä on opiskelijoilla valokuvauskielto. Salassapito yrityksen asioita kohtaan ja työntekijöihin liittyvä tieto.

Kysymys 31 huonosti muotoiltu, koska pakko arvioida uusien työntekijöiden tietotekninen osaaminen, vaikka en ole palkannut uusia työntekijöitä. Eli tuolta osin vastaukseni vääristää tuloksianne, koska on vain pakko laittaa täppä johonkin, että saa lomakkeen lähetettyä.

Haluatko koulutusta? Kyllä/Ei. Miksi ei voi valita ehkä. Saako nyt kaikki kouluttajat niskaansa roskapostittajina. Suurin ongelma on "paska", jota tulee sähköpostiin niin julkiselta kuin yksityiseltä puolelta. Seassa on yksi tuhannesta joka on tärkeä ja kiinnostaa, niin kaikkia ei viitsi blogata.

Kysymys 31 on todella vaikea yksintoimivalle yrittäjälle! Uusia työntekijöitä ei ole, joten heidän tietotaitonsa arvioiminen on hatusta vedetty!

Kuulostaa siltä, että yrityksiin ollaan puuhaamassa taas yhtä pakollista maksullista korttia?

Nykyään kuuluu yleissivistykseen medialukutaito sekä haittaohjelmien mahdolllisuuden tunnistaminen. tietojen kalastelu on jatkuva riesa ja sitä tapahtuu enenevässä määrin.

Viestintävirasto voisi tuottaa perehdyttävän verkkokurssin tai vastaavan useista vaiheista koostuvan koulutuksen, jonka työntekijät voisivat suorittaa muun työn ohessa ja omaan

tahtiin. Sekalainen ohjenippu, joka tällä hetkellä on tarjolla, ei ole paras tapa perehdyttää työntekijää. Koulutukset ovat myös liian työläitä useille pienyrityksille. Oppiminen ja tiedon saaminen pitää tehdä helpommaksi.

Tietoturvakortti voi olla vapaaehtoinen, mutta en näe järkevänä lisätä pakollisia kortteja/koulutuksia. Jokainen yritys voi miettiä, millaista osaamista tarvitsee.

Yleensäkin ammatillisessa koulutuksessa tulee käyttää paljon tietokoneita, sillä työelämä vaatii jatkuvaa koneiden hallintaa. Koneiden perusteiden hallinnan opetukseen ei yrityksellä ole aikaa, mutta tietenkin erikoisohjelmiston opettamiseen käytetään aikaa. Sen helpommin saa töitä, mitä näppärämpi on käyttämään tietokonetta.

Kiinnostaa miten tätä asiaa/kyselyä voidaan hyödyntää yrityksessämme

Ei yhtään korttia enää lisää tähän maahan.

Turvallisuusasioista on paljon tietoa saatavilla. Tieto ja koulutukset pitäisi muotoilla siten, että se sisältää konkreettisia tärkeysjärjestyksessä tärkeimmästä lähtien asioiden kuntoon laittoa tai työkirja siihen. Mahdollisimman vähän "yleistä alan asiaa" jolla arkitoiminta ei parane.

Tämä kysely oli oikein hyvä, sopivan mittainen mutta silti riittävästi kysymyksiä. Tämän perusteella voisi kehittää valistuspäivän johon olisin halukas tulemaan

Jälleen kerran aivan naurettava projekti: Suomessa ei ole pankkisalaisuutta, miksi yrityksellä tietoturva? Taloustiedot ovat julkisia Tuotekehitys- ja tuotteen tiedot ovat julkisia kun ensinmäinen tuote menee ovesta pihalle. Henkilökunnalla on aina menetelmät siirtää tietoa ulos yrityksestä. Yleisesti ottaen Suomi on sellainen takapajula että ei tänne kannata paljon tiedustelua kohdistaa Jos löydätte jostain rehellisen ihmisen, kloonatkaa se. Tämä on tie kyperturvallisuuteen.

10 Huomioita kyselyistä

Ristiintaulukoinnin ja muiden kohderyhmien vertailun avulla löydetään melkein aina jotain mielenkiintoisia havaintoja. Alapuolelle on listattuna muutamia olennaisia asioita tämän kyselyn pohjalta. Kappaleen alussa on ilmoitettu kohderyhmä ja sitten havainnot.

Yrittäjä/Omistaja (N=112) ja Toimitusjohtaja (N=43) versus muut. Noin 63 % toimitusjohtajista oli sitä mieltä, että tärkeimpänä yrityksen kehittämiskohteena on henkilöstön perehdyttäminen ja kouluttaminen. Koulutuskysymyksissä toimitusjohtajien vastaukset olivat järjestäen korkeampi kuin koko otannan. Yrittäjistä samaa mieltä oli vain noin 35 % ja koulutuskysymyksissä vastaukset olivat pienempiä kuin koko otanta. Tähän vaikuttaa todennäköisesti yrityksen koko. Yleensä toimitusjohtajien yritykset ovat useamman henkilön työllistäviä, jolloin näkemyserot tulevat kyseeseen.

EU- Lainsäädäntö (N=33). Henkilöt, jotka olivat tietotoisia EU-lainsäädännöstä, pitivät asiakasrekisterin ja tuotetietojen turvaamista tärkeämpänä kuin vastaajat, jotka eivät olleet lainsäädännöstä tietoisia. Kohdassa yritykselle on laadittu tietoturvaohjeistus kohderyhmän osuus (58 %) oli huomattavasti suurempi kuin koko otanta (26 %). Myös häiriötilanteisiin varautuminen on järjestäen korkeampi kuin koko otanta.

Tietoturvaohje (N=52). Kohdassa oletko tietoinen EU-lainsäädännöstä kohderyhmän osuus (37 %) oli huomattavasti suurempi kuin koko otanta (16 %). Myös häiriötilanteisiin varautuminen on järjestäen korkeampi kuin koko otanta. Tärkeimpänä kehittämiskohteena tämä ryhmä näkee koulutuksen lisäämisen (65 %) ja käyttäjien osaamisen kasvattamisen (62 %). Luvut ovat huomattavasti suurempia kuin koko otannan (37 % ja 46 %). Yrityksistä, joissa ei ole tietoturvaohjetta, 10 % kertoo, että tietoturva-asiat eivät ole kenenkään vastuulla. Vastaava luku yrityksissä, joissa on tietoturvaohje, on nolla. Myös häiriötilanteisiin varautumisessa on selkeä ero yritysten välillä, joissa on tai ei ole tietoturvaohjetta. Tietoturvaohjeen olemassa ololla näyttäisi siis olevan merkittävä vaikutus yrityksen asenteisiin ja toimintatapoihin tietoturvan suhteen.

Negatiivinen julkisuus. Yritykset, jotka arvioivat kyberhyökkäyksestä aiheutuvan negatiivisen julkisuuden ei suureksi tai vähemmän suureksi, pitivät myös yrityksen muiden tietojen turvaamista vähemmän tärkeänä, kuin yritykset, joille negatiivinen julkisuus on suuri tai erittäin suuri asia.

Yritykseen on tehty tietoturvahyökkäys (N=15). Yritykset, jotka ovat joutuneet tietoturvahyökkäyksen kohteeksi, pitivät ammatillisen perustutkinnon suorittaneiden tietoturvataitoja huomattavasti tärkeämpinä, kuin yritykset, jotka eivät ole joutuneet tietoturvahyökkäyksen kohteeksi. Kaikkiin kyberturvauhkiin suhtautumisessa on nähtävissä ero näiden yritysten välillä. Toinen havainto on, että näissä yrityksessä käytetään enemmän tablet laitteita ja älypuhelimia verrattuna koko otantaan. Vastaavasti omien laitteiden käytön osuus ja tietämys EU-lainsäädännöstä oli huomattavasti suurempi.

Viranomaiset ilmoittivat tietomurrosta. Tietomurron, josta tieto oli tullut viranomaisilta, kohteeksi joutuneita yrityksiä oli neljä kappaletta ja kaikki olivat alle 20 hengen yrityksiä ja kaikki toimivat vain suomessa palvelualalla ja rakennusalalla. Tietoturvaohjeen laadinnassa ei näiden tapausten välillä ollut eroa. Tietoturvaohjeen sisällössä puolestaan oli erona, että nämä neljä yritystä eivät käsitelleet ohjeessa lainkaan etätyötä/etäkäyttöä eikä tietoturvan vastuualueita ja organisointia. Vastaavasti tietoturvauhkiin varautuminen on paremmalla tasolla kuin muilla yrityksillä.

11 Johtopäätökset

Tutkimuksesta voidaan vetää useita johtopäätöksiä. Yritykset eivät tiedosta kyberturvallisuus riskejä tai eivät halua huolehtia niistä. Useassa kysymyskohdassa vastaajat kommentoivat, että ei ole aikaa hoitaa niihin liittyviä toimia. Myös ongelmiin varautuminen oli monen pienen yrittäjän kohdalla heikkoa. Ne yritykset, jotka olivat tehneet tietoturvaohjeen, suhtautuivat asioihin myönteisemmin kuin ne yritykset joilla tietoturvaohjetta ei ollut. Myös koulutukseen panostaminen oli selkeästi tavoitteellista.

Myös asioiden tiedostaminen nousi useammassa kohdassa. Pienet yritykset keskittyvät omaan toimialaan, jolloin tietoturvauhkiin keskittyminen jää kokonaan pois. Useammat eivät usko, että joku haluaisi murtautua pienen yrityksen järjestelmiin. Pienille yrityksille tarvittaisiin tietoturvan tärkeyden korostamista ja asenteiden muuttamista.

Tietoturvakoulutusta pitäisi lisätä kaikissa yrityksissä. On ymmärrettävää, että jokaisella yrityksellä ei ole aikaa lähettää työntekijää useamman päivän koulutukseen, jolloin lyhyet täsmäkoulutukset nousevat vahvempaan rooliin ja ovat muutenkin kannattavampia erityisesti pienen yrittäjän näkökulmasta. Esimerkiksi vastauksissa nousi vahvasti esiin webinaarit, joihin yrittäjillä on helpompi osallistua haluamassaan ajankohdassa

Vastausten perusteella pienien yrityksien kannattaisi ulkoistaa tietoturva asiantuntevalle yritykselle. Aina ei välttämättä tarvita jatkuvaa sopimusta vaan riittäisi, että yritykselle tehtäisiin tietoturvariskien kartoitus. Tämän avulla yrittäjät saisivat nopeasti ja kustannustehokkaasti täsmätietoa yrityksen tietoturvatilanteesta.

12 Toimenpidesuunnitelma

Alapuolella on listattuna tutkimuksen pohjalta olennaisia vinkkejä yrityksille. Näiden avulla toimintaa voitaisiin kehittää yrityksessä eteenpäin.

- Tietoturvaohjeen luominen yritykselle.
- Koulutuksen lisääminen.
- Tietoturvakartoituksen tekeminen.
- Viestintäviraston CERT.FI listan seuraaminen tietoturvauhkista ja haavoittuvuuksista.
- Tietoturvan ulkoistaminen, jolloin aikaa jää yrityksen päätoimialalle.
- Paikallisten tietoturvaseminaarien seuraaminen

Lähteet

Kauppakamari, 2015. Yrityksiin kohdistuvat kyberuhat 2015. Viitattu 22.08.2016. http://helsinki.chamber.fi/media/filer_public/36/0f/360fddcd-4cfe-41a6-ab89-c028aa0bf15c/kyberturvallisuus_2015.pdf

Keski-Suomen Strategia, 2014, Viitattu 22.08.2016 http://www.keskisuomi2040.fi/lataukset/2014-06-06-Keski-Suomen-liitto-Keski-Suomen-Strategia-2040.pdf

Kivikoski, Jouni. Kauppinen, Tatu. 2016. Tutkimus suomalaisten PK-yritysten digitaalisuudesta ja tietoturvasta. Syyskuu 2016. Toimeksiantajat Elisa Oyj ja Yrittäjäsanomat. Viitattu 24.08.2016. http://hub.elisa.fi/download/9327/

Rousku, Kimmo. Kyberturvaopas – Tietoturvaa kotona ja työpaikalla. Talentum. 2014.

Valtiovarainministeriö (2016). EU-tietosuojan kokonaisuudistus. Viitattu 16.08.2016. https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

von Solms, R. & van Niekerk, J (2013). From information security to cyber security. Computers & security 38: 101. Viitattu 15.08.2016. https://www.researchgate.net/profile/Johan_Van_Niekerk2/publication/278325582_From_information_security_to_cyber_security/links/55e052e908aecb1a7cc39eb2.pdf

Liitteet

Liite 1. Yrityskyselyn kysymykset

1. Vastaajan tiedot (vapaaehtoinen)

Nimi _____

Yritys _____

Sähköpostiosoite _____

2. Yrityksen toimipaikan postinumero

_____

3. Olen alla olevan järjestön jäsen?

[ ] Suomen yrittäjät
[ ] Kauppakamari

4. Asemanne yrityksessä?

( ) Toimitusjohtaja
( ) Yrittäjä/omistaja
( ) Muu johtaja
( ) Muu työntekijä
( ) Tietoturva-asioista vastaava henkilö
( ) Tietohallintopäällikkö
( ) Jokin muu, mikä _____

5. Henkilöstön määrä?

( ) 1–4
( ) 5–9
( ) 10–19
( ) 20–49
( ) 50–99
( ) 100–

6. Yrityksellänne on liiketoimintaa?

[ ] Suomessa
[ ] Muissa EU-maissa
[ ] EU:n ulkopuolella

7. Millaista kaupankäyntiä yrityksenne harjoittaa?

[ ] Business-to-business (b2b) eli yritysten välinen kauppa
[ ] Business-to-consumer (b2c) eli kuluttajille suunnattu kauppa
[ ] Business-to-government (b2g) eli julkishallinnolle suunnattu kauppa

8. Yrityksen päätoimiala

( ) Teollisuus
( ) Rakentaminen
( ) Liiketoiminta ja kauppa
( ) Palvelualat
( ) Logistiikka
( ) Teknologia
( ) Jokin muu, mikä _____

9. Millä laitteilla yrityksessänne on pääsy tietoverkkoon (internet)?

[ ] Pöytätietokoneilla
[ ] Kannettavilla tietokoneilla
[ ] Tablet-laitteilla
[ ] Älypuhelimilla
[ ] Yrityksen tuotantoon liittyvillä koneilla/laitteilla
[ ] Jokin muu, mikä _____

10. Käytätkö työasioiden hoitamiseen muita kuin yrityksen laitteita?

( ) Kyllä
( ) Ei

11. Onko yrityksessänne laadittu tietoturvaohje?

( ) Kyllä
( ) Ei

12. Oletko tietoinen EU-lainsäädännöstä kyberturvallisuuteen liittyen?

( ) Kyllä
( ) En

13. Valvotaanko yrityksessänne henkilöstön tietoturva-ohjeen noudattamista?

( ) Kyllä
( ) Ei
( ) En osaa sanoa

14. Mitä seuraavia asioita yrityksenne tietoturvaohjeessa käsitellään?

[ ] Päätelaitteiden ja työvälineiden käyttö
[ ] Käyttöoikeudet, tunnukset ja salasanat
[ ] Internetin ja sähköpostin käyttö
[ ] Toimitilojen turvallisuus
[ ] Sosiaalisen median käyttö
[ ] Tietojen salassapito (vaitiolo)
[ ] Etätyö ja etäkäyttö
[ ] Vastuualueet ja organisointi
[ ] Ongelmatilanteet ja seuraamukset
[ ] Jokin muu, mikä _____

15. Onko henkilökunta perehdytetty tunnistamaan liiketoiminnan kannalta luottamukselliset tiedot?

( ) Kyllä
( ) Ei
( ) En tiedä

16. Miten yrityksen tietoturva-asiat on resurssoitu?

( ) Asioita hoidetaan oman työn ohella
( ) Tehtävään on palkattu asioista vastaava henkilö
( ) Tehtävä on ulkoistettu
( ) Tehtävä ei ole kenenkään vastuulla
( ) Jokin muu, mikä _____

17. Mihin häiriöitilanteisiin yrityksessänne on varauduttu?

[ ] Väärinkäytöksiin
[ ] Järjestelmien toimimattomuuteen
[ ] Sähkökatkoihin
[ ] Tietovuotoihin
[ ] Yritys ei ole varautunut häiriötilanteisiin
[ ] Jokin muu, mikä _____

18. Miten tärkeänä pidät seuraavien asioiden turvaamista?

	Ei tärkeä	Vähemmän tärkeä	Melko tärkeä	Tärkeä	Erittäin tärkeä
Asiakasrekisteri	( )	( )	( )	( )	( )
Tuotetiedot/tuotteet	( )	( )	( )	( )	( )
Taloushallinto	( )	( )	( )	( )	( )

Oma ammattitaito/osaaminen/tieto-taito	( )	( )	( )	( )	( )
Tuotekehitys/tuotekehitystiedot	( )	( )	( )	( )	( )
Pankkitiedot/pankkiyhteydet	( )	( )	( )	( )	( )

19. Miten suurina kyberturvallisuusuhkina pidätte seuraavia asioita yrityksessänne?

	Ei suuri	Vähemmän suuri	Melko suuri	Suuri	Erittäin suuri
Yhtiön sisäinen uhka (omat työntekijät)	( )	( )	( )	( )	( )
Phishing- (verkkourkinta, tietojen kalastelu) ja haittaohjelmahyökkäykset	( )	( )	( )	( )	( )
Tietojärjestelmiin tunkeutumiset	( )	( )	( )	( )	( )
Palvelunestohyökkäykset (tarkoituksena on estää verkkopalvelun toiminta)	( )	( )	( )	( )	( )
Hyökkäykset jotka kohdistuvat yrityksen tuotantoprosesseihin (esim. verkkoon kytketty tuotantoon liittyvä kone tai laite)	( )	( )	( )	( )	( )

20. Miten suurena esteenä pidätte seuraavia asioita tehokkaan kyberturvallisuuden toteuttamiseksi yrityksessänne?

	Ei suuri	Vähemmän suuri	Melko suuri	Suuri	Erittäin suuri
Osaavien ammattilaisten löytämisen vaikeus	( )	( )	( )	( )	( )
Nykyisen henkilökunnan tieto-taidon ylläpitäminen kyberuhkien suhteen	( )	( )	( )	( )	( )

Henkilökunnan piittaamattomuus tietoturvallisuudesta ja kyberuhista	( )	( )	( )	( )	( )
Kyberuhkiin liittyvän tiedon riittämättömyys	( )	( )	( )	( )	( )
Turvallisuustoimiin ja menetelmiin liittyvän tiedon riittämättömyys	( )	( )	( )	( )	( )
Sopimattomat/vanhentuvat työvälineet (ohjelmistot ja laitteet joissa verkkoyhteys)	( )	( )	( )	( )	( )

21. Miten merkittävinä pidätte seuraavia kyberhyökkäyksestä aiheutuvia seurauksia?

	Ei suuri	Vähemmän suuri	Melko suuri	Suuri	Erittäin suuri
Aineettoman omaisuuden menetys	( )	( )	( )	( )	( )
Negatiivinen julkisuus	( )	( )	( )	( )	( )
Markkinaosuuden menetys	( )	( )	( )	( )	( )
Yksityisyyden (henkilökunnan tai asiakkaiden tiedot) loukkaus	( )	( )	( )	( )	( )
Tuoton menetys – suora tai epäsuora	( )	( )	( )	( )	( )

22. Tärkeimmät kehittämiskohteet yrityksenne kyberturvallisuudessa?

[ ] Oma/yrittäjän tietoturvaosaaminen
[ ] Henkilökunnan/käyttäjien osaaminen
[ ] Varmuuskopiointi/varmistukset
[ ] Koulutuksen/tiedon lisääminen
[ ] Laitteet/laitteisto/koneet
[ ] Varajärjestelmät
[ ] Ohjelmistojen päivittäminen
[ ] Kulunvalvonta
[ ] Jokin muu, mikä _____

23. Mitkä seuraavista tietoturvauhkista ovat toteutuneet yrityksessänne?

[ ] Käyttäjätunnuksia ja salasanoja on varastettu ja niitä on väärinkäytetty
[ ] On yritetty urkkia tai vakoilla työtehtäviin liittyviä tietoja
[ ] Identiteetti on varastettu ja sitä on väärinkäytetty
[ ] Organisaatio on menettänyt rahaa nettihuijauksen takia
[ ] Yrityksen tietoja on vuotanut
[ ] Yritys on menettänyt tärkeitä tietoja laiterikon tai vastaavan takia
[ ] Päätelaite on varastettu tai hävinnyt
[ ] Työntekijä on saanut näkyville tai tietoonsa salassa pidettäviä tietoja, joihin hänellä ei ole ollut oikeutta
[ ] Työpaikan luottokorttia on käytetty väärin
[ ] Yritykseen on tehty tietoturvahyökkäys
[ ] Yritykseen ei ole kohdistunut tietoturvauhkaa
[ ] Jokin muu, mikä _____

24. Miten havaitsitte edellisessä kysymyksessä tarkoitetun tietoturvauhkan?

[ ] Havaitsimme sen itse käyttäen omia torjunta- ja hälytysjärjestelmiämme
[ ] Käyttäjämme tunnistivat sen ja ilmoittivat eteenpäin
[ ] Tunnistimme itse, koska tarkastamme ja analysoimme lokejamme
[ ] Kotimaiset lainvalvontaviranomaiset tai tiedusteluorganisaatiot varoittivat meitä
[ ] Kolmas taho, kuten internet operaattori tai palveluntarjoaja, ilmoitti meille
[ ] Jokin muu, mikä _____

25. Minkälaista tietoa luulette tunkeutujien etsivän?

[ ] Ylempään johtoon kuuluvien henkilökohtaista tietoa
[ ] Henkilökuntaan liittyvää tietoa, kuten nimet, vastuualueet ja yksiköt
[ ] Tietoa alihankkijoista, yhteistyökumppaneista, tavarantoimittajista tai asiakkaista
[ ] Luottamuksellista tietoa tuotteistamme tai palveluistamme
[ ] Tietoverkkoonne liittyvää tietoa, kuten verkon rakennetta ja muita laitteita yrityksen verkossa
[ ] Emme osaa sanoa
[ ] Jokin muu, mikä _____

26. Onko yrityksenne henkilöstö ollut viimeisen vuoden aikana tietoturvaan liittyvässä koulutuksessa?

( ) Ei
( ) Kyllä, missä? _____

27. Mistä tietoturva osa-alueista haluaisit saada koulutusta?

[ ] Hallinnollinen tietoturva - Tietoturvan johtaminen ja hallinnointi
[ ] Fyysinen tietoturva - Toimitilojen ja laitteiden fyysinen suojaaminen
[ ] Laitteistoturvallisuus - Esimerkiksi tietokoneiden yleinen suojaaminen
[ ] Ohjelmistoturvallisuus - Ohjelmistojen tietoturvaan liittyvät asiat
[ ] Tietoaineiston turvallisuus - Sähköisten ja paperisten dokumenttien käsittely ja suojaaminen

[ ] Tietoliikenneturvallisuus - Esimerkiksi tiedonsiirtoon liittyvät tietoturvamekanismit
[ ] Henkilöstöturvallisuus - Rooleihin, vastuihin ja tietoturvaohjeistuksiin liittyvät asiat
[ ] Käyttöturvallisuus - Esimerkiksi salasanoihin liittyvät asiat
[ ] Jokin muu, mikä _____

28. Mikä olisi mielestäsi sopiva pituus koulutukselle?

( ) 4 tuntia
( ) Koko päivä
( ) Kaksi päivää
( ) Jokin muu, mikä _____

29. Olisiko yrityksenne kiinnostunut osallistumaan tietoturvaseminaariin/työpajaan?

( ) Kyllä
( ) Ei

30. Kun olette palkanneet/palkkaamassa uutta henkilöstä, he ovat pääasiassa

[ ] Ammatillisen tutkinnon
[ ] Alemman korkeakoulututkinnon
[ ] Ylemmän korkeakoulututkinnon suorittaneita henkilöitä
[ ] Jokin muu, mikä _____

31. Arvioi uusien työntekijöiden tietotekninen osaamistaso.

( ) Heikko
( ) Keskitaso
( ) Hyvä

32. Miten tärkeänä pidät ammatillisen perustutkinnon suorittaneen työntekijän seuraaviin asioihin liittyviä yleisiä tietoturvataitoja?

	Ei tärkeä	Vähän tärkeä	Melko tärkeä	Tärkeä	Erittäin tärkeä
Tietosuojalaki	( )	( )	( )	( )	( )
Medialukutaito	( )	( )	( )	( )	( )
Pilvipalvelut	( )	( )	( )	( )	( )
Sähköposti	( )	( )	( )	( )	( )
Sosiaalinen media	( )	( )	( )	( )	( )
Tietoverkot	( )	( )	( )	( )	( )

Mobiililaitteet	( )	( )	( )	( )	( )
Jokin muu, mikä	( )	( )	( )	( )	( )

33. Millaisia asioita ammatillisen perustutkinnon opiskelijoille pitäisi opettaa tietoturvasta?

_____
_____
_____
_____

34. Pitäisikö kehittää tietoturvakortti, jolla taataan tietty tietämys tietoturvasta?

( ) Kyllä
( ) Ei
( ) En osaa sanoa

35. Mitä osaamista tietoturvakorttikoulutuksen pitäisi pitää sisällään?

_____
_____
_____
_____

36. Vapaa sana:

_____
_____
_____
_____