Suomen energia-alan kyberturvallisuuden tila vuonna 2021

MIKKO LUOMALA | TERO VARTIAINEN | JYRI PAASONEN

VAASAN YLIOPISTON RAPORTTEJA 43

Vaasan yliopisto
UNIVERSITY OF VAASA

Julkaisija Vaasan yliopisto
Tekniikan ja innovaatiojohtamisen yksikkö, Tietojärjestelmätiede
Johtamisen yksikkö, Julkisoikeus.

Authors Mikko Luomala https://orcid.org/0000-0002-4125-6606
Tero Vartiainen https://orcid.org/0000-0003-3843-8561
Jyri Paasonen https://orcid.org/0000-0003-4012-3809

Selvitys

ISBN 978-952-395-085-6 (online)
URN https://urn.fi/URN:ISBN:978-952-395-085-6

ISSN 2489-2580 (Vaasan yliopiston raportteja 43)

Julkaisun nimi
Suomen energia-alan kyberturvallisuuden tila vuonna 2021

Asiasanat kyberturvallisuus, organisaatiot, yritykset, riskienhallinta, turvallisuus, hallinta, johtaminen

Rahoittaja Wärtsilä, ABB, Vaasan sähköverkot, Wapice, Arcteq, VASEK

Tiivistelmä

Energiasektori on perustavanlaatuisessa muutoksessa ja siten alttiina kyberturvallisuushyökkäyksille. Tässä selvityksessä luodaan tilannekuvaa Suomen energia-alan kyberturvallisuuden tilasta. Selvityksessä lähetettiin Suomen energia-alan toimijoille kyberturvallisuuskysely, jossa tiedusteltiin vastaajien käsityksiä muun muassa kyberturvallisuusjohtamisesta, riskienhallinnasta, toimitilaturvallisuudesta, kyberturvallisuusosaamisesta ja kyberturvallisuuspoikkeamista. Kyselyssä oli väittämäkysymyksiä ja avoimia kysymyksiä.

Suomen energia-alan toimijat kokevat hoitaneensa kyberturvallisuuden organisaatioissa, vaikka myös kokevat puutteita oman organisaationsa kyberturvallisuudessa. Vastaajista pieni osa koki puutteita sidosryhmien välisessä yhteistyössä, viranomaisyhteistyössä, organisaation tavoitteiden saavuttamisessa ja riskienhallinnan toteuttamisessa. Kyberturvallisuuden osaamistasoja ei osata arvioida. Myös kyberturvallisuusosaamisessa koetaan puutteita ja kyberturvallisuusharjoituksia on vähäisesti järjestetty. Vastaajista puolet koki havaitsevansa kyberturvallisuuspoikkeamat, ja myös puolet vastaajista raportoi kyberturvallisuuspoikkeamat organisaationsa johdolle, mutta viranomaisille enemmistö vastaajista jätti raportoimatta kyberturvallisuuspoikkeamat. Vastaajista enemmistö koki huolta erilaisista realisoituvista kyberhyökkäyksistä ja kyberturvallisuusloukkauksista.

Sisältö

Kuviot

Taulukot

1 JOHDANTO

Energia-alan kyberturvallisuuden tutkimukselle, opetukselle ja kehittämiselle on ainakin kaksi perustetta: 1) Energiasektori ei ole pelkästään yksi kriittisistä infrastruktuureista, vaan muut kriittiset infrastruktuurit, kuten vesihuolto ja sosiaali- ja terveydenhuolto ovat riippuvaisia tästä sektorista. 2) Energiasektori käy parhaillaan läpi syvällistä muutosta (engl. energy transition). EU:n alueella tapahtuvaa energiasektorin muutosta kuvaillaan kolmen trendin kautta (Fischer et al. 2018):

Trendi 1: Energiaketjun digitalisaatio: Älykkään teknologian kuten älykotien ja älykkäiden sähkömittareiden integrointi energiajärjestelmään edellyttää IT-ratkaisujen kehittämistä ja käyttöönottoa. Trendi 2: Hiilidioksidipäästöjen vähentäminen ja hajautettu energiantuotanto: EU pyrkii tuottamaan energiaa yhä enemmän uusiutuvilla menetelmillä, mikä tarkoittaa hajautettua energiatuotantoa. Trendi 3: Rajoja ylittävät energiamarkkinat ja integraatio: EU tavoittelee rajoja ylittäviä, reaaliaikaisia ja integroituja energiamarkkinoita, joihin toimijoilla on tasapuolinen pääsyoikeus.

Kaikille näille trendeille on yhteistä, että tietoa välitetään yhä enemmän paikasta toiseen tietoliikenneverkkoja pitkin digitaalisesti (Fischer et al. 2018). Tämä puolestaan lisää niin sanottua hyökkäyspinta-alaa, eli kyberhyökkääjillä on enemmän mahdollisuuksia aiheuttaa tuhoja. Mitä pidemmälle nämä trendit etenevät, sitä sosioteknisesti monimutkaisemmaksi energiajärjestelmä muodostuu, ja kyberturvallisuushaasteet lisääntyvät. Pohjanmaan energia-alan toimijoiden kyberturvallisuuden kehittämisen tueksi suunnittelimme Digitaalisten energiajärjestelmien kyberturvallisuus ja resilienssi (Cybersecurity and Resilience of Digital Energy Systems, CR-DES) -hankkeen (Vartiainen 2020).

Hankkeen osa-alueita ovat reaaliaikasimulaattorialusta, kyberturvallisuusprotokollan kehittäminen, energiajärjestelmien resilienssin mittaaminen sekä arviointi ja myös simulaatiomallien resilienssin arviointimenetelmien vertailu ja lopuksi energiajärjestelmissä realisoituneesta riskeistä palautuminen niin sanottuun normaaliin tilaan. Lisäksi hankkeessa käsitellään kyberturvallisuuden johtamista.

Tässä selvityksessä tehdään katsaus aiempaan tutkimukseen ja raportoidaan Suomen energia-alan toimijoiden kyselyn vastauksia. Lisäksi esitellään yhden kyberturvallisuuden johtamisen kehittämiseen liittyvän työpajan ryhmätöiden tuloksia. Lopuksi esitetään selvityksen johtopäätöksiä. Selvitys on luonteeltaan eksploratiivinen eli kartoittava, eli varsinaisia tutkimuskysymyksiä ei määritetä. Kirjallisuuskatsaus tehdään suppeasti valitsemalla SCOPUS-tietokannasta mahdollisimman uudet energia-alan teollisuusautomaatiota koskevat kansainväliset julkaisut.

2 AIEMPI TUTKIMUS

Suomessa kyberturvallisuutta on käsitelty mediassa ja kyberturvallisuusloukkauksista on tullut yhteiskunnallisesti ajankohtainen ongelma (Salminen 2021). Kirjallisuuskatsauksessa nousivat esille energia-alan järjestelmiin kohdistuvat moniulotteiset haasteet (Salminen 2021), (Ozcelik et al. 2021), (Zhang et al. 2021), (Stout 2012), (Nussbaum ja Dupuy 2017), (Basnet ja Ali 2021), (Qassim et al. 2021), (Sarker et al. 2020), (Larkin, Wagner, and Mullins 2020).

Teollisuusautomaatiojärjestelmien kyberturvallisuutta on tutkittu taloustieteellisestä, sotilasnäkökulmasta ja insinöörinäkökulmasta. Teollisuusautomaatiojärjestelmien toimintakyvystä sekä näiden järjestelmien toiminnan jatkuvuuden häiriöttömyydestä on tullut huolenaihe eri valtioiden viranomaisille ja eri valtioiden hallituksille. Vakavuutta ovat lisänneet laajassa julkisuudessa olleet kyberturvallisuuteen liittyvät kyberturvallisuusloukkaukset, jotka ovat herättäneet huolta teollisuusautomaatiojärjestelmien kyberturvallisuuden toteutumisesta (Ozcelik et al. 2021). Rikollisissa aikeissa olevat kyberhyökkääjät voivat tunkeutua valvontajärjestelmiin ja valvomo-ohjelmistojärjestelmiin sekä sitä kautta vaikuttaa vedenjakeluun asiakkaille esimerkiksi keskeyttämällä vedenjakelu kyberhyökkäyksen avulla (Zhang et al. 2021).

Viimeaikaisten kyberhyökkäysten määrät ja kyberhyökkäysten teknologinen kehittyneisyys ovat osoittaneet, että monien suurten yritysten, hallituksien ja sotilasviranomaisten käyttämät kyberturvallisuustoimenpiteet ovat olleet riittämättömiä (Stout 2012). Anonyymista hakkerijoukosta koostuva ryhmä nimeltä "AntiSec" oli julkaisut tiedoston, joka sisälsi sähköposteja ja henkilökohtaisia tietoja, jotka oli saatu 56 eri lainvalvontaviranomaisen tietokoneilta, vaikka tietojärjestelmien piti olla kyberturvallisia (Stout 2012). Organisaatioiden osaamiskyvyttömyyden on todettu lisäävän kriittisten infrastruktuurin järjestelmien turvaamisen haasteita, koska perinteisiä tietotekniikkaan tietoturvakäytäntöjä ei ole kyetty toteuttamaan kriittisten infrastruktuurin järjestelmiin (Ozcelik et al. 2021). Teollisuusautomaatiojärjestelmien häiriönsietokyvystä on tullut huolenaihe päätöksentekijöille (Ozcelik et al. 2021).

Nykymaailmassa kybermaailman tietoverkkojen ja energia-alan sähköverkojen yhteydet keskenään ovat kiistattomia. Tämä pätee käytännöllisesti katsoen kaikilla ihmistoiminnan aloilla, mukaan lukien sodankäynnissä, taloudessa ja myös politiikassa. Vähemmän tunnettuja toimintoja ovat kriittiset yhteydet eri energiajärjestelmien välillä ja energiajärjestelmien toimitusketjujärjestelmät, jota tarvitaan kybermaailmassa sekä sotilaallisissa toiminnoissa. Siis energiaa, jota tarvitaan sotilasoperaation voittamiseen ja menestyksen varmistamiseen. (Nussbaum ja Dupuy 2017).

Valvomo-ohjelmistojärjestelmiin (Supervisory Control And Data Acquisition; SCADA) on palveluestohyökkäyksellä tartuntapinta 5G-teknologian kautta, jonka seuraamukset

vaikuttavat energiajärjestelmien toiminnan jatkuvuuteen. (Basnet ja Ali 2021). Uudenlaisella sähköiseen sormenjälkeen perustuvalla Long Short-Term Memory (LSTM) -tunkeutumisenhavaitsemisjärjestelmän avulla voidaan havaita lähes sataprosenttisella havaitsemistarkkuudella salakavalat kyberhyökkäykset, jotka jäävät muuten huomaamatta valvontajärjestelmässä (Basnet ja Ali 2021).

Valvomo-ohjelmistojärjestelmien teknologinen monimutkaisuus ja kehittyneisyys ovat dramaattisesti lisääntyneet viime vuosina (Qassim et al. 2021). Erilaiset kyberverkkohyökkäykset ovat kohdistuneet näihin järjestelmiin, ja kyberhyökkäyksissä on hyödynnetty haavoituksia, joista ei ole julkista tai virallista tietoa, tai tätä tietoa ei ole organisaatiolla. Näitä haavoituksia kutsutaan nollapäivän haavoittuvuuksiksi (Qassim et al. 2021). Vaihtoehtoisesti myös kyberhyökkäykset on kohdistettu valvomo-ohjelmistojärjestelmien yhteyksissä oleviin, internetyhteydellä varustettuihin päätelaitteisiin tai tietokonejärjestelmiin (Qassim et al. 2021). Valvomo-ohjelmistojärjestelmiin kohdistuvien uhkien mallintamisella voitaisiin vaikuttaa vähentävästi katastrofaalisten seurauksien realisoitumiseen näissä järjestelmissä (Qassim et al. 2021).

Kyberhyökkäyksiä, jotka kohdistuvat vedenjakelujärjestelmiin, voidaan mallintaa Semi-Markov-prosessimallilla (SMP) (Zhang et al. 2021). Myös Monte Carlo (MCS) -simulointimallilla voidaan arvioida valvomo-ohjelmistojärjestelmien tappioita kyberhyökkäystilanteessa (Zhang et al. 2021). Kriittisissä energiajärjestelmien mikrosähköverkkoasennuksissa on välttämätöntä, että kriittiset energiaverkon kuormat pystytään ottamaan vastaan useista ennakoimattomista tilanteista huolimatta (Sarker et al. 2020). Sotilaalliselle energiajärjestelmien mikrosähköverkolle ehdotetaan tehtäväksi häiriönsietokykyanalyysia (Sarker et al. 2020). Kyberturvallisuuden arvioinnin lisäksi tutkijat (Larkin, Wagner ja Mullins 2020) tarkastelivat taloudellisia näkökohtia datadiodien hankkimiseksi teollisuusautomaatiojärjestelmiin. Taloudelliset näkökohdat huomioon ottaen datadiodien käyttäminen energiaverkon kyberturvallisuuden ensisijaisena suojakeinona ei ole taloudellisesti toteuttamiskelpoista asuinalueilla (Larkin, Wagner ja Mullins 2020). Kyberturvallisuusvakuutuksilla on mahdollisuudet ja potentiaalia kehittyä lupaavaksi rahoitusvälineeksi järjestelmäriskien hallinnassa (Zhang et al. 2021).

3 TUTKIMUSAINEISTO JA -MENETELMÄT

Tutkimusaineisto kerättiin kyselytutkimuksen avulla Suomen energia-alan toimijoilta. Kyselytutkimuksessa käytettiin Likert-asteikkoa, jota käytetään yleisesti asenne- ja motivaatiomittareissa (Likert 1932). Yleensä asteikko jakaantuu täysin eri mieltä – täysin samaa mieltä -tyyliselle vastakkainasettelulle. Tutkittavat pisteyttävät oman käsityksensä kysymyksen tai väitteen sisällöstä. Kyseinen asteikko yhdistää laadullisia sekä määrällisiä elementtejä (Metsämuuronen 2006). Tässä kyselytutkimuksessa Likert-asteikko vaihteli 1 (= täysin eri mieltä), 2 (= jokseenkin eri mieltä), 3 (= ei samaa eikä eri mieltä), 4 (= jokseenkin samaa mieltä) ja 5 (= täysin samaa mieltä) välillä.

Suomen energia-alan kyberturvallisuuden tutkimiseen soveltuvaa valmista kyselylomaketta ei löytynyt tehdyn kirjallisuuskatsauksen perusteella. Näin ollen tässä kyselytutkimuksessa käytetyt väittämäkysymykset pohjautuvat osittain edellisen turvallisuuskyselyn väittämiin (Paasonen 2021) ja Suomen Kauppakamarin tekemään rikosturvallisuuden kyselyyn suomalaisille yrityksille (Vesterinen 2020) sekä Utahin osavaltion kyberturvallisuustarkistuslistaan (Utahin osavaltio 2021). Väittämäkysymyksien lisäksi kyselylomake sisälsi avoimia kysymyksiä. Laadulliset avoimet kysymykset tuovat analyysiin mukaan sellaista tutkimustietoa, jota pelkästään valmiita vastausvaihtoehtoja sisältävillä väittämillä ei ole mahdollista saada (Hirsjärvi ja Helena 2008). Avoimissa kysymyksissä tiedusteltiin vastaajilta kyberturvallisuuden kehittämisalueita omassa organisaatiossa sekä mitä koulutusta sekä harjoitusta vastaajat tarvitsivat kyberturvallisuudesta ja riskienhallinnasta.

Kyselytutkimuksesta tiedotettiin Suomen energia-alan toimijoille laajana sähköisenä vastauspyyntönä. Tätä vastauspyyntöä välitettiin eteenpäin Suomen energia-alan toimijoille, joita on Suomessa 176. Vastauksia saimme 30. Verkkopohjaisen kyselyn vastausaika oli aikavälillä 11.6.–30.6.2021. Suomen energia-alan toimijat haettiin Energiateollisuuden yhdistyksen julkisesta jäsenluettelosta (Energiateollisuus ry, 2021). Syytä vastaajakatoon ei voitu selvittää.

Verkkokyselyihin liittyvää "vastauskäyttäytymistä" ja -prosentteja on tutkittu aiemmin. Vaikka verkkokyselyllä voidaan tavoittaa iso joukko ihmisiä (Couper 2000, s. 464–465), niin kyselyiden massiivinen määrä luo ongelman, että ihmiset eivät viitsi vasta niihin. Kyselyiden isoa määrää pidetään yhtenä syynä, josta vastaamatta jättäminen voi aiheutua (Couper 2000), (Evans ja Mathur 2005), (Baruch and Holtom 2008), sillä organisaatioille tyypillinen suuri vastaamattomuusaste otantatutkimuksissa luo mahdollisuuden suuriin tilastollisiin vääristymiin lopullisessa otoksessa (Tomaskovic-Devey, Leiter ja Thompson 1994, s. 439). Cook, Heath ja Thompson (2000) ovat kuitenkin korostaneet, että "kyselytutkimuksen otoksen edustavuus on tärkeämpi kuin vastausprosentti". Tilastollisen vääristymän havainnoimiseksi ja otoksen edustavuuden varmistamiseksi ei voida tehdä vertailua, koska sellaista aikaisempaa tutkimusta ei ole, joka sopisi tämän kyselyn tuloksien

vertailuun. Suomen energia-alan kyberturvallisuuden tutkimuksen ongelma on, että toimialasta ei ole saatavilla tarkkoja tilastotietoja sen suhteen, että miten alan toimijat ovat käytännössä toteuttaneet kyberturvallisuutensa.

Vastaajista kaksi oli naisia ja loput 28 vastaajaa olivat miehiä (Taulukko 1). Ylemmän korkeakoulututkinnon oli suorittanut 14 ja alemman 12 henkilöä. Yksi vastaajista ilmoitti opiskelleensa erikseen alemman ja ylemmän korkeakoulututkinnon. Kaksi vastaajista kertoi opiskelleensa ammatillisen perustutkinnon, sekä yksi vastaajista kertoi opiskelleensa tieteellisiä jatko-opintoja yliopistossa.

Vastaajista 33 prosentilla oli keskimääräisesti 4–10 vuotta työkokemusta energia-alalta. Vastaajista noin 43 prosenttia työskentelee johtajan tehtävissä, 26 prosenttia vastaajista on työssä esimiestehtävissä ja saman verran asiantuntijatehtävissä sekä yksi vastaajista ilmoitti erikseen työskentelevänsä päällikön tehtävässä.

Vastaajien energia-alan organisaatioiden toiminnot jakaantuivat maantieteellisesti eniten kahteen maakuntaan, Uudellemaalle ja Pirkanmaalle. Näissä maakunnissa ilmoitetaan olevan kahdeksan kappaletta energia-alan toimijoiden toimintoja. Pohjanmaalle ilmoitetaan olevan toimintoja kuusi kappaletta, eli toiseksi eniten. Moodimittauksen perusteella neljällä maakunnalla on kaksi energia-alan toimijan toimintoa sijoitettuna.

Taulukko 1. Vastaajien taustatiedot (N=30).

Muuttuja	**Luokka**	**prosenttia**	**N**
Sukupuoli	Mies	94	28
	Nainen	7	2
Ikä	18–25 vuotta	0	0
	26–35 vuotta	10	3
	36–49 vuotta	57	17
	Yli 50 vuotta	33	10
Toimenkuva	Asiantuntija	27	8
	Esimies	27	8
	Johtaja	43	13
	Muu: Päällikkö	3	1
Alan työkokemus	0–3 vuotta	7	2
	4–10 vuotta	33	10
	11–20 vuotta	27	8
	Yli 20 vuotta	33	10
Alan koulutus	ammatillinen perustutkinto	7	2
	alempi korkeakoulututkinto	40	12

Muuttuja	Luokka	prosenttia	N
	ylempi korkeakoulututkinto	47	14
	alempi ja ylempikorkeakoulututkinto	3	1
	jatko-opinnot (lisensiaatti/tohtori)	3	1

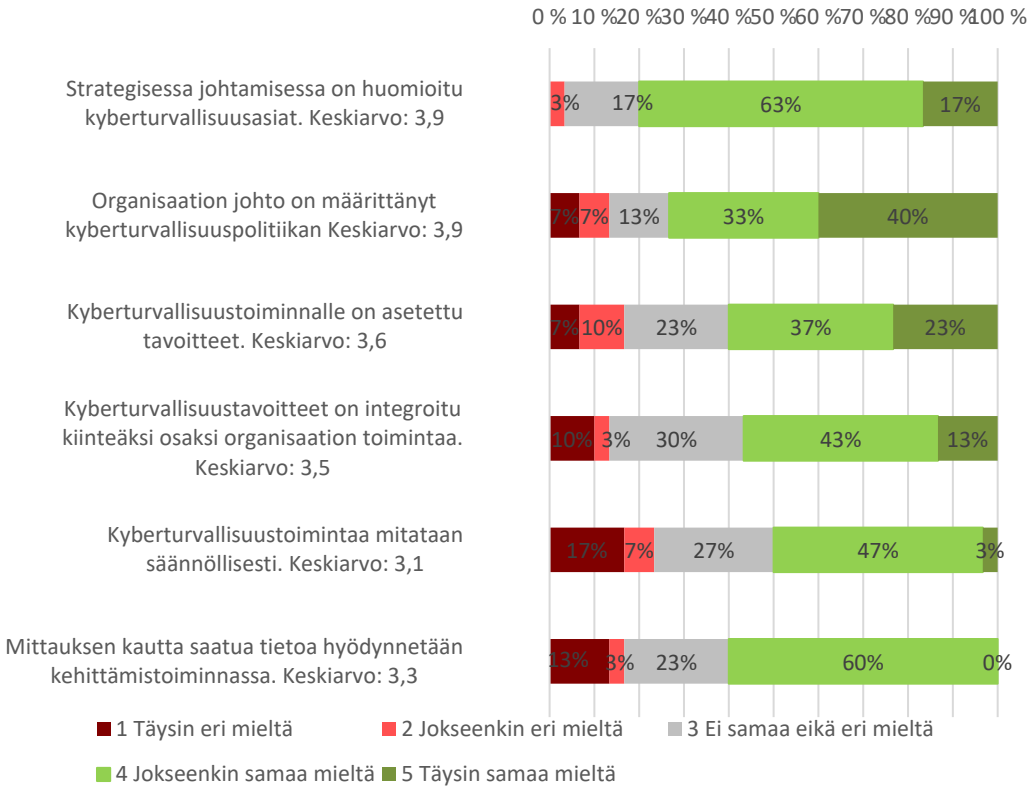
Kuusi vastaajaa antoi avoimeen kysymykseen vastauksen koulutuksestansa. Heillä oli suoritettuna kursseja kyberturvallisuudesta ja turvallisuudesta. Nämä koulutukset oli suoritettu joko suomalaisessa yliopistossa, suomalaisessa ammattikorkeakoulussa tai ammatillisessa oppilaitoksessa. Myös yrityksen omia sisäisiä koulutuksia oli suoritettuna ja muita koulutuksia.

Ensimmäiseksi tulosten raportoinnissa tarkastellaan väittämäkysymysten tuloksia. Väittämäkysymysten vastausjakaumat on esitetty kuvioissa 1–18, ja väitteiden tulokset avataan jokaisen kuvion kohdalta erikseen. Avoimet vastaukset puolestaan analysoitiin laadullisella tutkimusmenetelmällä. Yksittäisten kysymysten havaintoja analysoitiin kvantifioimalla ja teemoittelemalla. Laadullisen aineiston analyysin tarkoituksena on luoda aineistoon selkeyttä ja tuottaa tietoa tutkimuksen kohteesta. Kvantifioinnilla tarkoitetaan mainintojen määrän laskemista, kun teemoitetulla puolestaan tarkoitetaan aineiston järjestämistä tiettyjen näkökulmien mukaisesti. (Eskola ja Suoranta 1998).

Avoimiin kysymyksiin oli vastattu monipuolisesti, joten niihin annetut vastaukset tukivat väittämäkysymysten vastauksia. Vastaajien vastauksia ei esitetä suorina lainauksina vaan heidän vastauksiansa mukaillen. Tämän myötä voidaan todeta kyselyn soveltuvan tutkimuskysymyksien analysoimiseen. Validiteettia ja reliabiliteettia voidaan siten pitää hyvänä (Heinonen, Keinänen, ja Paasonen 2013).

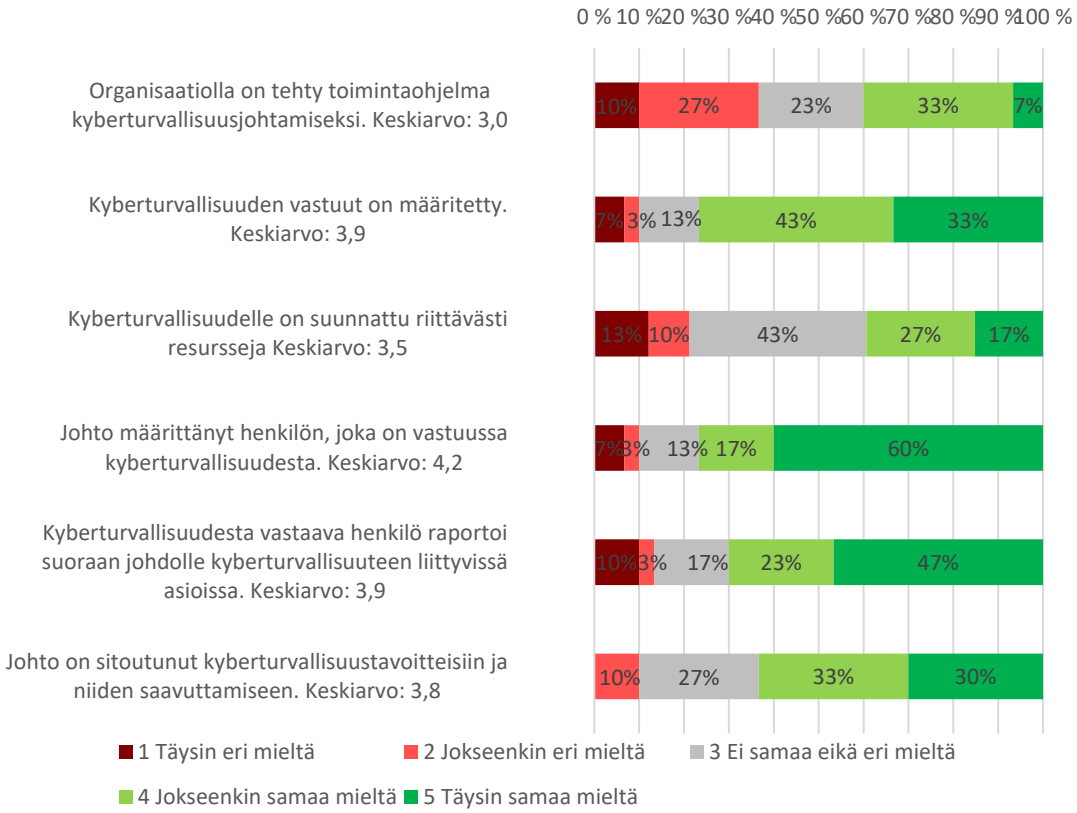
4 TULOKSET

Vastaajista 80 prosenttia koki, että kyberturvallisuusjohtaminen on huomioitu organisaation strategisessa johtamisessa (kuvio 1). Vastaajista 73 prosenttia koki, että organisaation johto olisi heidän mukaansa määritellyt organisaatiossa kyberturvallisuuspolitiikan. Vastaajista 60 prosenttia koki, että kyberturvallisuustoiminnalle olisi määritelty tavoitteet. Vähän yli puolet, eli 56 prosenttia vastaajista koki, että kyberturvallisuustavoitteet oli integroitu osaksi organisaation toimintaa. Vastaajista puolet koki, että kyberturvallisuustoimintaa mitataan riittävästi heidän organisaatiossaan. Vastaajista 60 prosenttia koki, että kyberturvallisuusmittauksen tuloksia hyödynnetään riittävästi organisaation toiminnan kehittämisessä.



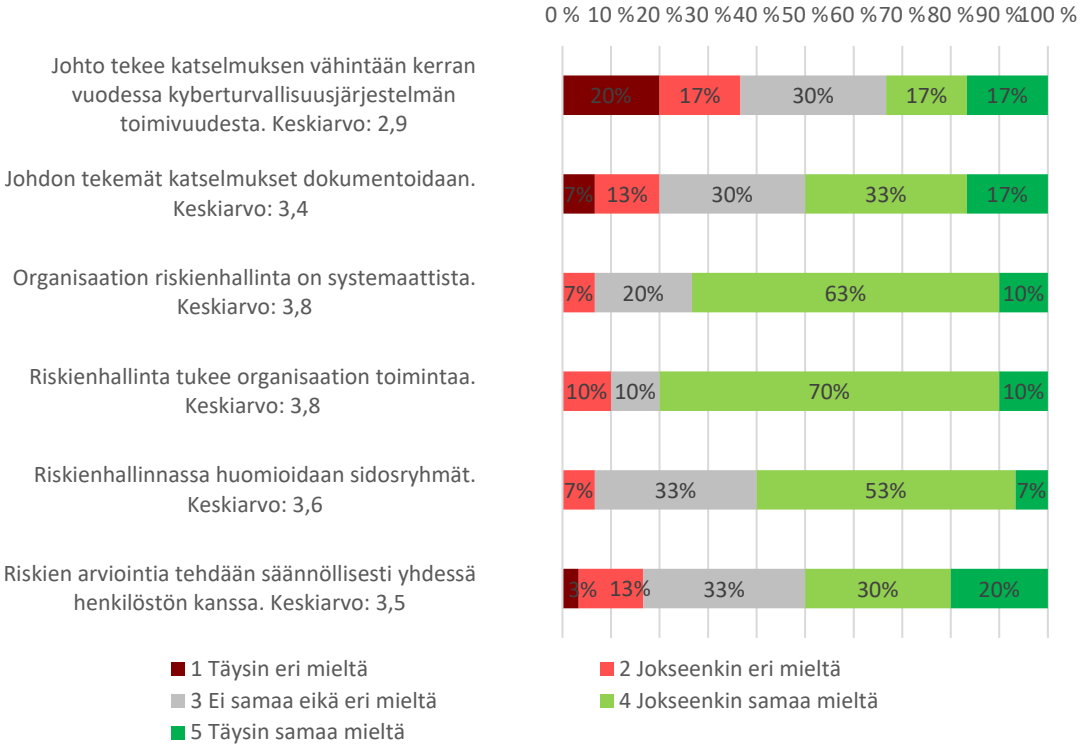
Kuvio 1. Kyberturvallisuusjohtaminen 1.

Vastaajista vain 40 prosenttia koki, että organisaatiolla on tehty toimintaohjelma kyberturvallisuuden johtamiseen (kuvio 2). Vastaajista 76 prosenttia koki, että kyberturvallisuuden vastuut on määritelty organisaatiossa. Vastaajista 43 prosenttia ei osannut arvioida, että onko heidän organisaatiollansa kyberturvallisuudelle suunnattu riittävästi resursseja. Vastaajista 23 prosenttia ei kokenut, että heidän organisaatiollansa olisi resursseja riittävästi suunnattu kyberturvallisuudelle ja 44 prosenttia katsoi, että kyberturvallisuudella on annettu riittävästi resursseja heidän organisaatiossaan. Vastaajista 77 prosenttia ei kokenut, että organisaation johto on määritellyt kyberturvallisuudesta vastaavan henkilön organisaatioon. Vastaajista 70 prosenttia koki, että organisaation kyberturvallisuuden vastuuhenkilö raportoi kyberturvallisuusasioista organisaation johdolle. Vastaajista 63 prosenttia koki, että organisaationsa johto on sitoutunut kyberturvallisuuden tavoitteisiin sekä niiden saavuttamiseen.



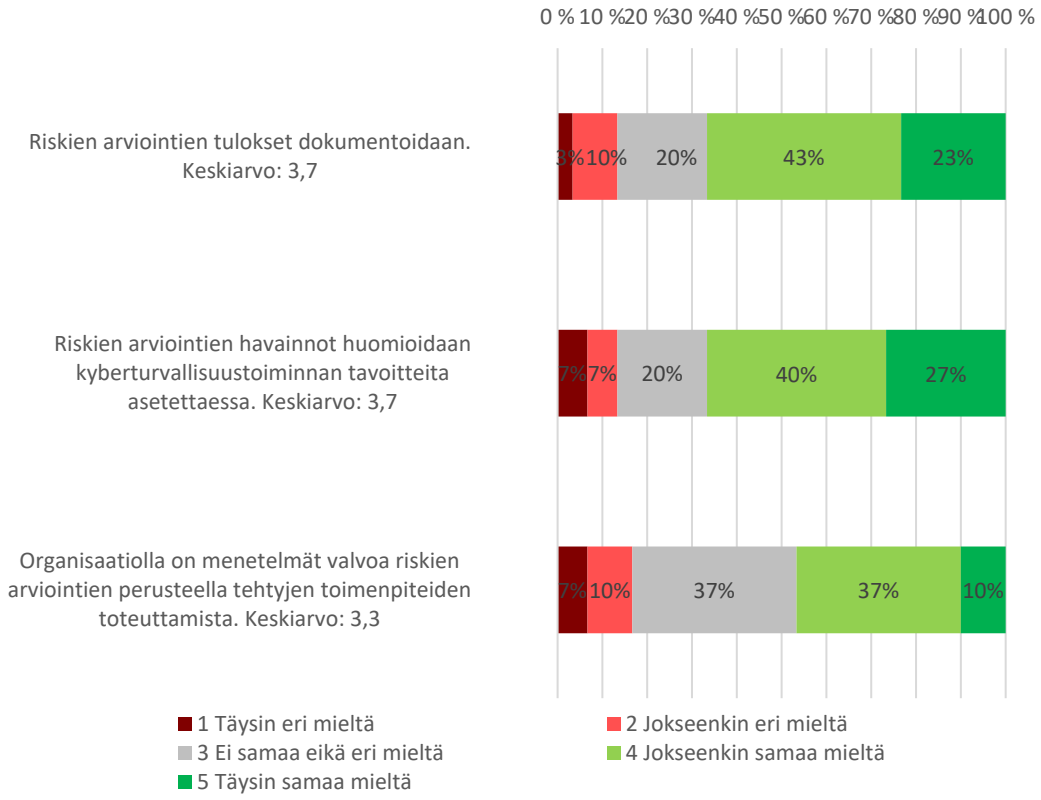
Kuvio 2. Kyberturvallisuusjohtaminen 2.

Vastaajista 30 prosenttia ei osannut arvioida, että tehdäänkö organisaatiossa johtohenkilöstön osalta katselmuksia vähintään kerran vuodessa kyberturvallisuusjärjestelmiin, kun taas 34 prosenttia vastaajista arvioi, että katselmuksia olisi tehty kerran vuodessa johdon toimesta organisaatiossa sekä 37 prosenttia, että niitä ei heillä tehdä laisinkaan (kuvio 3). Vastaajista puolet koki, että johdon katselmukset dokumentoidaan, mutta 30 prosenttia ei ollut samaa eikä eri mieltä. Kaksikymmentä prosenttia näki, että organisaatiossa ei dokumentoida johdon katselmuksia laisinkaan. Vastaajista 73 prosenttia katsoi, että organisaation riskienhallinta on systemaattista. 80 prosenttia näki, että riskienhallinta tukee organisaation toimintaa. Vastaajista 60 prosenttia oli sitä mieltä, että organisaation riskienhallinnassa huomioidaan sidosryhmät. Vastaajista 33 prosenttia ei osannut arvioida, että tehdäänkö riskien arviointia säännöllisesti yhdessä henkilöstön kanssa, mutta 50 prosenttia vastaajista katsoi, että riskien arviointia tehdään säännöllisesti yhdessä henkilöstön kanssa ja 19 prosenttia koki, että sitä ei tehdä laisinkaan Vastaajista 53 prosenttia koki, että organisaatiossa huomioidaan sidosryhmät riskienarvioimisessa. Vastaajista puolet koki, että henkilöstö osallistuu säännöllisesti riskienhallinnan tekemiselle. On siis todettava, että kyberturvallisuusjohtaminen koetaan hoidetuksi yli puolessa organisaatioista.



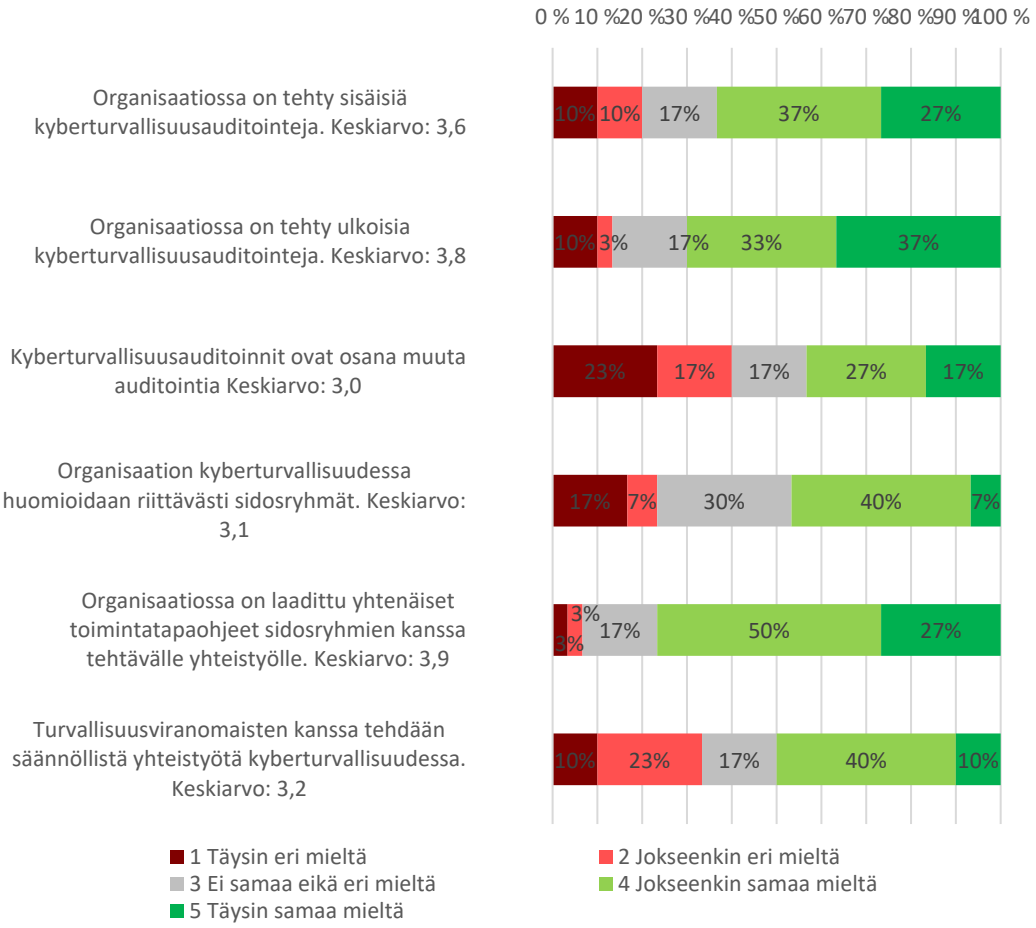
Kuvio 3. Kyberturvallisuusjohtaminen 3.

Vastaajista 66 prosenttia koki, että riskien arviointien tulokset dokumentoidaan organisaatiossa (kuvio 4). Vastaajista 67 prosenttia koki, että riskien arviointien havainnot huomioidaan kyberturvallisuustoiminnan tavoitteita asettaessa. Vastaajista 37 prosenttia ei osannut arvioida ja 37 prosenttia oli jokseenkin samaa mieltä, että organisaatiolla on menetelmät valvoa riskien arviointien perusteella tehtyjen toimenpiteiden toteutumista. 47 prosenttia vastaajista koki, että se toiminto on organisaatiossa ja vastaajista 17 prosenttia koki, että toimenpiteiden toteutumista ei arvioida laisinkaan organisaatiossa. Vastaajat kokevat, että kyberriskienhallinta on suurimmilta osin toteutettu heidän organisaatiossaan, mutta noin alle kolmasosa vastaajista koki heidän organisaationsa riskienhallinnan toimenpiteiden toteutuksessa olevan parannettavaa. Lisäksi kahdeksan viidesosaa vastaajista ei osannut arvioida, että onko riskienhallinnan toimenpiteitä toteutettu heidän organisaatiossaan.



Kuvio 4. Kyberriskienhallinta.

Vastaajista 64 prosenttia koki, että organisaatiossa on tehty sisäisiä kyberturvallisuusauditointeja (kuvio 5). Vastaajista 70 prosenttia koki, että organisaatiossa on tehty ulkoisia kyberturvallisuusauditointeja. Vastaajista 44 prosenttia koki, että kyberturvallisuusauditoinnit on toteutettu osana muuta auditointia organisaatiossa. Vastaajista 47 prosenttia koki, että heidän organisaationsa kyberturvallisuudessa huomioidaan riittävästi sidosryhmät. Vastaajista 77 prosenttia koki, että organisaatiossa on laadittu yhtenäiset toimintatapaohjeet sidosryhmien kanssa tehtävälle yhteistyölle. Vastaajista 50 prosenttia koki, että organisaatiossa tehdään turvallisuusviranomaisten kanssa säännöllistä yhteistyötä kyberturvallisuudessa. Voidaan siis päätellä, että kyberturvallisuusauditoinnit koetaan tehdyksi suurimmassa osassa organisaatioita.



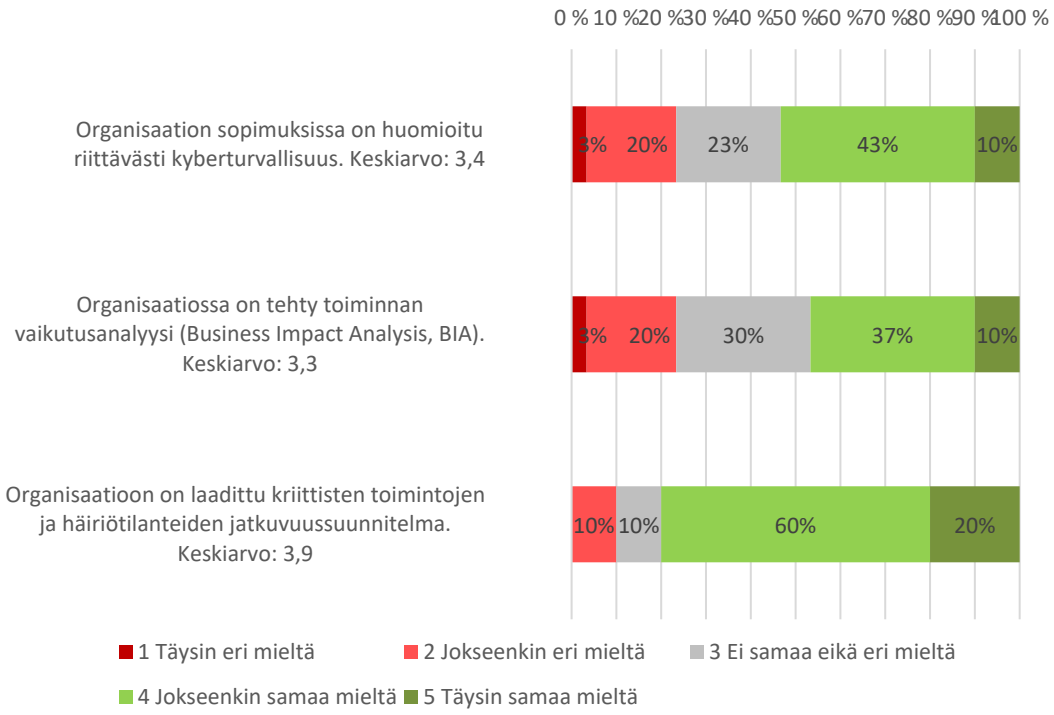
Kuvio 5. Kyberturvallisuusauditoinnit.

Avoimessa kysymyksessä kysyttiin vastaajilta, mitä riskienarviointimenetelmiä vastaajien organisaatioissa käytetään. Vastauksissa tuotiin esille erilaisia riskienarviointimenetelmiä. Ne ovat Event-Based Risk Management (EBRM), avainhenkilöiden haastattelu, kvalitatiivinen riskimatriisiarviointi, SWOT-analyysi, PESTEL-arviointimenetelmä, vaikutusanalyysi, laatujärjestelmä, tietoturvakonsulttien konsultointi, auditoinnit, NIST Cyber risk management framework ja vuosittainen arviointi kyberturvallisuusriskeistä. Kyselyyn

vastanneiden organisaatioiden riskienarviointimenetelmät eivät ole yhdenmukaisia, ja vastaajien organisaatiot käyttävät erilaisia riskienarviointimenetelmiä kyberturvallisuuden riskeihin.

Avoimessa kysymyksessä kysyttiin vastaajilta, mitä turvallisuusauditointikriteeristöjä käytetään organisaatioissa. Vastauksissa tuotiin esille erilaisia auditointikriteeristöjä (esim. CIS20, ISO 27001, KATAKRI, OSI/IEC 27001). Vastanneiden organisaatioiden turvallisuuskriteeristöt eivät siis ole yhdenmukaisia. Tästä voidaan päätellä, että kyberturvallisuusauditointikriteeristöjä ei ole harmonisoitu vastanneissa organisaatioissa.

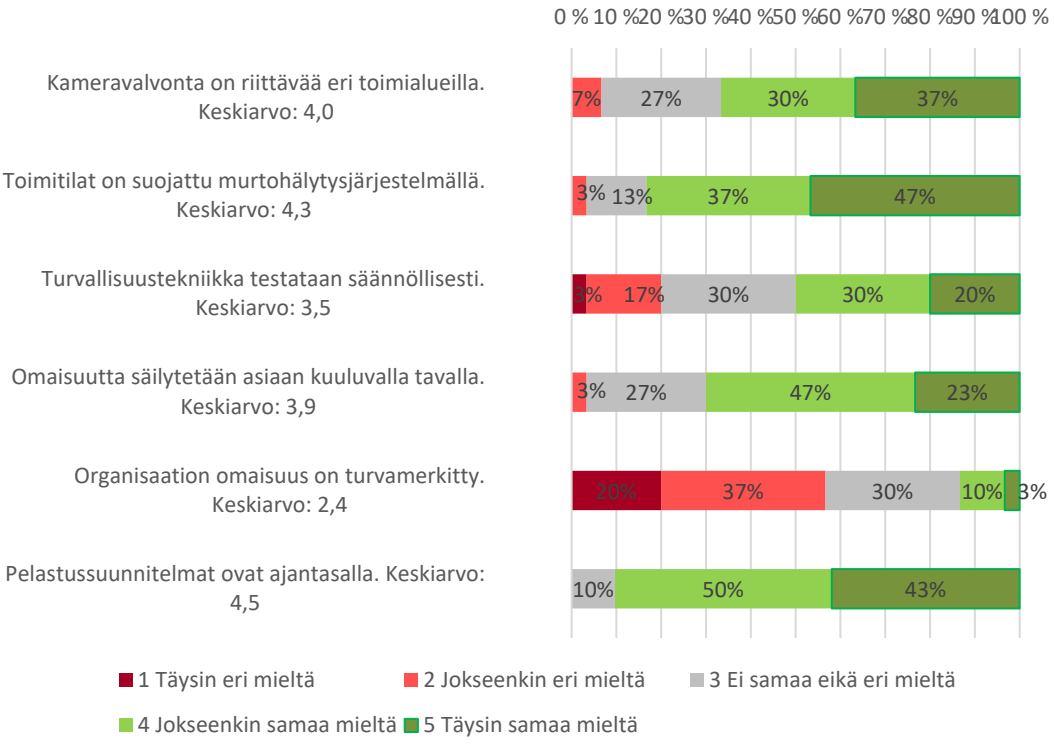
Vastaajista 53 prosenttia koki, että organisaation sopimuksissa on huomioitu riittävästi kybertuvallisuus ja 23 prosenttia koki, että kyberturvallisuutta ei huomioida organisaation sopimuksissa (kuvio 6). Vastaajista 47 prosenttia koki, että organisaatiossa on tehty toiminnan vaikutusanalyyseja ja 30 prosenttia ei osannut arvioida, että onko vaikutusanalyyseja tehty heidän organisaatiossaan. Vastaajista 80 prosenttia koki, että organisaatiossa on laadittu kriittisten toimintojen osalta jatkuvuussuunnitelma ja myös häiriötilanteista oli laadittu jatkuvuussuunnitelma.



Kuvio 6. Toimitilaturvallisuus 1.

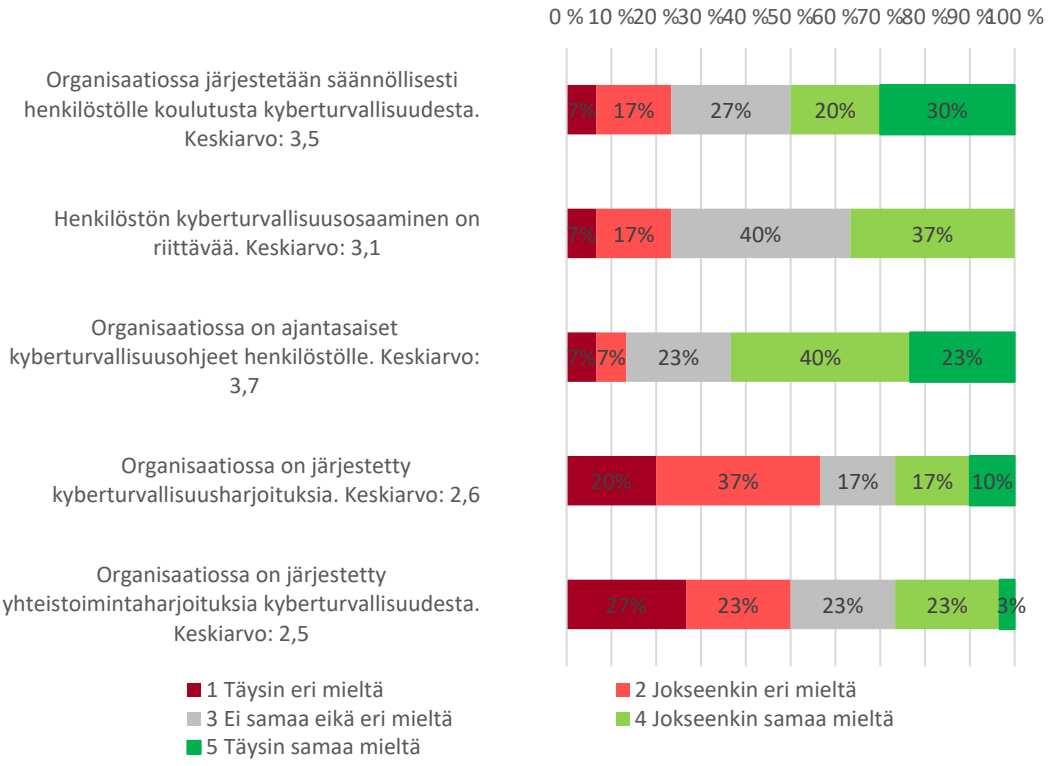
Vastaajista 67 prosenttia koki, että kameravalvonta on riittävä eri toimialueilla organisaatiossa (kuvio 7). Vastaajista 84 prosenttia koki, että toimitilat on suojattu murtohälytysjärjestelmillä organisaatiossa. Vastaajista 30 prosenttia ei osannut arvioida, että testataanko turvallisuustekniikkaa säännöllisesti heidän organisaatiossaan. Vastaajista 20

prosenttia koki, että turvallisuustekniikkaa ei testata säännöllisesti heidän organisaatiossaan, mutta 50 prosenttia oli kuitenkin sitä mieltä, että turvallisuustekniikkaa testataan säännöllisesti heidän organisaatiossaan. Vastaajista 70 prosenttia koki, että organisaation omaisuutta säilytetään asiaan kuuluvilla tavoilla. Vastaajista 57 prosenttia koki, että organisaation omaisuus ei ole turvamerkitty, ja vastaajista 30 prosenttia ei osannut arvioida, että onko organisaation omaisuutta turvamerkitty sekä vastaajista 13 prosenttia koki, että organisaation omaisuutta on turvamerkitty. Vastaajista 93 prosenttia koki, että organisaation pelastussuunnitelmat ovat ajan tasalla, ja 10 prosenttia ei osannut arvioida, että ovatko pelastussuunnitelmat ajan tasalla heidän organisaatiossaan. Suurin osa vastaajista siis kokee, että toimitilaturvallisuus on teknisesti ja teknillisen ylläpidon osalta hoidettu vastaajien organisaatiossa. Vastaajista 57 prosenttia koki omaisuuden turvamerkitsemisessä puutteita organisaatiossaan.



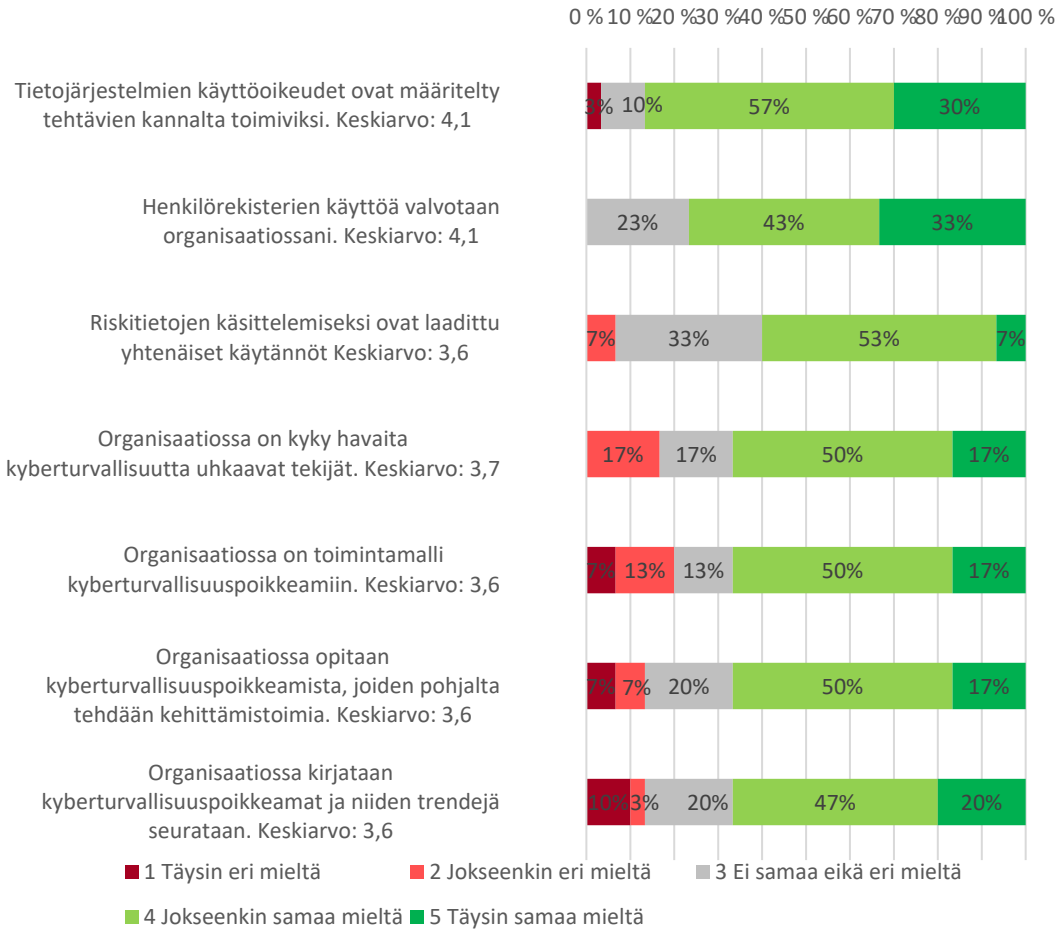
Kuvio 7. Toimitilaturvallisuus 2.

Vastaajista 30 prosenttia oli täysin samaa mieltä, että organisaatiossa järjestetään säännöllisesti henkilöstölle koulutusta kyberturvallisuudesta (kuvio 8). Vastaajista 40 prosenttia ei osannut arvioida, että onko heidän organisaatiossaan henkilöstön kyberturvallisuusosaaminen riittävää. Vastaajista 63 prosenttia koki, että organisaatiossa on ajantasaiset kyberturvallisuusohjeet henkilöstölle. Vastaajista 57 prosenttia koki, että heidän organisaatiossaan ei ole järjestetty kyberturvallisuusharjoituksia. Vastaajista 50 prosenttia koki, että heidän organisaatiossaan ei ole järjestetty yhteistoimintaharjoituksia kyberturvallisuudesta. Vastaajien mielestä organisaatioiden kyberturvallisuusosaamisessa on siis puutteita, kun ei osata arvioida, että millä tasolla kyberturvallisuus on organisaatiossa. Myös noin yli puolet vastaajista on sitä mieltä, että kyberturvallisuusharjoituksia ei ole järjestetty organisaatioissa sisäisesti eikä myöskään järjestetty yhteiskyberturvallisuusharjoituksia. Vain pieni osa vastaajista on sitä mieltä, että kyberturvallisuusharjoituksia on järjestetty, joka on siis noin parikymmentä prosenttia vastaajista.



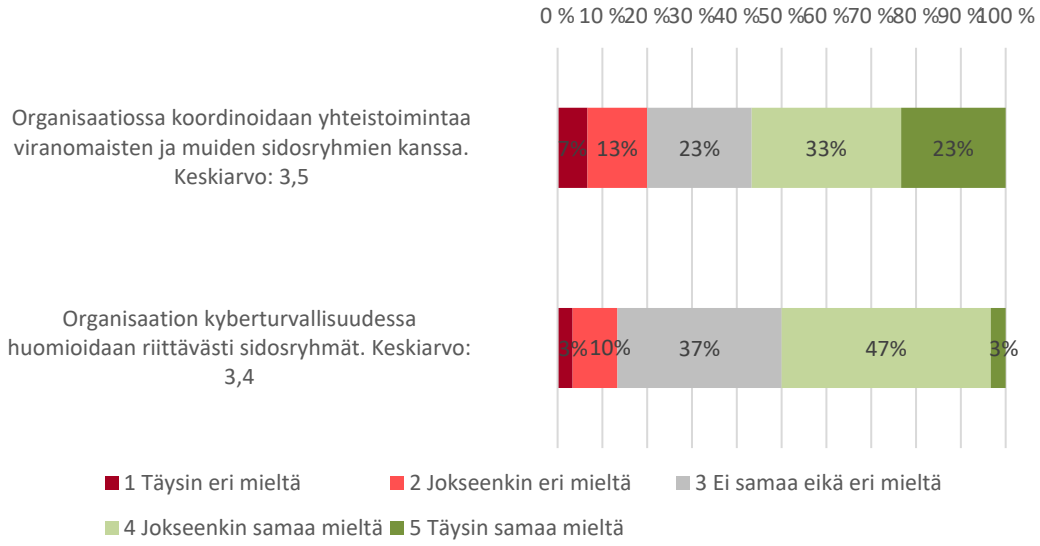
Kuvio 8. Henkilöstön kyberturvallisuusosaaminen.

Vastaajista 87 prosenttia koki, että tietojärjestelmien käyttöoikeudet on määritelty tehtävien kannalta toimiviksi heidän organisaatiossaan (kuvio 9). Vastaajista 76 prosenttia koki, että henkilörekisterien käyttöä valvotaan heidän organisaatiossaan. Vastaajista 60 prosentin mielestä riskitietojen käsittelemiseksi on laadittu yhtenäiset käytännöt heidän organisaatiossaan. Vastaajista 67 prosenttia koki, että organisaatiolla on kyky havaita kyberturvallisuutta uhkaavat tekijät. Sama osuus, eli 67 prosenttia vastaajista 67 koki, että heidän organisaatiossaan on toimintamalli kyberturvallisuuspoikkeamien käsittelyyn. Vastaajista myös 67 prosenttia koki, että heidän organisaatiossaan opitaan kyberturvallisuuden poikkeamista, ja niiden pohjalta tehdään kehittämistoimia heidän organisaatiossaan. Lisäksi vastaajista 67 prosenttia katsoi, että heidän organisaatiossaan kirjataan kyberturvallisuuspoikkeamat ja niiden trendejä seurataan heidän organisaatiossaan. Vastaajien mielestä kyberturvallisuuspoikkeaminen hallinta näyttäisi olevan toteutettu yli puolessa vastaajien organisaatioissa.



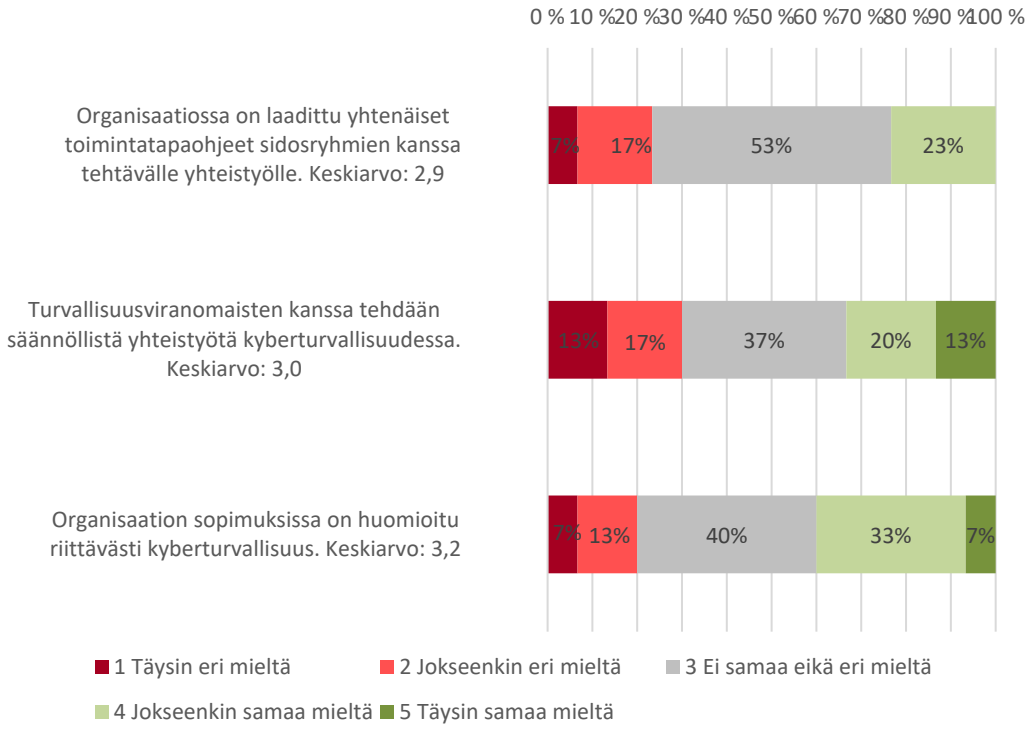
Kuvio 9. Kyberrikostorjunta ja poikkeamien hallinta.

Vastaajista 56 prosenttia koki, että heidän organisaatiossaan koordinoidaan yhteistoimintaa viranomaisten ja muiden sidosryhmien kanssa (kuvio 10). Vastaajista 50 prosenttia koki, että heidän organisaatiossaan kyberturvallisuudessa huomioidaan riittävästi sidosryhmät. Vastaajista 37 prosenttia ei osannut arvioida, että miten heidän organisaatiossaan kyberturvallisuudessa huomioidaan sidosryhmät. Lisäksi vastaajista 13 prosenttia oli eri mieltä siitä, että heidän organisaatiossaan kyberturvallisuudessa huomioitaisiin sidosryhmät.



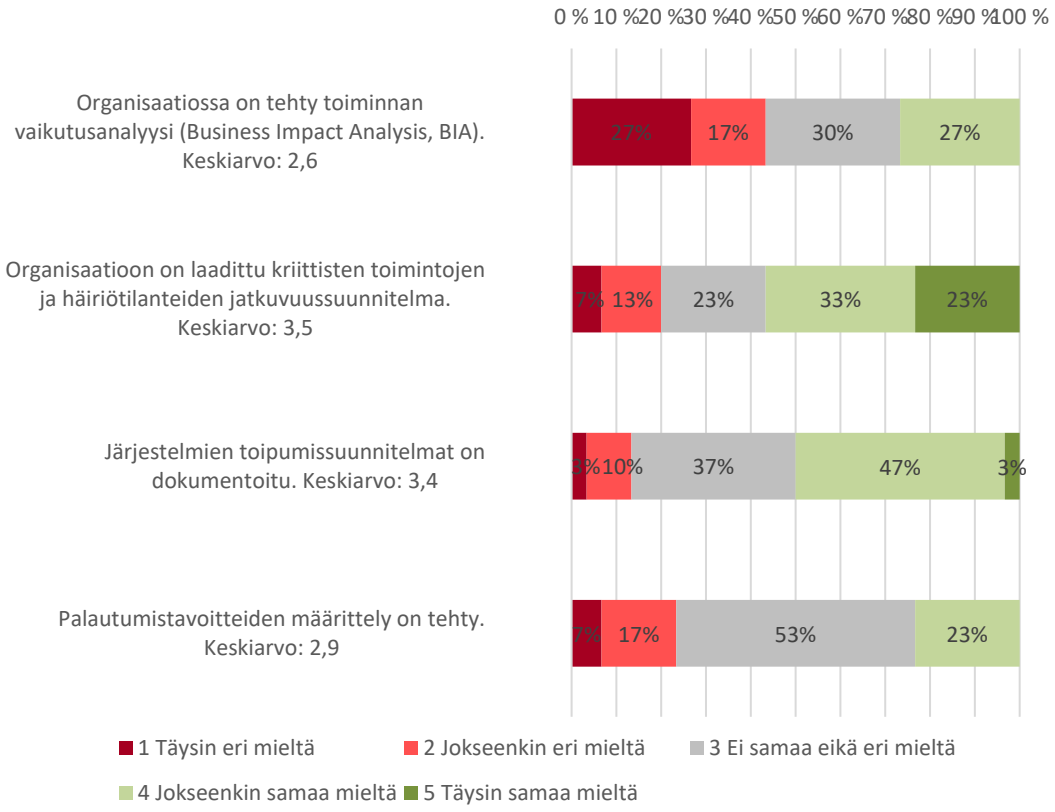
Kuvio 10. Viranomais- ja sidosryhmäyhteistyö 1.

Vastaajista 53 prosenttia ei osannut arvioida, että onko heidän organisaationsa laadittu yhtenäiset toimintatapaohjeet sidosryhmien kanssa toteutettavalle yhteistyölle, mutta 23 prosenttia koki, että ohjeet oli laadittu sidosryhmien kanssa tapahtuvalle yhteistyölle organisaatiossa ja 24 prosenttia koki, että niitä ei ollut laadittu (kuvio 11). Vastaajista 37 prosenttia ei osannut arvioida, että tehdäänkö heidän organisaatiossaan turvallisuusviranomaisten kanssa säännöllistä yhteistyötä kyberturvallisuudessa. Vastaajista 33 prosenttia oli sitä mieltä, että kyberturvallisuuden osalta tehdään säännöllistä yhteistyötä turvallisuusviranomaisten kanssa, mutta 30 prosenttia mielestä tätä yhteistyötä ei säännöllisesti toteuteta heidän organisaationsa. Vastaajista 40 prosenttia ei osannut arvioida, että onko heidän organisaationsa sopimuksissa huomioitu riittävästi kyberturvallisuus, mutta vastaajista 40 prosenttia koki, että heidän organisaationsa sopimuksissa on riittävästi huomioitu kyberturvallisuus. Vastaajista 20 prosenttia oli eri mieltä siitä, että heidän organisaationsa sopimuksissa olisi riittävästi huomioitu kyberturvallisuutta.



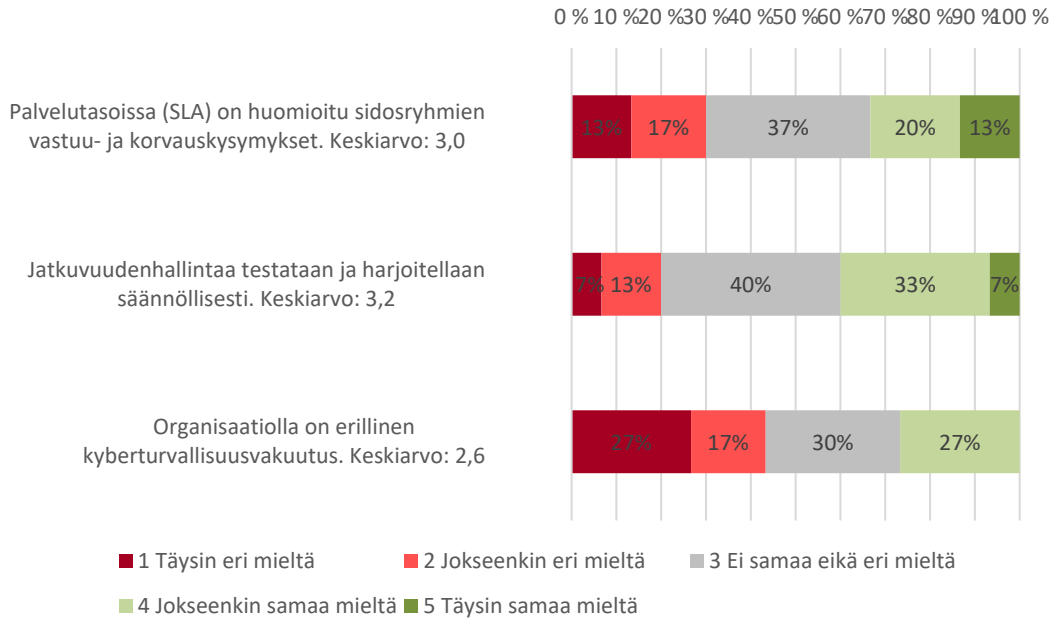
Kuvio 11. Viranomais- ja sidosryhmäyhteistyö 2.

Vastaajista 30 prosenttia ei osannut arvioida, että onko heidän organisaatiossaan tehty toiminnan vaikuttavuusanalyyseja (kuvio 12). Vastaajista 44 prosenttia koki, että organisaatiossa ei ole tehty vaikuttavuusanalyyseja. Vastaajista 56 prosenttia koki, että heidän organisaatiossaan on laadittu kriittisten toimintojen ja häiriötilanteiden jatkuvuussuunnitelma. Vastaajista 37 prosenttia ei osannut arvioida, että onko heidän organisaationsa järjestelmien toipumissuunnitelmat dokumentoitu, mutta vastaajista 50 prosenttia koki, että toipumissuunnitelmat oli dokumentoitu heidän organisaatiossaan. Vastaajista 53 prosenttia ei osannut arvioida, että onko heidän organisaatiossaan määritelty palautumistavoitteet. Vastaajista 24 prosenttia oli eri mieltä ja katsoi, että heidän organisaatiossaan ei ole määrittely palautumistavoitteita. Vastaajista 23 prosenttia koki, että heidän organisaatiossaan on määritelty palautumistavoitteet.



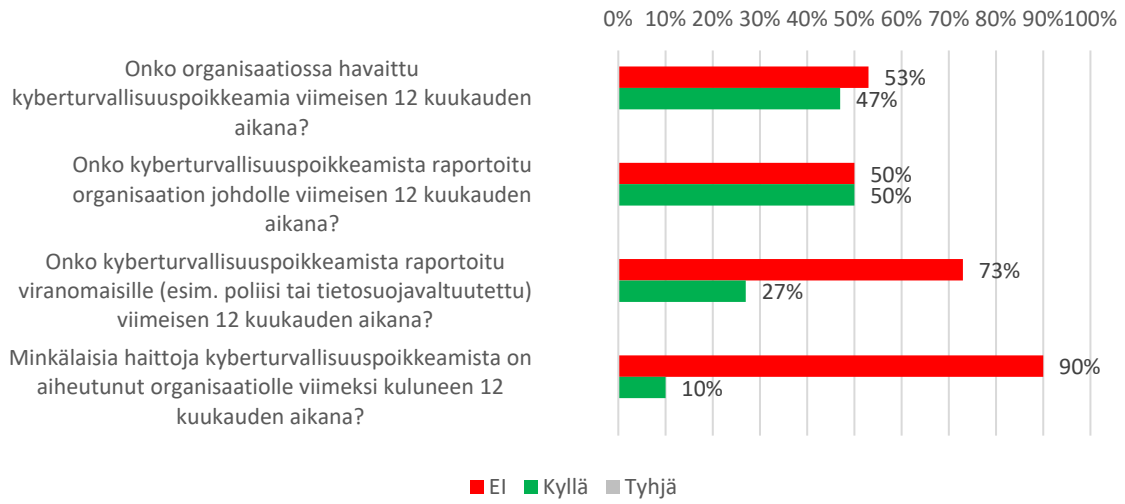
Kuvio 12. Jatkuvuudenhallinta 1.

Vastaajista 37 prosenttia ei osannut arvioida, että onko heidän organisaationsa palvelutasoissa (SLA) huomioitu sidosryhmien vastuu- ja korvauskysymykset. Vastaajista 33 prosenttia koki, heidän organisaatiossaan on huomioitu palvelutasoissa sidosryhmien vastuu- ja korvauskysymykset (kuvio 13). Vastaajista 30 prosenttia oli eri mieltä ja katsoi, että heidän organisaatiossaan ei ole huomioitu palvelutasoissa sidosryhmien vastuu- ja korvauskysymyksiä. Vastaajista 40 prosenttia ei osannut arvioida, että testataanko heidän organisaatiossaan säännöllisesti jatkuvuuden hallintaa ja harjoitellaanko säännöllisesti jatkuvuudenhallintaa. Vastaavasti vastaajista 40 prosenttia koki, että heidän organisaatiossaan testataan säännöllisesti jatkuvuuden hallintaa ja myös harjoitellaan säännöllisesti jatkuvuudenhallintaa. Vastaajista 20 prosenttia oli eri mieltä ja katsoi, että heidän organisaatiossaan ei testata säännöllisesti jatkuvuuden hallintaa eikä myöskään harjoitella säännöllisesti jatkuvuudenhallintaa. Vastaajista 30 prosenttia ei osannut arvioida, että onko heidän organisaatiossaan erillinen kyberturvallisuusvakuutus, vastaajista 44 prosenttia oli eri mieltä ja katsoi, että heidän organisaatiollaan ei ole erillistä kyberturvallisuusvakuutusta ja vastaajista 27 prosenttia koki, että heidän organisaatiollaan on erillinen kyberturvallisuusvakuutus. Vastaajista noin kolmasosa ei tiedä, miten jatkuvuushallinta ja sen toteutus on tehty heillä sekä vastaavasti noin kolmasosa on sitä mieltä, että heillä on jatkuvuuden hallintaa ja sitä on toteutettu. Lisäksi loput, eli noin kolmasosa vastaajista on sitä mieltä, että heillä ei ole jatkuvuuden hallintaa eikä sitä ole toteutettu.



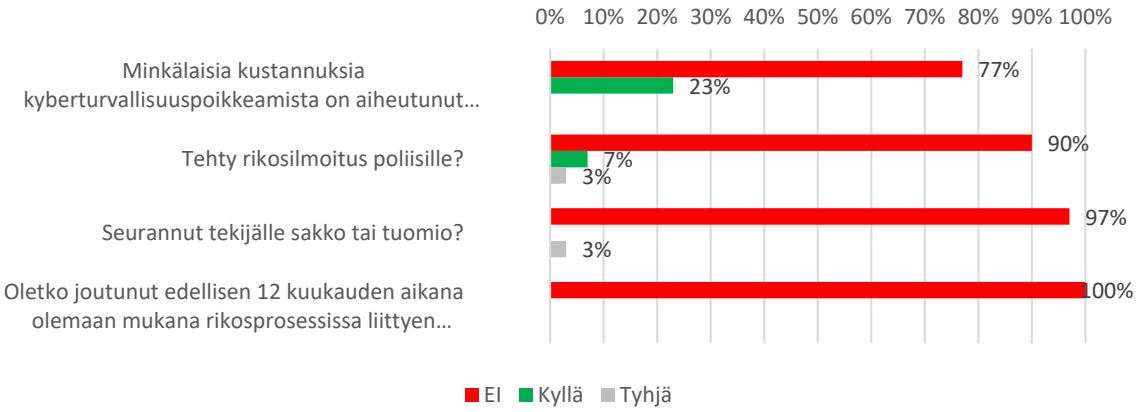
Kuvio 13. Jatkuvuudenhallinta 2.

Vastaajien mielipiteet ovat lähes tasaisesti jakautuneet kyllä- ja ei-puolelle kyberturvallisuuspoikkeamien havaitsemisessa (kuvio 14). Vastaajista puolet koki, että kyberturvallisuuspoikkeamista on raportoitu johdolle viimeisen 12 kuukauden aikana ja vastaavasti puolet koki, että kyberturvallisuuspoikkeamista ei ole raportoitu johdolle viimeisen 12 kuukauden aikana. Vastaajista 73 prosenttia katsoi, että heidän organisaationsa eivät ole ilmoittaneet havaittuja kyberturvallisuuspoikkeamia Suomen viranomaisille, esimerkiksi poliisille tai tietosuojavaltuutetulle, viimeisen 12 kuukauden aikana. Vastaajista 90 prosenttia koki, että heidän kyberturvallisuuspoikkeamat eivät ole aiheuttaneet haittoja heidän organisaatiolleen viimeisen 12 kuukauden aikana.



Kuvio 14. Kyberturvallisuuspoikkeamat viimeisen 12 kuukauden aikana.

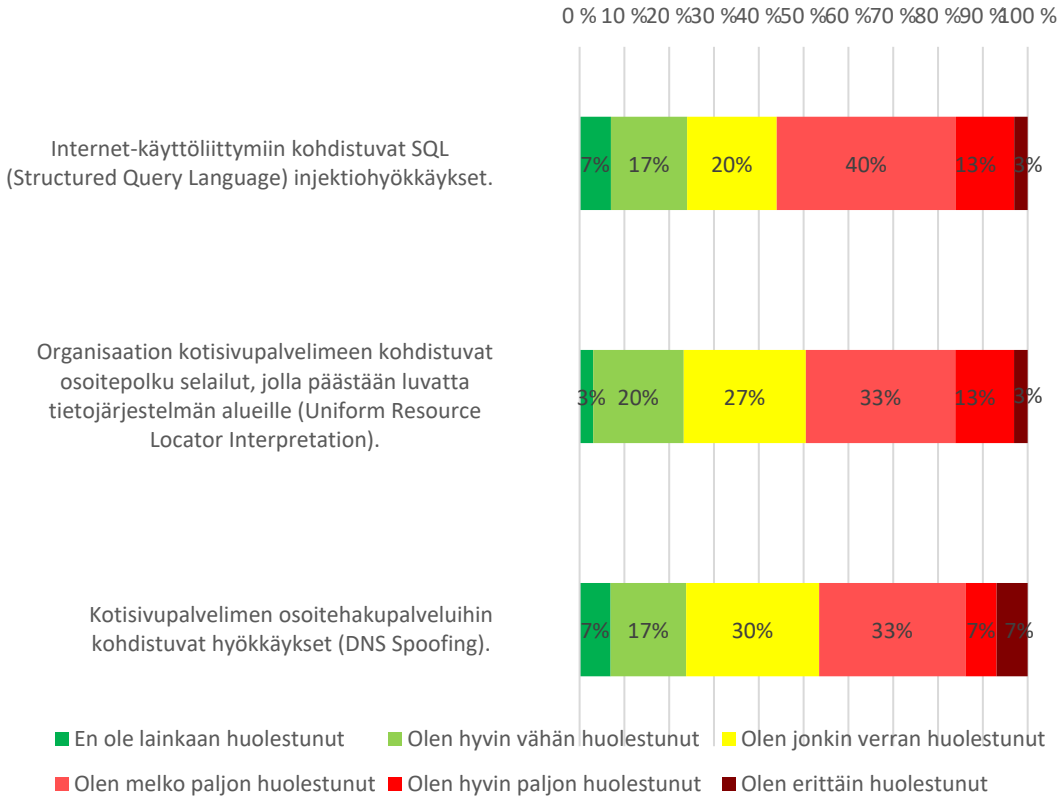
Vastaajista 77 prosenttia koki, että heidän organisaatiolleen kyberturvallisuuspoikkeamat eivät ole aiheuttaneet rahallisia kuluja viimeisen 12 kuukauden aikana (kuvio 15). Vastaajista 90 prosenttia koki, että heidän organisaationsa eivät ole tehneet rikosilmoituksia kyberturvallisuuspoikkeamista organisaatioissa Suomen poliisille viimeisen 12 kuukauden aikana. Vastaajista 97 prosenttia koki, että rikoksentekijä ei ole saanut rikosoikeudellista seuraamusta. Vastaajista jokainen oli sitä mieltä, että heidän organisaationsa eivät ole joutuneet osaksi rikosoikeudellisia prosesseja. Vastaajista suurin osa olivat sitä mieltä, että kyberturvallisuuspoikkeamat eivät ole aiheuttaneet haittoja ja kustannuksia organisaatiolle 12 kuukauden aikana. Myös enemmistö vastaajista oli sitä mieltä, että heidän organisaationsa eivät ole tehneet rikosilmoitusta poliisille kyberturvallisuusloukkauksista. Muutama vastaajista koki, että rikoksentekijälle ei ole tullut niissä seuraamuksia. Vastaajien mielipiteissä vallitsi yksimielisyys, että yksikään organisaatio ole ollut mukana rikosprosessissa viimeisen 12 kk aikana. Tässä herää kuitenkin kysymys, että ymmärsivätkö vastaajat kysymykset osallistumisesta rikosprosessiin kunnolla, koska poliisille rikoksen ilmoittaminen on osallistumista rikosprosessiin, kun kaksi vastaajista oli raportoinut ilmoittaneensa kyberturvallisuusloukkauksen rikosilmoituksena poliisille, mutta kaikki vastaajat ovat sitä mieltä, että he eivät ole olleet osallisena rikosprosessissa? Ristiriita on havaittavissa kahden vastaajan osalta.



Kuvio 15. Kyberturvallisuuspoikkeamat viimeisen 12 kuukauden aikana.

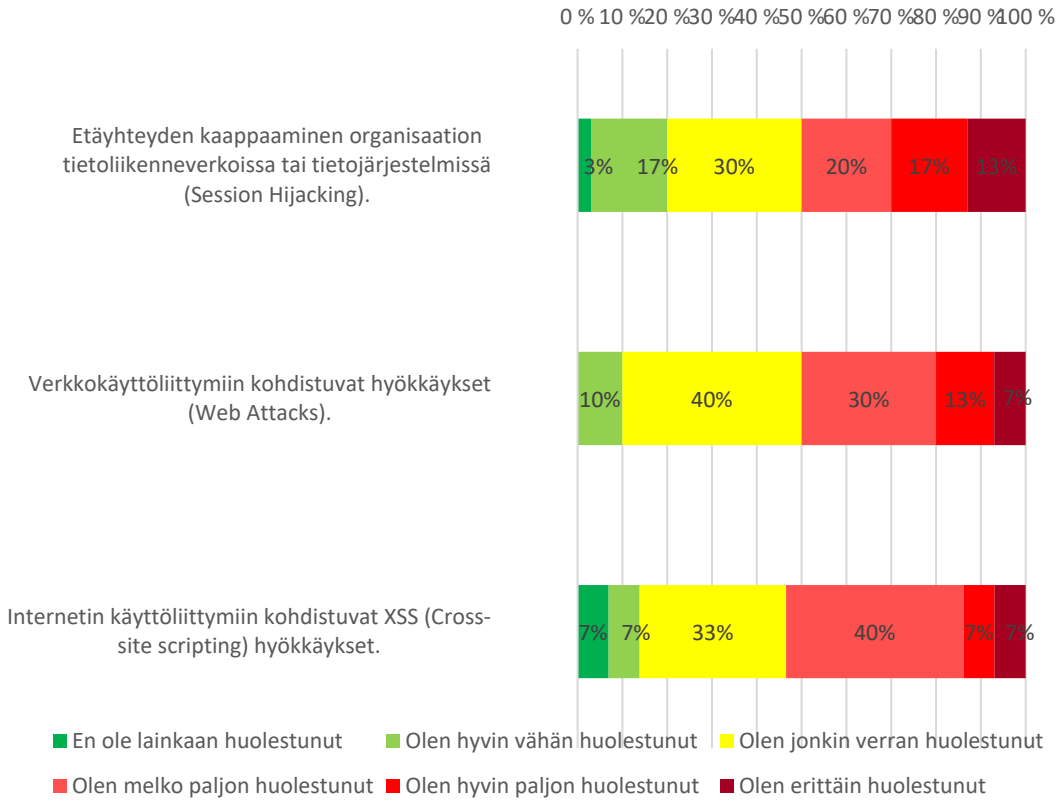
Seuraavaksi esitellään organisaatioiden kyberrikollisuuspelkoa. Kuvioiden 13–16 vastausvaihtoehdot perustuivat kuuteen eri asteikkoon, jossa tutkitaan kyselyyn vastaajien pelkokokemuksen voimakkuutta kyberhyökkäyksistä.

Vastaajista seitsemän prosenttia koki, että eivät kokeneet olleensa huolestuneita Internet-käyttöliittymiin kohdistuvista SQL-injektiohyökkäyksistä, mutta vastaajista 93 prosenttia oli huolestuneita eriävissä määrin Internet-käyttöliittymiin kohdistuvista SQL-injektiohyökkäyksistä (kuvio 16). Vastaajista 97 prosenttia oli huolestuneita heidän organisaationsa kotisivupalvelimeen kohdistuvasta osoitepolkuselailuista, joilla päästään tietojärjestelmän alueille, jonne ei pitäisi päästä. Vastaajista 93 prosenttia oli huolestuneita heidän organisaationsa kotisivujen osoitehakupalveluun kohdistuvasta DNS-hyökkäyksestä.



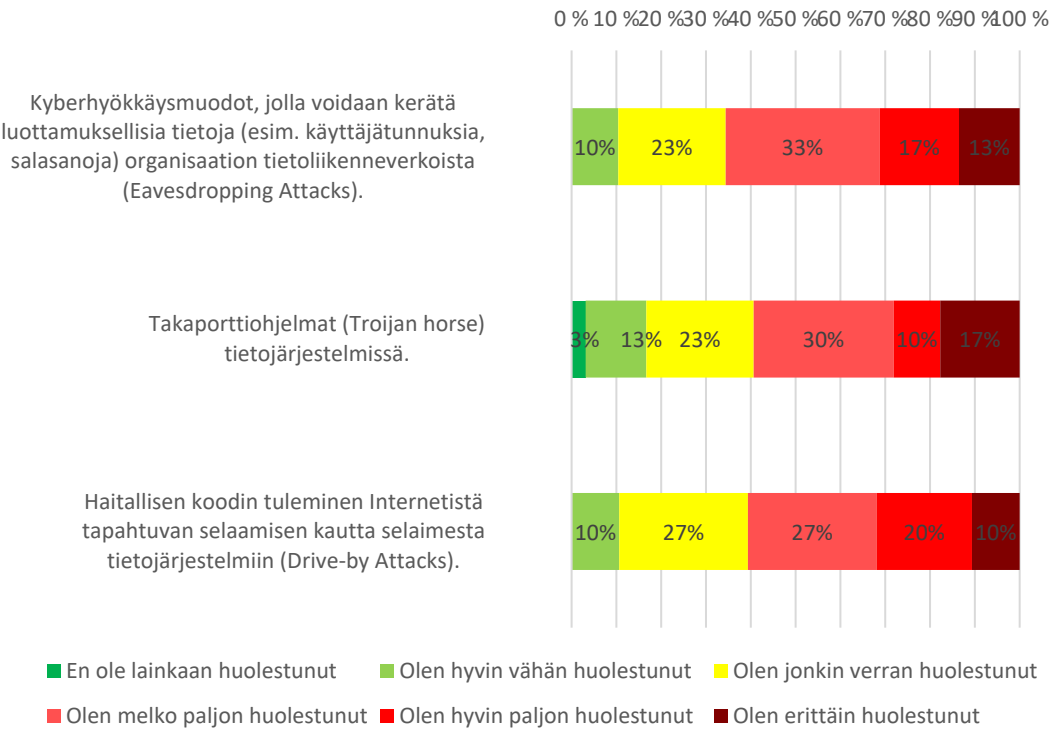
Kuvio 16. Kyberturvallisuuspoikkeamat viimeisen 12 kuukauden aikana. Kuinka huolissasi olet siitä, että organisaatioon kohdistuu seuraavia kyberturvallisuushyökkäyksiä seuraavan 12 kuukauden aikana?

Vastaajista 97 prosenttia oli huolestuneita etäyhteyden kaappaamishyökkäyksistä (kuvio 17). Kaikki vastaajat olivat huolestuneita heidän organisaationsa verkkokäyttöliittymiin kohdistuvista hyökkäyksistä. Vastaajista 93 prosenttia oli huolestuneita heidän organisaationsa Internet-käyttöliittymiin kohdistuvista Cross-site-scripting hyökkäyksistä.



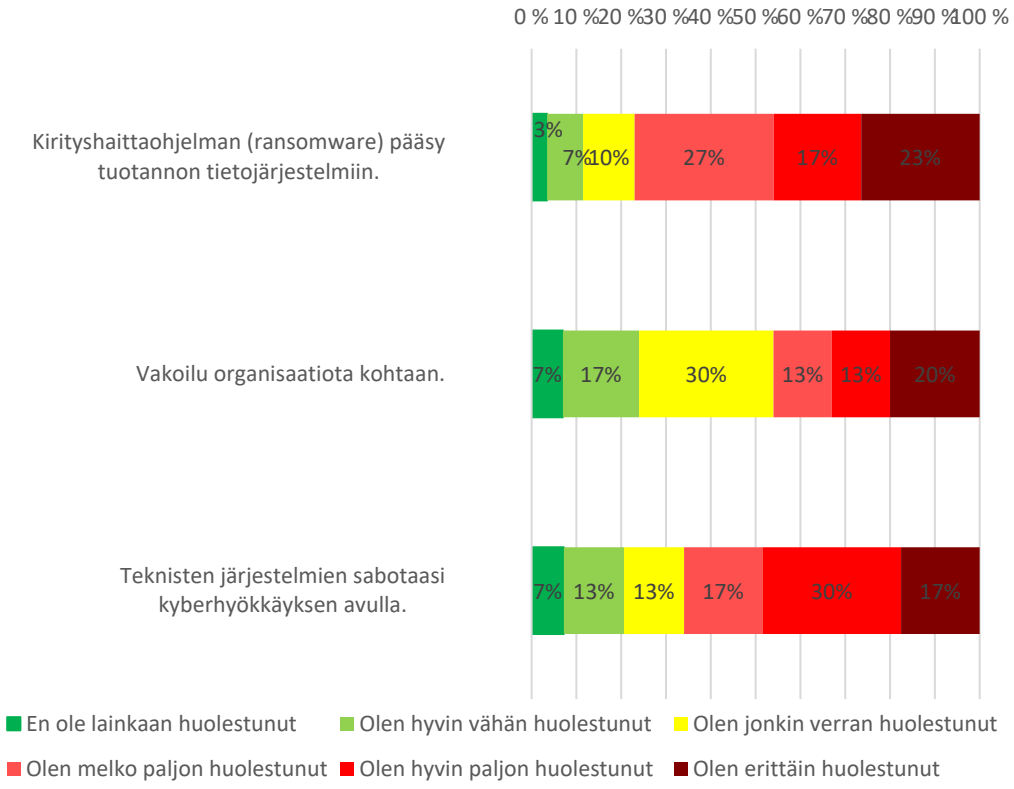
Kuvio 17. Kyberturvallisuuspoikkeamat viimeisen 12 kuukauden aikana. Kuinka huolissasi olet siitä, että organisaatioon kohdistuu seuraavia kyberturvallisuushyökkäyksiä seuraavan 12 kuukauden aikana?

Vastaajista kaikki olivat huolestuneita hyökkäyksestä, jolla voidaan varastaa heidän organisaationsa käyttäjätunnuksia sekä tietoja (kuvio 18). Vastaajista 97 prosenttia oli huolestuneita takaporttiohjelmista heidän organisaatiossaan. Kaikki vastaajat olivat huolestuneita selaimen kautta tulevista haittaohjelmista, joiden avulla voidaan manipuloida heidän organisaationsa järjestelmiä.



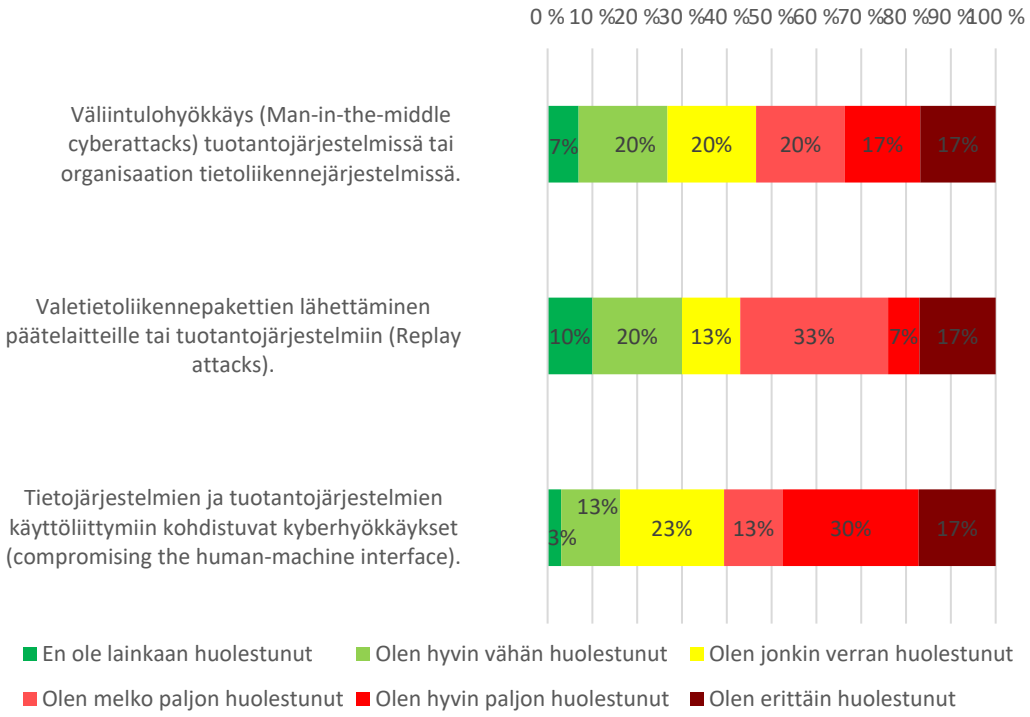
Kuvio 18. Kyberturvallisuuspoikkeamat viimeisen 12 kuukauden aikana. Kuinka huolissasi olet siitä, että organisaatioon kohdistuu seuraavia kyberturvallisuushyökkäyksiä seuraavan 12 kuukauden aikana?

Vastaajista 97 prosenttia oli huolestuneita kiristysohjelman tulemisesta heidän organisaationsa tietojärjestelmiin (kuvio 19). Vastaajista 93 prosenttia oli huolestuneita heidän organisaatioonsa kohdistuvasta vakoilutusta. Vastaajista 93 prosenttia oli huolestuneita heidän organisaationsa järjestelmiin kohdistuvasta teknisestä sabotaasista.



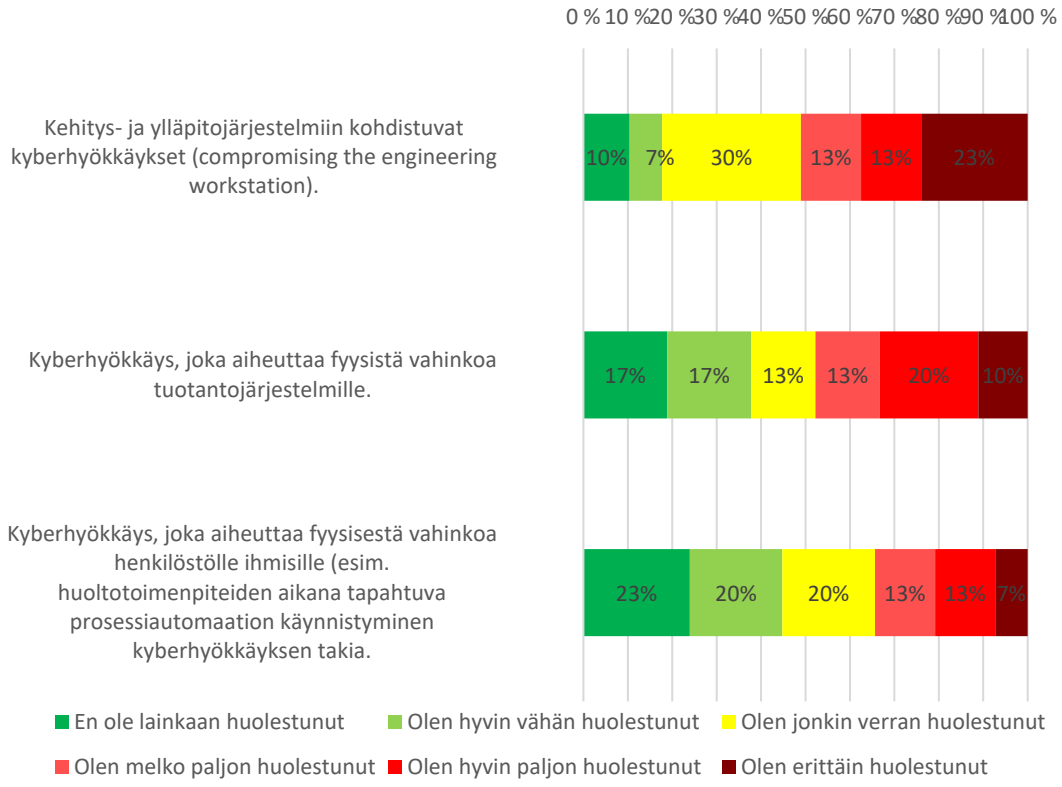
Kuvio 19. Kyberturvallisuuspoikkeamat viimeisen 12 kuukauden aikana. Kuinka huolissasi olet siitä, että organisaatioon kohdistuu seuraavia kyberturvallisuushyökkäyksiä seuraavan 12 kuukauden aikana?

Vastaajista 93 prosenttia oli huolestuneita heidän organisaatiossaan realisoituvista väliintulohyökkäyksistä tuotanto- ja tietoliikennejärjestelmissä (kuvio 20). Vastaajista 90 prosenttia oli huolestuneita valetietoliikennepakettihyökkäyksen kohdistumisesta heidän organisaationsa päätelaitteille ja tuotantojärjestelmiin. Vastaajista 97 prosenttia oli huolestuneita kyberhyökkäyksestä, joka kohdistuu tuotantojärjestelmien käyttöliittymiin.



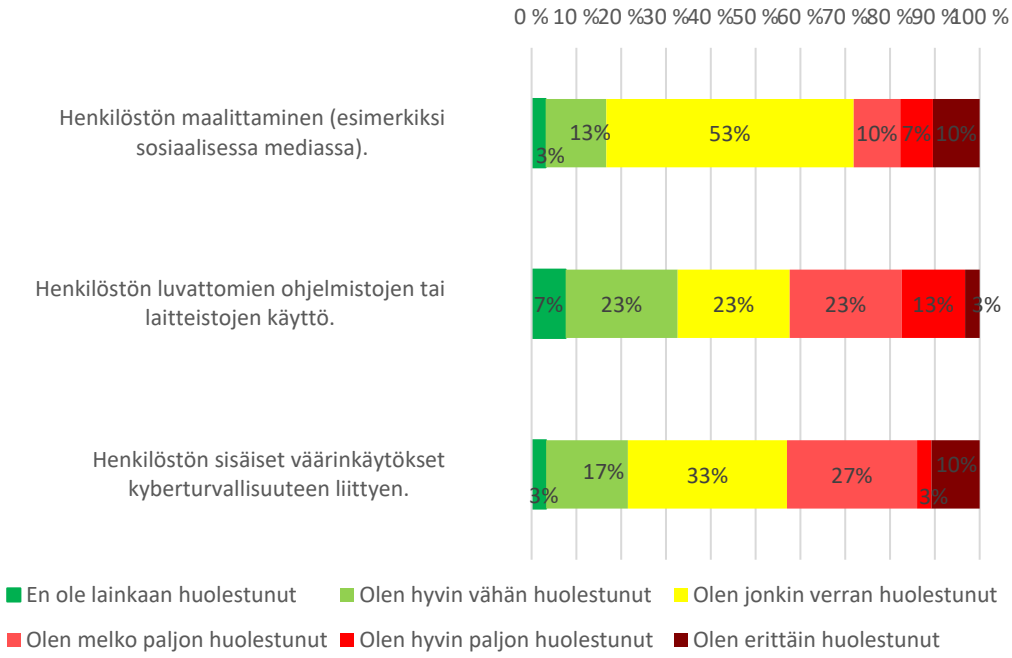
Kuvio 20. Kyberturvallisuuspoikkeamat viimeisen 12 kuukauden aikana. Kuinka huolissasi olet siitä, että organisaatioon kohdistuu seuraavia kyberturvallisuushyökkäyksiä seuraavan 12 kuukauden aikana?

Vastaajista 90 prosenttia oli huolestuneita heidän organisaationsa kehitysjärjestelmiin ja ylläpitojärjestelmiin kohdistuvasta kyberhyökkäyksestä (kuvio 21). Vastaajista 83 prosenttia oli huolestuneita kyberhyökkäyksestä, joka aiheuttaa fyysistä vahinkoa heidän organisaationsa tuotantojärjestelmille. Vastaajista 77 prosenttia oli huolestuneita kyberhyökkäyksestä, joka aiheuttaa vahinkoa ihmisille heidän organisaatiossaan.



Kuvio 21. Kyberturvallisuuspoikkeamat viimeisen 12 kuukauden aikana. Kuinka huolissasi olet siitä, että organisaatioon kohdistuu seuraavia kyberturvallisuushyökkäyksiä seuraavan 12 kuukauden aikana?

Vastaajista 97 prosenttia kokee huolestuneisuutta itseensä kohdistuvasta maalittamisesta sosiaalisessa mediassa (kuvio 22). Vastaajista 93 prosenttia oli huolestuneita heidän organisaatioonsa kohdistuvasta kyberhyökkäyksestä seuraavan 12 kuukauden aikana, jonka syynä olisi henkilöstön luvaton ohjelmistojen ja laitteiden käyttö. Vastaajista 97 prosenttia oli huolestuneita kyberhyökkäyksestä seuraavan 12 kuukauden aikana, jonka syynä olisi heidän organisaationsa henkilöstön sisäiset väärinkäytökset. Enemmistö vastaajista on sitä mieltä, että realisoituvaa kyberhyökkäystä pidetään ilmeisenä pelkona. Vastaajien pelkokokemuksen vahvuus vaihteli, mutta selvä havainto on, että enemmistöllä vastaajista eriasteista huolestuneisuutta koskien realisoituvaa kyberhyökkäystä heidän organisaatiossaan.



Kuvio 22. Kyberturvallisuuspoikkeamat viimeisen 12 kuukauden aikana. Kuinka huolissasi olet siitä, että organisaatioon kohdistuu seuraavia kyberturvallisuushyökkäyksiä seuraavan 12 kuukauden aikana?

Avoimissa kysymyksissä vastaajilta kysyttiin organisaatioiden kyberturvallisuusloukkauksien ilmoittamisesta viranomaiselle, johon vastasi vain kolme vastaajaa. Vastattiin, että kyberturvallisuusloukkausilmoituksia oli tehty kolme tai viisi kertaa viranomaiselle. Kaksikymmentäseitsemän vastaajaa ei vastannut avoimeen kysymykseen, että ovatko he ilmoittaneet kyberturvallisuusloukkauksista viranomaisille viimeisen 12 kuukauden aikana. Enemmistö vastaajista, eli 27, ei ole ilmoittanut kyberturvallisuusloukkauksia Suomen turvallisuusviranomaisille. Kolmen organisaation osalta ilmoituskeskiarvo 12 kk aikana tapahtuneesta kyberturvallisuusloukkauksesta viranomaiselle oli vain noin kolme kertaa.

Avoimeen kysymykseen, että onko teidän organisaatiossanne havaittu kyberturvallisuuspoikkeamia viimeisen 12 kuukauden aikana, vastattiin, että kyberturvallisuuspoikkeamat olivat muutamista kyberturvallisuuspoikkeamista satoihin kyberturvallisuuspoikkeamiin. Vastaajat kertoivat raportoineensa yhdestä kerrasta kymmeneen kertaan havaituista kyberturvallisuuspoikkeamasta organisaationsa johdolle.

Yksittäisissä vastauksissa kyberturvallisuuspoikkeamia raportoitiin 1–100. Haittoja ja kuluja avoimissa vastauksissa raportoitiin vähän. Tämä johtuu todennäköisesti siitä, kyberhyökkäykset ja niiden seuraukset pidetään organisaation sisäisenä asiana. Kyberturvallisuus vaatii kuitenkin kuluja, koska toimenpiteet eivät ole ilmaisia:

> *”Ylimääräistä työtä/kuluja, kun pitää tutkia, että haavoja ei ole hyväksikäytetty”*

> *”Joitain tuhansia euroja sen varmistamiseen nollapäivähaavoittuvuuden paljastumisen jälkeen tehtävien suositeltujen tarkistusten toteuttamiseen”*

Kyberturvallisuudella ja sen kehittämisellä on taloudellisia seurauksia kuten vakuutusten hintojen nousu:

> *”Vakuutusten hinnat nousevat (omasta toiminnasta riippumaton yleinen kehitys)”*

Vastaajien organisaatioilla on käytössä eurooppalaisia tietoturvastandardeja ISO 27002, ISO 27000, ISO27001 sekä amerikkalaisia National Institute of Standards and Technology (NIST) -laitoksen ohjeistuksia. Lisäksi on käytössä suomalaisten turvallisuusviranomaisten kehittämän KATAKRI I ja KATAKRI II -arviointikriteeristön viitekehys ja valtiovaraministeriön Vahti-ohjeiden mukaisia ohjeistuksia organisaation tietoturvatoteutuksessa. Kaikilla toimijoilla ei kuitenkaan ole tarvittavaa standardia käytössään:

> *”Tavoitellaan ISO27001-standardia”*

Joissain tapauksissa standardia ei tarkkaan tiedetä, koska ulkoiset kumppanit käyttävät niitä:

> *”Käytössämme on ulkoistettu tietohallinto, jonka kautta mallit kyberturvallisuuden soveltamiseen tulevat.”*

> *”Erityisiä viitekehyksiä tms. ei käytetä itse, mutta kyberturvallisuuttamme arvioivat ulkoiset tahot hyödyntävät näitä, kun arviointeja tehdään epäsäännöllisesti ja eri toimijoiden puolesta.”*

Standardeja voi myös yhdistellä kuten eräs vastaaja ilmaisi:

> *”KATAKRI 2, perustaso (IV). Lisäksi poimittu asioita ISO27001-standardista.”*

Vastaajat toivoivat kyberturvallisuusharjoituksia, joissa todelliset kyberhakkerit toteuttaisivat niin sanotun aidon kyberhyökkäyksen, jossa kiristysohjelma ajautuu organisaation tietojärjestelmiin. Myös toivottiin koulutusta kyberhyökkäyksien havaitsemiseen ja riskienarviointiin sekä toivottiin huoltovarmuusalan toimijoiden yhteistä kyberturvallisuusharjoitusta, jossa julkiset ja yksityiset toimijat harjoittelevat keskenään, kuten myös erilaisia seminaareja ja keskustelutilaisuuksia. Yhteistyön lisäksi säännöllisyyttä arvostettiin:

> *”Julkisella puolella on keskitetty jokavuotinen harjoittelumahdollisuus, tällainen olisi hyvä saada myös huoltovarmuuskriittisille toimialoille.”*

> *”Yhteiskunnan toiminnan kannalta kriittisillä toimialoilla voisi olla vuosittain yhteisiä harjoitusskenaarioita, joita kukin organisaatio sitten voisi harjoitella. Esimerkiksi Huoltovarmuuskeskuksen poolien kautta tarjoamana. Ei siis mitenkään pakotettuna, mutta kannustaen ja materiaalia toimittaen. Ajatus voisi olla, että harjoitellaan yhteisen teeman ympärillä, mutta jokainen omalla tavallaan. Vuoden aikana teemaa voisi tukea sitten muussa huoltovarmuustoiminnassa vaikkapa keskusteluin ja seminaarein. (esim. poolitoiminnan kautta)”*

Toimialakohtaisuus on myös tärkeää kyberturvallisuusharjoituksissa. Yhdessä vastauksessa esille tulevat erityisesti sähköverkon haasteet:

> *”Toimialakohtaisia harjoituksia, missä käsitellään erityisesti sähköverkon tietoliikenteeseen ja OT-verkkoihin liittyviä haasteita. Haavoittuvuus-skannauksia ja valkohattuhakkereiden johdolla tehtäviä tietoturvapoikkeamien tunnistamisia.”*

Vastaajien kokemuksissa heidän organisaationsa nykytilanteesta ja kehittämiskohteista arviot organisaation kyberturvallisuuden tasosta vaihtelevat heikosta hyvään:

> *”Kyky on oman organisaation osalta heikko. Tukeudumme toisaalta emokonsernin tietoturva-asiantuntijuuteen ja prosesseihin ja toisaalta IT-palvelukumppanimme tekniseen osaamiseen ja valvontaan”*

> *”Melko hyvällä tasolla ulkopuolisen tahon tekemän arvioinnin mukaan. Myös henkilöstö ymmärtää kyberturvallisuuteen liittyviä haasteita melko hyvin.”*

Vaikka usean vastaajan mukaan kyberturvallisuus on hyvällä tasolla, niin he nostivat esille jatkuvan hereillä olon kriittisyyden:

> *”Tilanne on hallinnassa, mutta tämä vaatii jatkuvaa kehittämistä ja valvontaa, jotta tilanne pysyy hallinnassa myös jatkossa.”*

Joillain organisaatioilla kehitystyö on kuitenkin vasta alkamassa:

> *”Olemme kartoittamassa juuri meidän lähtötasoa ja rakentamassa organisaatiota tietoturvan ympärille.”*

Kyberturvallisuuden kehittäminen on kuitenkin pitkäjänteistä ja siihen täytyy koko organisaation osallistua:

> *”Kyberturvallisuuden taso on keskimääräinen tai siitä hieman parempi. Kehitystyötä kyberturvallisuuskulttuurin kohentamiseksi on tehty muutamia vuosia. Perusteet (johdon sitoutuminen ja seuranta) alkavat olla normaalia toimintaa. Haluttujen toimintamallien muuttaminen käytännön tekemiseksi kestää pidempään. Kyberturvallisuuden kehittämisessä on kuitenkin pyritty noudattamaan tasapainoa, että kaikki osa-alueet tulisi huomioiduksi niin hyvin kuin mahdollista.”*

Kyberturvallisuus vaatii jatkuvaa organisaation toiminnan kehittämistä ja valveilla oloa ulkoisen toimintaympäristön muutoksista. Keskeisimpinä kehittämiskohteina vastaajat nostivat esille monet johtamiseen ja organisaation toiminnan suunnitteluun liittyvät teemat kuten johdon tuen. Kyberturvallisuus nähdään myös koko toimialan haasteena:

> *”Johdon saaminen aktiivisemmin mukaan toimintaan. Toimialan yhteistyön lisääminen.”*

> *”Kyberturvallisuuteen liittyvien asioiden vastuuttaminen ja resursointi”*

> *”Teknisesti ja operatiivisesti kyberturvaa kehitetään ja ylläpidetään erityisesti auditointien kautta, mutta hallintoa ja dokumentaatiota pitää kehittää, eli systematisoida lisää tekemistä.”*

Kyberturvallisuus nähdään kokonaisvaltaisena kulttuurin kehittämistyönä, johon tarvitaan koko organisaation sitoutumista:

> *”Kyberturvallisuuden vieminen käytännön teoiksi ja esimerkiksi sopimuksiin ja sopimusvaatimuksiin tarvitsee lisää tukea. Henkilöstön ja kyberturvallisuuskulttuurin luominen vaatii vielä työtä, asenteissa on vielä korjattavaa useammalla tasolla. Organisaation kokoon ja toimintatapaan suhteutettujen systemaattisten toimintamallien etsiminen jatkuu. Tietoturvahavainnoinnin tason nostaminen ja korjaustoimenpiteiden konkretisointi, ettei jää pelkäksi riskien hyväksynnäksi.”*

> *”Kyvykkyys kehittää muuttuvan maailman mukana on vajavainen. Siksi nyt käyttöön otetaan ISMS, jotta johtokin saadaan osallistettua. … Jatkuvuuden varmistamisen suunnittelussa on puutteita. Kyberturvallisuus ajateltu pelkkänä teknologia-asiana, jota ICT hoitaa."*

Projektissa järjestettiin 17.1.2022 kyberturvallisuuden johtamisen kehittämiseen liittyvä seminaari, jonka alussa professori Mikko Siponen luennoi kyberturvallisuuden johtamisen standardeista. Työpajaosuudessa osallistujat jaettiin kolmeen pienryhmään (3–5 henkilöä / ryhmä) ja heille annettiin tehtäväksi kehittää ideoita organisaatioiden

kehittämistyön, koulutuksen ja tutkimuksen kehittämiseksi kyberturvallisuuden johtamisen alueella. Pääteemoiksi nousivat seuraavat:

Teema 1: Standardeihin liittyvä koulutus ja tutkimus

- Yleistä standardeihin liittyvää koulutusta tarvitaan.
- Tarvitaan johtajille suunnattu ohjausjärjestelmä, joka ohjaa valitsemaan standardin ja joka kertoo standardien päällekkäisyyksistä.
- Mikä estää tai vaikeuttaa standardien käyttöönottoa?
- Standardien käytöstä saatava liiketoimintahyödyn näkyväksi tekeminen.

Teema 2: Kyberhyökkäyksiin liittyen

- Kuinka reagoida kyberhyökkäykseen?

Teema 3: Ei-tekniset teemat

- Ohjeistus organisaation kyberturvatoiminnon kehittämiseksi.
- Kyberturvallisuuden kehittämistä ei-teknisistä näkökulmista kuten talous.

5 YHTEENVETO JA JOHTOPÄÄTÖKSET

Suomen energia-alan kyselyyn vastasi 30 Suomen energia-alan organisaatioiden edustajaa. Kyberturvallisuuden johtamisen ja hallinnoinnin osalta vastaajat kokivat, että kyberturvallisuus on huomioitu suurimmassa osassa organisaatioita ja kyberturvallisuutta hoidetaan organisaatiossa. Voidaan siis todeta, että kyberturvallisuutta johdetaan suurimmassa osassa organisaatioita. Kyberturvallisuutta myös mitataan, ja sillä on vastuuhenkilöt suurimmassa osassa organisaatiota.

Vähäinen osa vastaajista kokee puutteita sidosryhmien riskienarvioinnissa sekä organisaatioiden tavoitteiden saavuttamisen valvomisessa. Koetaan, että riskienarvioinnit ja dokumentaatiot sekä osallistuminen kyberturvallisuuteen olisi toteutettu suurimassa osassa vastaajien organisaatioita. Silti pieni osa vastaajista koki, että resursseja kyberturvallisuuden hoitamiseen ei olisi tarpeeksi, ja iso joukko vastaajista ei osannut arvioida, että onko resursseja riittävästi kyberturvallisuuteen organisaatiossa. Noin kolmasosa vastaajista koki, että riskienhallinnan toimenpiteiden toteutuksessa oli parannettavaa, mutta noin 40 prosenttia ei osannut sanoa, tehdäänkö kyberturvallisuusauditointien perusteella toimenpiteitä organisaatiossa. Enemmistö vastaajista koki, että kyberturvallisuusauditoinnit on toteutettu vastaajien organisaatioissa. Myös johdon sitoutumisesta kyberturvallisuuden katselmukseen noin kolmasosa vastaajista koki, ettei siihen tehdä riittävästi organisaation johdon puolelta katselmuksia sekä toinen kolmasosa ei osannut sanoa, osallistuuko organisaation johto kyberturvallisuuden katselmukseen organisaatiossa.

Vastaajien vastauksista havaittiin erilaisia riskienarviointimenetelmiä. Vastauksien perusteella riskienarviointimenetelmät eivät siis ole yhdenmukaisia organisaatioissa. Kyselyyn vastaajilla oli käytössä eurooppalaisia ja amerikkalaisia kyberturvallisuusstandardeja sekä Traficomin tarjoama kriteeristö ja valtiovaraministeriön vahtiohjeet ja puolustusministeriön KATAKRI I ja II -kriteeristöt kyberturvallisuuden viitekehykseksi. Riskienarviointimenetelmien toimivuudesta SWOT-analyysi ja PESTEL-arviointimenetelmä herättävät jatkokysymyksiä, että ovatko nämä sopivia laadukkaan riskienarvioinnin tekemiseen Suomen energia-alan organisaatiossa?

Kyberturvallisuuden auditoinnit koetaan toteutetuksi suurimmassa osassa organisaatiota myös sidosryhmien osalta. Erilaiset yhteistyöt sidosryhmien ja viranomaisten kanssa koetaan tehdyiksi suurimmassa osassa organisaatioita. Toimitilaturvallisuus koetaan suurimmassa osassa organisaatioita toteutetuksi. Puutteita koettiin vähän yli puolessa organisaatiossa omaisuuden turvamerkitsemissä. Suurimmassa osassa organisaatioita koettiin, että koulutusta kyllä järjestetään henkilöstölle ja ohjeistukset ovat ajantasaiset, mutta puutteita koettiin vähän yli puolessa organisaatioista kyberturvallisuuden harjoituksissa ja kyberturvallisuuden yhteistoimintaharjoituksissa. Vastaajat kokevat, että organisaatioiden kyberturvallisuusosaamisessa on siis puutteita. Tämä johtuu siitä, että organisaation

kyberturvallisuusosaamista ei kyetä arvioimaan. Vain pieni osa vastaajista ilmoittaa, että kyberturvallisuusharjoituksia on järjestetty organisaatiossa ja yhteistyöryhmien kanssa. Tämä on noin kolmisenkymmentä prosenttia vastaajista. Kyselyn perusteella noin yli puolet vastaajista koki, että kyberturvallisuuspoikkeaminen hallinta olisi toteutettu organisaatiossa.

Kyberrikoksien torjunnan osalta suurin osa organisaatioista koki, että siihen on panostettu. Vastaajien joukossa oli paljon kokemuksia, että ei osata sanoa, että onko organisaation sopimuksissa ja sidosryhmien välisessä yhteistyössä huomioitu kyberturvallisuus. Jatkuvuudenhallinnan osalta noin kolmasosa vastaajista ei osannut sanoa, onko sitä hoidettu heillä, sekä noin puolet vastaajista koki, että he eivät tiedä, onko heidän organisaatiossaan määritelty, mitkä ovat tavoitteet palautumisen osalta. Kyselyssä nousi esille, että organisaatioissa on tasaisesti jakautunut kyllä- ja ei-puolelle kyberturvallisuuspoikkeamien havaitseminen. Samantyylinen vastaaminen on myös kyberturvallisuuspoikkeamien raportoinnissa organisaation johdolle. Kyselyn perusteella enemmistö vastaajista jätti raportoimatta kyberturvallisuuspoikkeamat viranomaisille.

Vastaajista enemmistö raportoi, että kyberturvallisuuspoikkeamat eivät ole aiheuttaneet haittoja ja kustannuksia heidän organisaatiolleen 12 kuukauden aikana. Myös kyselyn perusteella enemmistö vastaa, että he eivät ole tehneet rikosilmoitusta poliisille kyberturvallisuusloukkauksista. Myös vastattiin, että muutamassa tapauksessa rikoksentekijälle ei ole tullut rikosoikeudellisia seuraamuksia ja vastattiin, että yksikään organisaatio ei ole ollut mukana rikosprosessissa viimeisen 12 kuukauden aikana. Tässä on mahdollisuus, että kaikki vastaajat eivät ole ymmärtäneet, mitä kysymys tarkoittaa. Poliisille rikoksen ilmoittaminen on osallistumista rikosoikeudelliseen prosessiin. Kaksi vastaajista oli raportoinut kyberturvallisuusloukkauksen rikosilmoituksena poliisille, ja täten vastauksissa on ristiriita.

Kyselyn perusteella vastaajat raportoivat enemmän kyberloukkauksia organisaation sisäisesti kuin organisaation ulkopuolisille viranomaisille. Kyselyn perusteella enemmistö Suomen energia-alan toimijoista ilmoitti pelkäävänsä realisoituvaa kyberturvallisuusloukkausta. Kyselyn perusteella vastaajat olivat huolissaan kyberhyökkäyksen uhriksi joutumisesta, ja vastauksissa korostui maalittaminen sosiaalisessa mediassa sekä kiritysohjelmahyökkäykset. Merkille pantavaa on, että jokaiseen kyberhyökkäysväitteeseen tullut vastaus valikoitui enimmäkseen johonkin asteikkoon huolestunut kriteeristössä.

Osa vastaajista näki, että viimeisen 12 kuukauden aikana kyberturvallisuuspoikkeamat ovat aiheuttaneet sisäisiä kuluja alkaen sadoista euroista tuhansiin euroihin asti, kun on jouduttu selvittelemään kyberturvallisuuspoikkeamatilanteita tai tekemään kyberturvallisuustoimenpiteitä nollapäivähaavoittuvuuksien takia. Myös kerrottiin vakuutusmaksujen nousseen. Vastaajista osa arvioi oman kyberturvallisuustasonsa korkeammaksi kuin alan toimijoilla. Kuitenkin vastattiin, että organisaatioilla oli puutteita viranomaisyhteistyön ja

sidosryhmäyhteistyön kanssa, ja kyselyn määrällisten vastausten perusteella havaittujen kyberturvallisuuspoikkeamat olivat tasaisesti kyllä tai ei, joka herättää kysymyksiä, että mikä on kyberturvallisuuden absoluuttinen taso organisaatiossa? Vastaajat toivovat kyberturvallisuusharjoituksia ja koulutuksia kyberhyökkäyksien havaitsemiseen, kokemusta oikeasta kyberhyökkäyksestä, kykyä havaita kyberhyökkäyksiä ja torjua niitä sekä yhteistyöalustaa julkiselle ja yksityiselle sektorille energia-alan kyberturvallisuudessa.

Kyberturvallisuuden koetaan osittain olevan kunnossa Suomen energia-alan organisaatioissa, ja kyselyyn vastanneet alan toimijat osaavat nimetä kehittämiskohteita omissa organisaatioissaan. Ristiriita syntyy niiden vastauksien kohdalla, kun arvioidaan oman organisaation toiminnan olevan korkeampaa kuin muilla alan toimijoilla ja samaan aikaan kerrotaan, että kehittämiskohteita on kyberturvallisuuden osa-alueella, niin ovatko nämä kokemukset uskottavia ja realistisia? Jatkotutkimuskohteena olisi huoltovarmuuskriittisten energia-alan toimijoiden tutkiminen samalla kysymyspatteristolla, jotta saadaan tietoa, että miten toimivasti ja tehokkaasti he ovat toteuttaneet oman organisaationsa kyberturvallisuuden. Myös onko muita keinoja saada alan toimijoilta tietoa, että miten he kokevat kyberturvallisuutensa olevan toteutettu?

Suositukset

Tämä selvityksen perusteella esitämme suosituksia (Taulukko 2).

Taulukko 2. Suosituksia organisaatioille

Suositus	**Kuvaus**
1: Standardien käyttöönotto	Organisaatioille suositellaan standardeja, joilla voidaan säädellä organisaation ihmisten johtamista ja teknisiä toteutuksia. Suositeltavia standardeja kyberturvallisuuden hallinnalla ovat ISO/IEC 27000 -sarjan standardit sekä erityisesti energia-alan tietojärjestelmien, prosessiautomaatiolaitteiden ja kenttälaitteiden kyberturvallisuudelle ISO/IEC 27019:2017-standardit.
2: Kyberturvallisuuskulttuurin kehittäminen	Kyberturvallisuuskulttuurin kehittäminen tarkoittaa organisaation kaikkien jäsenten sitoutumista tietoturvasääntöihin, kyberturvallisuussääntöihin ja oman toiminnan tarkastelua tietoturvan näkökulmasta. Johdon tukea ja johdon toiminnan kehittämistä tarvitaan kyberturvallisuuden takaamiseksi. Käytännön kyberturvallisuustyön laadukkuutta on kehitettävä ajantasaisten ohjeiden avulla, harjoittelulla sekä riskienhallinnan avulla. Kyberturvallisuus on vietävä teoriasta käytännöksi, ja kyberturvallisuuskulttuurin

Suositus	**Kuvaus**
	luominen vaatii työtä. Myös asenteiden muokkaamisessa kohdistuen kyberturvallisuuteen on tekemistä organisaation jokaisella hierarkkisella tasolla. Organisaatioiden on nostettava kyberturvallisuustasoa, ja korjaustoimenpiteiden pitää konkretisoitua, jotta toiminta ei jää pelkäksi riskien hyväksynnäksi organisaatioissa.
3: Toimialan yhteistyö	Yksittäisellä toimialalla on kyberturvallisuuden suhteen omat haasteensa, joiden suhteen toimialan toimijoiden yhteistoimintaa tulee vahvistaa ja täten koko toimialan yhteistä kyberturvallisuutta. Alan toimijoille on luotava kumppanuusturvallisuusverkosto heidän yhteistoimintansa kehittämistä varten. Tietojärjestelmästandardien käyttöönoton yhteydessä tulee osallistuttaa ihmisiä.
4: Toimintaympäristön jatkuva tarkkailu ja oman toiminnan kehittäminen	Ylimmän johdon tulee sitoutua organisaatiossa kyberturvallisuustavoitteiden saavuttamiseen. Kyberturvallisuuteen liittyvien asioiden vastuuttaminen ja resursointi olisi tärkeää toteuttaa. Toimialan välistä yhteistyötä haluttaisiin lisätä. Toimialalla on lisättävä kyberuhkien havainnointi- ja reagointikykyä. Henkilöstön säännöllistä koulutusta, opastusta ja tiedottamista on myös toteutettava ja kehitettävä.
5: Kyberturvallisuusharjoitukset	Energia-alalla tulee järjestää kyberturvallisuusharjoituksia, jotta saadaan annettua kokemus, että miltä todellinen kyberhyökkäys näyttää, miten kyberhyökkäyksiä voidaan havaita ja torjua. On myös annettava koulutusta riskienhallintaan ja kyberturvallisuustoimintojen dokumentointiin energia-alalla.

Lähteet

Baruch, Yehuda, and Brooks C Holtom. 2008. "Survey Response Rate Levels and Trends in Organizational Research." *Human Relations* 61(8): 1139–60.

Basnet, M, and M H Ali. 2021. "Exploring Cybersecurity Issues in 5G Enabled Electric Vehicle Charging Station with Deep Learning." *IET Generation, Transmission and Distribution*.

Cook, Colleen, Fred Heath, and Russel L Thompson. 2000. "A Meta-Analysis of Response Rates in Web- or Internet-Based Surveys." *Educational and Psychological Measurement* 60(6): 821–36. https://doi.org/10.1177/00131640021970934.

COUPER, MICK P. 2000. "Review: Web Surveys: A Review of Issues and Approaches*." *Public Opinion Quarterly* 64(4): 464–94. https://doi.org/10.1086/318641.

Energiateollisuusyhdistys. 2021. "Jäsenluettelo." *https://energia.fi/meista/jasenet/jasenluettelo*.

Eskola, J., and J Suoranta. 1998. *Johdatus Laadulliseen Tutkimukseen*. Tampere: Vastapaino.

Evans, Joel, and Anil Mathur. 2005. "The Value of Online Surveys." *Internet Research* 15: 195–219.

Fischer Lars, Mathias Uslar, Doug Morrill, Michael Döring, Edwin Haesen 2018. Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector. Ecofys. Germany. EC Reference: ENER/B3/2017-465.

Heinonen, Jarmo, Anssi Keinänen, and Jyri Paasonen. 2013. "2.7 Luotettavuus." In *Turvallisuustutkimuksen Tekeminen*, ed. Jyri Paasonen. Helsinki: Tietosanoma Oy, 91–94.

Hirsjärvi, Sirkka, and Hurme Helena. 2008. *Tutkimushaastattelu : Teemahaastattelun Teoria Ja Käytäntö*. Helsinki: Gaudeamus Ab.

Larkin, R D, T J Wagner, and B E Mullins. 2020. "Securing Photovoltaic System Deployments with Data Diodes." In *Conference Record of the IEEE Photovoltaic Specialists Conference*, Institute of Electrical and Electronics Engineers Inc., 2525–31.

Likert, R. 1932. "A Technique for the Measurement of Attitudes." *Archives of Psychology* 22 140: 55.

Metsämuuronen, Jari. 2006. *Laadullisen Tutkimuksen Käsikirja*. 1. laitos. 1 painos. Jyväskylä: Gummerus Kirjapaino Oy.

Nussbaum, D, and A Dupuy. 2017. "The Cyber-Energy Nexus: {The} Military Operational Perspective." In *European {Conference} on {Information} {Warfare} and {Security}, {ECCWS}*, ed. Le-Khac N.-A. Scanlon M. Curran Associates Inc., 713–18. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85027987640&partnerID=40&md5=dd8cce248e11cc220a1f874ef331b87f.

Ozcelik, I et al. 2021. "CENTER Water: A Secure Testbed Infrastructure Proposal for Waste and Potable Water Management." In *9th International Symposium on Digital Forensics and Security, ISDFS 2021*, ed. Varol C Varol A. Karabatak M. Institute of Electrical and Electronics Engineers Inc.

Paasonen, Jyri. 2021. *Rikosseuraamuslaitoksen Turvallisuuden Ja Valvontatyön Ulkoinen Arviointi*. https://www.rikosseuraamus.fi/material/collections/20210510163048/7QCVnaVHV/2021-2_Risen_turvallisuuden_ja_valvontatyon_ulkoinen_arviointi.pdf.

Qassim, Q S et al. 2021. "Threat Assessment Model in Electrical Power Grid Environment." In *Journal of Physics: Conference Series*, IOP Publishing Ltd.

Salminen, Mirva. 2021. "Arkipäivän Digitaalinen Turvallisuus Euroopan Pohjoisilla Alueilla: Tapaustutkimus Tunturi-Lapista ." Media & Viestintä 44(1): 158–80. https://journal.fi/mediaviestinta/article/view/107305.

Sarker, P S et al. 2020. "Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5." In *8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2020 - Proceedings*, Institute of Electrical and Electronics Engineers Inc.

Stout, M A. 2012. "Uninterruptible Power Supplies and Cybersecurity." *InTech* 59(1–2).

Tomaskovic-Devey, Donald, Jeffrey Leiter, and Shealy Thompson. 1994. "Organizational Survey Nonresponse." *Administrative Science Quarterly* 39(3): 439–57. http://www.jstor.org/stable/2393298.

Utahin osavaltio. 2021. "Cyber Security Controls Checklist." *BRUCyberSecurityChecklist.pdf* https://beready.utah.gov/utah-hazards/cybersecurity/ (June 3, 2021).

Vartiainen, Tero. 2020. *Digitaalisten Energiajärjestelmien Kyberturvallisuus Ja Resilienssi (CR-DES)*. Vaasa. https://www.uwasa.fi/fi/tutkimus/hankkeet/cr-des

Vesterinen, Panu. 2020. *Yritysten Rikosturvallisuus 2020*. Helsinki.

Zhang, Y, L Wang, Z Liu, and W Wei. 2021. "A Cyber-Insurance Scheme for Water Distribution Systems Considering Malicious Cyberattacks." *IEEE Transactions on Information Forensics and Security* 16: 1855–67.