Camilla Mild

YRITYSTEN KYBERTURVALLISUUS

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutus
Toukokuu 2024

TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Toukokuu 2024	**Tekijä/tekijät** Camilla Mild
Koulutus Tieto- ja viestintätekniikka		☒ AMK ☐ YAMK
Työn nimi YRITYSTEN KYBERTURVALLISUUS		
Työn ohjaaja Henry Paananen		**Sivumäärä** 49 + 1
Työelämäohjaaja		

Opinnäytetyön tarkoituksena oli selvittää, millaisia toimenpiteitä eri kokoisissa yrityksissä tehdään kyberturvallisuuden edistämiseksi. Vertailua tehtiin myös yritysten toimialojen ja -paikkojen välillä.

Opinnäytetyö toteutettiin pääosin kvantitatiivisena tutkimuksena, yhdistellen työhön myös kvalitatiivisen tutkimuksen menetelmiä. Tutkimus toteutettiin kyselytutkimuksena Webropol-ohjelmalla, ja vastausten kerääminen tapahtui henkilökohtaisilla sähköpostiin lähetetyillä kyselylinkeillä.

Tutkimuksen tuloksena voitiin todeta, että kyberturvallisuutta toteutetaan hyvin vaihtelevasti erikokoisissa yrityksissä. Suuryrityksissä kyberturvallisuuteen panostettiin enemmän, kun taas pienissä yrityksissä toimenpiteitä oli käytössä vähemmän. Keskisuuret yritykset sijoittuivat toimenpiteiden laajuudessa kahden edellä mainitun välille. Toimialoista teollisuus erottui kyberturvallisuuteensa panostavana alana, ja alueita vertaillessa huomattiin, että kansainvälisesti sekä koko Suomessa toimivat yritykset panostivat kyberturvallisuuteensa keskimääräistä enemmän.

Asiasanat
Kyberhyökkäys, kyberturvallisuus, tietosuoja, tietoturvallisuus

ABSTRACT

Centria University of Applied Sciences	**Date** May 2024	**Author** Camilla Mild
Degree programme Information Technology		
Name of thesis Corporate Cybersecurity		
Centria supervisor Henry Paananen		**Pages** 49 + 1
Instructor representing commissioning institution or company		

The purpose of the thesis was to find out what kind of measures were taken in companies of different sizes to promote cyber security. The comparison was also made between the industries and locations of the companies.

The thesis was mainly carried out as a quantitative study, combining qualitative research methods into the work as well. The research was carried out as a survey using the Webropol application, and responses were collected through personal survey links sent via email.

As a result of the research, it was found that cyber security was implemented very differently in companies of different sizes. Larger companies invested more in cyber security, while in small companies fewer measures were used. Medium sized companies fell between the two categories mentioned earlier in terms of the extent of their measures. Among the industries, manufacturing sector stood out as the sector that invested in its cyber security, and when comparing the regions, it was noticed that companies operating internationally as well as in the whole Finland invested in their cyber security more than average.

Key words
Cyber attack, cyber security, data protection, data security

KÄSITTEIDEN MÄÄRITTELY

DRP

Toipumissuunnitelma (*Disaster Recovery Plan*)

GDPR

Yleinen tietosuoja-asetus (*General Data Protection Regulation*)

IAM

Identiteetin- ja pääsynhallinta (*Identity and Access Management*)

IT

Informaatioteknologia

OT

Operatiivinen teknologia

On-Premise

Ratkaisu, jossa laitteet sijaitsevat paikallisesti yrityksen omissa tiloissa.

VPN

Virtuaalinen erillisverkko

TIIVISTELMÄ
ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

1 JOHDANTO 1

2 KYBERTURVALLISUUS KÄSITTEENÄ 2
2.1 Kyberturvallisuus 2
2.2 Tietosuoja 2
2.3 Tietoturva 3
2.4 Tietoturvan osa-alueet 3
2.4.1 Hallinnollinen tietoturva 3
2.4.2 Henkilöstön tietoturva 4
2.4.3 Toimitilojen tietoturva 4
2.4.4 Laitteiden tietoturva 4
2.4.5 Ohjelmistojen tietoturva 5
2.4.6 Tietoliikenteen turvallisuus 5
2.4.7 Tietoaineiston turvallisuus 5

3 YLEISIÄ KYBERTURVALLISUUSUHKIA 6
3.1 Kiristysohjelmat 6
3.2 Haittaohjelmat 7
3.2.1 Virukset 7
3.2.2 Madot 7
3.2.3 Troijalaiset 8
3.3 Sosiaalinen manipulointi 8
3.4 Dataan kohdistuvat uhat 8
3.5 Palvelunestohyökkäykset 9
3.6 Internetin saatavuuteen kohdistuvat uhat 10
3.7 Tiedon manipulaatio ja häirintä 10
3.8 Toimitusketjuhyökkäykset 11

4 KYBERTURVALLISUUSRISKIT 12

5 KYBER- JA TIETOTURVALLISUUDEN TOTEUTTAMINEN 15
5.1 Päivitykset 15
5.2 Torjuntaohjelmat 15
5.3 Vahva autentikointi ja salasanakäytännöt 15
5.4 Palomuurit 16
5.5 Varmuuskopiointi 17
5.6 Fyysinen turvallisuus 17
5.7 Tietojen salaus ja luokittelu 17
5.8 Käyttäjätietojen- ja käyttöoikeuksien hallinta 18
5.9 Perehdytys ja koulutus 18

6 KYSELYTUTKIMUS 20
6.1 Tutkimusmenetelmä ja kohderyhmä 20
6.2 Aineiston käsittely ja analysointi 21

7 TUTKIMUSTULOKSET 22
7.1 Taustatiedot 22
7.2 Kyberturvallisuuspolitiikka ja DRP 26
7.3 Käytänteet 31
7.4 Uhat ja toiminta hätätilanteissa 38
7.5 Ulkoiset palvelut 40
7.6 Tulevaisuuden haasteet 43

8 POHDINTA JA PÄÄTELMÄT 45

LÄHTEET 47
LIITTEET

KUVIOT

KUVIO 1. Kyberturvallisuusriskien hallinnan kerrokset 13
KUVIO 2. Yritysten kokoluokat 22
KUVIO 3. Yritysten päätoimialueet 23
KUVIO 4. Yritysten toimialat 25
KUVIO 5. Kyberturvallisuuspolitiikan käyttö eri yrityskokojen välillä 26
KUVIO 6. Kyberturvallisuuspolitiikan käyttö koko vastaajaryhmän kesken 27
KUVIO 7. Kyberturvallisuuspolitiikan päivittäminen koko vastaajaryhmän kesken 29
KUVIO 8. Toipumissuunnitelman käyttö eri yrityskokoluokissa 30
KUVIO 9. Toipumissuunnitelman käyttö koko vastaajaryhmän kesken 30
KUVIO 10. Tietoturvakäytänteet koko vastaajaryhmän kesken 32
KUVIO 11. Tietoturva-arvioinnit ja -testaukset koko vastaajaryhmän kesken 33
KUVIO 12. Fyysiset turvatoimet eri yrityskokoluokissa 34
KUVIO 13. Fyysiset turvatoimet yrityksissä koko vastaajaryhmän kesken 35
KUVIO 14. Tietoturvakoulutusten järjestämistiheys yrityksissä 36
KUVIO 15. Tietoturvauhkien kokeminen yrityksissä koko vastaajaryhmän kesken 38
KUVIO 16. Toimenpiteet hätätilanteissa koko vastaajaryhmän kesken 40
KUVIO 17. Ulkopuolisten kyber- ja tietoturvapalveluiden käyttö yrityksissä koko vastaajaryhmän kesken 41
KUVIO 18. Ulkopuoliset kyber- ja tietoturvapalvelut yrityksissä koko vastaajaryhmän kesken 42

1 JOHDANTO

Nyky-yhteiskunnassa teknologisten ratkaisujen käyttö ja digitaalisten palvelujen hyödyntäminen ovat vahvasti läsnä niin työelämässä, hallinnossa kuin yksityishenkilöidenkin arjessa. Kaikkeen tähän liittyy aina myös riskejä, jotka voivat uhata niin yksittäisten ihmisten kuin yritystenkin turvallisuutta. Tämä on yksi syy, jonka vuoksi kyberturvallisuus on noussut keskeiseksi aiheeksi niin yksityisen kuin julkisenkin sektorin yrityksissä.

Kyberturvallisuus käsitteenä kattaa useita osa-alueita, kuten tietosuojan, tietoturvan ja erilaiset kyberuhat. Tässä opinnäytetyössä tarkastellaan kyberturvallisuuden peruskäsitteitä, toimenpiteitä sekä yleisimpiä kyberuhkia, joita organisaatioissa voidaan kohdata. Näiden lisäksi käsitellään kyberturvallisuusriskejä ja keinoja niiden hallintaan.

Kyselytutkimuksen avulla on tavoitteena selvittää, millaisia toimenpiteitä eri kokoisissa yrityksissä tehdään kyberturvallisuuden edistämiseksi. Lisäksi vertaillaan vastauksia yritysten toimialan ja -paikan perusteella. Tarkastelun kohteena ovat erilaiset käytännön toimenpiteet, kuten päivitykset, torjuntaohjelmat, vahva autentikointi ja salasanakäytännöt sekä palomuurit ja varmuuskopiointi. Lisäksi tarkastellaan, onko yrityksissä käytössä kyberturvallisuuspolitiikkaa tai DRP:tä (Disaster Recovery Plan), jotka ovat olennainen osa kyberuhkiin varautumista ja kriisitilanteisiin valmistautumista. Tutkimuksen avulla on tavoitteena saada tietoa organisaatioiden kyberturvallisuuskäytännöistä, -haasteista ja tulevaisuuden näkymistä.

Opinnäytetyön lähteinä käytetään kyberturva-alan sivustoja, viranomaisten julkaisuja sekä kansainvälisiä tutkimuksia ja raportteja. Näiden avulla pyritään varmistamaan opinnäytetyön sisällön ajankohtaisuus kyberturvallisuuden nykytilanteen kannalta.

2 KYBERTURVALLISUUS KÄSITTEENÄ

Kyber- ja tietoturvallisuus ovat tänä päivänä keskeisiä aiheita, ja teknologian rooli arjessamme on jatkuvasti kasvussa. Kehitys on tuonut mukanaan sekä mahdollisuuksia että haasteita. Samalla kun jatkuvasti kehittyvät teknologiat ja palvelut helpottavat päivittäistä elämäämme, ne myös altistavat meidät jatkuvasti uusille riskeille ja uhille. Tässä luvussa käsitellään tarkemmin kyberturvallisuuteen liittyviä käsitteitä.

2.1 Kyberturvallisuus

Kyberturvallisuudella tarkoitetaan tietoverkkojen, järjestelmien ja ohjelmien suojaamista erilaisilta hyökkäyksiltä ja uhilta, joita ovat tyypillisesti kalastelu, virukset tai erilaiset haittaohjelmat. Kyberturvallisuushyökkäykset voivat yksilötasolla johtaa esimerkiksi identiteettivarkauksiin tai tietojen katoamiseen. (Cisco 2024a.) Myös yrityksiin voi kohdistua laajasti erilaisia kyberhyökkäyksiä ja näiltä onkin ensiarvoisen tärkeää suojautua parhain mahdollisin keinoin. Suomessa viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta valvoo ja kehittää Liikenne- ja viestintäviraston Kyberturvallisuuskeskus (Kyberturvallisuuskeskus 2024).

2.2 Tietosuoja

Tietosuojalla tarkoitetaan perusoikeutta, jonka avulla turvataan rekisteröidyn oikeuksien ja vapauksien toteutuminen käsiteltäessä henkilötietoja. Sen tarkoituksena on määritellä millä edellytyksillä ja milloin henkilötietoja voidaan käsitellä. Tietosuojasta puhuttaessa esille nousevat termit henkilötieto, rekisteröity, rekisterinpitäjä ja henkilötietojen käsittelijä. Henkilötietojen käsittelyn tulee aina olla lakiperusteista. Henkilötiedoilla tarkoitetaan kaikkea tietoa, joka liittyy luonnolliseen henkilöön, joka on tunnistettavissa. Luonnollinen henkilö on tunnistettavissa, jos hänet voidaan suoraan tai epäsuorasti tunnistaa erilaisten tunnistetietojen avulla. Näitä tietoja voivat olla esimerkiksi nimi, henkilötunnus, verkkotunnistetiedot, osoitteet ja sijaintitiedot, mielipiteet, ammattinimike, ääni tai kuva, taikka ainutlaatuiset henkilökohtaiset ominaisuudet, kuten fyysiset, fysiologiset, psykologiset, biologiset, taloudelliset, kulttuurilliset tai sosiaaliset piirteet. Tiedot voivat olla tallennettuina esimerkiksi tietokannoissa, sähköisinä tiedostoina, paperisina, mapeissa, tai ääni- ja kuvatallenteena. Osa henkilötiedoista on riskialttiimpia kuin toiset, ja niitä tulee myös suojata korkeammalla suojaustasolla. (Tietosuojavaltuutetun toimisto 2024.)

Rekisteröidyllä tarkoitetaan henkilöä, jota henkilötieto koskee. Rekisterinpitäjä taas on taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Se voi olla yksityishenkilö, organisaatio, virasto tai muu yhteisö. Kun puhutaan henkilötietojen käsittelijästä, tarkoitetaan rekisterinpitäjästä ulkopuolista tahoa, joka toimii rekisterinpitäjän puolesta henkilötietojen parissa. (Tietosuojavaltuutetun toimisto 2024.)

Tietosuoja ja tietoturva eroavat toisistaan, vaikka ne liittyvätkin vahvasti samaan aihealueeseen. Tietoturva on keino, jolla tietosuojaa toteutetaan. Sen avulla suojataan tietoaineisto ja tietojärjestelmät, varmistetaan tiedon luottamuksellisuus ja eheys sekä järjestelmien käytettävyys ja rekisteröidyn oikeuksien toteutuminen. (Tampereen yliopisto 2020.)

2.3 Tietoturva

Tietoturvallisuudella, puhekielessä tietoturvalla, tarkoitetaan toimenpiteitä ja menetelmiä, joilla suojataan tietoaineistot ja tietojärjestelmät sekä palvelut niin, että luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit ovat otettu huomioon. Toisin sanoen tietojärjestelmät ja tiedot tulee pitää vain niiden henkilöiden saatavilla, jotka ovat oikeutettuja niiden käyttöön. Sivullisille ei tule antaa mahdollisuutta muuttaa, käsitellä tai poistaa tietoja. Vaikka henkilö olisi oikeutettu käyttämään tietoja ja tietojärjestelmiä työssään, tulee niitä käyttää vain asianmukaisesti työtehtävissä, joihin niitä tarvitaan. (Tampereen yliopisto 2020.)

2.4 Tietoturvan osa-alueet

Tietoturva on tavallisesti jaoteltu seitsemään eri osa-alueeseen, joita ovat hallinnollinen, henkilöstön, toimitilojen, ohjelmistojen, tietoliikenteen ja tietoaineiston tietoturvallisuus. Tietoturva on aina kokonaisuus, ja vaikka osa siitä olisi kunnossa, voivat riskit toteutua heikommin suojatun osan kautta. Tästä syystä on ehdottoman tärkeää, että kaikki tietoturvan osa-alueet ovat kartoitettu ja suojattu. (Data Group 2021.)

2.4.1 Hallinnollinen tietoturva

Hallinnollinen tietoturva on kriittinen alue organisaation tietoturvassa. Siihen kuuluvat yrityksen tietoturvakäytäntöihin- ja strategiaan liittyvät toimet, joita ovat esimerkiksi ohjeistukset, menettelyt, kontrollit ja koulutukset. Hallinnollista tietoturvaa ohjataan eri tavalla, kuin muita tietoturvan osa-alueita.

Tarkoituksena on varmistaa kaikkien tietoturvan osa-alueiden olevan riittävällä tasolla. Hallinnollisen tietoturvan osa-alueisiin kuuluvat mm. tietoturvakoulutus, tietoturvastrategia, tietoturvavalvonta ja riskienhallinta. Tavallisesti hallinnollinen tietoturva viittaa yritysten kohdalla tietoturvan johtamiseen. Yrityksen olisi ideaalia luoda tietoturvapolitiikka, joka ohjaa sen toimintaa, ja määrittelee tavoitteita, ohjeita, vastuita ja sääntöjä tietoturvan hallintaa varten. Politiikkaa luodessa tulisi ottaa huomioon liiketoiminnan ja lainsäädännön vaatimukset. (Jurvanen 2023b.)

2.4.2 Henkilöstön tietoturva

Henkilöstön tietoturvaan kuuluvat henkilökunnan ohjeistukset, roolit ja vastuut. Yritykseen voidaan kohdistaa hyökkäyksiä, joita pyritään tekemään henkilöstön kautta. Työntekijä saattaa päätyä helposti klikkaamaan saastunutta liitettä tai linkkiä, joka on lähetetty työntekijälle tutun henkilön nimissä. Näitä tapauksia on vaikeaa estää ainoastaan teknisillä ratkaisuilla. Organisaatiossa on tärkeää olla käytössä selkeät tietoturvakäytännöt ja -ohjeet, joiden avulla voidaan parantaa tietoturvaan liittyvien sääntöjen toteutumista ja noudattamista. Henkilökuntaa on myös tärkeää kouluttaa tietoturvaan liittyen säännöllisesti. Kun kaikki yrityksen työntekijät ja kumppanit tuntevat selkeän toimintasuunnitelman ja ohjeet erilaisiin tilanteisiin, pienentää se riskejä ja tehostaa työn suorittamista odottamattomien tilanteiden sattuessa kohdalle. (Data Group 2021.)

2.4.3 Toimitilojen tietoturva

Toimitilojen tietoturva, jota usein kutsutaan myös fyysiseksi tietoturvaksi, on joukko keinoja, joilla pyritään suojaamaan yrityksen tietoja fyysisiltä uhilta. Perustana ovat fyysiset rakenteet, jotka suojaavat tietojen käsittelyyn ja säilytykseen käytettäviä tiloja. Fyysiseen tietoturvaan kuuluvat myös esimerkiksi näkösuojat, kulunvalvonta ja äänieristys. Sen vastuulla on suojata työ- ja tuotantotiloja sekä niiden sisällä sijaitsevia laitteita, dokumentteja ja tietojärjestelmiä erilaisia uhkia vastaan. (Jurvanen 2023a.)

2.4.4 Laitteiden tietoturva

Käytössä olevien laitteiden suojaaminen on ensisijaisen tärkeää yrityksen tietoturvan kannalta, ja yli 70 % tietoturvatapahtumista ja hyökkäyksistä tapahtuukin päätelaitteen kautta (Reimaa 2023). Laitteiden tulee olla käyttötarkoitukseensa sopivia ja niiden päivityksien olla osaavan henkilön vastuulla. Laitteita voidaan hallita automaattisesti, jolloin käyttäjän ei tarvitse huolehtia asiasta. Keskitetty hallinta tehostaa laitteiden ja palveluiden käyttöönottoa, jatkuvaa seurantaa sekä päivityksiä vastaamaan

tarvittavia profiileja. Tämän kaltainen automatisointi ja asetukset vähentävät inhimillisiä erehdyksiä. (Data Group 2021.)

2.4.5 Ohjelmistojen tietoturva

Käytettävien ohjelmistojen turvallisuus on tärkeä osa yrityksen tietoturvaa. Yrityksessä käytössä olevissa laitteissa tulisi olla asennettuna ainoastaan sellaiset ohjelmistot, jotka ovat olennaisia yritystoiminnan sujuvuuden kannalta sekä yrityksen hyväksymiä ja turvalliseksi varmistettuja. Näiden lisäksi on tärkeää määritellä, millaisia pilvipalveluja yrityksessä voidaan turvallisesti käyttää. Erityistä huomiota tulisi kiinnittää myös vahvaan tunnistautumiseen, etenkin jos kyseessä on ohjelmisto, joka sisältää arkaluonteisia tietoja tai toimintoja. (Data Group 2021.)

2.4.6 Tietoliikenteen turvallisuus

Tietoliikenteen turvallisuus on tiedonsiirtoon liittyvää turvallisuutta. Yrityksen tiedon siirtyminen verkossa, olipa kyseessä sitten sisäinen verkko tai internet, edellyttää asianmukaisia verkkoja, laitteita ja konfiguraatioita, jotka on valittava ja toteutettava huolellisesti sekä pidettävä päivitettynä. Tämän lisäksi on tärkeää varmistaa sähköpostin ja muun internetliikenteen turvallisuus. (Data Group 2021.) Turvallisuuteen voidaan investoida suuria summia ja vaikka käytössä olisi uusia koneita, laitteita tai järjestelmiä, voi niiden hyöty jäädä olemattomaksi, mikäli yrityksellä ei ole toimintavarmaa ja turvallista tietoliikennettä (Erillisverkot 2024.)

2.4.7 Tietoaineiston turvallisuus

Tietoaineiston turvallisuus on yrityksen tietoturvallisuuden osa-alue, johon kuuluu tietoa sisältävien dokumenttien hallinta ja turvallisuus. Hyvän tiedonhallinnan avulla voidaan minimoida useita tietoturvariskejä. On olennaista määrittää, mitä tietoa käsitellään, missä sitä säilytetään, kuka sitä saa käsitellä ja miten sen käsittely suoritetaan. Selkeät ja yksinkertaiset toimintatavat auttavat säilyttämään tiedot ja niiden eri versiot järjestyksessä ja saatavilla oikeille tahoille. Tämä tekee myös tiedon varmistamisesta helpompaa. Viranomaisvaatimusten, kuten GDPR:n noudattaminen on sujuvampaa, kun yrityksellä on selkeä tiedonhallintapolitiikka ja kattava dokumentaatio tietoaineistoista. (Data Group 2021.)

3 YLEISIÄ KYBERTURVALLISUUSUHKIA

Maailma muuttuu kyberturvallisuuden osalta vauhdilla ja uhkakuvat ovat hyvin erilaisia, kuin vielä kymmenen vuotta sitten. ENISA (European Union Agency for Cybersecurity) on listannut vuosittaisessa katsauksessaan vuoden 2023 tärkeimpiä trendejä uhkien, toimijoiden, hyökkäystekniikoiden ja motivaatiotekijöiden osalta. Kahdeksan pinnalla olevaa uhkaa olivat kiristysohjelmat, haittaohjelmat, sosiaalinen manipulointi, dataan kohdistuvat uhat, palvelunestohyökkäykset, internetin saatavuuteen kohdistuvat uhat, tietojen manipulointi ja toimitusketjuhyökkäykset. (ENISA 2023.) Oman havaintoni mukaan osa teemoista on ollut pinnalla jo pitkään, mutta hyökkäykset toki kehittyvät ja monipuolistuvat jatkuvasti.

Kyberrikollisuus on kasvussa ja eSentire on arvioinut vuoden 2023 virallisessa kyberrikollisuusraportissaan maailmanlaajuisten kyberrikollisuuteen liittyvien kulujen saavuttavan 9,5 biljoonaa Yhdysvaltain dollaria vuonna 2024 (eSentire 2023). Kyberrikollisuuden kulut voivat koostua tietojen tuhoutumisesta ja vahingoittumisesta, kavalluksista, petoksista, henkilö- ja taloustietojen varkauksista, immateriaalioikeuksien varkauksista, rahavarkauksista, rikosteknisestä tutkinnasta, tuottavuuden menetyksestä, hakkeroitujen tietojen tai järjestelmien palauttamisesta, hyökkäyksen jälkeisistä häiriöistä liiketoiminnassa tai mainevahingoista (Cybercrime Magazine 2020).

3.1 Kiristysohjelmat

Kiristysohjelmat ovat hyökkäystyyppi, jossa hyökkääjät estävät yritystä tai käyttäjää pääsemästä käsiksi oman organisaationsa dataan salaamalla sen salausalgoritmilla ja vaatimalla lunnaita vastineeksi tietojen palauttamisesta. Rikolliset eivät ainoastaan salaa tietoja, vaan saattavat myös varastaa arkaluonteista dataa uhatakseen organisaatiota tietojen julkaisemisella. Kiristyshaittaohjelmat ovat osoittautuneet taloudellisesti tuottoisiksi keinoiksi kyberrikollisille, sillä niihin valmistautumattomat yritykset ovat usein alttiita tällaisille iskuille. Lunnaiden maksaminen ei kuitenkaan tarjoa varmaa ratkaisua tilanteen korjaamiseen, sillä se ei takaa tietojen palautusta, eikä myöskään estä tulevia hyökkäyksiä. Joskus rikollisten ainoa tarkoitus saattaa olla tiedon tuhoaminen ja tässä tapauksessa lunnaiden maksaminen ei auta tiedon palautuksessa millään tavalla. (Kyberturvallisuuskeskus 2022b, 2–3.)

Poikkeustilanteisiin varautuminen on keskeistä hyökkäyksen aiheuttamien haittojen vähentämisessä, toipumisen nopeuttamisessa sekä liiketoiminnan normaalin jatkumisen varmistamisessa. Hyvin suunniteltu poikkeamanhallintasuunnitelma on olennainen osa valmistautumista, joka ohjaa toimintaa häiriötilanteiden sattuessa. Organisaation kyky hallita poikkeamia ja palautua niistä nopeasti vaatii jatkuvaa valmistautumista, koulutusta, sekä teknisten ja hallinnollisten toimenpiteiden tehokasta käyttöä. (Kyberturvallisuuskeskus 2022b, 2–3.)

3.2 Haittaohjelmat

Haittaohjelmilla tarkoitetaan haitallisia ohjelmia, jotka ovat kehitetty tunkeutumaan tietokoneverkkoon tai korruptoimaan sitä. Niiden avulla pyritään aiheuttamaan tuhoa ja niitä käytetään myös tietojen varastamiseen. Tavoiteltu hyöty on usein rahallista, mutta joskus ohjelmilla halutaan ainoastaan aiheuttaa sabotaasia hyökkäyksen kohteelle. Esimerkkejä haittaohjelmista ovat madot, virukset ja troijalaiset. (Cisco 2024b.)

3.2.1 Virukset

Virukset ovat haitallisia ohjelmia, jotka monistavat itseään ja leviävät tietokoneesta toiseen aiheuttaen vahinkoa järjestelmän toiminnoille ja datalle. Virukset voivat levitä esimerkiksi sähköposti- tai tekstiviestiliitteiden, sosiaalisessa mediassa lähetettyjen huijauslinkkien tai verkosta ladattujen tiedostojen kautta. Vaikka virukset voivat joskus olla huomaamattomia, on olemassa joitakin varoitusmerkkejä, joihin kannattaa kiinnittää huomiota. Virusta on syytä epäillä, jos tietokone muuttuu ilman syytä erityisen hitaaksi, näytölle ilmestyy usein ponnahdusikkunoita, järjestelmä kaatuu epätavallisen usein, salasanoissa on muutoksia tai tietokoneella on tuntemattomia ohjelmia, joita et ole itse ladannut. Viruksilta voi suojautua pitämällä ohjelmistot päivitettynä, käyttämällä viruksentorjuntaohjelmaa ja olemalla varuillaan, kun klikkaa linkkejä tai lataa tiedostoja ja ohjelmia. Kaikki tärkeä data kannattaa myös varmuuskopioida. (Corrons 2024.)

3.2.2 Madot

Madot ovat haittaohjelmatyyppi, joka kykenee leviämään tietokoneesta toiseen itsestään. Se kykenee monistumaan ilman ihmisen osallistumista, eikä sen tarvitse kiinnittyä ohjelmaan aiheuttaakseen tuhoa. Madot voivat levitä tietokoneisiin esimerkiksi ohjelmistohaavoittuvuuksien tai sähköpostin liite-

tiedostojen kautta. Ne voivat muokata tai poistaa tiedostoja, varastaa tietoja ja asentaa muita haittaohjelmia tietokoneelle. Madot hidastavat usein tietokoneen toimintaa, joten on hyvä pitää silmällä kiintolevyn tilaa ja suorituskykyä. Paras tapa suojautua madoilta on pitää käyttöjärjestelmä ja ohjelmat ajan tasalla sekä olla varovainen epäilyttävien sähköpostien ja liitetiedostojen kanssa. (Norton 2019.)

3.2.3 Troijalaiset

Troijalaiset ovat haittaohjelmia, jotka naamioituvat aidoiksi ohjelmiksi. Käyttäjän ladatessaan tällaisen sovelluksen tai avatessaan tiedoston, tulee käyttäjä tietämättään ladanneeksi haittaohjelman laitteelleen. Troijalaisia saatetaan usein kutsua viruksiksi, vaikka ne eivät niitä ole. Troijalainen ei voi levitä itsenäisesti, kun taas virus voi. Paras tapa suojautua troijalaisilta on pitää käyttöjärjestelmä päivitettynä ja olla varovainen sähköpostien ja linkkien kanssa netissä. (Johansen 2020.)

3.3 Sosiaalinen manipulointi

Sosiaalisen manipuloinnin avulla pyritään psykologisia keinoja käyttäen saamaan käyttäjä tekemään virheitä tai jakamaan arkaluonteisia tietoja. Haitalliset toimet suoritetaan henkilöiden vuorovaikutuksen avulla. Yksi suosituimmista sosiaalisen manipuloinnin muodoista on kalastelu, jossa tavoitteena on usein sähköpostitse tai tekstiviestitse saada käyttäjä klikkaamaan linkkejä, jotka johtavat haitallisille sivustoille. Tavoitteena voi myös olla saada käyttäjä jakamaan arkaluonteista tietoa hyökkäyksen tekijöille tai avaamaan liitteitä, jotka sisältävät haittaohjelmia. Kalasteluviestien piirteitä ovat esimerkiksi kiireen tuntu, pelon herättäminen tai jokin sellainen piirre, joka herättää hyökkäyksen kohteen uteliaisuuden. Toimenpiteitä, joilla hyökkäyksiä voidaan estää ovat monivaiheinen tunnistautuminen, varuillaan olo liian houkuttelevan tarjouksen saadessaan, virustorjuntaohjelman pitäminen ajan tasalla ja epäilyttävistä lähteistä tulevien sähköpostien ja liitteiden avaamatta jättäminen. (Imperva 2024.) Aina kannattaa myös miettiä, ennen kuin avaa viesteissä mukana olevia linkkejä. Jos jokin kuulostaa liian hyvältä, sitä se myös todennäköisesti on.

3.4 Dataan kohdistuvat uhat

Brittiläinen matemaatikko Clive Humby on vuonna 2006 lausunut ”*Data is the new oil*”, data on uusi öljy. Tähän on viitattu myös The Economist -lehden artikkelissa, jossa väitetään, että maailman arvokkain luonnonvara ei ole enää öljy, vaan data. (The Economist 2017.) Ei siis ihme, että dataan kohdistuvat hyökkäykset ovat yksi suurimmista uhista nykypäivänä. Yksi dataan kohdistuvan uhan tyyppi on

tietovuoto, johon eivät liity tahalliset hyökkäykset. Tietovuodon voivat aiheuttaa haavoittuvuudet, inhimilliset virheet tai virheelliset määritykset. Tietovuoto voi aiheuttaa arkaluontoisten tietojen katoamisen tai paljastumisen väärille henkilöille. (ENISA 2023, 83.)

Toinen dataan kohdistuva uhka on tietomurto, jolla tarkoitetaan luvatonta pääsyä tietojärjestelmiin, palveluihin, laitteisiin tai sovelluksiin tunnusten väärinkäytön kautta. Tällaisen toiminnan päämääränä on usein taloudellisen edun hankkiminen, esimerkiksi varastettujen tietojen jälleenmyynnin kautta. Toisinaan hyökkääjä ei suoraan varasta tietoja, vaan kauppaa pääsyä järjestelmään eteenpäin toiselle rikolliselle. Lisäksi hakkeroitua järjestelmää voidaan käyttää levittämään haittaohjelmia tai sen toiminta voidaan pysäyttää käyttämällä kiristyshaittaohjelmia. Järjestelmiä voidaan hyödyntää myös osana laajempia kyberhyökkäyksiä, kuten palvelunestohyökkäyksiä. (Kyberturvallisuuskeskus 2023.)

Tietomurrot tuottavat taloudellista vahinkoa ja mainehaittaa uhriorganisaatiolle, ja ne voivat pysäyttää organisaation normaalin toiminnan joksikin aikaa, esimerkiksi järjestelmien korjaus- tai uudelleenasennustyön ajaksi. Tietomurtojen avulla voidaan toteuttaa myös laskutuspetoksia, joissa taloudelliset menetykset saattavat olla huomattavia. Väärennetty lasku voidaan lähettää organisaation sisältä, jolloin se saatetaan helpommin hyväksyä aitona ja laittaa maksuun. Tietomurron hyödyntäminen voi myös tapahtua paljon myöhemmin, usein murtohetken jälkeen, jolloin organisaatiolta saattaa puuttua kriittisiä lokitietoja tapahtuma-ajankohdalta, mikä taas tekee tilanteen selvittämisestä erityisen haasteellista. (Kyberturvallisuuskeskus 2023.)

3.5 Palvelunestohyökkäykset

Palvelunestohyökkäys on menetelmä, jossa hyökkääjä pyrkii tekemään verkkopalvelun tai resurssin käyttökelvottomaksi häiritsemällä sen normaalia toimintaa. Tämä voi tapahtua ylikuormittamalla kohdetta liiallisella dataliikenteellä tai hyväksikäyttämällä järjestelmän heikkouksia. Useimmat nykyaikaiset palvelunestohyökkäykset ovat laajamittaisia ja hajautettuja, mikä tarkoittaa, että hyökkäysliikenne syntyy monista eri lähteistä samanaikaisesti, tyypillisesti bottiverkkoa käyttäen. Bottiverkko koostuu internetiin liitetyistä laitteista, jotka ovat otettu hallintaan ilman omistajien lupaa. Palvelunestohyökkäykset voivat ilmetä eri tavoin: joko suurella liikennemäärällä tai sellaisen datan lähettämisellä, joka vaatii kohdelaitteelta runsaasti muisti- tai laskentakapasiteettia. Joissakin tapauksissa liikenteen volyymi ei ole suuri, mutta se on suunniteltu kuormittamaan kohdesysteemiä. Esimerkiksi sovellustason palvelunestohyökkäykset voivat kohdistua suoraan sovellusten taustajärjestelmiin, kuten tietokantoihin, aiheuttaen niille ylikuormitusta. (Kyberturvallisuuskeskus 2022c, 2.)

Nykyään palvelunestohyökkäykset ovat helposti toteutettavissa ja niitä voidaan jopa ostaa pimeästä verkosta palveluna. Hyökkäysten motiivit vaihtelevat kiristyksestä poliittiseen häirintään, ja usein hyökkäyksen tilaaja ja toteuttaja ovat eri henkilöitä. Hyökkäystekniikat vaihtelevat, mutta kaikissa on yhteisenä tavoitteena estää laitteen tai palvelun normaali toiminta. Yksi yleisimmistä teknisistä hyökkäystavoista on käyttää bottiverkkoa lähettämään kohteeseen suuria määriä TCP SYN -paketteja ilman vastauspakettien lähettämistä, mikä johtaa kohdejärjestelmän ylikuormittumiseen. Torjunnassa on tärkeää keskittyä tunnistamaan ja ehkäisemään yleisimmät hyökkäystavat, jotta organisaatiossa voidaan suojautua tehokkaasti ja ylläpitää verkkoresurssien saatavuutta. (Kyberturvallisuuskeskus 2022c, 2.)

3.6 Internetin saatavuuteen kohdistuvat uhat

Tänä päivänä pääsy internetiin koetaan usein pakollisena tarpeena. Sitä käytetään niin opiskeluun, työskentelyyn, kuin sosiaaliseen vuorovaikutukseenkin. Tästä huolimatta pääsy internetiin ei ole mahdollinen kaikille.

Internetsulkuja esiintyy useissa maissa ympäri maailmaa. Niiden syyt voivat vaihdella mielenosoitusten, konfliktien, vaalien tai humanitääristen kriisien välillä. Hallitukset ympäri maailmaa löytävät jatkuvasti uusia syitä häiritä internetyhteyksiä. Access Now tunnisti alustavasti 19.5.2023 mennessä ainakin 80 internetsulkua 21:ssä eri maassa vuonna 2023. Internetsulut eivät Access Now’n mukaan ainoastaan ole lisääntymässä, vaan ne myös kohdistuvat erityisesti tiettyihin väestöryhmiin ja otetaan käyttöön nimenomaan silloin, kun yhteydenpidon tarve ihmisten keskuudessa on suurimmillaan. (Access Now 2023.)

3.7 Tiedon manipulaatio ja häirintä

Datamanipulaatiolla tarkoitetaan datan tarkoituksellista muokkaamista tai vääristämistä siten, ettei se enää vastaa todellisuutta. Datan manipuloijien motiivit voivat olla monenlaisia, ja niitä voivat olla esimerkiksi vaalihäirintä, taloudellisen hyödyn tavoittelu, henkilön tai yrityksen mustamaalaaminen, pyrkimys vaikuttaa julkiseen keskusteluun ja poliittiseen päätöksentekoon tai pyrkimys vähentää luottamusta tieteeseen, yhteiskuntaan ja koulutukseen. (Opetushallitus 2024.)

3.8 Toimitusketjuhyökkäykset

Toimitusketjuun kohdistuvassa hyökkäyksessä hyökkääjät pääsevät käsiksi yrityksen tietojärjestelmiin käyttäen hyväksi sen toimittajien, kuten palveluntarjoajien, tuotteiden valmistajien tai avoimen lähdekoodin projektien tarjoamia yhteyksiä. Tällainen hyökkäys perustuu siihen, että yritykset luottavat verkostoonsa kuuluviin tahoihin. Hyökkäys voi tapahtua esimerkiksi kumppaneiden, ohjelmistojen tai laitteiden kautta, kun hyökkääjä tunkeutuu ensin yhden tällaisen toimijan järjestelmiin ja asettaa sitten haittaohjelmansa toimitusketjun osaan, minkä seurauksena haittaohjelma leviää edelleen normaalin jakeluprosessin kautta yhteistyökumppaneille ja loppuasiakkaille. Toimitusketjuun suunnattujen hyökkäysten päätavoitteena on luoda pääsykohta useisiin organisaatioihin toimitusketjussa. Pääsyn saavutettuaan hyökkääjä voi toteuttaa lisähyökkäyksiä, joita voivat olla esimerkiksi tietomurrot tai kiristyshaittaohjelmien levittäminen. (Kyberturvallisuuskeskus 2022d, 2.)

Toimitusketjuhyökkäyksen tunnistaminen ja hallitseminen ovat keskeisiä toimia, sillä ne vaikuttavat merkittävästi yrityksen maineeseen ja sen suhteisiin yhteistyökumppaneidensa kanssa. Hyökkäyksen kohteena oleviin tahoihin kuuluvat sekä toimittaja että loppuasiakas, ja tilanteen ratkaiseminen edellyttää avointa kommunikaatiota ja yhteistyötä kaikkien osapuolten kesken. (Kyberturvallisuuskeskus 2022d, 2.)

4 KYBERTURVALLISUUSRISKIT

Tietotekniikka kehittyy jatkuvasti, jonka takia myös tietoturvaan liittyen kohdataan koko ajan uusia uhkia ja tekniikoita, joiden pyrkimyksenä on hyötyä tietotekniikan ja ihmisten haavoittuvuuksista. Tietoturva on nykyään yksi yritysten riskienhallinnan keskeisimmistä osista, sillä hyökkäysten kasvava määrä voi aiheuttaa yrityksille suuria kustannuksia. Niihin voi sisältyä esimerkiksi maineen vahingoittumista, yksityisyyden rikkomuksia, toimintojen häiriöitä tai osakearvon laskua. (Lee 2021.)

Riskienhallintaan liittyy tavallisesti neljä mekanismia, joita voidaan myös yhdistellä, mikäli tarve vaatii. Ensimmäisessä mekanismissa korjataan se seikka, joka riskin aiheuttaa. Esimerkkinä tästä voidaan käyttää löydetyn haavoittuvuuden korjausta. Toisessa mekanismissa pyritään pienentämään riskiä, esimerkiksi rajaamalla palveluun pääsyä vain organisaation IP-verkkoalueeseen. Kolmannessa mekanismissa pyritään pienentämään riskin vaikutusta esimerkiksi reagointikyvyn ja valvonnan lisäämisellä riskin realisoitumiseen. Neljännessä mekanismissa taas ei varsinaisesti tehdä muuta, kuin päätetään, ettei asialle tarvitse tehdä mitään. Tällöin yrityksessä asiasta päättävät ovat saaneet tiedon ongelmasta sekä sen vaikutuksista ja kustannuksista, jonka jälkeen on tehty päätös, että asia voidaan hyväksyä ilman sen suurempia toimia. (Kyberturvallisuuskeskus 2019.)

Lee (2021) taas esittää, että kyberturvallisuusriskien hallinnan voisi jaotella neljään osaan: kyberekosysteemikerros, kyberinfrastruktuurikerros, kyberriskien arviointikerros ja kybersuorituskykykerros. (KUVIO 1.) Kyberekosysteemikerros on kyberriskien hallinnan ylin kerros. Kyberturvallisuuteen liittyy pääasiassa itsenäisiä tai toisiinsa kytkeytyneitä sidosryhmiä, joiden edut ja tavoitteet eivät aina ole yhteneväisiä. On tärkeää ymmärtää, kuinka nämä sidosryhmät ovat vuorovaikutuksessa IT-resurssien ja -palveluiden, kuten verkkojen, datan ja sovellusten kanssa. Tämän ymmärtäminen on ehdotonta, jotta yrityksen puolustusstrategiaa voidaan kehittää ja sen IT-resursseja suojella kyberhyökkäyksiltä. Kyberekosysteemi myös edistää yhteistyötä sidosryhmien kanssa tukeakseen kyberturvallisuustoimia. On tärkeää, että yritys seuraa ja arvioi jatkuvasti kyberekosysteemiä ja raportoi muutoksista myös muille kerroksille. (Lee 2021.)

KUVIO 1. Kyberturvallisuusriskien hallinnan kerrokset (mukaillen Lee 2021)

Kyberinfrastruktuurikerros on kyberriskien hallinnan keskikerros, jonka tehtäviin kuuluu turvata IT-omaisuutta ja -palveluita. Kerroksen kolme avainelementtiä ovat sisäiset käyttäjät, organisaatiot ja kyberteknologiat. Kerros keskittyy teknologisten ja inhimillisten näkökohtien hallintaan ja heijastaa organisaation nykyistä kyberturvallisuuskykyä. Organisaatioelementin avulla määritellään vastuut, käytännöt, roolit ja prosessit kyberturvallisuuden hallinnassa. Sisäisten käyttäjien elementti taas keskittyy kyberkoulutukseen, työtyytyväisyyteen, moraaliin ja työntekijöiden tietoisuuteen yleisesti. Kyberteknologiaa hyödynnetään havaitsemaan ja torjumaan kyberhyökkäyksiä, minimoimaan riskejä sekä varmentamaan tietojen luottamuksellisuus ja käyttäjien todentaminen. (Lee 2021.)

Kyberriskien arviointikerroksella on keskeinen rooli kyberriskien hallinnassa. Abraham ym. (2019) ovat esittäneet kolmivaiheisen lähestymistavan, joka tarjoaa keinon ymmärtää, lieventää ja arvioida kyberturvallisuusriskejä. Ensimmäinen vaihe on riskien tunnistaminen, jonka avulla keskitytään kyberturvallisuusuhkien paikantamiseen. Toinen vaihe on riskien määrittäminen, jossa määritetään kyberhyökkäysten laajuus ja priorisoidaan hyökkäystyyppejä. Viimeisenä vaiheena on kyberinvestointianalyysi, jossa tarkastellaan kyberinvestointien kustannus–hyöty–suhdetta ja tehdään päätöksiä investoinneista kyberinfrastruktuurissa. (Abraham ym. 2019.) Organisaatioissa tehdään usein riskinarviointeja vain siksi, että yrityksessä noudatettaisiin vaatimuksenmukaisuutta. Vaatimukset voivat olla ulkoisista tekijöistä johtuvia vaatimuksia, asiakkailta tulevia vaatimuksia tai lakisääteisiä vaatimuksia. Riskinä näissä tilanteissa on ajattelumalli, että riskit olisivat automaattisesti hallinnassa, kun toimitaan protokollan mukaan. Niin ei kuitenkaan ole, sillä vaatimusten turvallisuus ja noudattaminen ovat kaksi

eri asiaa. Niissä voi olla päällekkäisyyksiä, mutta heikoillakin turvallisuuskäytännöillä voidaan toteuttaa turvallisuusvaatimuksia. Riskienhallinnan voidaan sanoa olevan silloin hyvällä tasolla, kun se ei ole pelkästään vaatimusten noudattamista. (Kyberturvallisuuskeskus 2020a.)

Kyberarviointikerrokseen kuuluvien investointipäätösten jälkeen siirrytään kybersuorituskykykerrokseen. Kerros keskittyy varsinaisten tietoturvajärjestelmien kehitykseen ja toimintaan, samalla noudattaen riskinarviointikerroksen määrittelemiä suorituskykytavoitteita. Kolme pääkohtaa, jotka kybersuorituskykykerrokseen liittyvät, ovat toteutus, valvonta ja jatkuva parantaminen. Toteutukseen kuuluvat kyberteknologian kehittäminen, kouluttaminen, testaaminen, käyttöönotto sekä uusien käytäntöjen luominen. Valvontaan taas kuuluu kyberhyökkäyksien valvonta, joiden ilmetessä tulee niihin reagoida heti. Tärkeitä samaan aikaan toteutettavia toimintoja ovat ennaltaehkäisy, havaitseminen ja palauttaminen. Valvonnan on pidettävä kirjaa hyökkäyksistä, kuten niiden tyypeistä, esiintymistiheydestä ja vaikutuksista yrityksen toimintaan esimerkiksi sanktioiden, myyntimenetysten tai varastettujen tietojen muodossa. (Lee 2021.)

5 KYBER- JA TIETOTURVALLISUUDEN TOTEUTTAMINEN

Tehokas kyberturvallisuuden toteuttaminen on olennainen osa nykyaikaista tietoturvaa. Tässä osiossa käsitellään erilaisia strategioita ja käytäntöjä, joiden avulla voidaan varmistaa organisaation tietojärjestelmien ja verkkojen turvallisuus. Päivitykset, torjuntaohjelmat, vahva autentikointi ja salasanakäytännöt, palomuurit, varmuuskopiointi, fyysinen turvallisuus, tietojen salaus ja luokittelu, käyttäjätietojen- ja käyttöoikeuksien hallinta sekä perehdytys ja koulutus ovat kaikki keskeisiä osa-alueita kyberturvallisuuden toteuttamisessa. Näiden toimintojen toteuttaminen ja ylläpitäminen auttaa suojaamaan organisaation arkaluonteisia tietoja ja estämään mahdollisia kyberhyökkäyksiä.

5.1 Päivitykset

Ohjelmistojen, laitteiden ja sovellusten päivittäminen on tärkeä osa kyberturvallisuuden toteuttamista. Julkisesti tiedossa olevien haavoittuvuuksien hyväksikäyttö on ollut yleistä jo pitkään. Valmistajien julkaistessa päivityksiä, rikolliset saattavat hyödyntää nopeasti mahdollisuuden hyökätä niihin kohteisiin, joihin ei ole vielä tehty päivityksiä. Päivitykset tulisi tehdä säännöllisesti ainakin käyttöjärjestelmään, tietoturvaohjelmistoon, selaimeen ja sen liitännäisiin, mobiililaitteeseen sekä sovelluksiin ja ohjelmistoihin. (Kyberturvallisuuskeskus 2020b.)

5.2 Torjuntaohjelmat

Torjuntaohjelmien tarkoituksena on pitää tietokoneet ja mobiililaitteet suojassa viruksilta ja muilta haittaohjelmilta (F-Secure 2024a). Opinnäytetyöhön liittyvässä kyselytutkimuksessa huomattiin, että useilla yrityksillä oli käytössä ulkoisia ratkaisuja virustorjuntaan, joiden palveluntarjoajina olivat esimerkiksi F-Secure ja Norton. Osassa yrityksiä käytettiin myös integroituja suojausratkaisuja, esimerkiksi Microsoft Defender -ratkaisua.

5.3 Vahva autentikointi ja salasanakäytännöt

Kaksivaiheinen tunnistautuminen on tapa suojata käyttäjätilejä luvattomalta pääsyltä. Kaksivaiheisessa tunnistautumisessa käyttäjän tulee vahvistaa kirjautuminen toisella tavalla tavallisen salasanan lisäksi.

Tämä tapahtuu useimmiten tekstiviestinä lähetettävällä koodilla tai autentikointisovelluksella. (Mondragon 2020.)

Organisaatiossa olisi hyvä olla käytössä oma salasanakäytäntö, jonka avulla salasanat saadaan pidettyä monimuotoisina ja hankalasti arvattavina. Käytäntö voi määrittää esimerkiksi salasanan vähimmäispituuden ja muita ominaisuuksia. Tärkeitä käytäntöjä salasanaa valitessa on jättää käyttämättä samaa salasanaa, joka on jo käytössä muilla sivustoilla. Salasanaksi ei myöskään kannata valita vain yhtä sanaa tai yleisesti käytössä olevaa lausetta. Salasanasta kannattaa tehdä mahdollisimman vaikeasti arvattava niin, etteivät edes tutut ihmiset voi keksiä sitä arvaamalla. (Microsoft 2023.) Salasanana ei siis välttämättä kannata käyttää syntymävuotta, ikää, perheen ja lemmikkien nimiä tai näiden yhdistelmiä.

5.4 Palomuurit

Palomuurilla tarkoitetaan ohjelmistoa, joka asennetaan tietokoneeseen estämään haitallista verkkoliikennettä. Sen tärkein tehtävä on yrityksen suojaaminen sisä- ja ulkoverkon uhilta. Nykyään palomuurin vaatimukset ovat kuitenkin osittain muuttuneet johtuen kyberrikollisuuden kasvusta, ja sen tulisi olla kykeneväinen useaan muuhunkin asiaan, kuin vain tavalliseen verkkoyhteyksien suodatukseen. Moderni palomuuri on usein keskeinen osa yrityksen tietoverkkoratkaisua, joka tarjoaa kattavan näkymän koko yrityksen verkkoliikenteeseen. Palomuurin avulla voidaan analysoida eri liiketoimintojen verkossa toimimista, luoda segmenttejä sisäverkolle ja rajoittaa yhteyksiä järjestelmäkohtaisesti. Palomuuri myös mahdollistaa pilvipalveluiden käyttämien sovellusten verkkoliikenteen seurannan. (F-Secure 2024b; Cinia 2023.)

Palomuurilta vaaditaan nykyään aina vain enemmän erilaisia tietoturvaominaisuuksia muiden ominaisuuksien lisäksi. Moderni palomuuri suorittaa virustarkistuksen yrityksen verkon reunalla, estäen haittaohjelman pääsyn päätelaitteille. Tämän lisäksi palomuuri kykenee suurimmilta osin havaitsemaan yrityksen verkkoon kohdistuvat hyökkäykset ja tunnistamaan poikkeavuuksia yrityksen sisäverkossa. Palomuurin VPN-toiminnallisuuksien avulla voidaan edesauttaa joustavaa ja tietoturvallista työskentelyä sekä mahdollistaa pääsy yrityksen verkossa oleviin palveluihin missä ja milloin tahansa. (Cinia 2023.)

5.5 Varmuuskopiointi

Tiedostojen varmuuskopiointi on tärkeä osa kyberturvallisuuden toteuttamista käytännössä. Varmuuskopiot tulevat hyödylliseksi esimerkiksi tilanteessa, jossa tietoja menetetään tietomurron yhteydessä. Varmuuskopiot tulee säilyttää eri paikassa kuin suojattavat tiedot ja järjestelmät, jotta varmuuskopioista ei voida tehdä käyttökelvottomia esimerkiksi kiristyshaittaohjelman avulla. Varmuuskopioiden palauttamista tulisi testata säännöllisesti, jotta voidaan varmistaa palauttamisen onnistuminen myös oikeissa tilanteissa. (Kyberturvallisuuskeskus 2021.)

5.6 Fyysinen turvallisuus

Fyysiseen turvallisuuteen kuuluvat ne keinot, joiden avulla suojataan tärkeitä tietoja fyysisiä uhkia vastaan. Perustaan kuuluvat fyysiset rakenteet, jotka suojaavat tiloja, joissa tietoja käsitellään. Suojauksessa voidaan lisäksi käyttää apuna esimerkiksi kameravalvontaa, palonilmaisin- ja hälytysjärjestelmiä, kulunvalvontaa ja vartiointipalvelua. Käytettävien turvallisuustoimenpiteiden tulisi perustua riskinarviointiin, jotta tiedetään, että käytössä olevat ratkaisut ovat tarpeeseen nähden riittäviä, muttei ylimitoitettuja. (Seclion 2021.)

5.7 Tietojen salaus ja luokittelu

Tietojen luokittelulla tarkoitetaan menettelyä, jossa yrityksen tietoja asetetaan eri luokkiin tietojen tyypin mukaan. Tyypillisesti tiedot luokitellaan viiteen kategoriaan, joita ovat julkinen tieto, yksityinen tieto, sisäinen tieto, luottamuksellinen tieto ja rajoitettu tieto. (Indeed 2023.)

Julkinen tieto on tietojen luokittelun matalin taso. Se voi olla esimerkiksi lehdistötiedotteita ja muuta tietoa, joka on vapaasti saatavilla kaikelle yleisölle. Yksityinen data on tietoluokituksen toiseksi matalin taso ja siihen kuuluvat tiedot voivat olla esimerkiksi henkilökohtaisia sähköposteja tai puhelimen sisältöä. Sisäiset tiedot ovat yrityksen sisäistä tietoa, jota ei haluta jakaa ulkopuolisille. Sisäiset tiedot voivat olla esimerkiksi yrityksen intranetin sisältöä, arkistoituja tiedostoja tai IP-osoitteita. Sisäiseen tietoonkaan ei välttämättä pääse käsiksi koko yrityksen henkilöstö, vaan pääsyjä saatetaan hallinnoida eri tasoilla. Luottamuksellinen tieto taas voi sisältää esimerkiksi henkilötunnuksia, ajoneuvotietoja tai taloustietoja. Luottamuksellisiin tietoihin ei ideaalitilanteessa pääse käsiksi, kuin vain rajoitettu joukko henkilöstöä. Viimeinen tietojen luokittelun taso on rajoitettu tieto, joka on kaikista arkaluontoisin tietotyyppi. Rajoitettua tietoa suojataan tarkoin toimenpitein ja pääsyoikeuksia näihin tietoihin rajoitetaan

tiukasti. Tiedot voivat olla esimerkiksi salassapitosopimuksen alaisia tietoja, joiden vuotaminen vaarantaisi yrityksen toiminnan. Tietojen luokittelu on tärkeää, sillä sen avulla voidaan auttaa pitämään yrityksen tietoja turvassa sekä suojaamaan tiedon eheyttä, saatavuutta ja luottamuksellisuutta. (Indeed 2023.)

Kyberturvallisuudessa tietojen salaamisella tarkoitetaan toimintaa, jossa tietoja muunnetaan luettavasta muodosta koodimuotoon. Salattujen tietojen käsittely ja lukeminen vaativat salauksen purkamisen, jota ennen nämä toimet eivät ole mahdollisia. Salaus on olennainen osa tietoturvaa ja tärkeä tapa varmistaa, ettei ulkopuolinen taho voi anastaa tai lukea tietokonejärjestelmän tietoja haitalliset tarkoitukset mielessään. (Kaspersky 2024.)

5.8 Käyttäjätietojen- ja käyttöoikeuksien hallinta

Käyttäjätietojen- ja käyttöoikeuksien hallinnan, eli IAM-järjestelmän (Identity and Access Management) avulla on tarkoitus mahdollistaa henkilön identiteetin ja pääsyoikeuksien tarkistaminen organisaation järjestelmissä nopeasti ja tehokkaasti. Ennen valtavasti yleistynyttä hybridityötä yrityksen resursseja on pidetty palomuurin takana ja yrityksen tiloissa olleet, järjestelmiin sisäänkirjautuneet työntekijät ovat voineet käyttää tarvitsemiaan resursseja helposti. Nykyään hybridityön yleistyttyä yrityksille on muodostunut tarve tarjota työntekijöille suojatut käyttöoikeudet resursseihinsa, riippumatta paikasta, jossa työtä tehdään. IAM-järjestelmän tarkoituksena on turvata suojatut käyttöoikeudet vahvistetuille henkilöille yrityksen järjestelmiin, eli esimerkiksi tietokantaan, sovelluksiin ja sähköpostiin. Päätavoite on hallita käyttöoikeuksia siten, että työntekijät voivat suorittaa työnsä ilman häiriötä ja etteivät luvattomat käyttäjät saa käyttöoikeuksia yrityksen järjestelmiin. IAM-järjestelmän avulla voidaan myös suojata organisaatiota tietomurroilta, vaikkakaan minkään järjestelmän avulla ei voida täysin välttyä riskeiltä. Järjestelmän käyttö kuitenkin pienentää riskiä huomattavasti ja on olennainen osa modernia IT-teknologiaa. (Microsoft 2024.)

5.9 Perehdytys ja koulutus

Kyber- ja tietoturva on koko yrityksen asia, ei pelkästään yrityksen tietohallinnon tai IT-osaston. Yrityksen tietoturvasta tulisi tehdä yhteinen prioriteetti, jonka avulla yrityksen tietoturvaa voidaan parantaa ja tehdä kyberhyökkäysten toteuttaminen hyökkääjille haastavammaksi. Toimintamallien ja tieto-

turvatietoisuuden avulla voidaan pienentää virheiden ja vahinkojen määrää. Kukaan ei tee virheitä tahallaan, mutta silti niitä sattuu aina välillä. Näitä tilanteita varten on hyvä olla olemassa tieto, miten toimitaan virheen tai vahingon sattuessa. (Kyberturvallisuuskeskus 2023.)

Työntekijöiden perehdytys ja säännöllinen kouluttaminen on ensiarvoisen tärkeää, jotta jokaisen tietoturvatietoisuus pysyy hyvällä tasolla. Teemoja, joita perehdytyksissä ja koulutuksissa kannattaa käsitellä ovat esimerkiksi huijaukset, haittaohjelmat, työvälineet, etätyö ja matkustus sekä suojattava tieto ja toiminta poikkeamatilanteissa. Kouluttamisen avulla voidaan mahdollisesti välttyä monilta turhilta virheiltä. (Kyberturvallisuuskeskus 2023.)

6 KYSELYTUTKIMUS

6.1 Tutkimusmenetelmä ja kohderyhmä

Tutkimus toteutettiin kyselytutkimuksena Webropol-alustalla käyttäen sekä kvantitatiivista että kvalitatiivista tutkimusmenetelmää. Yrityksille lähetettiin kysely, jossa käytettiin pääasiassa kvantitatiivista menetelmää. Tutkimuksessa haluttiin saada tietoon myös yritysten asenteita ja näkökulmia aiheeseen liittyen, jonka vuoksi kyselyssä käytettiin myös avoimia kysymyksiä.

Kvantitatiivisen tutkimuksen avulla pyritään selvittämään kysymyksiä liittyen lukumääriin ja prosenttiosuuksiin. Tutkimuksen tekeminen vaatii tarpeeksi suuren ja edustavan otoksen. Kvalitatiivisessa tutkimuksessa taas pyritään ymmärtämään tutkimuskohdetta, ja otos on usein pieni. Koska tuloksia on vain pieni määrä, niitä pyritään analysoimaan hyvin tarkasti. (Heikkilä 2014.) Alasuutari (2011) toteaa, että kvantitatiivinen ja kvalitatiivinen analyysi voidaan kyllä erottaa toisistaan, mutta niitä voidaan myös hyvin soveltaa saman aineiston analysoinnissa.

Tutkimuskysymys oli: Millaisia toimenpiteitä eri kokoisissa yrityksissä tehdään kyberturvallisuuden edistämiseksi? Tavoitteena oli saada kokonaiskuva yritysten tekemistä toimenpiteistä kyberturvallisuuden edistämiseksi sekä vertailla eroja eri kokoisten yritysten välillä. Vertailua tehtiin myös eri toimialoilla toimivien yritysten välillä sekä pääasiallisen toimipaikan perusteella.

Kysely lähetettiin 1 035 yritykselle. Kysely pyrittiin lähettämään yrityksille ympäri Suomea niin, että vastaanottajia olisi suunnilleen sama määrä jokaisesta kunnasta, ja että ne toimisivat laajasti eri toimialoilla. Kyselyyn vastasi 145 yritystä, eli 14,01 % kyselykutsun saaneista. Vastaajamäärä oli positiivinen yllätys, sillä kyberturvallisuus on aiheena suhteellisen arkaluontoinen. Vastauksia saatiin heti kyselyn lähettämisen jälkeen paljon, mutta kyselyajan ollessa vielä auki lähetettiin muistutusviesti niille yrityksille, jotka eivät olleet vielä vastanneet. Yrityksille kerrottiin, että kysely toteutetaan anonyymisti, eikä vastauksia käsitellä yksilötasolla niin, että yritystä voisi yhdistää vastauksiin. Tämä on mahdollisesti lisännyt kiinnostusta ja rohkeutta vastata kyselyyn.

6.2 Aineiston käsittely ja analysointi

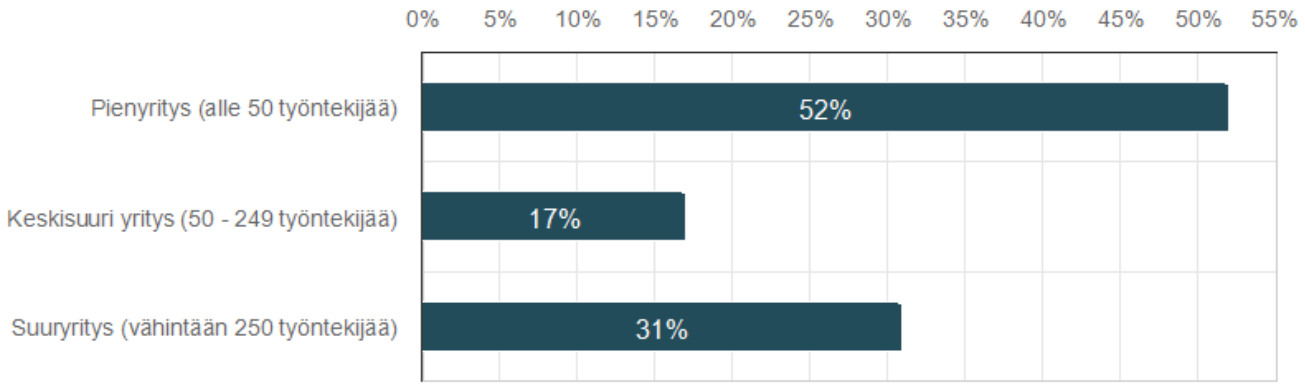
Aineisto käsiteltiin anonyymisti, tarkastellen vastauksia yleistasolla. Vastaukset vietiin Word-raporttiin Webropol-palvelusta, jossa tulokset esitettiin pylväsdiagrammina. Kysymyksien tulokset käytiin läpi yksitellen diagrammien avulla ja tämän lisäksi analysoitiin yrityskoon, päätoimipaikan ja toimialan vaikutusta kyberturvallisuuteen suhtautumiseen ja toimenpiteisiin, joita yrityksessä sen eteen tehdään. Vastaukset avoimiin kysymyksiin käsiteltiin yhteenvetoina, jotta minkäänlaista riskiä vastaajan henkilöllisyyden paljastumiselle ei ollut. Muutaman vastauksen kohdalla tehtiin tekstin tueksi kaavioita Excel-ohjelmalla, sillä Webropol-palvelulla kaavioista muodostui liian suurikokoisia, kun verrattiin vain muutamaa toimipaikkaa- tai alaa. Vertailua tehtiin yrityskokojen välillä kaikkien vastaajien kesken, mutta toimipaikan- ja alan vertailuun valittiin viisi suurinta vastaajaryhmää kustakin kategoriasta.

Aineiston analysoinnissa haasteeksi osoittautuivat vastaajamäärät, jotka vaihtelivat etenkin yritysten toimialan ja -paikan kohdalla, joiden avulla vertailua tehtiin. Vaikka vertailuun valittiin viisi suurinta vastaajaryhmää molempien kategorioiden kohdalla, esiintyi vastaajamäärissä suhteellisen paljon vaihtelua, joka on voinut osittain vaikuttaa tulokseen.

7 TUTKIMUSTULOKSET

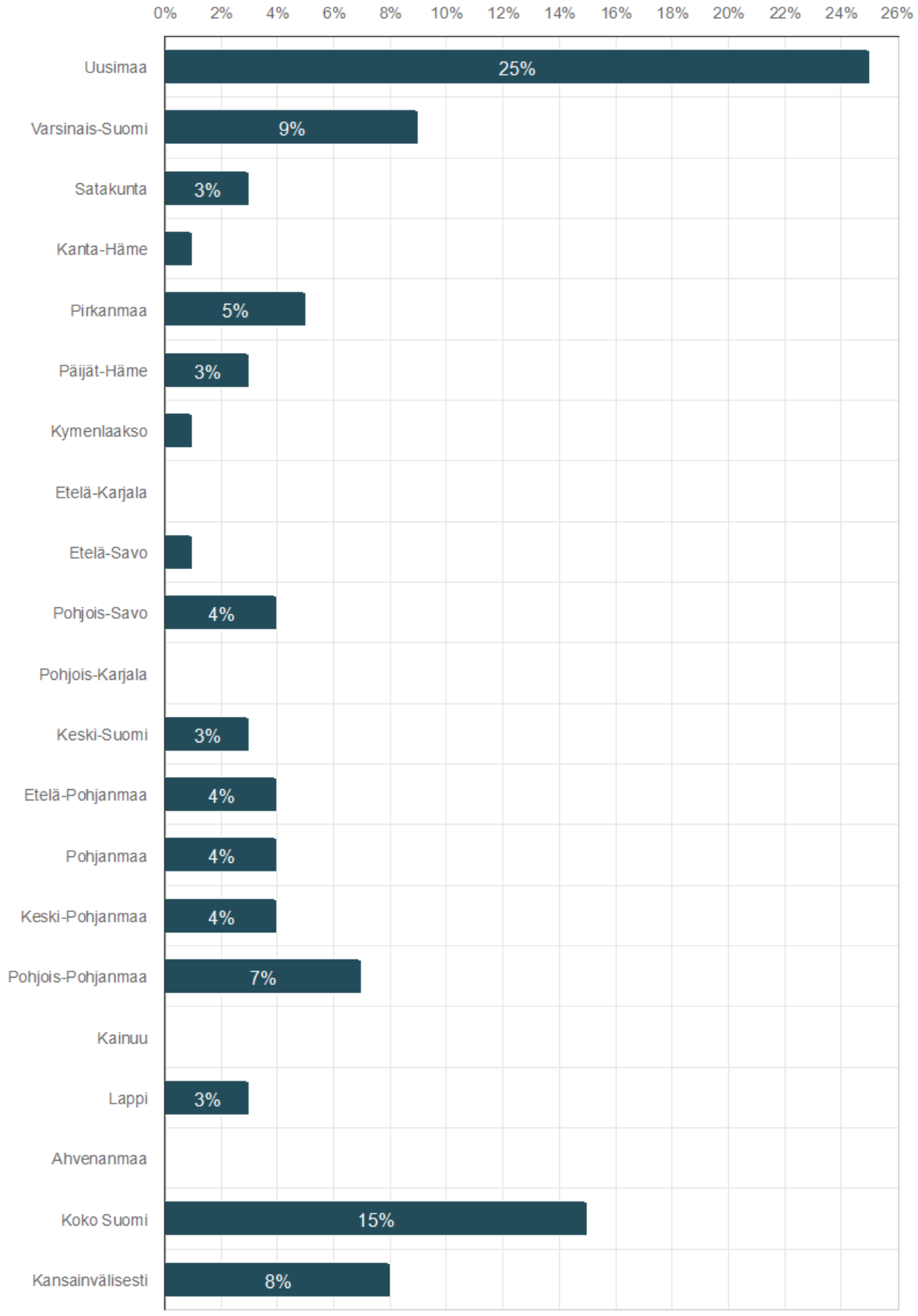
7.1 Taustatiedot

Kyselyn ensimmäinen kysymys koski yrityksen kokoluokkaa. Suurin osa vastanneista yrityksistä oli pienyrityksiä, joita oli kokonaisuudessaan 52 % vastanneista. Keskisuurten yritysten osuus oli 17 %, kun taas suuryritysten 31 %. (KUVIO 2.) Yritysten vastauksia vertailtiin kokoluokittain kyselyn muissa valinta- ja monivalintakysymyksissä.



KUVIO 2. Yritysten kokoluokat

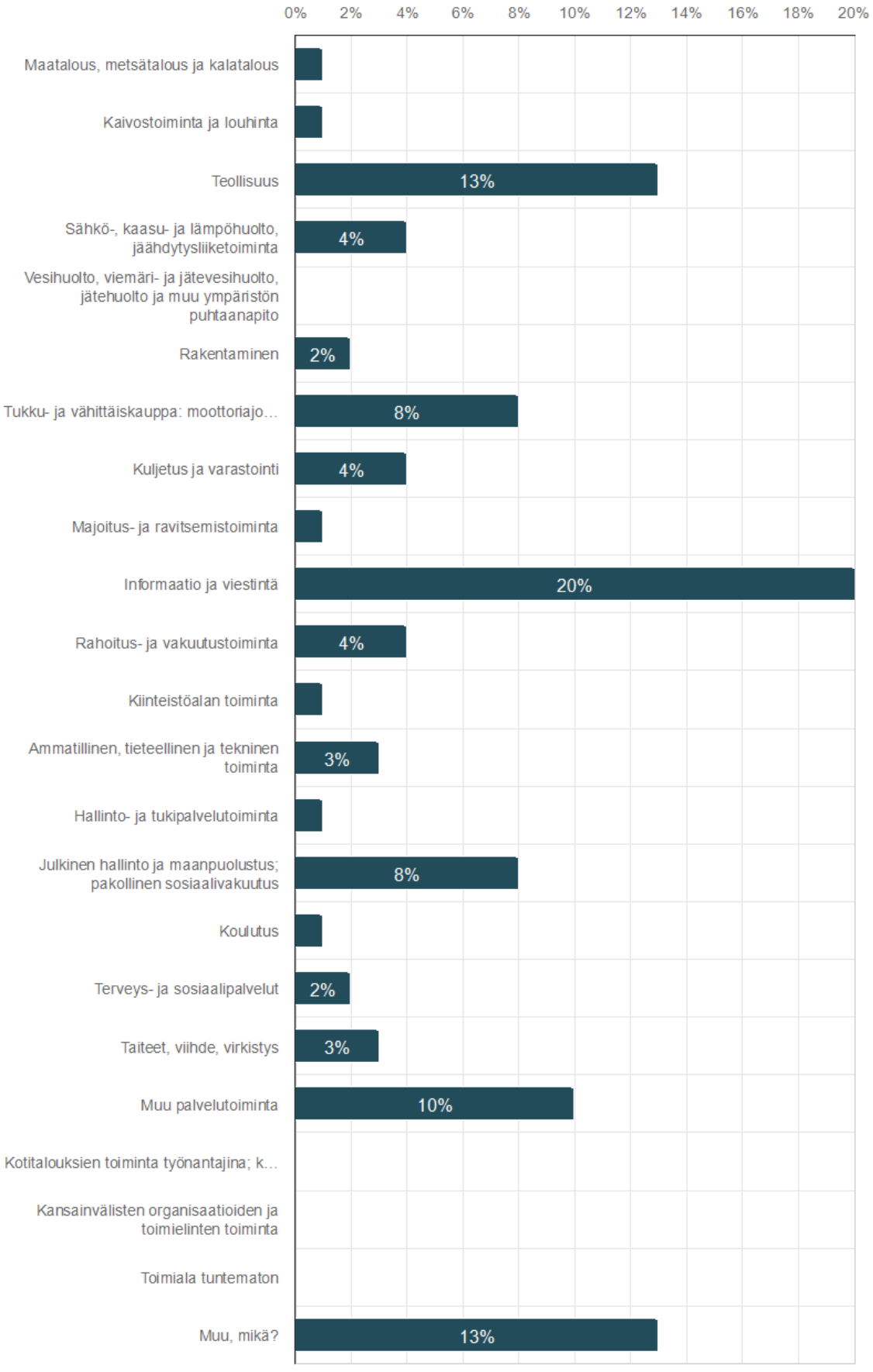
Toisessa kysymyksessä tiedusteltiin millä alueella yritys ensisijaisesti toimii. (KUVIO 3.) Vastauksia kyselyyn saatiin lähes joka puolelta Suomea, mutta Etelä-Karjalasta, Pohjois-Karjalasta, Kainuusta, eikä Ahvenanmaalta löytynyt kyselyyn vastaajia, vaikka sitä toimitettiin näissäkin kunnissa toimiville yrityksille. Eniten vastauksia saatiin Uudeltamaalta, koko Suomessa toimivilta yrityksiltä, Varsinais-Suomesta, kansainvälisesti toimivilta yrityksiltä sekä Pohjois-Pohjanmaalla toimivilta yrityksiltä. Viiden eniten kyselyssä edustusta saaneen yrityksen välillä tehtiin vertailua muissa kyselyn valinta- ja monivalintakysymyksissä.



KUVIO 3. Yritysten päätoimialueet

Kolmas kysymys käsitteli yrityksen toimialaa. Vastausvaihtoehdot ovat peräisin Tilastokeskuksen toimialaluokituksesta (Tilastokeskus 2024). Vastausvaihtoehdot, esimerkiksi ”Tukku- ja vähittäiskauppa; moottoriajoneuvojen ja moottoripyörien korjaus” hämmensivät osaa vastaajista. Luokitukset olivat mahdollisesti hieman vaikeita ymmärtää, mutta siitä huolimatta päädyttiin käyttämään virallista toimialaluokitusta.

Eniten vastauksia saatiin informaatio – ja viestintäalalta (20 %) ja teollisuudesta (13 %). ”Muu, mikä?” -vaihtoehdon vastanneita oli myös 13 %. (KUVIO 4.) Tämän vastauksen kohdalla korkea prosenttiosuus voi kuitenkin johtua siitä, etteivät vastaajat ole olleet varmoja, mikä vastausvaihtoehto tulisi valita, sillä toimialaluokitus voi olla hieman hankalasti ymmärrettävä. Muuta palvelutoimintaa harjoittavia yrityksiä oli 10 % ja julkisen hallinnon ja maanpuolustuksen alalla toimivia 8 %. Tukku- ja vähittäiskaupan alalla toimivia oli myös 8 %. (KUVIO 4.) Näistä viisi alaa valittiin vertailuryhmäksi, kun käsiteltiin toimialan vaikutusta kyselyn vastauksiin. ”Muu, mikä?” jätettiin vertailuryhmän ulkopuolelle, sillä vastaajat olivat monilta eri aloilta, eikä niitä näin ollen olisi voinut vertailla tarkoituksenmukaisesti.

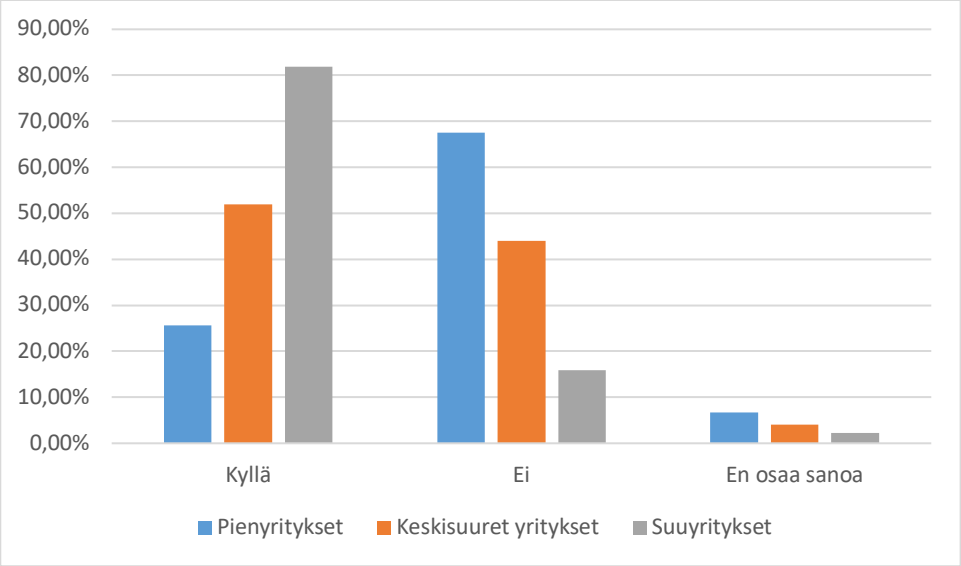


KUVIO 4. Yritysten toimialat

7.2 Kyberturvallisuuspolitiikka ja DRP

Neljännessä kysymyksessä tiedusteltiin, onko yrityksellä käytössä virallista kyberturvallisuuspolitiikkaa. Vastaukset jakautuivat hyvin tasaisesti ”Kyllä” ja ”Ei” vastausten välille. (KUVIO 6.) Oli hyvin yllättävää huomata, että lähes puolella vastanneista ei ollut käytössä minkäänlaista kyberturvallisuuspolitiikkaa.

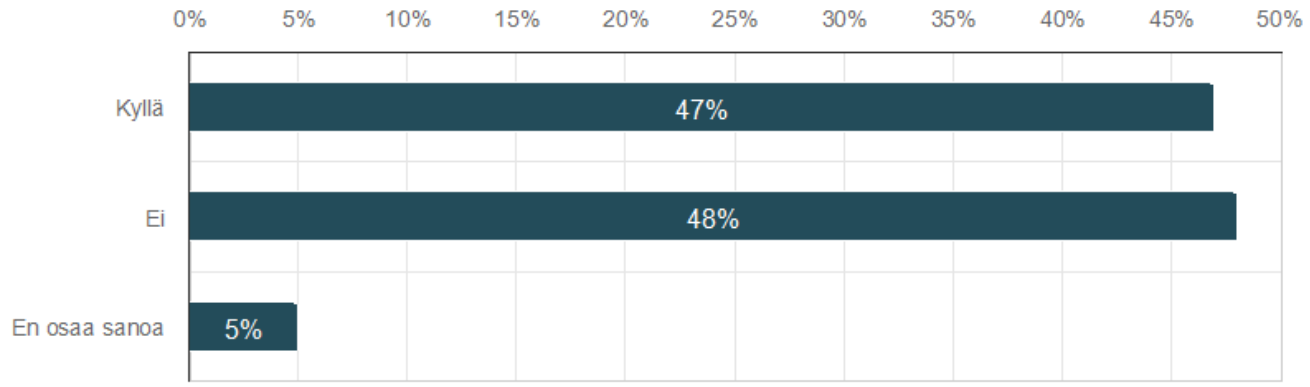
Suuryrityksissä yli 80 %:lla oli kyberturvallisuuspolitiikka käytössä, kun taas pienyrityksissä vastaava luku oli 25,7 %. Keskisuuret yritykset sijoittuivat vastauksissaan näiden välimaastoon 52 %:n lukemalla. (KUVIO 5.) Vastaukset olivat osittain ennalta arvattavia, mutta huolestuttavia. Suuryrityksillä voi usein olla enemmän resursseja käytettäväksi kyberturvallisuuden edistämiseen, mutta pienyritysten 25,7 % oli silti huomattavan matala, vaikka resursseja ja osaamista olisikin vähemmän käytössä. Keskisuuret yritykset jakautuivat vastauksissaan lähes puoliksi, joka oli myös yllättävää. Enemmistöllä oli käytössä kyberturvallisuuspolitiikka, mutta 44 % vastaajista oli silti suuri määrä yrityksiä, joilla ei tällaista hyvin tarpeellista politiikkaa ole. Kaiken kokoisissa yrityksissä oli vastaajia, jotka eivät tienneet oliko heillä käytössä kyberturvallisuuspolitiikkaa, mikä sai pohtimaan, olivatko kyselyyn vastanneet henkilöt yrityksen kyber- ja tietoturvasta vastaavia henkilöitä, vai muuta henkilöstöä. Toinen asia, joka on voinut vaikuttaa vähäisesti tuloksiin, on termi kyberturvallisuuspolitiikka, sillä usein käytetään myös muita termejä, kuten tietoturvapolitiikka, johon kyberasiat voivat sisältyä. Osa vastaajista ei ole mahdollisesti tunnistanut juuri tätä termiä heillä käytettäväksi.



KUVIO 5. Kyberturvallisuuspolitiikan käyttö eri yrityskokojen välillä

Vastauksia tarkasteltiin myös viiden eniten edustusta saaneen toimialueen välillä ja niistä voitiin huomata, että etenkin kansainvälisesti ja koko Suomessa toimivien yritysten kohdalla kyberturvallisuuspolitiikka oli käytössä huomattavasti useammassa yrityksessä, kuin muilla alueilla. Vastauksista havaittiin myös, että Pohjois-Pohjanmaalla jopa 80 %:lla vastanneista yrityksistä ei ollut kyberturvallisuuspolitiikkaa käytössä. Kysymyksen vastauksista voitiin myös havaita, että Uudenmaan ja Varsinais-Suomen alueita edustavien yritysten vastausprosentit olivat hyvin samaa luokkaa. Niissäkin oli enemmän yrityksiä, joilla kyberturvallisuuspolitiikkaa ei ollut käytössä, kuin niitä, joilla sellainen oli.

Eri toimialojen vastauksia vertaillessa havaittiin, että julkista hallintoa ja maanpuolustusta sekä muuta palvelutoimintaa lukuun ottamatta muista vertailuryhmän aloista yli puolella oli kyberturvallisuuspolitiikka käytössä. Julkisen hallinnon ja maanpuolustusalan edustajista lähes 2/3 vastasi, ettei heillä ole kyberturvallisuuspolitiikkaa käytössä. Myös muuta palvelutoimintaa harjoittavista yrityksistä yli puolella ei ollut kyberturvallisuuspolitiikkaa käytössä. Teollisuusalalla taas oli selkeästi eniten yrityksiä, joilla tämä politiikka oli käytössä (69 %). Yllättävää oli etenkin julkisen hallinnon ja maanpuolustusalan vastaukset. Alan olisi olettanut olevan sellainen, jossa kyberturvallisuuspolitiikan olemassaolo olisi erityisen tärkeää.



KUVIO 6. Kyberturvallisuuspolitiikan käyttö koko vastaajaryhmän kesken

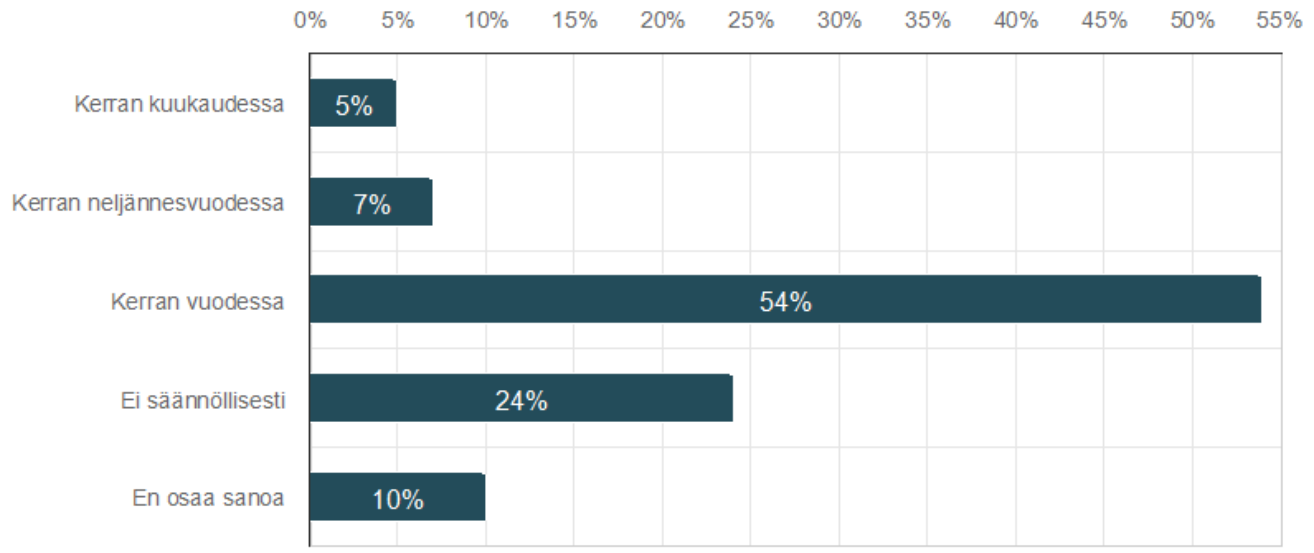
Mikäli vastaaja vastasi edelliseen kysymykseen kyllä, esitettiin hänelle lisäkysymys (kysymys 5) liittyen siihen, kuinka usein yrityksen kyberturvallisuuspolitiikkaa päivitetään. Hieman yli puolet yrityksistä päivittävät kyberturvallisuuspolitiikkaansa kerran vuodessa. 5 % vastanneista kertoivat tekevänsä

päivityksiä kerran kuukaudessa, kun taas 7 % vastanneista päivittävät politiikkaansa kerran neljännesvuodessa. 24 % eivät päivitä kyberturvallisuuspolitiikkaansa säännöllisesti ja 10 % vastaajista eivät osanneet sanoa kuinka usein päivityksiä tehdään. (KUVIO 7.)

Yrityskokojen vaikutusta tarkastellessa huomattiin, että kaiken kokoisille yrityksille tavallisinta oli päivittää kyberturvallisuuspolitiikkaa kerran vuodessa. Edellisessä kysymyksessä voitiin huomata, että kyberturvallisuuspolitiikkaa ei ollut kovinkaan paljon käytössä pienissä yrityksissä. Tämän kysymyksen kohdalla voitiin kuitenkin huomata, että ne, joilla se oli käytössä, päivittivät sitä keskimäärin ahkerammin kuin muun kokoisissa yrityksissä tehdään. Yllättävää vastauksissa oli se, että yli 20 % jokaisesta yrityskokoluokasta eivät päivitä kyberturvallisuuspolitiikkaansa säännöllisesti. Kyberturvallisuus on alati muuttuvaa ja kyberturvallisuuspolitiikkaa olisi suotavaa päivittää edes jokseenkin säännöllisesti.

Yritysten ensisijaisen toimialueen vaikutusta vastauksiin tarkasteltaessa, nousivat esiin etenkin kansainvälisesti toimivat yritykset, Uudellamaalla toimivat yritykset sekä koko Suomessa toimivat yritykset, jotka päivittävät kyberturvallisuuspolitiikkaansa kerran vuodessa. Osa Varsinais-Suomessa toimivista yrityksistä oli hyvin ahkeria päivittämään kyberturvallisuuspolitiikkaansa. Lähes kaikki vertailuryhmän toimialueiden yrityksistä, jotka päivittävät politiikkaansa kerran kuukaudessa tai kerran neljännesvuodessa, olivat Varsinais-Suomessa toimivia yrityksiä.

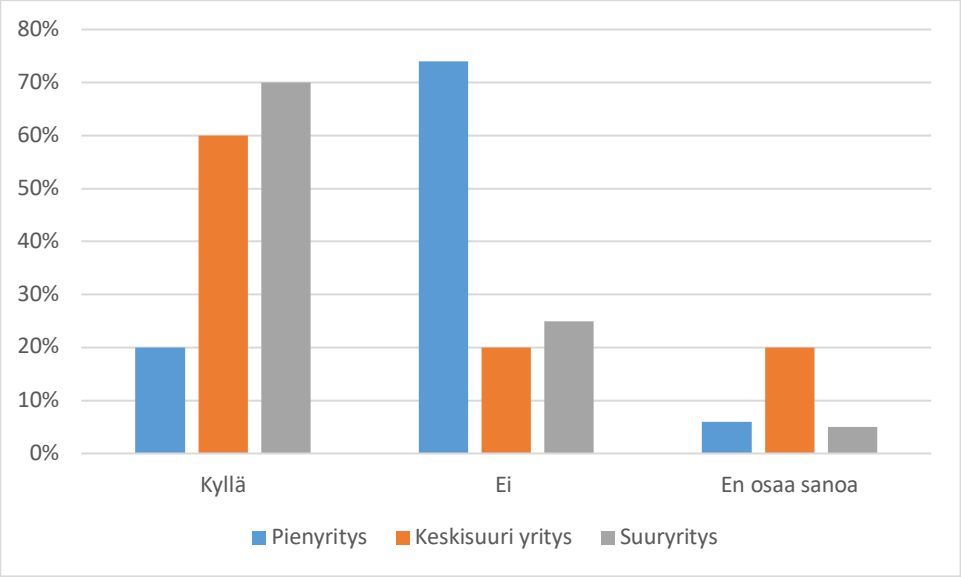
Toimialan vaikutuksista voitiin huomata, että usein kyberturvallisuuspolitiikkaansa päivittävät olivat pääasiassa muun palvelutoiminta-alan edustajia. Näistä yrityksistä 20 % päivitti politiikkaansa kerran kuukaudessa ja 20 % kerran neljännesvuodessa. Tämän lisäksi ainoastaan informaatio- ja viestintäalan yrityksistä 12 % päivitti politiikkaansa kerran kuukaudessa, muut alat harvemmin. Julkisen hallinnon ja maanpuolustusalan yrityksistä 75 % kertoivat, etteivät he päivitä politiikkaansa säännöllisesti. Teollisuudessa sekä informaatio- ja viestintäalalla politiikkaa päivitettiin useimmiten kerran vuodessa. Tukku- ja vähittäiskaupan alalla puolet vastaajista eivät osanneet sanoa, kuinka usein politiikkaa päivitetään, mutta toiseksi suosituin vastaus oli ”Ei säännöllisesti”.



KUVIO 7. Kyberturvallisuuspolitiikan päivittäminen koko vastaajaryhmän kesken.

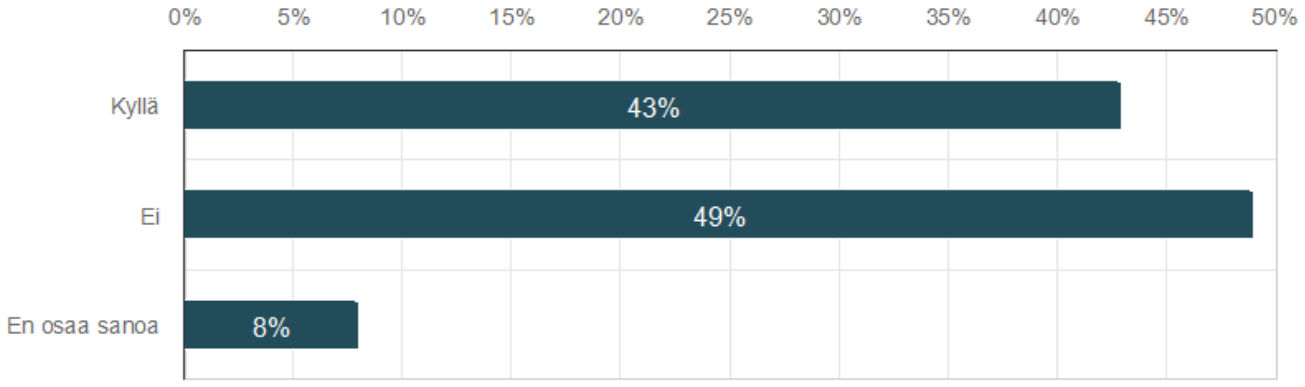
Kuudennessa kysymyksessä tiedusteltiin, oliko yrityksellä käytössä toipumissuunnitelma, eli DRP (Disaster Recovery Plan) häiriötilanteiden varalle. 43 % kertoivat omaavansa toipumissuunnitelman, kun taas 49 % ei suunnitelmaa omannut. 8 % ei osannut sanoa onko heidän edustamallaan yrityksellään käytössä toipumissuunnitelmaa. (KUVIO 9.)

Eri kokoisten yritysten vastauksista voidaan jälleen huomata, että vastaukset painottuvat siten, ettei suurella osalla pienyrityksistä ollut lainkaan virallista suunnitelmaa häiriötilanteiden varalle, kun taas suuryrityksillä tilanne oli toisinpäin. (KUVIO 8.) DRP:n osalta suuryritysten ja keskisuurten yritysten vastausten välillä ei ollut niin suurta eroa, kuin esimerkiksi aiemman kysymyksen kohdalla liittyen kyberturvallisuuspolitiikkaan.



KUVIO 8. Toipumissuunnitelman käyttö eri yrityskokoluokissa

Toimipaikkavertailun kohdalla voitiin havaita, että DRP oli käytössä eniten koko Suomessa ja kansainvälisesti toimivissa yrityksissä. Yrityksiä, joilla tätä ei ollut lainkaan käytössä oli eniten Uudellamaalta, Pohjois-Suomesta ja Varsinais-Suomesta. Eri toimialoilla DRP oli käytössä eniten teollisuusalalla ja muun palvelutoiminnan alalla. ”Ei” vastanneissa korostui etenkin julkinen hallinto ja maanpuolustusala. Informaatio- ja viestintäalan vastaukset jakautuivat lähes samoilla prosenteilla kuin alla olevassa kuviossa (KUVIO 7). Tukku- ja vähittäiskaupan vastaukset jakautuivat kaikkien kolmen vastausvaihtoehdon välillä tasaisesti.



KUVIO 9. Toipumissuunnitelman käyttö koko vastaajaryhmän kesken

7.3 Käytänteet

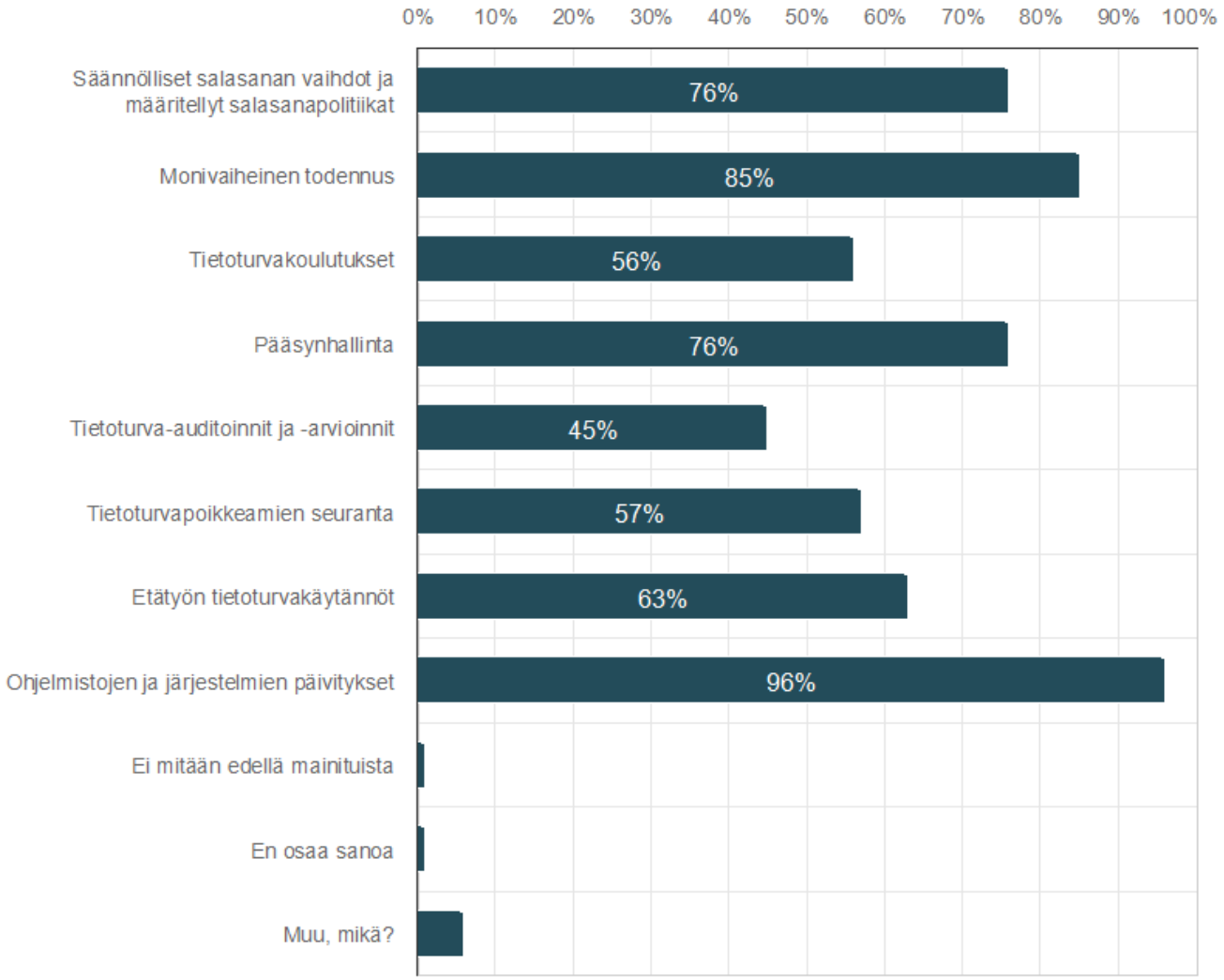
Seitsemännessä kysymyksessä kysyttiin, mitä tietoturvakäytänteitä yrityksessä noudatetaan. Kyseessä oli monivalintakysymys ja monella yrityksellä olikin käytössä useampia eri toimenpiteitä tietoturvan edistämiseksi. Suosituimpia käytänteitä olivat ohjelmistojen ja järjestelmien päivitykset, monivaiheinen todennus, säännölliset salasanan vaihdot ja määritellyt salasanapolitiikat sekä pääsynhallinta. Avoimissa vastauksissa osa vastaajista kertoi ostavansa tietoturvapalveluita ulkoisesti. Myös SOC, SIEM, 24/7 turvallisuusmonitorointi, jatkuvuuden hallinnan palauttamiskäytännöt ja haavoittuvuusskannaukset mainittiin avoimissa vastauksissa. (KUVIO 10.)

Vastauksia vertaillessa yrityskoon perusteella, oli heti huomattavissa, että suuryritykset korostuivat vastauksissa. Jokaisen vastausvaihtoehdon kohdalla oli 93–100 %:n edustus suuryritysten osalta lukuun ottamatta tietoturva-auditointeja ja -arviointeja, joita tekivät 84 % suuryrityksistä. Tietoturvakoulutuksia järjesti 95 % suuryrityksistä. Keskisuurten yritysten osalta prosentit vaihtelivat vastausvaihtoehtojen välillä 72–96 %:n välillä, jälleen lukuun ottamatta auditointeja ja arviointeja, joita tekivät 60 % keskisuurista yrityksistä. 72 % keskisuurista yrityksistä järjestävät tietoturvakoulutuksia.

Pienyritysten kohdalla prosentit olivat jälleen matalampia kuin keskisuurissa ja suurissa yrityksissä. Erityisen vähän pienyrityksissä järjestettiin tietoturvakoulutuksia (26 %), tietoturva-auditointeja ja -arviointeja (18 %), tietoturvapoikkeamien seurantaa (27 %) ja etätyön tietoturvakäytänteitä (38 %). Prosentit olivat suhteellisen pieniä siihen nähden, kuinka helppo osa käytänteistä olisi toteuttaa, esimerkkinä säännölliset salasanan vaihdot ja monivaiheinen todennus. Tietoturva-auditointeja ja -arviointeja käyttävien pienyritysten osuus oli pieni, mutta varsinkin arviointeja olisi syytä toteuttaa ihan kaiken kokoisissa yrityksissä. Tietoturvakoulutuksia järjestävien pienyritysten osuus oli myös pieni, joka voi johtua osittain siitä, että osa vastaajista oli varmasti yksinyrittäjiä. Vaikka toimisi yksinyrittäjänä, voi itseään kuitenkin kouluttaa asiaan liittyen ja esimerkiksi osallistua ulkoisten palveluntarjoajien koulutuksiin. Etätyön tietoturvakäytäntöjen prosentti oli myös jokseenkin alhainen, mutta läheskään kaikissa yrityksissä ei varmastikaan tehdä etätöitä.

Erilaisia käytänteitä oli selvästi eniten käytössä kansainvälisesti ja koko Suomessa toimivissa yrityksissä. Etenkin tietoturva-auditointeja ja -arviointeja sekä tietoturvakoulutuksia oli käytössä näissä yrityksissä enemmän muihin alueisiin verrattuna. Huomattavasti vähiten erilaisia toimenpiteitä oli käytössä Pohjois-Pohjanmaalla, lukuun ottamatta monivaiheista todennusta ja ohjelmisto- ja järjestelmäpäivityksiä, jotka olivat laajalti käytössä.

Julkinen hallinto ja maanpuolustusala sekä teollisuusala erottuivat toimialoista eniten erilaisia toimenpiteitä käyttävinä aloina. Muutkin alat käyttivät eri toimenpiteitä laajalti, mutta pienemmät prosentit voitiin havaita tukku- ja vähittäiskaupan alalla tietoturva-auditoinneissa ja -arvioinneissa (25 %) sekä tietoturvakoulutuksissa muun palvelutoiminta-alan osalta (29 %).



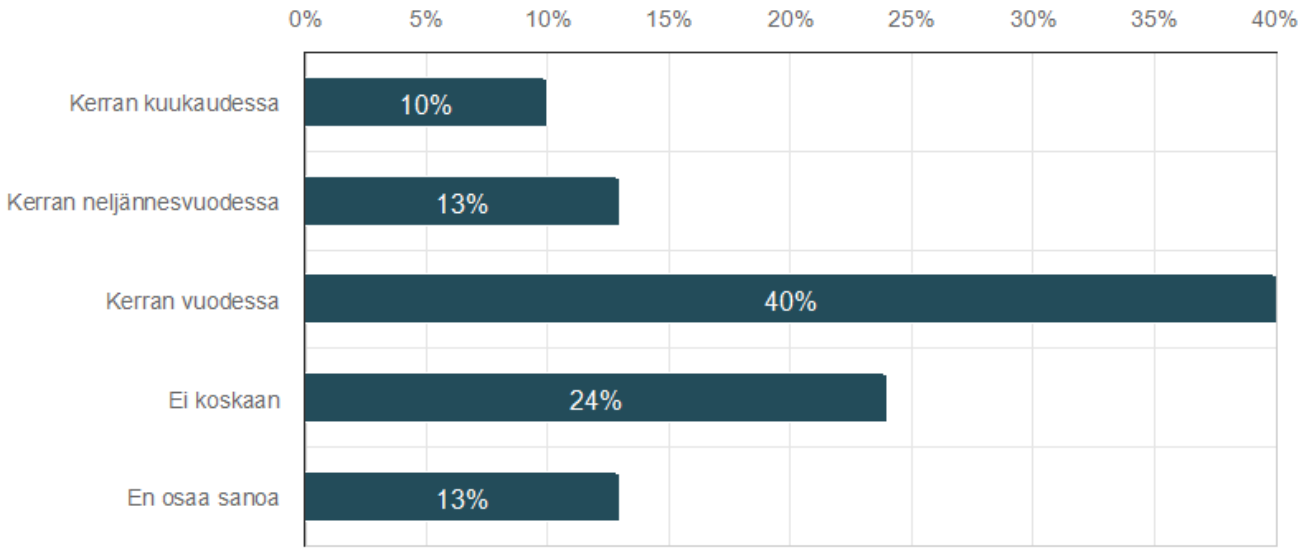
KUVIO 10. Tietoturvakäytänteet koko vastaajaryhmän kesken

Kahdeksannessa kysymyksessä kysyttiin yrityksen tietoturva-arvioinneista ja -testauksista, tarkemmin ottaen siitä, kuinka usein niitä suoritetaan. 10 % kertoi suorittavansa näitä kerran kuukaudessa. 13 % suoritti arviointeja ja testauksia kerran neljännesvuodessa ja 40 % kerran vuodessa. 24 % yrityksistä ei suorittanut arviointeja tai testauksia koskaan ja 13 % ei osannut sanoa suoritetaanko näitä heidän edustamassaan yrityksessä. (KUVIO 11.)

Suuryritykset tekivät tietoturva-arviointeja ja -testauksia säännöllisemmin kuin pienet tai keskisuuret yritykset, joka voi heijastaa resurssien ja tietoturvan priorisointia. Kaikkien yrityskokojen kesken vuosittaiset arvioinnit ja testaukset olivat yleisimpiä. Erityisesti tämä oli nähtävissä suuryritysten kohdalla, joka voi viitata standardien noudattamiseen tai vuosittaisiin tarkastuksiin. Suuri osa pienyrityksistä ei tehnyt tietoturva-arviointeja ja -testauksia lainkaan, joka voi altistaa niitä suuremmille riskeille. Näiden toimenpiteiden vähyys voi myös kieliä tietoturvatietoisuuden tai resurssien puutteesta pienyritysten kohdalla. Keskisuuret yritykset suorittivat tietoturva-arviointeja ja -testauksia useammin kuin pienyritykset, mutta jäivät silti jälkeen suuryrityksistä.

Tietoturva-arviointeja ja testauksia suoritettiin tiheimmällä aikavälillä kansainvälisesti toimivissa yrityksissä, useimmiten kerran neljännesvuodessa. Varsinais-Suomessa ja koko Suomessa toimivat yritykset tekivät arviointeja tavallisimmin kerran vuodessa. Uudellamaalla ja Pohjois-Pohjanmaalla toimivien yritysten kohdalla arviointeja ja testauksia ei useimmissa yrityksissä tehty koskaan.

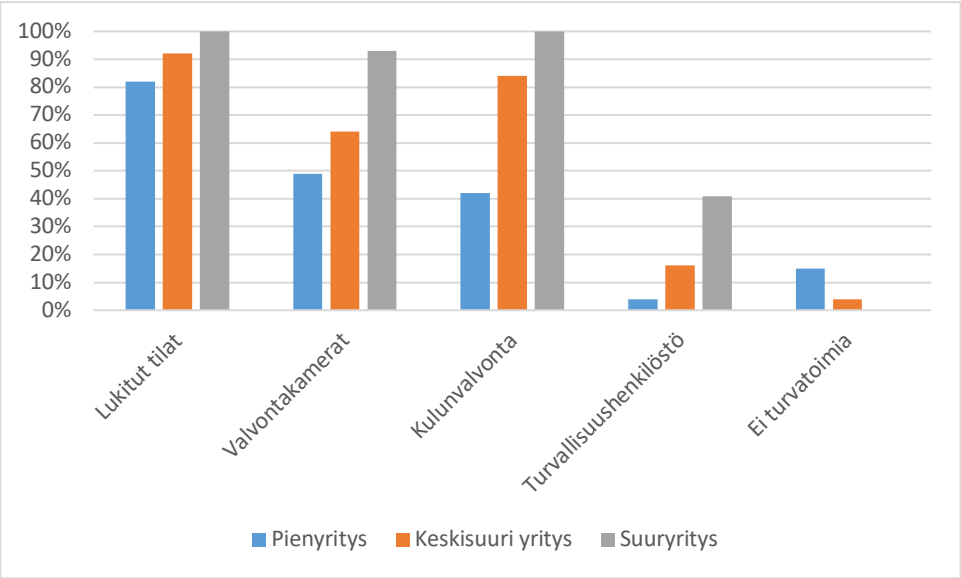
Kaikilla vertailuryhmän toimialoilla suoritettiin tietoturva-auditointeja ja -testauksia useimmiten kerran vuodessa. Ainoastaan muun palveluliiketoiminta-alan vastausprosentti oli sama niin ”Kerran vuodessa”, kuin ”Ei koskaan” -vastauksenkin kohdalla. Toisaalta saman alan vastaajista 14 % olivat myös toisessa ääripäässä, ja suorittivat auditointeja ja testauksia kerran kuukaudessa. Voidaankin todeta, että saman alan sisällä esiintyy usein suhteellisen paljon vaihtelua.



KUVIO 11. Tietoturva-arvioinnit ja -testaukset koko vastaajaryhmän kesken

Yhdeksäs kysymys käsitteli yritysten fyysisiä turvatoimia. Kysymys oli monivalinta, jossa vastaajan oli mahdollista kertoa ”Muu, mikä?” -kentässä, mikäli yrityksellä oli käytössä muita fyysisiä turvatoimia, kuin vaihtoehdoissa oli valmiiksi annettu. 90 %:ssa yrityksiä oli huolehdittu lukituista tiloista. Valvontakameroita oli käytössä 65 %:ssa yrityksistä. Kulunvalvontajärjestelmiä oli 67 %:lla ja turvallisuushenkilöstöä 18 %:lla. Vastaajista 8 % eivät käyttäneet minkäänlaisia fyysisiä turvatoimia. (KUVIO 13.) Avoimeen kenttään oli saatu yksi vastaus, jossa kerrottiin yrityksellä olevan käytössä tutkalla toimivat hälytysjärjestelmät.

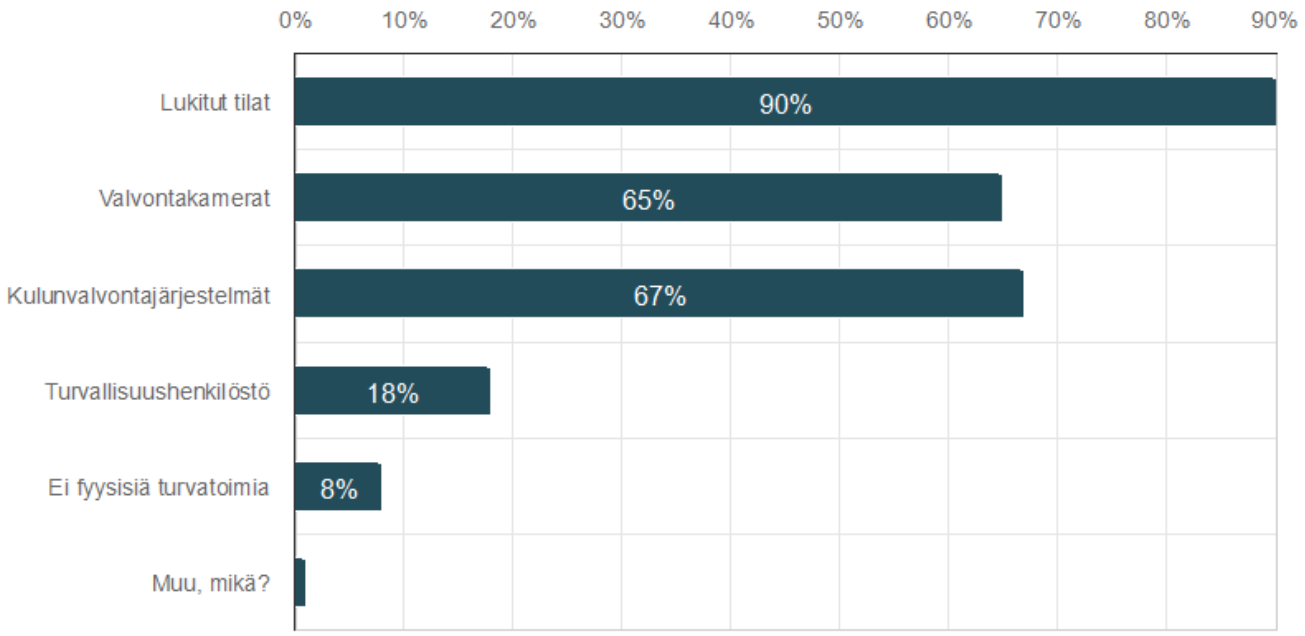
Fyysiset turvatoimet vaihtelivat yrityskoon mukaan. (KUVIO 12.) Ainoa vastaus, jossa vaihtelu oli hieman maltillisempaa, oli lukitut tilat. Suuryrityksillä oli käytössä laajimmin erilaisia turvatoimia, keskisuurilla tätä vähemmän ja pienyrityksissä kaikkein vähiten. Vastausprosentit olivat jokseenkin odotettavissa. Läheskään kaikki vaihtoehdot eivät olisi esimerkiksi pienyritykselle välttämättä tarkoituksenmukaisia, jos ajatellaan, että pienyrityksen edustaja olisi vaikkapa yksinyrittäjä ja tekisi töitä kotonaan. Tällöin kulunvalvontajärjestelmä ei olisi asia, joka tällaisella yrityksellä olisi todennäköisesti käytössä. Yllättävää kuitenkin oli, että 15 %:lla pienyrityksistä ja 4 %:lla keskisuurista yrityksistä ei ollut minkäänlaisia fyysisiä turvatoimia käytössä. Voisi ajatella, että jokaisella yrityksellä olisi vähintään lukitut tilat käytössä, mutta näin ei ollut.



KUVIO 12. Fyysiset turvatoimet eri yrityskokoluokissa

Yritykset, joiden pääasiallinen toimipaikka oli Varsinais-Suomi, käyttivät eniten erilaisia fyysisiä turvatoimia. Toiseksi eniten näitä käyttivät koko Suomessa ja kansainvälisesti toimivat yritykset, sekä

hieman näitä vähemmän Uudellamaalla toimivat yritykset. Vertailuryhmästä vähiten fyysisiä turvatoimia oli käytössä Pohjois-Pohjanmaalla toimivilla yrityksillä, joista 20 % ei käyttänyt niitä ollenkaan. Kaikissa vertailuryhmän toimialojen yrityksissä käytettiin laajasti erilaisia fyysisiä turvatoimia. Eniten näitä oli käytössä teollisuusalalla sekä julkisen hallinnon ja maanpuolustuksen alalla. Muun palvelutoiminta-alan ja informaatio- ja viestintäalan turvatoimet olivat selkeästi muita aloja vähäisempiä, vaikkakaan eivät erityisen pieniä prosentiltaan.



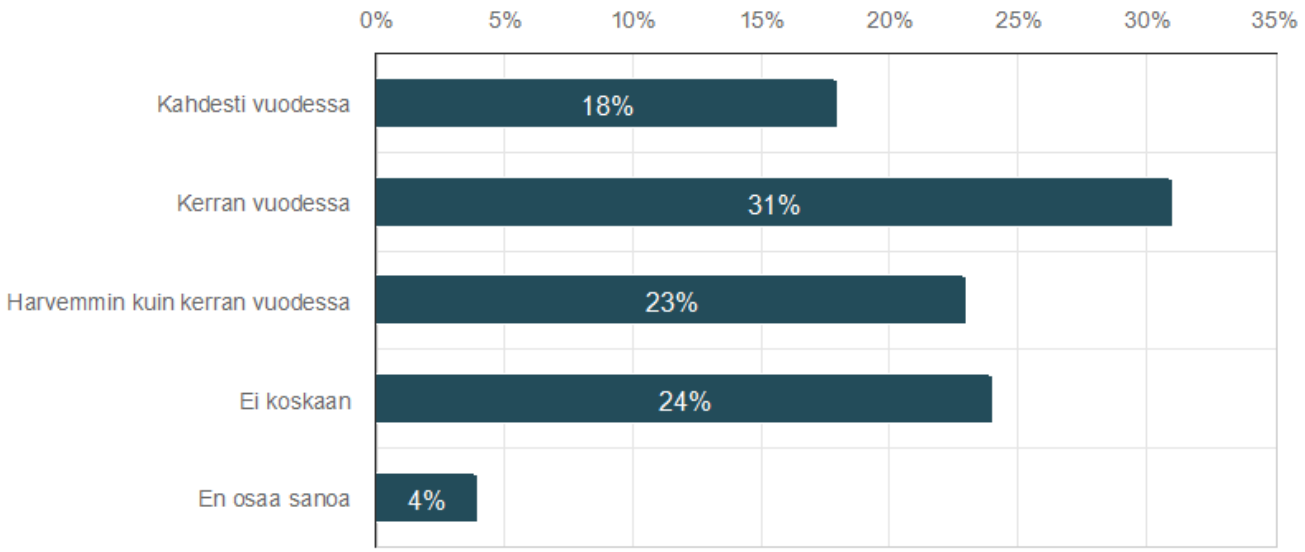
KUVIO 13. Fyysiset turvatoimet yrityksissä koko vastaajaryhmän kesken

Kymmenennessä kysymyksessä kysyttiin kuinka usein yritys järjestää tietoturvakoulutuksia työntekijöilleen. 18 % kouluttivat henkilöstöään tietoturvaan liittyen kaksi kertaa vuodessa, 31 % kerran vuodessa, 23 % harvemmin kuin kerran vuodessa ja 24 % eivät kouluttaneet työntekijöitään tietoturvaan liittyen koskaan. (KUVIO 14.)

Kerran tai kahdesti vuodessa tietoturvakoulutuksia järjestivät pääasiassa suuret ja keskisuuret yritykset, pienyritysten osuuden ollessa huomattavasti pienempi. Pienyritysten määrä taas korostui ”Ei koskaan” -vastauksen kohdalla, jonka vastasi lähes puolet pienyrityksistä. Keskisuurista yrityksistä vain yksi yritys ei järjestänyt tietoturvakoulutuksia koskaan ja suuryrityksistä kaikki järjestävät vähintään harvemmin kuin kerran vuodessa.

Tietoturvakoulutuksia järjestettiin tiheimmin koko Suomessa toimivissa yrityksissä, joista yli puolet kertoivat järjestävänsä koulutuksia kahdesti vuodessa. Kaikkien muiden alueiden prosentit olivat alle 15 % tämän vastausvaihtoehdon kohdalla. Kansainvälisesti toimivat yritykset järjestivät koulutuksia useimmiten kerran vuodessa (73 %). Varsinais-Suomen edustajilla suosituin vastaus oli harvemmin kuin kerran vuodessa. Uudenmaan ja Pohjois-Pohjanmaan yrityksistä suurin osa ei järjestänyt koulutuksia koskaan.

Toimialan vaikutus ei ollut tietoturvakoulutusten kohdalla kovinkaan suuri, sillä kaikilta aloilta löytyi molempia ääripäitä ja kaikkea siltä väliltä, eikä mikään ala erottunut erityisesti joukosta. Yhtenä huomiona voidaan mainita, että julkisen hallinnon ja maanpuolustuksen alalta ei löytynyt ollenkaan yrityksiä, jotka eivät järjestäisi tietoturvakoulutuksia.



KUVIO 14. Tietoturvakoulutusten järjestämistiheys yrityksissä

Yhdestoista kysymys oli avoin kysymys, jossa kysyttiin millaisia työkaluja tai ohjelmistoja yritys käyttää kyber- ja tietoturvallisuuden hallintaan. Kysymykseen oli myös lisätty lisähuomautus ”Vastaa halutessasi.”, sillä kysymys oli melko arkaluontoinen, eikä haluttu, että vastaaja mahdollisesti jättäisi kyselyn kesken tällaisen kysymyksen tultua vastaan. Vastauksia kertyi 50 kappaletta.

Vastauksia tarkastellessa eniten toistuva vastaus oli Microsoftin eri ohjelmat, joita oli käytössä ainakin 21:llä eri yrityksellä. Näihin kuuluivat useimmiten Microsoftin koko tuoteperhe, mutta joissakin vastauksissa tuotiin tarkemmin esille palvelut, joita yrityksellä oli käytössä. Näitä olivat mm. Microsoft

XDR, Microsoft Sentinel, Microsoft Defender, Microsoft E5 Security tuotteet, Microsoft Entra ID, Microsoft Intune ja Microsoft Azure. Vastauksissa toistui usein myös virustorjunta, ja osassa vastauksista oli tarkennettu käytössä oleva ohjelma. Näitä olivat F-secure ja Norton. Moni yritys kertoi heillä olevan käytössä kaksivaiheinen tai monivaiheinen tunnistus ja autentikointipalvelut tärkeissä sovelluksissa. Jatkuvan koulutuksen työkalut mainittiin muutamassa vastauksessa ja näillä tarkoitettiin esimerkiksi kalastelusimulaatioita.

17 yritystä mainitsi vastauksissaan palomuurit, ja joidenkin vastauksissa mainittiin tarkemmin palomuurinsäätöanalysaattorit, palomuurien lokitiedostot, NGFW (A Next-generation firewall), älykkäät palomuurit ja palomuurin ATP. VPN-yhteydet tulivat esille neljän yrityksen vastauksissa, joista yhdessä oli tarkennuksena Palo Alto Global Protect VPN. Moni yritys kertoi käyttävänsä erilaisia kyber- ja tietoturvaratkaisuja, joiden palveluntarjoajana olivat mm. WithSecure, Lenovo, Fortinet, Aruba, OKTA, Proofpoint ja Zscaler. Vastauksissa tuli esille myös EDR, SOC, SIEM, SAST, DAST, haavoittuvuusskannaukset ja levyjen salaus.

Muita vastauksia olivat mm. Ccleaner, Granite koulutukset, salasanapankit, varmuuskopiointi, tietoturvallisuuden hallintajärjestelmä, jonka viitekehyksenä ISO27001 tietoturvastandardi, Katakri, tietosuoja-asetus ja NIST2-direktiivi. Lisäksi yksi yritys kertoi ulkoistaneensa ohjelmistojen ylläpidon ja tietoturvan. Toisessa yksittäisessä vastauksessa kerrottiin, että yrityksessä luotetaan palomuuriin ja omaan harkintakykyyn, joten konekohtaista kybertorjuntaa ei ollut käytössä. Heillä myös suositeltiin työntekijöitä huolehtimaan tietoturvasta ja päivityksistä omatoimisesti. Eräässä yksittäisessä vastauksessa kerrottiin, että Mac-ympäristössä ei ollut tullut vastaan viruksiin liittyviä ongelmia kahteenkymmeneen vuoteen.

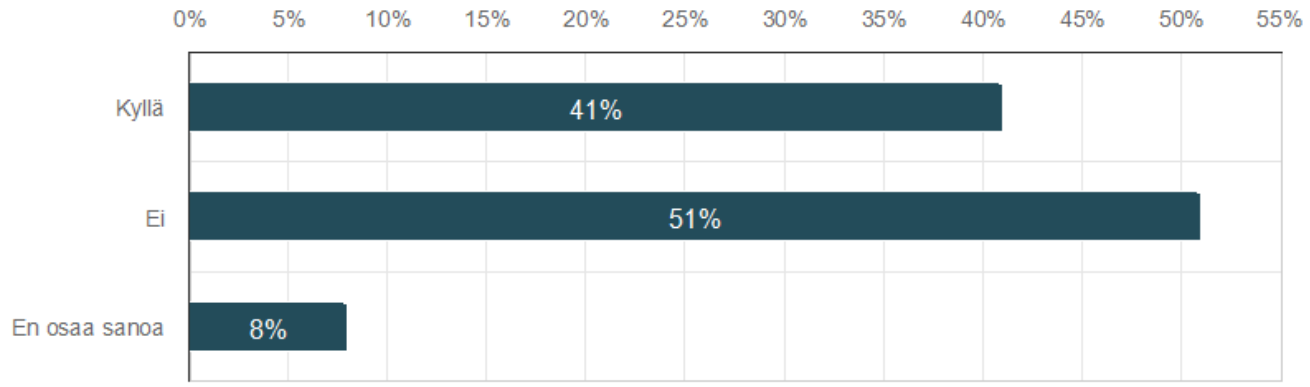
Kokonaisuudessaan yrityksillä on käytössä laajasti erilaisia kyber- ja tietoturvapalveluita eri palveluntarjoajilta. Myös monia työkaluja ja toimenpiteitä oli yrityksien itsensä hoidettavana ja ylläpidettävänä. Osalla vastaajista oli pitkä lista erilaisia työkaluja ja ohjelmia, joita heidän kyber- ja tietoturvansa hoitamisessa käytetään. Osasta vastauksia taas ilmeni, ettei yrityksessä ole kyber- ja tietoturvaan liittyen juurikaan minkäänlaisia työkaluja tai ohjelmia käytössä.

7.4 Uhat ja toiminta hätätilanteissa

Kahdennessatoista kysymyksessä kysyttiin onko yrityksessä kohdattu kyberturvallisuusuhkia viimeisen vuoden aikana. 41 % yrityksistä oli kohdannut kyberturvallisuusuhkia viimeisen vuoden aikana, kun taas 51 % ei ollut. 8 % vastaajista ei osannut sanoa. (KUVIO 15.)

Yrityskokoluokkien kohdalla voitiin huomata, että suuryritykset olivat kohdanneet kyberturvallisuusuhkia huomattavasti enemmän, kuin pienet yritykset. Suuryrityksistä 70 % oli kohdannut kyberturvallisuusuhkia, keskisuurista yrityksistä 50 % ja pienyrityksistä 23 %. Suuryrityksillä voi tavallisesti olla hallussaan suurempia rahallisia varoja ja arvokkaita tietoja, jotka voivat tehdä niistä houkuttavamman kohteen hyökkääjille.

”Kyllä” vastattiin useammin kuin ”Ei” kansainvälisesti toimivien yritysten, Varsinais-Suomessa toimivien yritysten, ja koko Suomessa toimivien yritysten kohdalla. Uudellamaalla ja Pohjois-Pohjanmaalla taas oli useammin vältytty kyberturvallisuusuhkien kohtaamiselta. Teollisuusalalla yli puolet yrityksistä olivat kohdanneet kyberturvallisuusuhkia viimeisen vuoden aikana. Julkisen hallinnon ja maanpuolustuksen alalla sekä tukku- ja vähittäiskaupassa uhkia oli kohdattu vähemmän. Informaatio- ja viestintäalan sekä muun palvelutoiminnan alan vastaukset jakautuivat tasaisesti ”Kyllä” ja ”Ei” vastausten välillä.



KUVIO 15. Tietoturvauhkien kokeminen yrityksissä koko vastaajaryhmän kesken

Mikäli edelliseen kysymykseen vastattiin kyllä, avautui vastaajalle kysymys numero 13, jossa kysyttiin millaisia kyberturvallisuusuhkia yrityksessä oli kohdattu. Kysymykseen vastasi 50 yritystä.

Vastauksista ei löytynyt kovin montaa yritystä, joka ei olisi vastauksessaan maininnut kalasteluyrityksiä. Muutama yritys tarkensi kalastelun kohdistuneen käyttäjätunnuksiin ja pari yritystä kertoi kohdanneensa etenkin spear phishing-hyökkäyksiä, eli kohdennettua tietojenkalastelua. Kuusi yritystä kertoi kohdanneensa hajautettuja palvelunestohyökkäyksiä ja yksi yritys palveluntarjoajansa olevan usein hyökkäysten kohteena, joka on vaikuttanut myös heidän omaan toimintaansa. Useammassa vastauksessa tuli ilmi palomuuriin kohdistuneet hyökkäykset ja yhdellä yrityksellä hyökkäykset kohdistuivat niin omiin, kuin asiakkaidensa palomuureihin. Yrityksissä oli kohdattu myös brute force-hyökkäyksiä, eli väsytyshyökkäyksiä, joiden kohteena oli ollut esimerkiksi VPN. Paljon esillä olleena teemana olivat myös haavoittuvuuksien hyväksikäyttöyritykset.

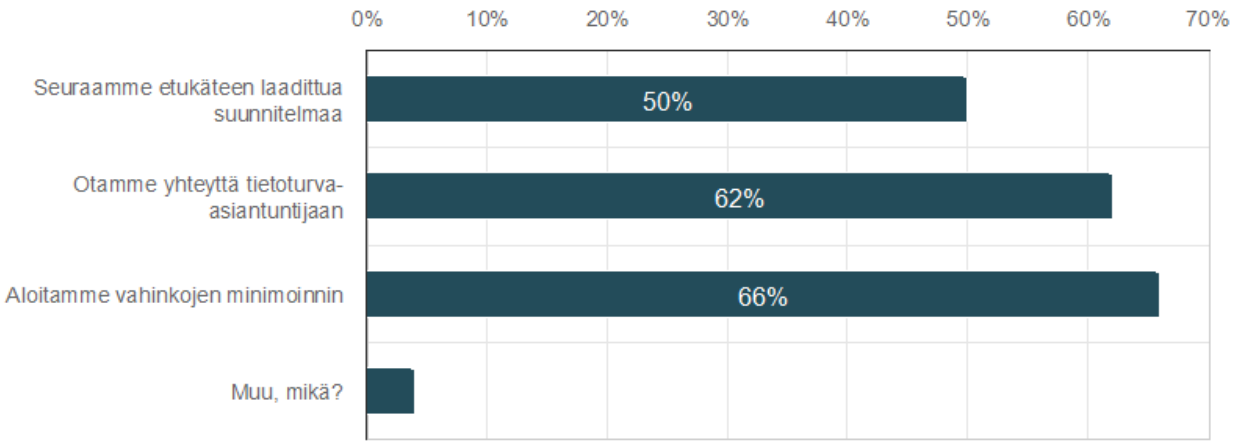
Jotkin yritykset olivat kohdanneet erilaisia huijausviestejä- ja puheluita, joita oli tehty esimerkiksi Microsoftin nimissä. Osaan yrityksistä oli yritetty kohdistaa niin sanottu toimitusjohtajahuijaus, eli kohdistettu huijausyritys, jossa huijaaja tekeytyy yrityksessä johtavassa asemassa olevaksi henkilöksi ja pyytää huijattua tekemään jotain puolestaan. Muutama yritys oli joutunut myös tietomurron tai tietovuodon kohteeksi. Monessa yrityksessä oli kohdattu tilien kaappaus- ja hakkerointiyrityksiä, ja osassa hyökkäyksiä oli valitettavasti onnistuttukin. Joissakin tapauksissa, kun hakkeroinnissa oli onnistuttu, oli yrityksen sähköpostista lähetetty tietojenkalasteluviestejä. Yritysten kohtaamien uhkien joukossa oli myös viruksia ja haittaohjelmia, porttiskannauksia, tietojärjestelmien skannauksia, verkkoskannauksia, palveluiden toiminnan tiedustelua, saastuneita liitteitä ja verkkosivuille kohdistettuja hyökkäyksiä. Vastaukset olivat hyvin mielenkiintoista luettavaa ja ne myös avasivat hyvin tämänhetkisiä uhkia, joita yritykset kohtaavat. Vastauksista voitiin myös huomata, että opinnäytetyön teoriaosuudessa käsitellyt teemat esiintyivät vastauksissa laajalti.

Neljästoista kysymys käsitteli hätätilanteita ja sitä, miten yritykset näissä tilanteissa toimivat. Esimerkkinä hätätilanteista annettiin tietovuodot. Kysymys oli monivalintakysymys, jossa 50 % kertoi seuraavansa etukäteen laadittua suunnitelmaa, 62 % ottaisivat yhteyttä tietoturva-asiantuntijaan, 66 % aloittaisi vahinkojen minimoinnin ja 3,5 % vastasi ”Muu, mikä?”, jossa listattiin lakiosaston mukaan ottaminen heti alussa, GDPR toimintasuunnitelman mukainen toiminta ja SOC-palvelu. (KUVIO 16.)

Yrityskoon vaikutus ei ollut tämän kysymyksen kohdalla niin merkittävä kuin muissa kysymyksissä, lukuun ottamatta yhtä vaihtoehtoa. Etukäteen laadittua suunnitelmaa seurasi 22 % pienyrityksistä, 67 % keskisuurista yrityksistä ja 86 % suuryrityksistä. Aiemmin tuli ilmi, että suurella osalla pienyrityksistä ei ole minkäänlaista suunnitelmaa hätätilanteiden varalle, joten vastaus oli osakseen odotettavissa. Kysymyksessä numero kuusi tuli ilmi, että 20 %:lla pienyrityksistä, 60 %:lla keskisuurista yrityksistä

ja 70 %:lla suuryrityksistä oli toipumissuunnitelma häiriötilanteiden varalle. Prosentit eivät siis olleet täysin vastaavat näiden kahden kysymyksen välillä ja etenkin suuryritysten vastausprosentit eroavat toisistaan. Suunnitelmaa seuraisi 86 % suuryrityksistä, vaikka virallinen suunnitelma oli vain 70 %:lla yrityksistä. Kyseessä oli siis mahdollisesti jokin toinen, DRP:n tapainen suunnitelma.

Kansainvälisesti toimivista yrityksistä 91 % seuraisi etukäteen laadittua suunnitelmaa, kun taas kaikilla muilla vertailuryhmän toimialueilla (Koko Suomi, Varsinais-Suomi, Pohjois-Pohjanmaa ja Uusimaa) suosituin toimenpide olisi aloittaa vahinkojen minimointi. Toimialoista teollisuusalalla otettaisiin useimmiten yhteyttä tietoturva-asiantuntijaan, julkisessa hallinnossa ja maanpuolustusalalla seurattaisiin useimmiten etukäteen laadittua suunnitelmaa tai otettaisiin yhteyttä tietoturva-asiantuntijaan. Tukku- ja vähittäiskaupassa sekä informaatio- ja viestintäalalla aloitettaisiin ensimmäiseksi vahinkojen minimointi useimmissa yrityksissä. Muun palvelutoiminnan alalla otettaisiin todennäköisimmin yhteyttä tietoturva-asiantuntijaan.



KUVIO 16. Toimenpiteet hätätilanteissa koko vastaajaryhmän kesken

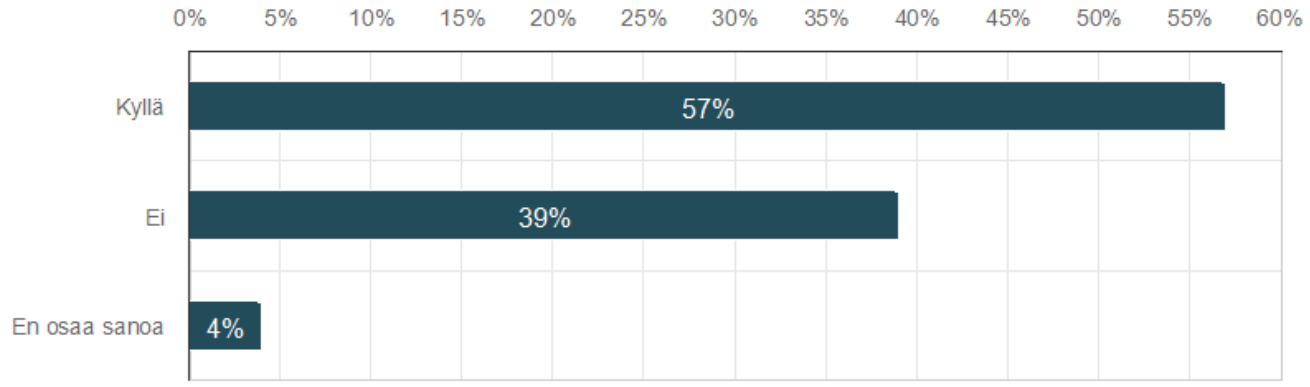
7.5 Ulkoiset palvelut

Viidennessätoista kysymyksessä kysyttiin käyttääkö yritys ulkopuolisia kyber- tai tietoturvallisuuspalveluita. 57 % vastasi käyttävänsä, 39 % eivät käyttäneet ja 4 % ei osannut sanoa. (KUVIO 17.)

Vastaukset vaihtelivat yrityskokojen välillä suhteellisen paljon. Suuryritykset käyttivät eniten ulkopuolisia kyber- tai tietoturvallisuuspalveluita, joka voi viestiä siitä, että suuryrityksillä oli käytössä enemmän resursseja tämänkaltaisiin palveluihin. Keskisuurten ja suurten yritysten välinen ero ei ollut niin

suuri, kuin verratessa pienyrityksiä edellä mainittuihin. Ainoastaan 39 % pienyrityksistä käytti tällaisia palveluita, suuryritysten prosentin ollessa 82 % ja keskisuurten yritysten 70 %. Olisin odottanut ulkopuolisia palveluita käyttävien pienyritysten osuuden olevan suurempi, sillä pienissä yrityksissä ei välttämättä ole omaa kyber- ja tietoturvasta vastaavaa henkilöstöä. Taloudelliset resurssit voivat osassa pienyrityksiä olla pienemmät, joka voi myös osaltaan vaikuttaa ulkoisten palveluiden käyttämättömyyteen.

Ulkopuolisia kyber- tai tietoturvallisuuspalveluita käytti yli 50 % kaikkien vertailtavien toimialueiden yrityksistä, lukuun ottamatta Pohjois-Pohjanmaata, jossa palveluita käytti 40 % yrityksistä. Toimialavertailussa teollisuusala erottui huomattavasti eniten (94 %) ulkopuolisia kyber- tai tietoturvallisuuspalveluita käyttävänä. Myös julkisen hallinnon ja maanpuolustusalan sekä muun palvelutoiminnan alan yrityksissä käytettiin näitä palveluita suhteellisen paljon, sillä molemmilla aloilla 64 % yrityksistä käytti näitä. Tukku- ja vähittäiskaupassa sekä informaatio- ja viestintäalalla käytettiin ulkoisia palveluita huomattavasti vähemmän.

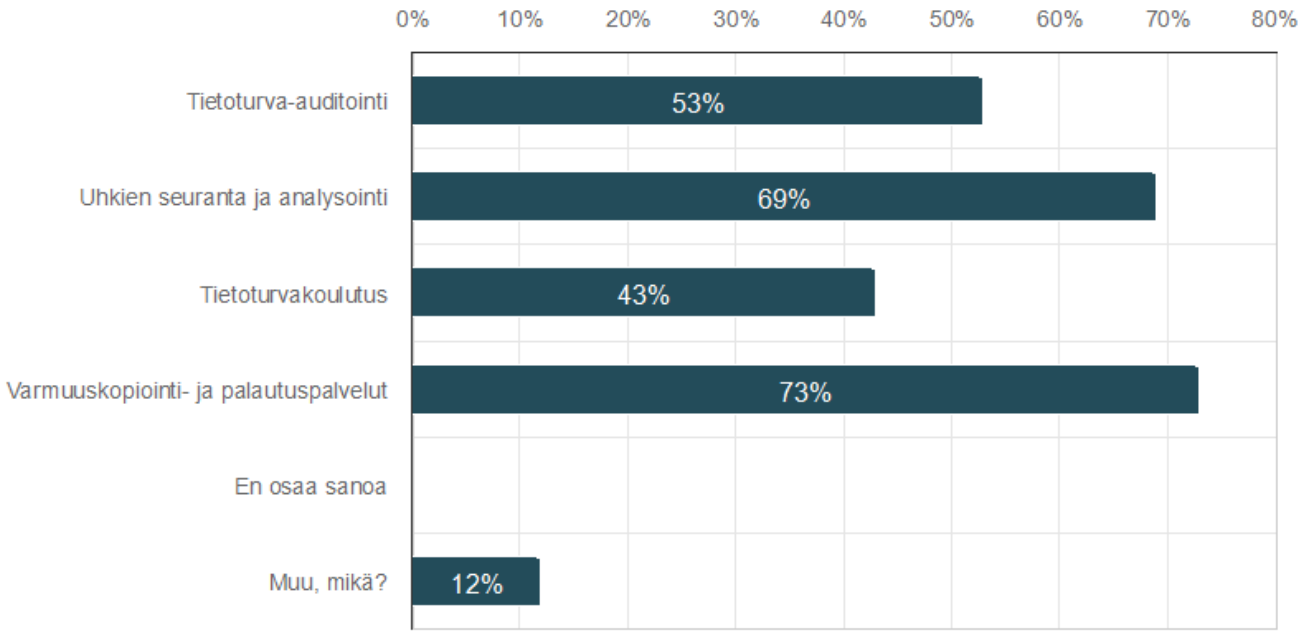


KUVIO 17. Ulkopuolisten kyber- ja tietoturvallisuuspalveluiden käyttö yrityksissä koko vastaajaryhmän kesken

Mikäli edelliseen kysymykseen vastattiin kyllä, tuli vastaajalle näkyviin kuudestoista kysymys, jossa tiedusteltiin mitä ulkoisia kyber- tai tietoturvallisuuspalveluita yritys käyttää. Kysymys oli monivalintakysymys. Eniten käytössä olivat varmuuskopiointi- ja palautuspalvelut, joita käyttivät 73 % yrityksistä sekä uhkien seuranta- ja analysointipalvelut, jotka olivat käytössä 69 %:lla yrityksistä. Ulkoista tietoturva-auditointia hyödynsi 53 % ja tietoturvakoulutuksia 43 % yrityksistä. (KUVIO 18.) ”Muu, mikä?” vastanneet kertoivat käytössä olevan mm. SOC-palvelu, tietoturvapäällikkö ja tietosuojavastaava palveluna, salasanojen hallinnointipalvelu, harjoitustoiminta sekä eri maailmanlaajuiset verkkopohjaiset ratkaisut ja F-secure.

Tämän kysymyksen kohdalla pienyritysten ja keskisuurten yritysten prosenttiosuudet vastauksissa olivat hyvin samaa luokkaa. Uhkien seuranta ja analysointi noin 54 %, tietoturvakoulutus 31 % ja varmuuskopiointi- ja palautuspalvelut noin 80 %. Ainoastaan tietoturva-auditoinnin kohdalla oli havaittavissa suurempi ero (Pienyritykset 24 % ja keskisuuret yritykset 44 %). Suuryrityksistä huomattavasti suuremmalla osalla oli käytössä erilaisia ulkoisia palveluita. Varmuuskopiointi- ja palautuspalveluita käytettiin kuitenkin suuryrityksissä vähemmän, kuin muissa yrityskokoluokissa. Näitä käyttivät 63 % suuryrityksistä. Suuyrityksissä mahdollisesti hoidetaan varmuuskopiointi ja palauttaminen oman henkilöstön toimesta.

Palveluista tietoturva-auditointia käyttivät eniten kansainvälisesti toimivat yritykset, varmuuskopiointi ja palautuspalveluita käytettiin eniten Pohjois-Pohjanmaalla, koko Suomessa sekä Uudellamaalla toimivissa yrityksissä. Varsinais-Suomessa käytössä oli eniten uhkien seuranta ja analysointipalvelut. Myös toimialojen vertailussa huomattiin, että varmuuskopiointi- ja palautuspalvelut olivat jokaisella toimialueella paljolti käytössä. Tätä suositumpaa teollisuusalalla sekä julkisessa hallinnossa ja maanpuolustusalalla olivat uhkien seuranta ja analysointi. Molemmat alat olivat luonteeltaan sellaisia, joissa tietoturvauhat voivat olla vakavia ja niillä voi olla laajoja vaikutuksia. Tukku- ja vähittäiskaupan alalla voitiin huomata, että tietoturva-auditoinnit ja tietoturvakoulutukset olivat harvinaisempia, sillä näitä järjestettiin vain 25 %:ssa yrityksistä. Informaatio- ja viestintäalalla taas voitiin huomata tietoturvakoulutusten olevan suuremmassa suosiossa, kuin muilla aloilla. Alalla tosin käsitellään paljon tietoa ja tietoturvariskit voivat joillain osa-alueilla olla muita korkeammat.



KUVIO 18. Ulkopuoliset kyber- ja tietoturvallisuuspalvelut yrityksissä koko vastaajaryhmän kesken

7.6 Tulevaisuuden haasteet

Viimeinen kysymys oli avoin kysymys liittyen kyberturvallisuuden haasteisiin tulevaisuudessa. Kysymykseen saatiin 77 hyvää vastausta. Suuri osa vastauksista voitiin ryhmitellä aihepiireittäin, sillä tulevaisuuden haasteet kyberturvallisuuteen liittyen olivat monella yrityksellä hyvin samanlaisia.

Ehdottomasti eniten huolta herättivät ihmiset. Suurimmaksi osaksi työntekijät, ja joissakin tapauksessa myös yrittäjät itse. Vastauksista voitiin huomata, että yrityksissä koettiin haastavaksi pitää henkilöstön osaaminen ajan tasalla kyberturvaan liittyen hyökkäystekniikoiden kehittyessä jatkuvasti ja hyökkääjien käyttäessä apuna esimerkiksi tekoälyä. Eräässä vastauksessa myös mainittiin, että on vaikeaa saada henkilöstö ymmärtämään kuinka vakavasta asiasta on kyse. Järjestelmien kehittyminen muodostaa henkilöstön kouluttamiselle entistä suurempia tarpeita ja haasteita. Henkilöstön lisääntyneen kiireen uskottiin lisäävän huijauksien onnistumisen mahdollisuutta, sillä ihmistä on helpompaa huijata kuin konetta. Eräs vastaaja myös kertoi, että pienenä toimijana monimutkaisessa maailmassa on vaikeaa hahmottaa, mitä kaikkea pitäisi edes tietää, toisen vastaajan taas uskoessa, että hyökkääjä olisi heidän yrityksensä kohdalla vahvoilla, koska osaamista ei maalaisjärjen lisäksi aiheeseen liittyen ole.

Tästä päästään toiseen haasteeseen, joita yritykset uskoivat kohtaavansa. Resurssit mietityttivät monia, mutta vastauksia siihen liittyen ei avattu paljoa sen enempää. ”Kutistuvilla resursseilla pitäisi luoda parempaa kyberturvallisuutta” eräässä vastauksessa mainittiin. Kalastelu, huijausyritykset ja sosiaalinen manipulointi tulivat laajasti esille vastauksissa. Näidenkin uhkien kohdalla mainittiin useasti hyökkäysten kehittyminen, jolloin henkilöstön on entistä vaikeampaa tunnistaa niitä. Näihin lankeamista pyrittiin välttämään kouluttamalla henkilöstöä ja pitämällä tietoisuutta yllä.

Useissa yrityksissä koettiin, että tulevaisuudessa esiintyvät haasteet voivat liittyä tekoälyyn ja sen potentiaaliin, joka tulisi aiheuttamaan harmia suuremmassa mittakaavassa. Tekoälyn kehittymisen uskotaan mahdollistavan laadukkaampia ja tehokkaampia hyökkäyksiä. Näihin liittyviä uhkakuvia ja ongelmia ei välttämättä täysin vielä tunnisteta, eikä kehitykseen ehditä mahdollisesti reagoida ajoissa.

Kehittyvät palvelunestohyökkäykset tulivat esille useissa vastauksissa ja kiristys- ja haittaohjelmien uskottiin olevan jatkossakin haaste useiden yritysten kohdalla. Monissa vastauksissa tuotiin ilmi yleisesti erilaiset hyökkäykset, sen enempää niitä tarkentamatta. Useat yritykset kokivat uhkana toiminnan ja järjestelmien häirinnän, ja jotkut tarkensivat, että erityisesti Idästä tuleva häirintä koetaan uhkana.

Globaali eriytyminen ja kauppasodat sekä maailmantilanne huolettivat joitakin vastaajia. Erilaiset tietomurrot, -varkaudet ja -vuodot lisäsivät huolta. Esimerkkeinä tulivat ilmi asiakastietojen vuodot ja identiteettivarkaudet. Yritysvakoilun uskottiin lisääntyvän ja toiminnan lamauttamisyrityksien sen myötä.

Tiedon vaatimusten mukainen käsittely ja tietoturva koettiin yleisesti asiana, joista tulee pitää huolta, jotta haasteilta voidaan välttyä. Kaikenlaisen yritysdatan turvallisen hallinnan ajateltiin olevan entistä tärkeämpää ja haasteena koettiin se, että yrityksillä on hallussaan asiakkaidensa arkaluonteisia tietoja, joita tulee suojata.

Pilvipalveluiden käytön lisääntyminen, pilvipalveluiden varmuuskopioinnit ja pilvipalveluiden hyökkäysten tunnistaminen koettiin haasteena. Esiin tuli myös globaalien pilvipalvelualustojen käytön epävarmuus. Kvanttitietokoneet herättivät muutamassa yrityksessä huolta tulevaisuuden osalta. Koneiden uskottiin tuovan suuria haasteita tulevaisuudessa, mutta vastauksissa haluttiin myös uskoa, että salaustekniikoita saataisiin kehitettyä tämänkin haasteen ratkaisemiseksi. Haasteita uskotaan olevan myös yleisesti kehityksen mukana pysymisessä ja uusiin haasteisiin vastaamisessa.

Yksittäisissä vastauksissa tuli esille OT-ympäristön tietoturva sekä IT ja OT ympäristön jakautuminen. ”Laitteita ei tunnisteta riittävän hyvin ja erityisesti OT-puolella ei ole mahdollisuuksia päivittää järjestelmiä”, eräässä vastauksessa kerrotaan. Haasteena koettiin myös riittävän vahvat salasanat, haavoittuvuuksien hyödyntäminen, vastuu- ja sopimusriskit, tiedonsiirto EU/ETA-maiden ulkopuolelle sekä kolmansien osapuolien ja toimittajaverkoston hallinta. On-Premisen ja pilven välillä koettiin olevan tasapainoilua, jonka uskottiin jatkuvan vuosikymmeniä eteenpäin. Eräässä vastauksessa huolta aiheuttivat julkiset yritystiedot, joiden avulla rikolliset voivat ennakkoon kartoittaa mihin yrityksiin hyökkäyksiä olisi kannattavaa kohdistaa.

Lainsäädäntö ja säädökset koettiin tulevaisuuden haasteena. Vastauksissa mainittiin EU-lainsäädännön vaatimusten, esimerkiksi NIS2 ja tiedon avaamiseen liittyvän regulaation asettavan merkittävää painetta tunnistaa, hallita ja ymmärtää niiden tietoturvaan ja tietosuojaan liittyvät ulottuvuudet.

Viimeisenä ryhmänä olivat vastaajat, jotka uskoivat, etteivät he ole rikollisten todennäköisiä uhreja tai ettei heillä ole mitään varastettavaa. Eräs vastaaja arvioi, että maailma, jossa uskotaan palomuurin sisäpuolella kaiken olevan turvassa kuten 90-luvulla, on edelleen voimissaan.

8 POHDINTA JA PÄÄTELMÄT

Tutkimuksen tavoitteena oli saada kokonaiskuva eri kokoisten yritysten tekemistä toimenpiteistä kyberturvallisuutensa edistämiseksi. Vertailua tehtiin myös toimialoittain ja pääasiallisen toimipaikan perusteella. Toimialojen- ja paikkojen vertailuun valittiin viisi suurinta vastaajaryhmää kustakin kategoriasta.

Tutkimus tehtiin kyselytutkimuksena Webropol-alustalla ja siinä käytettiin sekä kvantitatiivista, että kvalitatiivista tutkimusmenetelmää. Kyselyyn saatiin 145 vastausta ja oli odotettavissa, että vastauksia saataisiin suhteellisen paljon, sillä kysely lähetettiin yli tuhannelle yritykselle. Toisaalta huolenaiheena oli, että yritykset eivät haluaisi vastata kyselyyn, sillä kyseessä oli aihe, joka sisältää monen yrityksen kohdalla vain yrityksen sisälle tarkoitettua tietoa. Kyselykutsussa kerrottiin, että kysely on anonyymi, eikä yrityksiä voida tunnistaa vastauksista.

Tuloksista voitiin havaita, että osalla yrityksistä toimenpiteet kyberturvallisuuden eteen eivät olleet sillä tasolla, kuin niiden olisi hyvä olla. Vastaajista löytyi suuri määrä yrityksiä, joilla ei ollut käytössä kyberturvallisuuspolitiikkaa, eikä toipumissuunnitelmaa. Toimenpiteitä kyberturvallisuuden edistämiseksi oli käytössä laajemmin, mutta niidenkin osalta monissa yrityksissä olisi parantamisen varaa. Avoimista vastauksista voitiin havaita, että suhtautuminen kyberturvallisuuteen oli joidenkin yritysten osalta välinpitämätöntä, mutta suurimmassa osassa yrityksiä kuitenkin hyvällä tasolla.

Kyselyn tulokset osoittivat, että kyberturvallisuuden eteen tehdyt toimenpiteet vaihtelivat suuresti etenkin yrityskokojen välillä. Ennakko-odotuksena oli, että suuryrityksissä toimenpiteisiin voitaisiin käyttää enemmän resursseja, ja että kyberturvallisuus olisi näin ollen myös paremmalla tasolla, kuin pienemmissä yrityksissä. Odotuksena oli myös, että keskisuurten ja pienten yritysten joukostakin löytyisi jonkin verran poikkeuksia, jotka pitävät kyberturvallisuutta hyvin tärkeänä ja tekevät sen eteen laajasti eri toimenpiteitä. Odotukset osoittautuivat paljolti tuloksia vastaaviksi. Tuloksista ilmeni, että suuryritykset todellakin tekevät enemmän toimenpiteitä pitääkseen kyberturvansa tason korkeana. Pienissä yrityksissä oli keskimäärin huomattavasti vähemmän kyberturvallisuuden edistämistä parantavia toimenpiteitä käytössä. Keskisuuret yritykset sijoittuivat tuloksissa suurten ja pienten yritysten välille. Niin kuin oletettiin, joukosta löytyi joidenkin kysymysten kohdalla myös poikkeuksia, etenkin pienyritysten osalta.

Toimipaikan vaikutusta vertaillessa tuloksiin erot eivät olleet aivan niin selviä, kuin yrityskoon kohdalla. Alueita vertaillessa voitiin kuitenkin huomata, että kansainvälisesti ja koko Suomessa toimivissa yrityksissä oli käytössä yleensä laajemmin toimenpiteitä kyberturvallisuuden edistämiseksi, kuin muilla alueilla. Myös Varsinais-Suomessa ensisijaisesti toimivat yritykset olivat jokseenkin valveutuneempia kyberturvan suhteen, mutta useammissa kyberturvan aiheissa kuitenkin hieman vähemmän, kuin kansainväliset ja koko Suomen laajuudella toimivat yritykset. Uudellamaalla toimivissa yrityksissä toimenpiteet kyberturvallisuuden eteen olivat heikommalla tasolla, kuin edellä mainituilla alueilla. Pohjois-Pohjanmaa erottui vertailuryhmästä toimillaan, joiden taso oli vastausten mukaan heikkoa. Toimialojen vertailussa tulokset vaihtelivat kysymysten välillä useimmiten niin paljon, ettei suoria johtopäätöksiä toimialan vaikutuksesta aiheeseen voitu kaikkien alojen kohdalla tehdä. Ainoastaan teollisuusalan voitiin huomata erottuvan vastauksissa alana, jossa kyberturvallisuuteen kiinnitettiin erityisesti huomiota, ja jonka eteen tehtiin laajasti erilaisia toimenpiteitä.

Tulosten luotettavuuteen ja yleistettävyyteen vaikutti osakseen vastausmäärien vaihtelu jokaisen taustavaikuttajan kohdalla, joiden avulla vertailua tehtiin. Vaihtelua oli huomattavissa etenkin toimialan ja toimipaikan kohdalla, jossa vertailuun valittiin ainoastaan viisi suurinta vastaajaryhmää, joka on voinut vaikuttaa tuloksiin. Kyselyn vastaajamäärä oli kokonaisuudessaan kuitenkin suhteellisen korkea, ja sen avulla voitiin saada kattava käsitys yritysten suhtautumisesta kyberturvallisuuteen sekä niistä toimenpiteistä, joita yrityksissä sen eteen tehdään. Työtä voisi jatkossa kehittää tekemällä tutkimuksen, jossa käytettäisiin enemmän kvalitatiivisia menetelmiä, jonka avulla voitaisiin ymmärtää entistäkin syvällisemmin yritysten näkemyksiä ja kokemuksia kyberturvallisuudesta ja sen haasteista.

Opinnäytetyöprosessi tarjosi paljon uutta tietoa kyber- ja tietoturvallisuuteen liittyen, vaikka suurilta osin se oli ennestään tuttua, ja itselleni mielenkiintoista tutkia. Tietoperustan teemat olivat työelämän ja opintojen kautta pääosin tiedossa, mutta osa teemoista syvensi omaa osaamistani aiheisiin liittyen. Työn aikana mielenkiintoisimmat opit saatiin tutkimuksen avointen kysymysten vastauksista, joita lukiessa pystyttiin ymmärtämään laajemmin kaiken kokoisten yritysten edustajien ajatuksia liittyen kyberturvallisuuteen ja teemoihin sen ympärillä.

LÄHTEET

Abraham, C., Chatterjee, D., Ronald, R. 2019. Muddling through cybersecurity: Insights from the U.S healthcare industry. *Business horizons*. 62(4), 539-548. Viitattu 19.4.2024.

Access Now. 2023. *Who is shutting down the internet in 2023? A midyear update*. Saatavissa: https://www.accessnow.org/publication/internet-shutdowns-in-2023-mid-year-update/#join-us. Viitattu 16.3.2024.

Alasuutari, P. 2011. *Laadullinen tutkimus 2.0.* Tampere: Osuuskunta Vastapaino.

Cinia. 2023. *Nykyaikainen palomuuri on yrityksen tietoverkkoratkaisun ydin.* Saatavissa: https://www.cinia.fi/blogi/nykyaikainen-palomuuri-on-yrityksen-tietoverkkoratkaisun-ydin. Viitattu 18.4.2024.

Cisco. 2024a. *What is Cybersecurity?* Saatavissa: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html. Viitattu 6.3.2024.

Cisco. 2024b. *What is malware?* Saatavissa: https://www.cisco.com/site/in/en/learn/topics/security/what-is-malware.html. Viitattu 16.3.2024.

Cybercrime Magazine. 2020. *Cybercrime to cost the world $10,5 trillion annually by 2025.* Saatavissa: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. Viitattu 16.3.2024.

Corrons, L. 2024. *Computer viruses: How they spread and tips to avoid them.* Saatavissa: https://us.norton.com/blog/malware/what-is-a-computer-virus. Viitattu 16.4.2024.

Data Group. 2021. *Huolehdi näistä seitsemästä tietoturvan osa-alueesta.* Saatavissa: https://www.datagroup.fi/ajankohtaista/huolehdi-naista-seitsemasta-tietoturvan-osa-alueesta. Viitattu 16.4.2024.

ENISA. 2023. *Enisa Threat Landscape 2023*. Saatavissa: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023. Viitattu 31.3.2024.

Erillisverkot. 2024. *Ilman varmoja tietoliikenneyhteyksiä ei ole turvallisuutta. Saatavissa:* https://www.erillisverkot.fi/ilman-varmoja-tietoliikenneyhteyksia-ei-ole-turvallisuutta/. Viitattu 2.5.2024.

eSENTIRE. 2023. *Cybercrime to cost the world $9,5 Trillion USD Annually in 2024*. Saatavissa: https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024. Viitattu 16.3.2024.

F-Secure. 2024a. *Mikä on antivirus eli virustorjunta?* Saatavissa: https://www.f-secure.com/fi/articles/antivirus. Viitattu 2.5.2024.

F-Secure. 2024b. *Mikä on palomuuri?* Saatavissa: https://www.f-secure.com/fi/articles/firewall. Viitattu 18.4.2024.

Heikkilä, T. 2014. *Tilastollinen tutkimus*. 9. uudistettu painos. Porvoo: Bookwell Oy.

Imperva. 2024. *Social Engineering.* Saatavissa: https://www.imperva.com/learn/application-security/social-engineering-attack/. Viitattu 16.3.2024.

Indeed. 2023. *5 Types of Data Classification (With Examples).* Saatavissa: https://www.indeed.com/career-advice/career-development/data-classification-types. Viitattu 18.4.2024.

Johansen, A. 2020. *What is a trojan? Is it a virus or is it a malware?* Saatavissa: https://us.norton.com/blog/malware/what-is-a-trojan. Viitattu 16.4.2024.

Jurvanen, L. 2023a. *Mitä on fyysinen tietoturva?* Saatavissa: https://www.savelan.fi/mita-on-fyysinen-tietoturva/?_gl=1*1dpfg61*_up*MQ..*_ga*MTY4NzkyNTIwMi4xNzEzNzI-wNzQw*_ga_FSE92PCRQV*MTcxMzcyMDczOS4xLjAuMTcxMzcyMDczOS4wLjAuMA. Viitattu 3.5.2024.

Jurvanen, L. 2023b. *Mitä tarkoittaa hallinnollinen tietoturva?* Saatavissa: https://www.savelan.fi/mita-tarkoittaa-hallinnollinen-tietoturva/. Viitattu 3.5.2024.

Kaspersky. 2024. *Mitä on tietojen salaus? Määritelmä ja selitys.* Saatavissa: https://www.kaspersky.fi/resource-center/definitions/encryption. Viitattu 21.4.2024.

Kyberturvallisuuskeskus. 2020b. *Muista laitteiden, ohjelmistojen ja sovellusten päivittäminen.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/muista-laitteiden-ohjelmistojen-ja-sovellusten-paivittaminen. Viitattu 16.4.2024.

Kyberturvallisuuskeskus. 2020a. *Kyberturvallisuus ja yrityksen hallituksen vastuu.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf. Viitattu 21.4.2024.

Kyberturvallisuuskeskus. 2021. *Näin suojaudut tietomurroilta.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta. Viitattu 18.4.2024.

Kyberturvallisuuskeskus. 2023. *Tietoturva on koko organisaation asia – vinkkejä henkilöstön tietoturvakoulutuksen suunnitteluun.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/tietoturva-koko-organisaation-asia-vinkkeja-henkiloston. Viitattu 18.4.2024.

Kyberturvallisuuskeskus. 2022a. *Toimintaohje – Tietomurto.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TietomurtoToimintaohje.pdf. Viitattu 17.3.2024.

Kyberturvallisuuskeskus. 2024. *Toimintamme.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme. Viitattu 31.3.2024.

Kyberturvallisuuskeskus. 2022b. *Toimintaohje – Kiristyshaittaohjelma.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/KiristyshaittaohjelmaToimintaohje.pdf. Viitattu 17.3.2024.

Kyberturvallisuuskeskus. 2022c. *Toimintaohje – Palvelunestohyökkäys.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/PalvelunestohyökkäysToimintaohje.pdf. Viitattu 17.3.2024.

Kyberturvallisuuskeskus. 2022d. *Toimintaohje – Toimitusketjuhyökkäys.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/ToimitusketjuhyökkäysToimintaohje.pdf. Viitattu 17.3.2024.

Kyberturvallisuuskeskus. 2019. *Riskienhallinnan (hyvin) lyhyt oppimäärä.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/riskienhallinnan-hyvin-lyhyt-oppimaara. Viitattu 3.5.2024.

Lee, I. 2021. *Cybersecurity: Risk management framework and investment cost analysis.* Saatavissa: https://www-sciencedirect-com.ezproxy.centria.fi/science/arcle/pii/S0007681321000240?via%3Dihub. Viitattu 19.4.2024.

Microsoft. 2023. *Salasanakäytännön suositukset Microsoft 365 -salasanoille.* Saatavissa: https://learn.microsoft.com/fi-fi/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide. Viitattu 16.4.2024.

Microsoft. 2024. *Mitä käyttäjätietojen ja käyttöoikeuksien hallinta (IAM) on?* Saatavissa: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-identity-access-management-iam. Viitattu 18.4.2024.

Mondragon, L. 2020. *Kaksivaiheinen tunnistautuminen suojaa käyttäjätilejäsi*. Saatavilla: https://blog.f-secure.com/fi/kaksivaiheinen-tunnistautuminen/. Viitattu 16.4.2024.

Norton. 2019. *What is a computer worm, and how does it work?* Saatavissa: https://us.norton.com/blog/malware/what-is-a-computer-worm. Viitattu 16.4.2024.

Opetushallitus. 2024. *Kyberturvallisuusosaamisen perusteita perusopetukseen.* Saatavissa: https://www.oph.fi/fi/digiosaaminen/kyberturvallisuusosaamisen-perusteita-perusopetukseen/tiedon-manipulaatio-1. Viitattu 17.3.2024.

Reimaa, R. 2023. *Laitetason tietoturva: mitä se on ja miksi siitä tulee kiinnostua juuri nyt?* Saatavissa: https://www.tietokeskus.fi/blogi/laitetason-tietoturva-mita-se-on-ja-miksi-siita-tulee-kiinnostua-juuri-nyt/. Viitattu 3.5.2024.

Seclion. 2021. *Mitä on fyysinen tietoturvallisuus?* Saatavissa: https://blog.seclion.fi/turvallisuus/fyysinen-tietoturvallisuus. Viitattu 18.4.2024.

Tampereen yliopisto. 2020. *Tietoturva lyhyesti. Saatavissa:* https://www.tuni.fi/fi/it-palvelut/kasikirja/tietoturva/tietoturva-lyhyesti. Viitattu 31.3.2024.

Tietosuojavaltuutetun toimisto. 2024. *Tietosuoja.* Saatavissa: https://tietosuoja.fi/tietosuoja. Viitattu 31.3.2024.

The Economist. 2017. *The world's most valuable resource is no longer oil, but data.* Saatavissa: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Viitattu 16.3.2024.

Tilastokeskus. 2024. *Toimialaluokitus 2008*. Saatavissa: https://stat.fi/fi/luokitukset/toimiala/. Viitattu 1.5.2024.

Kysely yritysten kyberturvallisuuskäytänteistä

Tervetuloa osallistumaan yritysten kyberturvallisuuskäytänteitä käsittelevään anonyymiin kyselyyn!

Kyselyn tavoitteena on saada käsitys yritysten toimintatavoista kyberturvallisuuteen liittyen. Vastauksia hyödynnetään opinnäytetyössä, joka käsittelee yritysten kyberturvallisuutta.

Kyselyn täyttäminen vie noin 5 minuuttia ja vastaukset käsitellään täysin anonyymisti. Yksittäisiä vastaajia ei voida tunnistaa tuloksista. Kysely on avoinna 4.4.2024 saakka.

Kiitos, että otit hetken osallistuaksesi kyselyyn.

Taustatiedot

1. Edustamasi yrityksen kokoluokka

Valitse

2. Millä alueella yrityksenne ensisijaisesti toimii?

- Kirjoita tai valitse listalta avainsana -

3. Edustamasi yrityksen toimiala?

- (●) Maatalous, metsätalous ja kalatalous
- ( ) Kaivostoiminta ja louhinta
- ( ) Teollisuus
- ( ) Sähkö-, kaasu- ja lämpöhuolto, jäähdytysliiketoiminta
- ( ) Vesihuolto, viemäri- ja jätevesihuolto, jätehuolto ja muu ympäristön puhtaanapito
- ( ) Rakentaminen
- ( ) Tukku- ja vähittäiskauppa: moottoriajoneuvojen ja moottoripyörien korjaus
- ( ) Kuljetus ja varastointi
- ( ) Majoitus- ja ravitsemistoiminta
- ( ) Informaatio ja viestintä
- ( ) Rahoitus- ja vakuutustoiminta
- ( ) Kiinteistöalan toiminta
- ( ) Ammatillinen, tieteellinen ja tekninen toiminta
- ( ) Hallinto- ja tukipalvelutoiminta
- ( ) Julkinen hallinto ja maanpuolustus; pakollinen sosiaalivakuutus
- ( ) Koulutus
- ( ) Terveys- ja sosiaalipalvelut
- ( ) Taiteet, viihde, virkistys
- ( ) Muu palvelutoiminta
- ( ) Kotitalouksien toiminta työnantajina; kotitalouksien eriyttämätön toiminta tavaroiden ja palvelujen tuottamiseksi omaan käyttöön
- ( ) Kansainvälisten organisaatioiden ja toimielinten toiminta
- ( ) Toimiala tuntematon
- ( ) Muu, mikä? [ ]

4. Onko yrityksellänne käytössä virallinen kyberturvallisuuspolitiikka?

- (●) Kyllä
- ( ) Ei
- ( ) En osaa sanoa

5. Kuinka usein kyberturvallisuuspolitiikkaanne päivitetään?

- ( ) Kerran kuukaudessa
- ( ) Kerran neljännesvuodessa
- ( ) Kerran vuodessa
- ( ) Ei säännöllisesti
- ( ) En osaa sanoa

6. Onko yrityksellänne käytössä toipumissuunnitelma (DRP) häiriötilanteiden varalle?

- ( ) Kyllä
- ( ) Ei
- (●) En osaa sanoa

7. Mitä tietoturvakäytänteitä yrityksessänne noudatetaan?

- [ ] Säännölliset salasanan vaihdot ja määritellyt salasanapolitiikat
- [ ] Monivaiheinen todennus
- [ ] Tietoturvakoulutukset
- [ ] Pääsynhallinta
- [ ] Tietoturva-auditoinnit ja -arvioinnit
- [ ] Tietoturvapoikkeamien seuranta
- [ ] Etätyön tietoturvakäytännöt
- [ ] Ohjelmistojen ja järjestelmien päivitykset
- [ ] Ei mitään edellä mainituista
- [ ] En osaa sanoa
- [ ] Muu, mikä?

8. Kuinka usein yrityksessänne suoritetaan tietoturva-arviointeja ja testauksia?

- ○ Kerran kuukaudessa
- ○ Kerran neljännesvuodessa
- ○ Kerran vuodessa
- ○ Ei koskaan
- ◉ En osaa sanoa

9. Millaisia fyysisiä turvatoimia yrityksellänne on käytössä?

- ☐ Lukitut tilat
- ☐ Valvontakamerat
- ☐ Kulunvalvontajärjestelmät
- ☐ Turvallisuushenkilöstö
- ☐ Ei fyysisiä turvatoimia
- ☐ Muu, mikä? _____

10. Kuinka usein järjestätte tietoturvakoulutuksia työntekijöille?

- ○ Kahdesti vuodessa
- ○ Kerran vuodessa
- ○ Harvemmin kuin kerran vuodessa
- ○ Ei koskaan
- ◉ En osaa sanoa

11. Millaisia työkaluja tai ohjelmistoja käytätte kyber- ja tietoturvallisuutenne hallintaan? Vastaa halutessasi.

12. Onko yrityksessänne kohdattu kyberturvallisuusuhkia viimeisen vuoden aikana?

- (●) Kyllä
- ( ) Ei
- ( ) En osaa sanoa

13. Millaisia kyberturvallisuusuhkia olette kohdanneet?

1000 merkkiä jäljellä

14. Miten toimitte hätätilanteissa, kuten tietovuodoissa?

- [ ] Seuraamme etukäteen laadittua suunnitelmaa
- [ ] Otamme yhteyttä tietoturva-asiantuntijaan
- [ ] Aloitamme vahinkojen minimoinnin
- [ ] Muu, mikä?

15. Käyttääkö yrityksenne ulkopuolisia kyberturvallisuus- tai tietoturvallisuuspalveluita?

- (●) Kyllä
- ( ) Ei
- ( ) En osaa sanoa

16. Mitä palveluita?

- [ ] Tietoturva-auditointi
- [ ] Uhkien seuranta ja analysointi
- [ ] Tietoturvakoulutus
- [ ] Varmuuskopiointi- ja palautuspalvelut
- [ ] En osaa sanoa
- [ ] Muu, mikä?

17. Mitkä ovat suurimmat kyberturvallisuuteen liittyvät haasteet, joita uskot edustamasi yrityksen kohtaavan tulevaisuudessa?