Hyvinvointialojen turvallisuusraportti 2021

Selvitys hyvinvointialojen tietoturvallisuudesta, muista keskeisistä turvallisuushaasteista ja –ratkaisuista sekä turvallisuusalan tuotteiden ja palvelujen kysynnästä

Lith Consulting Group
Suunnittelu- ja tutkimuspalvelut Pekka Lith
Helsinki 30. kesäkuuta 2021
Pekka Lith

1 Alkusanat

Oheisen turvallisuusraportin tarkoituksena on tuottaa Hyvinvointiala HALI ry:n ja Lääkäripalveluyritykset LPY ry:n asiantuntijoille, jäsenistölle, turvallisuusalan sidosryhmille, päättäjille ja muille tahoille ajantasaista tietoa yksityisten hyvinvointialojen ajankohtaisesta turvallisuustilanteesta ja sen kehityksestä. Raportissa tarkastellaan keskeisiä turvallisuusuhkia ja onnettomuusriskejä ja sitä, kuinka niihin on pyritty alan yrityksissä ja järjestöissä varautumaan. Erityisteemoina selvityksessä ovat tietoturvallisuutta koskevat asiat.

Hyvinvointialojen turvallisuusraportin tärkein tietolähde on ollut HALI ry:n ja LPY ry:n jäsenistölle suunnattu kyselytutkimus, johon vastasi 90 yksityistä sosiaali- ja terveyspalvelualan sekä varhaiskasvatusalan palvelutuottajaa. Raportti on samalla osa Finnsecurity ry:n ja Turvaurakoitsijat ry:n laajempaa turvallisuusalan suhdanne- ja toimialaraporttia, jossa tarkastellaan myös yksityisen turvallisuusalan yritystoimintaa, tuote- ja palvelukirjoa sekä markkinoita. Raportin on laatinut tutkija Pekka Lith (Suunnittelu- ja tutkimuspalvelut Pekka Lith).[1][2]

[1] Liittojen yhteyshenkilöinä ovat toimineet asiantuntija Jarno Talvitie (HALI ry) ja LPY:n toiminnanjohtaja Ismo Partanen.

[2] Kyselyjen teknisessä suorittamisessa on hyödynnetty Mainio Tech Oy:n kyselytyökalua (www.mainiosurvey.com).

Sisältö

2 Hyvinvointialojen turvallisuusympäristö

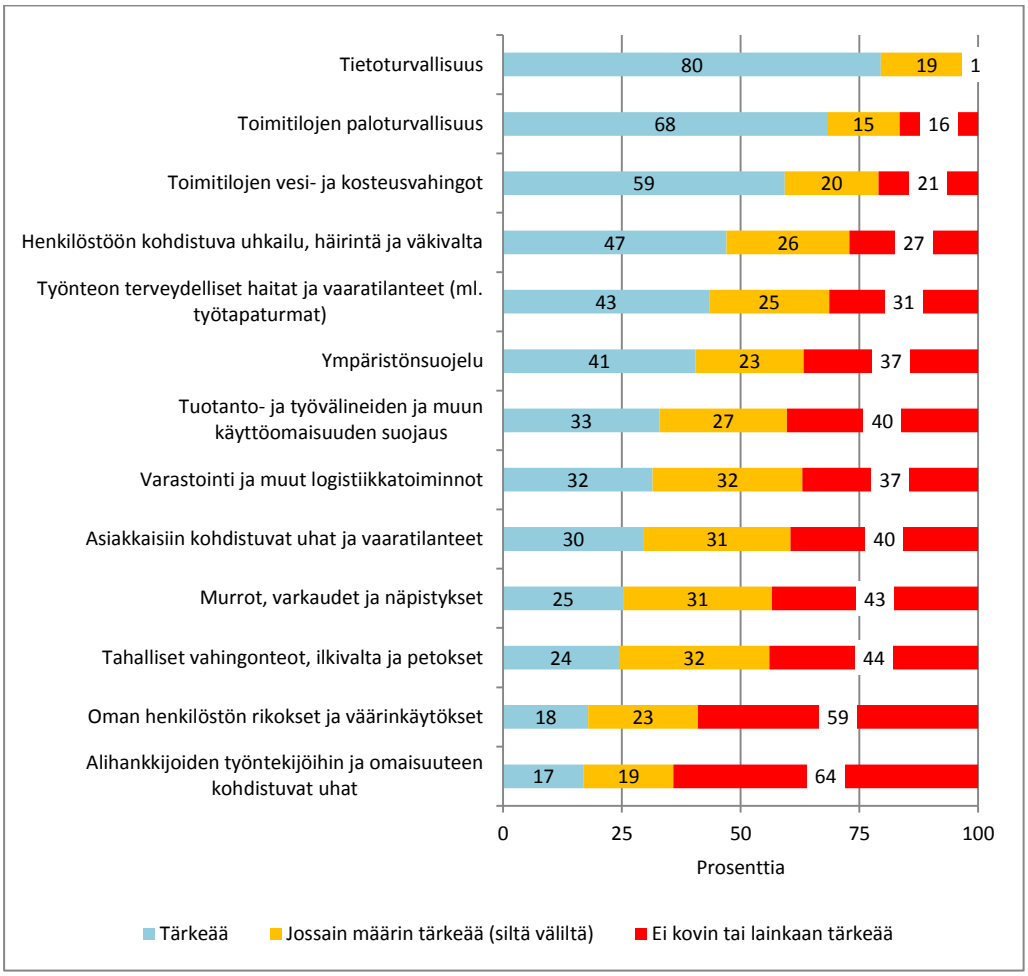
Yksityisillä hyvinvointialoilla tärkeimmät turvallisuuden uhkakuvat ja haasteet koskevat tietoturvallisuutta. Tietoturvallisuustuotteet, palvelut ja järjestelmät kuuluvat niihin turva-alan tuoteryhmiin, joiden kysyntä on suurinta. Kysyntää on myös tietoturvallisuuskoulutuksella.

Toimitilojen paloturvallisuuteen ja vesi- ja kosteusvahinkoihin voi liittyä merkittäviä turvallisuus- ja onnettomuusriskejä, joihin on syytä varautua. Asumisen sisältävissä sosiaalipalveluissa korostuvat lisäksi henkilöstöön kohdistuva uhkailu, häirintä ja väkivalta.

2.1 Keskeiset turvallisuusuhat ja onnettomuusriskit

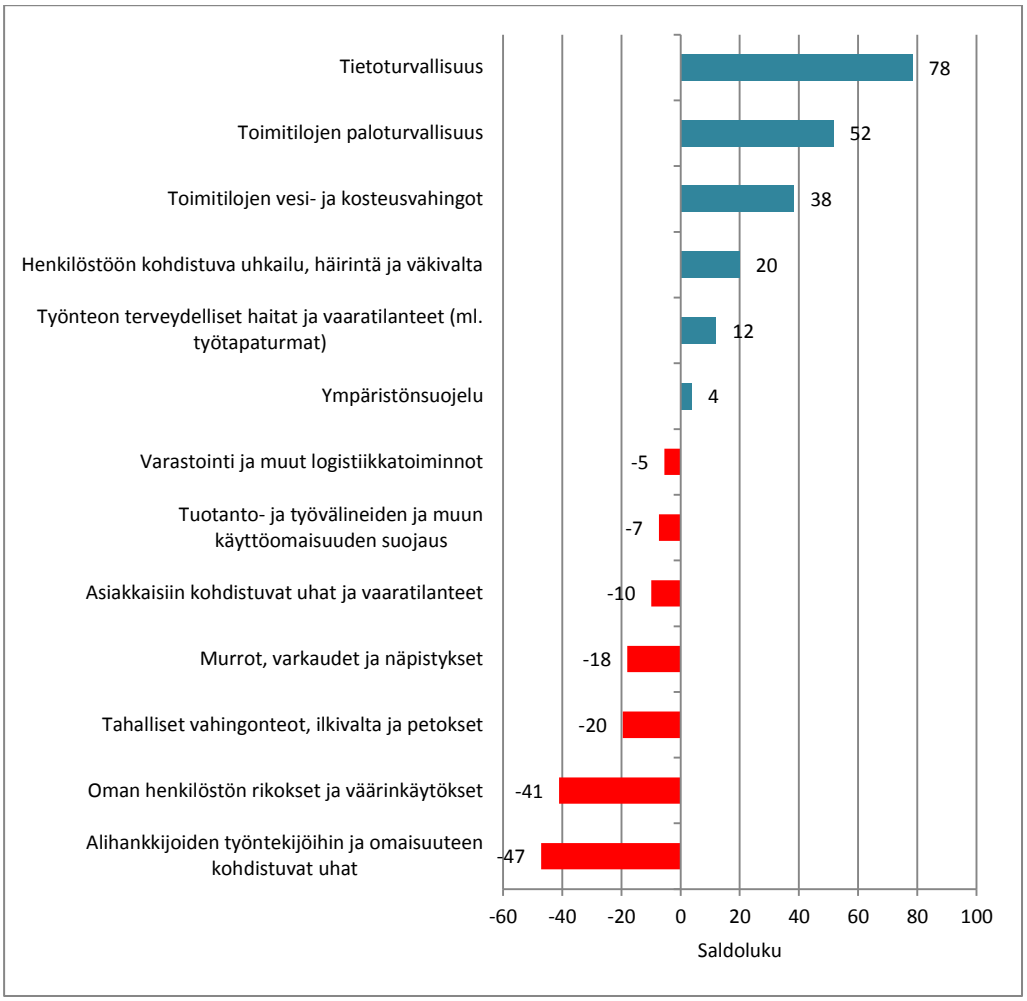
Turvallisuusalan kyselyihin vastanneista 80 prosenttia piti *tietoturvallisuutta* koskeviin uhkiin varautumista tärkeänä. Toiseksi ja kolmanneksi tärkeimpiä turvallisuus- ja onnettomuusuhkia *ovat toimitilojen paloturvallisuutta sekä vesi- ja kosteusvahinkoja*. Seuraavilla sijoilla olivat henkilöstöön kohdistuva uhkailu, häirintä ja väkivalta, työnteon terveydelliset haitat ja vaaratilanteet sekä ympäristösuojeluun liittyvät onnettomuusuhat. Vähiten pelättiin oman henkilöstön rikoksia ja väärinkäytöksiä sekä alihankkijoihin kohdistuvia uhkia (Kuvio 1).

Kuvio 1 *Hyvinvointialojen turvallisuusalan kyselyyn vastanneiden yritysten ja järjestöjen kokemat turvallisuus- ja onnettomuusuhat, prosenttia vastanneista (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



Edellä mainittuja asioita voidaan kuvata myös saldolukuina. Saldoluvut saadaan, kun turvallisuusuhkaa tai onnettomuusriskiä tärkeänä pitävien prosenttiosuudesta niiden vastaajien prosenttiosuus, jotka pitävät samaa asiaa erittäin vähän tai lainkaan tärkeänä. Tietoturvallisuus ja toimitilojen paloturvallisuus saivat myös näin mitattuna suurimmat saldoluvut. Alihankkijoiden työntekijöihin ja omaisuuteen kohdistuvat uhat sekä oman henkilöstön rikokset ja väärinkäytökset saivat puolestaan suurimmat negatiiviset saldoluvut (Kuvio 2).

Kuvio 2 *Hyvinvointialojen turvallisuusalan kyselyyn vastanneiden yritysten ja järjestöjen kokemat turvallisuus- ja onnettomuusuhat saldolukuina, prosenttia (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



Turvallisuusuhat ja riskit toimialoittain

Turvallisuuden uhkakuvia ja onnettomuusriskejä koskevat näkemykset eroavat hieman päätoimialoittain. Tietoturvallisuutta pidettiin hyvin tärkeänä kaikilla hyvinvointialoilla lukuun ottamatta varhaiskasvatusta, mutta sielläkin sitä pidetään melko tärkeänä. Toimitiloja koskeva paloturvallisuus on myös asia, joka on tärkeää asumisen sisältävissä sosiaalipalveluissa, varhaiskasvatuksessa ja pääosassa terveydenhuoltoa (sairaalat, lääkärikeskukset, yms.). Sama koskee kiinteistöjen (toimitilojen vesi- ja kosteusvahinkoja (Taulukko 1).

Henkilöstöön kohdistuva uhkailu, häirintä ja väkivalta koetaan tärkeäksi uhaksi asumisen sisältävissä sosiaalipalveluissa. Sama koskee työnteon terveydellisiä hait-

toja ja vaaratilanteita. Lastensuojelun laitoshoito ja ammatillinen perhe katsotaan olevan ainoa toimiala, jossa myös tahalliset vahingonteot ja ilkivalta nousevat keskeiseksi turvallisuusuhaksi. Sen sijaan esimerkiksi murtoja, varkauksia ja näpistyksiä taikka oman henkilöstön rikoksia ja väärinkäytöksiä ei koeta millään hyvinvointialalla keskeisiksi turvallisuushaasteiksi.

Taulukko 1 Hyvinvointialojen turvallisuusalan kyselyyn vastanneiden yritysten ja järjestöjen kokemat keskeiset turvallisuus- ja onnettomuusuhat toimialoittain (x = erittäin tai melko tärkeä) (Lähde: Hyvinvointialojen turvallisuuskysely 2021).

	Henkilöstöön kohdistuvat uhat	Työnteon terveyd. haitat ja vaaratilanteet	Tietoturvallisuus	Toimitilojen paloturvallisuus	Toimitilojen vesi- ja kosteusvahingot	Tahalliset vahingonteot, ilkivalta, yms.
Sosiaalipalvelut yhteensä	*x*		*x*	*x*	*x*	
- asumisen sisältävät palvelut[3]	x	x	x	x	x	
- lastensuojelupalvelut	x	x	x	x		x
- avohuollon sosiaalipalvelut			x			
Varhaiskasvatus			*x*	*x*		
Terveyspalvelut yhteensä			*x*	*x*	*x*	
- kuntoutus			x			
- muu terveydenhuolto			x	x	x	

2.2 Turvallisuusympäristön muutokset

Uhkakuvista ja riskeistä huolimatta 70 prosenttia hyvinvointialojen turvallisuuskyselyihin vastanneista yrityksistä ja järjestöistä totesi, että yleinen turvallisuustilanne on parantunut selvästi tai ainakin jonkin verran vuosina 2016-21 (Kuvio 3). Vajaa viidennes katsoi, että tilanne on pysynyt ennallaan. Ainostaan runsaat kymmenen prosenttia vastanneista ilmoitti, että turvallisuustilanne olisi heikentynyt. Päätoimialojen (sosiaali- ja terveyspalveluala sekä varhaiskasvatusala) välillä vastauksissa ei ollut tilastollisesti merkittäviä eroja.

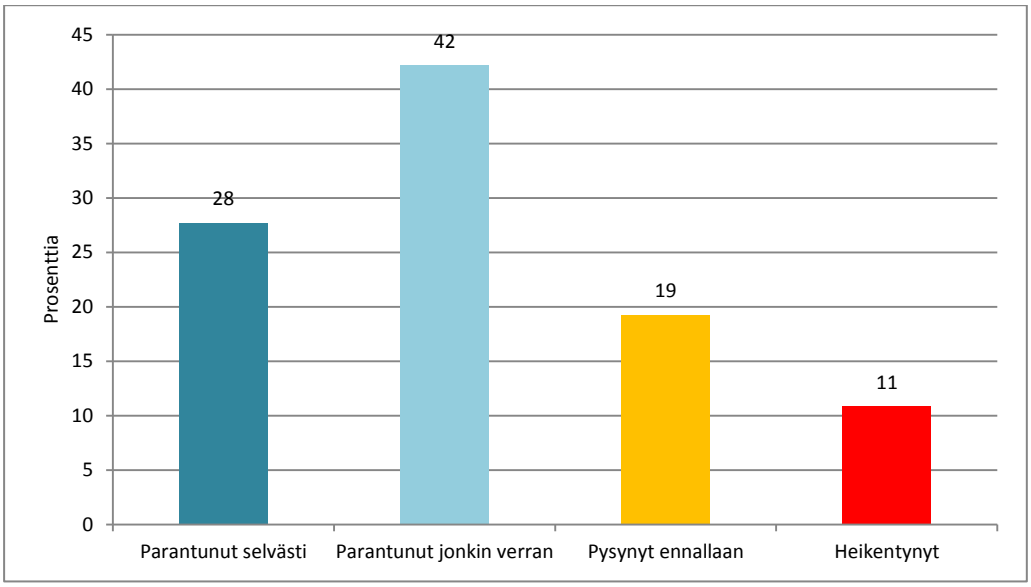
Myönteisen kehityksen taustalla ovat turvallisuusuhkiin ja –vaaroihin liittyvän tietoisuuden lisääntyminen ja turvallisuusasioiden merkityksen tunnustaminen kaikessa toiminnassa. Muuttuneet asenteet ovat myötävaikuttaneet siihen, että turvallisuuskulttuuri on kehittynyt ja turvallisuudesta huolehtimisesta on tullut osa normaalia arkea. Samalla säännöt ovat lisääntyneet ja selkeytyneet. Tietoturvan osalta kehitystä ovat edesauttaneet tekninen kehitys, ITC-arkkitehtuurin uudelleen rakentaminen ja henkilöstön yleisen ymmärryksen lisääntyminen.

Vastauksissa mainittiin, että henkilöstön perehdyttäminen turvalliseen työntekoon on tärkeää heti työsuhteen alussa samoin kuin asioiden jatkuva seuranta ja havaittujen epäkohtien korjaaminen mahdollisimman pian. Henkilöturvallisuutta ovat lisänneet henkilöstölle annettu uhka- ja väkivaltakoulutus, turvarannekkeet sekä asiakaskunnan parempi tuntemus. Tilojen uudelleen järjestelyillä, kameravalvontaa, lukitusjärjestelmiä uudistamalla ja muita sähköisiä turvalaitteita fiksusti hyödyntämällä on voitu vähentää turvallisuusriskejä.

[3] Pois lukien lastensuojelupalvelut.

Tosin uudet tietoturvauhat, verkkorikollisuus, henkilökunnan some-häirintä, omaisten uhkailu, nuorten häiritsevä käyttäytyminen, asiakkaiden päihteiden käyttö varsinkin huumeiden puolella ja mielenterveysongelmien kasvu ovat lisänneet haasteita. Erityisesti lasten perheiden ja lasten pahoinvointi ovat yleistyneet viime vuosina. Palvelulaitoksissa erityisryhmiin kuuluvien asiakkaiden, kuten muistisairaiden heikentynyt kunto on lisännyt onnettomuusriskejä. Vaaratilanteita voivat aiheuttaa myös henkilöstön puutteellinen kielitaito.

Kuvio 3 *Hyvinvointialojen turvallisuusalan kyselyyn vastanneiden yritysten ja järjestöjen näkemys yleisen turvallisuustilanteen kehityksestä 2016-21, prosenttia vastanneista (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



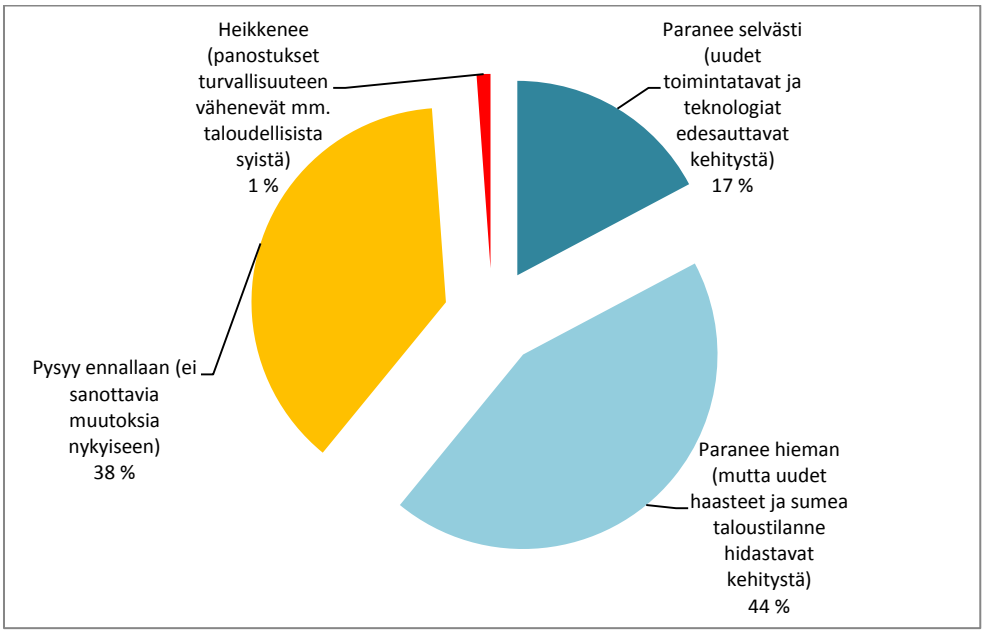
Tulevaisuuden näkymiä

Kokonaisuudessaan voidaan todeta, että pääosa kyselyihin vastanneista suhtautuu turvallisuustilanteen kehitykseen varsin luottavaisesti, jos näkymiä katsotaan seuraavan 1-2 vuoden perspektiivillä. Noin 61 prosenttia ennakoi turvallisuustilanteen paranevan, mitä asiaa uudet toimintatavat ja teknologian kehitys edesauttavat. Tosin taloudellisen tilanteen heikkeneminen voi hidastaa toivottua kehitystä. Vain yksi prosentti vastanneista ennusti turvallisuustilanteen huonontuvan. Ennallaan tilanne pysyy 38 prosentin mielestä (Kuvio 4).

Lähitulevaisuuden keskeiset haasteet koskevat tietoturvallisuutta ja henkilöturvallisuutta. Tietoturvallisuutta ovat vaarantaneet lisääntynyt kyberrikollisuus.[4] Palveluntuottajia huolestuttavat potilasjärjestelmä ja sen tietoturvallinen käyttö tutkimuksessa samoin kuin asiakkaiden anonymiteetti verkkopalveluissa. Osa kantaa huolta kasvavista tietosuojakustannuksista. Henkilöstön kokemien haitta- ja vaaratilanteiden pelätään lisääntyvät erityisryhmiä (muistisairaat, kehitysvammaiset ja mielenterveyspotilaat) koskevassa asiakastyössä.[5]

[4] Tietomurrot palveluntuottajan tietojärjestelmiin ja lähiverkkoon, yms.
[5] Henkilöstön osalta turvallisuusasioita tulisi käsitellä entistä enemmän alan koulutuksessa ja samalla ulkomaalaistaustaisen henkilöstön kielitaitoa tulisi kohentaa.

Kuvio 4 *Hyvinvointialojen turvallisuusalan kyselyyn vastanneiden yritysten ja järjestöjen ennuste turvallisuustilanteen kehityksestä seuraavan 1-2 vuoden aikana, prosenttia vastanneista (Lähde: Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



2.3 Turvallisuusalan tuotteita, palveluja ja järjestelmiä

Perinteisiä palveluja ovat paikallis-, alue- ja piirivartiointi. *Paikallisvartioinnin* kohteita ovat muun muassa tuotantolaitokset ja suuret toimistokokonaisuudet. Vartijat toimivat asiakkaan tiloissa ja työskentelevät usein valvomossa, mistä he teknisin laittein valvovat koko kiinteistöä ja siellä liikkuvia henkilöitä. *Aluevartiointi* on teollisuusalueiden ja vastaavien alueiden jatkuvaa kiertävää vartiointia tai se on osa kauppakeskusten tai liikealueiden yritysten yhteistä vartiointijärjestelmää, jonka tarkoituksena on ehkäistä näpistelyjä ja ilkivaltaa.

Piirivartioinnissa vartijat tekevät tarkastuskierroksia asiakkaiden kohteissa (kiinteistöt, työmaat) usein yöaikaan. Piirivartioinnin tarkoituksena on ehkäistä riskien toteutumista ja rajoittaa jo syntyneiden vahinkojen laajuutta. Piirivartijan tehtäviä ovat ikkunoiden, ovien ja porttien avaus- ja sulkemistehtävät, laitteiden päälle- ja poiskytkennät, palo- ja kiinteistöriskien ehkäisy sekä erilaiset tarkastus- ja hälytystehtävät. Piirivartijat tekevät myös muutakin valvontaa, mikä voi liittyä esimerkiksi tiloissa tai alueella havaittuihin henkilöihin.

Oman osaamisalueensa muodostavat *myymäläturvallisuuspalvelut***.** Niiden tavoitteena on vähentää kaupan hävikkiä, luoda henkilökunnalle sekä asiakkaille turvallinen ja viihtyisä kaupankäyntiympäristö sekä vapauttaa kaupan oma henkilöstö kaupan asiakaspalveluun. Myymälöiden turvallisuuspalvelut voivat sisältää turvapainikepalvelua, myymäläetsivätoimintaa, poistumistarkastuksia, koeostopalveluja ja henkilökunnan turvallisuuskoulutusta. Myymäläturvallisuus on kuitenkin turvallisuuden toimiala, joka ei koske hyvinvointialoja.

Henkilösidonnaisia turvallisuuspalveluja ovat myös turvatarkastukset, tapahtumaturvallisuus, rahan ja arvoesineiden kuljetus ja käsittely. *Turvatarkastus* on lentokentillä, laivaterminaaleissa, urheilutapahtumissa, konserteissa, oikeuslaitoksissa ym. isoissa tapahtumissa tapahtuvaa henkilöihin ja näiden mukana kulkeviin tavaroihin kohdistuvaa tarkastusta. *Tapahtumaturvallisuus* on sen sijaan järjestysmiestoimintaa, jota tehdään joskus yhteistyössä poliisin kanssa muun muassa urheilu- ja kulttuuritapahtumien tai messujen yhteydessä.[6]

Laveasti määriteltynä tapahtumaturvallisuus on osa *järjestyksenvalvontaa*, jota harjoitetaan kaikissa julkisissa ja yksityisissä tiloissa sekä tilaisuuksissa, kuten muun muassa kauppakeskuksissa, liikenneasemilla ja liikennevälineissä, toreilla tai ravintoloissa. Järjestyksenvalvojat ylläpitävät pelkällä läsnäolollaan turvallisuuden tunnetta, ennaltaehkäisevät rikoksia ja onnettomuuksia. Järjestyksenvalvojilla on tehtävään asianomainen koulutus ja he pystyvät tarvittaessa antamaan ensiapua onnettomuus- ja muissa kriisitilanteissa.

Läpivalaisu- ja skannausratkaisuja (röntgenkuvausjärjestelmät) hyödynnetään esimerkiksi henkilöiden läpivalaisussa (turvatarkastus), liikennevälineissä käsimatkatavaroiden ja ruumaan menevien matkatavaroiden läpivalaisussa, pakettien ja kirjeiden läpivalaisussa sekä rahdin, konttien ja ajoneuvojen läpivalaisussa. Aiemmin pitkään ainoastaan terveydenhuollossa käytetyillä röntgenkuvauslaitteilla on pyritty vastaamaan uusiin uhkakuviin (terroristiriskit) ja lisäämään turvallisuuden tunnetta muun muassa liikennevälineissä (lentoliikenne).

Rahan ja arvoesineiden kuljetus on turvakuljetustyötä, jota harjoitetaan tarkoitusta varten varatuilla ajoneuvoilla. Siinä työntekijät ovat tavallisesti vartijakoulutuksen saaneita henkilöitä. Myös rahanlaskenta ja muu käsittelypalvelu voi olla osa palvelua. *Vahtimestari- ja aulapalvelut* käsittävät vieraiden vastaanottoa, asiakaspalvelua ja neuvontaa, ovien avaamista ja sulkemista sekä varsin usein myös postitustyötä, puhelinvaihdetoimintaa, tilajärjestelyistä ja tarjoiluista huolehtimista sekä esimerkiksi kiinteistöjen pieniä teknisiä korjauksia.

Vartiointipalveluun yhdistetään teknisin laittein ja järjestelmin tapahtuvaa kohteiden valvontaa, jossa järjestelmä siirtää valvonta- ja hälytystiedon hälytyskeskukseen (etävalvonta). *Hälytyskeskuspalvelulla* (hälytysvalvonta) tarkoitetaan teknisten ilmaisimien antamien hälytysten vastaanottamista ja niiden edelleen välitystä. Hälytyskeskusten toimintaan kuuluu päivystyspalveluita taikka ohjauksia porteille ja oville sekä toimintaa, joka liittyy rikosturvallisuuden ohella muuhun valvontaan (ilmastointi-, lämmitys- ja kylmälaitteet, ym.).[7]

Sähköteknisiä turvajärjestelmiä ovat kameravalvonta-, murtohälytys-, kulunvalvonta- ja työajanseurantajärjestelmät sekä äänentoisto- ja kuulutusjärjestelmät[8]. Muita

[6] Tapahtumaturvallisuuteen voi liittyä pelastussuunnitelmien laadintaa, viranomaisten lupa-asioiden hoitoa ja turvatarkastuksia.

[7] Sisältää myös valvonta- ja hälytysjärjestelmien asennus- ja huoltopalvelut sekä mekaanisten tai sähköisten lukituslaitteiden, kassakaappien ja –holvien asennuksen, korjauksen ja säädön, jos palvelut tuotetaan etävalvontana. Etävalvontatehtävissä hyödynnetään muun muassa valvontakameroita ja muita automaattiseen tunnistamiseen liittyvää teknologiaa

[8] Äänentoisto- ja kuulutusjärjestelmät ovat erilaisiin vaaratilanteisiin ja toimitilojen yleiseen turvallisuuteen liittyviä äänievakuointi- tai vastaavia järjestelmiä, joilla tavoitetaan henkilöt huoneista, sosiaalitiloista ja muista yleisistä tiloista, porraskäytävistä sekä ovi- ja porttialueilta. Niihin liittyy myös paikannustekniikkaa.

sähköisiä turvajärjestelmiä ovat esimerkiksi turvavalaistus. *Rikoshälytysjärjestelmät* ovat teknisiä turvajärjestelmiä, joihin voi liittyä yhteyksiä valvomoihin ja mahdollisesti myös viranomaisiin (poliisi). Rikoshälytysjärjestelmillä valvotaan kiinteistöä ennen kaikkea silloin, kun kiinteistö on tyhjillään (vrt. kuitenkin myös 24 h/vrk aktiivisesti toimiva kiinteistö).

Kameravalvontajärjestelmät (valoisa- / pimeäkuvaus) ovat teknisiä turvajärjestelmiä, joihin voi sisältyä hahmon, tekstin tai esineen havainnointia ja/tai tunnistusta sekä tietojen tallentamista ja käsittelyä (henkilötiedot tai muuten rajoitetut tai salassa pidettävät tiedot). Kameravalvonnan käyttöä rajoittavat työelämän tietosuoja- ja tietolaki yms. *Kulunvalvontajärjestelmällä* ohjataan (oikeutetaan tai rajoitetaan) henkilöiden liikkumista. Kulunvalvontajärjestelmiin voi liittyä yhteyksiä valvomoihin ja niihin voi sisältyä työajanseurantaa.

Konsultointipalveluja ovat riskikartoitukset ja turvallisuusauditioinnit, yritysten ja henkilöiden taustaselvitykset, turvallisuuspäällikköpalvelut, tietoturvallisuuden ja tietosuojan konsultointia, turvallisuuspalvelujen ja –tuotteiden kilpailuttamisen konsultointia, kriisiviestinnän ja –johtamisen konsulttipalveluja sekä turvallisuussuunnitelmien ja –ohjeiden laadintaa. *Koulutustoiminta*[9] on määritelmällisesti turvallisuuden kurssitusta tai käyttökoulutusta turvajärjestelmiin ja –palveluihin, ja se sisältää mahdollisesti myös ohjattua itseopiskelua.[10]

Rakenteellisiin turvallisuustuotteisiin kuuluvat lukitusjärjestelmät ja oviautomatiikka. Lukitusjärjestelmät rakentuvat lukoista, pääsynvalvonnasta (ovi- ja porttipuhelinjärjestelmät), lokitiedoista, tunnistamisvälineistä ja -keinoista. Järjestelmiin vaikuttavat esimerkiksi lokien säilytysvelvoitteet, henkilötietolaki, muut valvontaa ja seurantaa koskevat säännökset. Oviautomatiikkatuotteita ovat muun muassa kääntöovet, liukuovet, balanssiovet, pyöröovet. Tuoteryhmään luetaan myös palo-oviautomatiikka ja ovipuhelinjärjestelmät.

Porttiautomatiikkatuotteita ovat ajoneuvo- ja rekkaliikenteelle soveltuvat liuku- ja saranaportit, joita käytetään logistiikkakeskuksissa, liikennekeskuksissa, teollisuuden ja kaupan varastoalueilla ja noutopihoilla. Porttiautomatiikka voi olla osa kiinteistön kulunvalvontaa ja se voi sopia myös pientaloihin. *Puomitekniikkatuotteita* ovat sähköhydraulisia tai sähkömekaanisia koneistoja ja nostopuomeja, jotka soveltuvat ajoneuvojen kulunohjaukseen. Muita rakenteellisia turvatuotteita ovat esimerkiksi erikoislasit ja kalterit, holvit, suoja-aidat ja esteet.

Oman erillisen tuoteryhmänsä muodostavat toisaalta paloilmoitin- ja varoitinjärjestelmät sekä toisaalta paloturvallisuus- ja väestönsuojelutuotteet. *Paloilmoitin- ja varoitinjärjestelmät* koostuvat palo- ja pelastustoimen järjestelmistä ja tunnistimista, kuten palohälyttimistä, palovaroittimista ja savunilmaisimista. *Paloturvallisuus- ja väestönsuojelutuotteisiin* kuuluvat esimerkiksi alkusammutusvälineet, peitteet, letkut, säiliöt, paloturvakaapit, ja suojavarusteet (suojavaatteet, -käsineet ja –jalkineet) väestösuojatilojen laitteet ja –tuotteet.

---

[9] Turvallisuuskoulutuksella ei tarkoiteta tässä tutkintoon johtavaa julkisten tai yksityisten oppilaitosten tuottamaa (julkisrahoitteista) peruskoulutusta tai täydennys- ja jatkokoulutusta.

[10] Koulutusta ovat muun muassa turvallisuusjohtamis- ja riskienhallintakoulutus, työturvallisuuskoulutus, tietoturvallisuuskoulutus, paloturvallisuus-, tulityö- ja väestönsuojelukoulutus, ensiapukoulutus, järjestyksenvalvoja- ja voimankäyttökoulutus.

Tietoturvallisuutta[11] ovat palomuuri- ja virustorjuntaohjelmistot ja –järjestelmät (ml. lisenssit), roskapostinsuodatus ja maksunvarmennuspalvelut, tietoturva- ja serverikaapit, tuhoojat ja tuhoamispalvelut, varkaudenestolaitteet sekä atk-laitteiden varavoimajärjestelmät, tietoliikenteen ja tiedon salausratkaisut, tietoliikenneverkot ja palvelimet, käyttäjien tunnistamisratkaisut, ja Data Mining –tuotteet. Tietoturvallisuus käsittää myös erilaisia raportointijärjestelmiä, asennus- sekä valvontapalveluja, konsultointia ja neuvontaa.

Edellä mainittujen tuoteryhmien ulkopuolella on pienempiä tuoteryhmiä, kuten esimerkiksi *työturvallisuustuotteet.* Työturvallisuustuotteita ovat muun muassa hengityssuojaimet, turvajalkineet ja suojavaatteet, ensiapuvälineet, turvakilvet ja opaste, turvavaljaat ja -varusteet. Muita turvatuotteita ovat myös *etsivätoiminta ja henkilösuojauspalvelut* (turvamiehet ja henkivartijat). Edellä mainituista turvallisuusalan hyödykeryhmistä hyvinvointialojen kyselyissä turvallisuuspalvelut ja -tuotteet on luokiteltu karkeasti 16 pääryhmään, jotka ovat

- *rikoshälytysjärjestelmät*
- *kulunvalvonta- ja työajanseurantajärjestelmät*
- *kameravalvontajärjestelmät*
- *paloilmoitin- ja varoitinjärjestelmät*
- *lukitusjärjestelmät (mekaaninen)*
- *lukitusjärjestelmät (elektromekaaninen ja digitaalinen)*
- *oviautomatiikka*
- *etähallinta- ja valvontapalvelut (järjestelmien tilan valvonta)*
- *hälytyskeskuspalvelut*
- *vartiointipalvelut*
- *vahtimestari- ja aulapalvelut*
- *työsuojelutuotteet, suojavarusteet ja -asut*
- *tietoturvaturvallisuus (tuotteet, palvelut, järjestelmät)*
- *tietoturvallisuuskoulutus*
- *muu turvallisuuskoulutus*
- *turvallisuussuunnittelu ja -konsultointi.*

Turvallisuusalan hyödykeryhmistä kyselyn ulkopuolelle on jätetty myymäläturvallisuuspalvelut, turvatarkastus, tapahtumaturvallisuus, portti- ja puomiautomatiikka, rahan ja arvoesineiden kuljetus, läpivalaisu- ja skannaustekniset ratkaisut, äänentoisto- ja kuulutusjärjestelmät sekä tavanomaiset paloturvallisuus- ja väestönsuojelutuotteet (pl. sähköiset palovaroittimet). Tosin tavanomaisten paloturvallisuustuotteiden tulisi kuulua kaikissa kiinteistöissä vakiovarusteisiin ja myös äänentoisto- ja kuulutusjärjestelmillä voi olla käyttöä palvelulaitoksissa.[12]

[11] Laveasti määriteltynä tietoturvallisuus on tiedon turvaamista luvatonta käyttöä, tiedon vääriin käsiin joutumista, tiedon muunnosta tai tiedon tuhoutumista vastaan. Tietoturvallisuutta käsitellään tarkemmin luvussa 4.4.

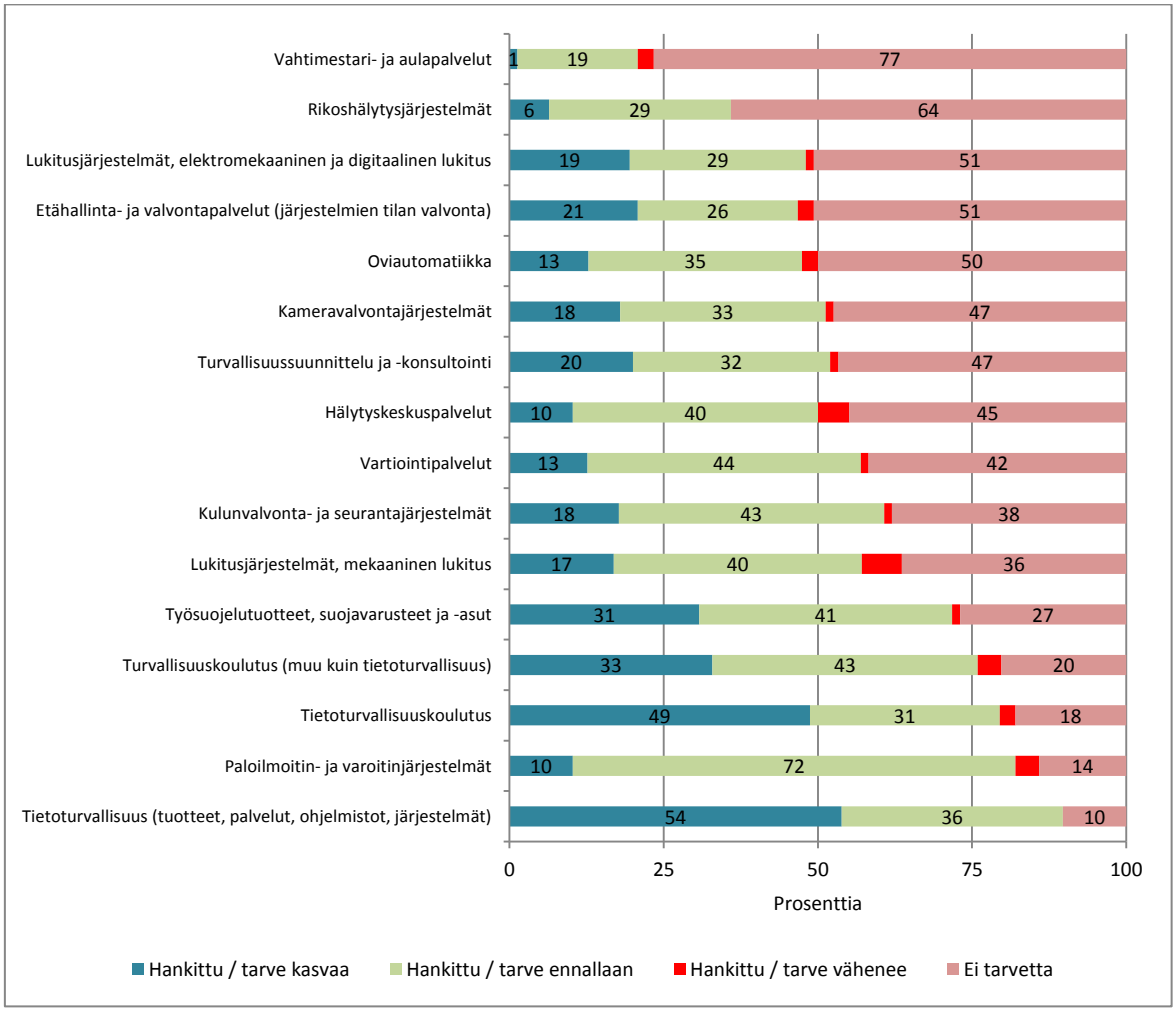
[12] Toisaalta kannattaa muistaa, että hyvinvointialoilla **kiinteistöjen omistajat** voivat olla muita kuin varsinaisia hyvinvointipalvelujen tuottajia, jotka vastaavat toimitilojen teknisistä turvallisuuspalveluista samoin kuin toimitilojen käyttäjäpalveluihin liittyvistä vartiointi, vahtimestari- ja aulapalveluista.

2.4 Turvallisuushyödykkeiden kysyntä hyvinvointialoilla

Hyvinvointialojen turvallisuuskyselyyn vastanneista 90 prosenttia ilmoitti hankkineensa tietoturvallisuustuotteita, palveluja ja järjestelmiä viime vuosina. Paloilmoitus- ja varoitinjärjestelmiä oli hankkinut 86 prosenttia. Vähintään 80 prosenttia oli ostanut tietoturvallisuuskoulutusta ja muuta turvallisuuskoulutusta omalle henkilöstölleen, mitä voidaan pitää myönteisenä asiana. Nämä turvallisuustuotteet ja -palvelut kohdistuvat sellaisiin asioihin, joilla voidaan pienentää hyvinvointialojen keskeisiä turvallisuusuhkia ja onnettomuusriskejä.

Työsuojelutuotteita (ml. suojavarusteet ja –asusteet), mekaanisia lukitusjärjestelmiä, kulunvalvonta- ja seurantajärjestelmiä, työsuojelutuotteita, suojavarusteita ja -asuja oli hankkinut vähintään 60 prosenttia vastanneista. Myös kameravalvontajärjestelmien, hälytyskeskus- ja vartiointipalvelujen sekä turvallisuussuunnittelu ja –konsultoinnin hankkiminen ulkoa on melko yleistä, sillä niitäkin oli ostanut yli puolet hyvinvointialojen palveluntuottajista. Vähiten on ostettu rikoshälytysjärjestelmiä sekä vahtimestari- ja aulapalveluja.

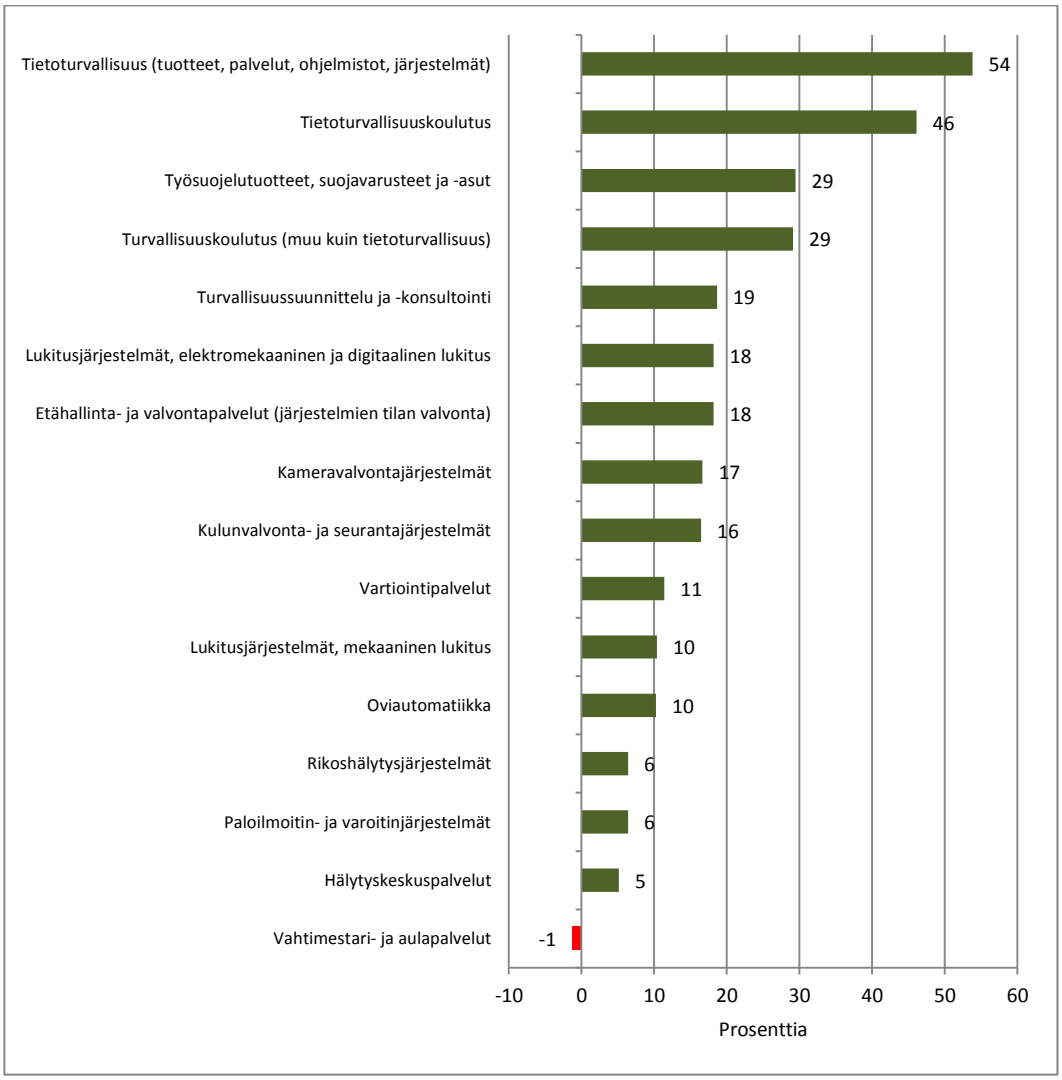
Kuvio 5 *Hyvinvointialojen turvallisuusalan kyselyyn vastanneiden yritysten ja järjestöjen näkemys turvallisuusalan tuotteiden, palvelujen ja järjestelmien kysyntänäkemyksistä lähivuosina, prosenttia vastanneista (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



Alan tuotteiden, palvelujen ja järjestelmien kysyntänäkemykset säilyvät hyvinvointialoilla varsin hyvinä lähivuosina. Kysyntänäkymien saldoluvut ovat plussalla kaikkien hyödykeryhmien osalta lukuun ottamatta vahtimestari- ja aulapalveluja, joita hyödynnetään muutoinkin varsin vähän. Saldoluku saadaan, kun kysynnän kasvua ennakoivien prosenttiosuudesta vähennetään kysynnän laskua ennakoivien prosenttiosuus. Parhaimmat ne ovat tietoturvallisuustuotteissa, palveluissa ja järjestelmissä sekä tietoturvallisuuskoulutuksessa.

Kysyntänäkymät ovat hyviä myös työsuojelutuotteissa ja muussa turvallisuuskoulutuksessa (pl. tietoturvallisuus). Selvää kasvua on nähtävissä lisäksi turvallisuuden konsulttipalveluissa, elektromekaanisissa lukitusjärjestelmissä, etähallinta- ja valvontapalveluissa, kameravalvontajärjestelmissä sekä kulunvalvonta- ja seurantajärjestelmissä. Ulkoa hankittaviin turvallisuusalan hyödykkeiden koostumukseen vaikuttaa organisaation toimiala. Jos palvelutoiminta ei tarvitse suuria toimitiloja, hankintojen kirjo on kapeammalla pohjalla.

Kuvio 6 *Hyvinvointialojen turvallisuusalan kyselyyn vastanneiden yritysten ja järjestöjen näkemys turvallisuusalan tuotteiden, palvelujen ja järjestelmien kysyntänäkemyksistä lähivuosina saldolukuina, prosenttia (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



3 Tietoturvallisuus hyvinvointialoilla

Hyvinvointialojen vuoden 2021 turvallisuuskyselyssä ajankohtaisten uhkakuvien ja riskien puolella tärkeimmäksi nousi pilvipalvelujen turvallisuus. Riskit liittyvät tietojen luottamuksellisuuteen, kun tiedot ja sovellukset on hajautettu ympäri maailmaa ja samat palvelut ovat usean käyttäjän hyödynnettävissä. Myös pilvipalvelujen tarjoajilla voi olla pääsy tärkeisiin tietoihin.

Hallinnollisen tietoturvallisuuden osalta vastaajat korostivat SoTe-alojen omavalvontaa, organisaation omiin lähtökohtiin pohjautuvaa sisäistä tietoturvakoulutusta, tietoturvaohjeiston kehittämistä ja tietoturvallisuuden standardien mukaisuutta. Noin 90 prosentilla vastanneista tietoturva-asiat oli kirjattu erilliseen tietoturvastrategiaan tai organisaation yleiseen strategiaan.

Lähes kaksi kolmasosaa kyselyyn vastanneista oli sitä mieltä, että sosiaali- ja terveydenhuollossa yhteisten tietoturvan minimivaatimusten määrittelyllä voidaan tehokkaasti parantaa potilas- ja asiakastietojen tietoturvan tasoa ja selkeyttää sitä, millaisia toimenpiteitä kaikilta sosiaali- ja terveydenhuollon toimijoilta edellytetään tietojen suojaamiseksi.

3.1 Verkkorikollisuuden ilmenemismuodot ja laajuus

Organisaatioissa on usein harhakäsityksiä toimintaan sisältyvistä riskeistä ja turvallisuudesta. Vaaroja, jotka ovat harvinaisia, abstrakteja tai pelottavia, kuten säteilyonnettomuudet ja terrorismi, yliarvioidaan ja niistä puhutaan paljon. Sen sijaan tuttuihin töihin, tilanteisiin ja toistuviin asioihin liittyviä vaaroja, kuten verkkoympäristössä liikkumiseen sisältyviä riskejä vähätellään. Silti yhteiskunta perustuu teknologiaan, toimintatapoihin ja osaamiseen, jossa tiedon tuottamisella, jakelulla, käsittelyllä ja tietoturvallisuudella on tärkeä merkitys.

Tietoturvallisuutta on tietojen, järjestelmien ja palvelujen suojaus hallinnollisten ja teknisten toimenpiteiden avulla. Tietoturva rakentuu tiedon *luottamuksellisuuden* (confidentiality), *eheyden* (integrity) ja *käytettävyyden* (availability) pohjalle. Luottamuksellisuus tarkoittaa sitä, että tietoa voivat käsitellä vain henkilöt, joilla on siihen oikeus. Tiedon eheydellä ymmärretään sitä, että tieto ei saisi muuttua tahattomasti tai tahallisesti, tai muutokset pitäisi ainakin havaita. Käytettävyys tarkoittaa, että tarvittava tieto on saatavilla silloin kuin sitä tarvitaan.

Tietoturvallisuuden tavoitteena on asiantila, joissa tiedon käytettävyyteen, eheyteen ja käytettävyyteen ei kohdistu merkittäviä riskejä. Riskit koostuvat siitä, että edellä mainitut tiedon ominaisuudet ovat vaarantuneet tai vaarantumassa tahattomien tai tahallisten tapahtumien vuoksi. Esimerkiksi verkkorikolliset keksivät jatkuvasti uusia keinoja, joilla huijataan yksityisiä henkilöitä, yrityksiä ja julkisyhteisöjä, sillä sähköposti ja Internet tarjoavat lukemattomia mahdollisuuksia tavoittaa suuria ihmismääriä lähes olemattomin kustannuksin.

Liikenne- ja viestintävirasto *Traficomin* mukaan tietoturvallisuutta vaarantavat esimerkiksi *tietojenkalastelu* (eng. phishing), jonka tavoitteena on saada rikollisten haltuun käyttäjätunnus- ja salasanapareja tai muita käyttäjälle tai organisaatiolle arvokkaita tietoja, kuten maksukorttitietoja. Verkkopalvelun käyttäjä voidaan huijata vierailemaan rikollisten tekemällä internetsivustolla, joka muistuttaa ulkoasultaan palvelun aitoa sisäänkirjautumisen sivustoa. Kun käyttäjä syöttää tiedot huijaussivustolle, ne päätyvät rikollisten käyttöön.

Useimmiten rikolliset pyrkivät huijaamaan itselleen mahdollisimman monta sähköpostitunnusta. Tämän jälkeen he kirjautuvat tileille ja etsivät laskutukseen liittyviä hakusanoja. Näiden tietojen pohjalta luodaan valelaskuja, jossa hyödynnetään oikean laskun tietoja ja kontekstia. Tiliä voidaan hyödyntää uusiin tietojenkalasteluviesteihin, joita lähetetään uhrin kontakteille. Varastetuilla käyttäjätunnuksilla on puolestaan mahdollista vakoilla yrityssalaisuuksia. Onnistuneeseen tietojenkalasteluun voi liittyä myös maine- ja sääntelyriskejä.

Haittaohjelmat ovat sen sijaan tietokoneohjelmia, jotka aiheuttavat ei-toivottuja tapahtumia tietojärjestelmässä tai sen osissa. Haittaohjelmat leviävät sähköpostien liitetiedostojen, haittaohjelmilla saastutettujen verkkosivustojen sekä haavoittuvien palvelinten kautta. Hyökkäyksessä rikollinen tunkeutuu organisaation järjestelmiin ja levittäytyy sen verkkoon. Lopuksi hyökkääjä voi käynnistää salatun kiristyshaittaohjelman, joka haittaa organisaation toimintaa tai lamauttaa sen lähes kokonaan ja kiristää lunnaita salauksen purkamiseksi.

Traficomin mukaan *palvelunestohyökkäykset* ovat internetissä arkipäivää. Palvelunestohyökkäyksessä verkkoa kuormitetaan ylimääräisellä tietoliikenteellä. Tavoitteena on lamaannuttaa jokin palvelu tai tietojärjestelmä. Usein hyökkäyksen kohteena on organisaation julkinen Internetsivusto tai esimerkiksi asiakkaiden hyödyntämä palvelu. Hyökkäykset kestävät yleensä niin kauan kuin niillä on vaikutusta kohteen toimintaan. Useimmiten ne loppuvat, kun palvelunestohyökkäys saadaan torjuttua ja palvelun toiminta palautettua entiselleen.[13]

Suurin osa kohdatuista tietoturvauhkista ei kohdistu yhteen ja tietoisesti valittuun organisaatioon. Verkkorikollisuus on luonteeltaan varsin opportunistista. Tavoitteena on lähinnä löytää organisaatioiden järjestelmistä ja prosesseista heikkouksia, joita voi hyödyntää rikolliseen tarkoitukseen ja nopeaan rahan saantiin. Toiminta on usein kansainvälistä ja pitkälle automatisoitua. Ongelmia on pahentanut teknologian yhdenmukaistuminen ja tietojärjestelmien yhä enenevä yhteen liittäminen, mikä on tehnyt niistä entistä haavoittuvampia.

Verkkohyökkäyksille on hyvin tunnusomaista, että vain osa tulee poliisin tietoon ja tutkittavaksi. Osa yrityksistä ja yhteisöistä ei edes ilmoita rikoksista viranomaiselle, koska ne haluavat varjella julkisuuskuvansa. Toisaalta taitavasti tehtyjä verkkorikoksia ei aina edes huomata. Toisaalta verkkohyökkäysten tarkoituksena voivat olla joskus vain kiusanteko tai suoranainen vandalismi, hakkerin näyttämisen halu tai maineen kasvattaminen. Myös mobiilien päätelaitteiden ja mobiilisovellusten kasvu on kiinnostanut verkkorikollisia.[14]

Verkkorikollisuuden oikeudellinen kehys

Verkkorikollisuutta ei ole määritelty tyhjentävästi lainsäädännössä johtuen sen monimuotoisuudesta. Suomessa tietoturvarikokset (loukkaukset) määritellään rikos-

[13] Hyökkäyksistä tietojärjestelmiä, organisaatioita ja yksityishenkilöitä vastaan käytetään nimitystä **haktivismi** (eng. *hacktivism*). Se tarkoittaa tietoverkossa aktivismia eli toimintaa, jolla halutaan saada aikaan huomiota tai muutosta johonkin tiettyyn asiaan. Termi koostuu sanoista hakkeri ja aktivismi. Haktivismia on esimerkiksi www-palveluun murtautuminen ja sen sotkeminen.

[14] Esimerkiksi älypuhelimet tietävät käyttäjästään paljon yksityiskohtaisia tietoja, minkä vuoksi niistä on tullut tärkeä haittaohjelmien kohde. Varsinkin mobiilipankkiasiakkaiden kasvu ja yritysten lisäämät toiminnallisuudet mobiilisovelluksiin ovat lisänneet osaltaan rikollisten kiinnostusta asiaan.

laissa (39/1889) ja niistä on säädetty rangaistuksiksi sakkoa tai vankeutta. Kun käyttää luvatta toisen käyttäjätunnusta ja salasanaa syyllistyy *tietomurtoon* (RL 38:8§ ja 8§a**)**. Tietomurroksi riittää, kun käyttää luvatta toisen oikeuksia ja ylittää omat oikeutensa. Tietomurto tulkitaan törkeäksi, jos se on erityisen suunnitelmallista tai osa järjestäytyneen rikollisryhmän toimintaa.

Viestintäsalaisuuden loukkaukseen (RL 38:3§) syyllistytään esimerkiksi silloin, jos avaa toiselle osoitetun viestin, taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta ja ulkopuoliselta suojatusta viestistä. Teon törkeästä muodosta (RL 38:4§) on kysymys silloin, kun rikoksen tekemiseen käytetään tarkoitusta varten suunniteltua atk-ohjelmaa, teknistä laitetta, rikos tehdään erityisen suunnitelmallisesti tai rikoksen kohteena oleva viesti on luokiteltu erityisen luottamukselliseksi.

Tietojärjestelmän häirinnällä (RL 38:7§-7b§) tarkoitetaan tapauksia, joissa toiselle aiheutetaan haittaa tai taloudellista vahinkoa dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla tavalla, jolla oikeudettomasti estetään häirinnänkohteena olevan tietojärjestelmän toimintaa. Törkeän tietojärjestelmän tunnusmerkkejä ovat tuntuvan haitan tai taloudellisen vahingon aiheuttaminen, rikoksen tekeminen suunnitelmallisella tavalla tai rikoksen kohdistaminen yhteiskunnallisesti tärkeään toimintoon.

Kysymys on *datavahingonteosta* (RL 35:3a§-3c§), kun toisen tietokoneelle asennetaan omia tarkoitusperiä palvelevia ohjelmia eli toista vahingoittaakseen hävitetään, turmellaan, kätketään, vahingoitetaan, muutetaan, tehdään käyttökelvottomaksi tai salataan tietovälineelle tallennettua tietoa tai muuta tallennusta taikka tietojärjestelmässä olevaa dataa. Vahingonteosta on säädetty rikoslaissa törkeä muoto, jos kohteelle aiheutetaan tuntuvaa haittaa ja taloudellisia tappioita tai rikos kohdistuu yhteiskunnallisesti tärkeään tietojärjestelmään.

Rikoslain tieto- ja viestintärikoksiin sisältyvät myös *salassapitorikokset* (RL 38:1§), *salassapitorikkomukset* (RL 38:2§) ja *identiteettivarkaudet* (RL 38:9a§). Uusimpina rikosmuotoina ovat *tietosuojarikokse*t (RL 38:9§). Näistä identiteettivarkauksilla tarkoitetaan rikoslaissa tapauksia, joissa pyritään erehdyttämään kolmatta osapuolta käyttämällä oikeudettomasti toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja tällä tavoin aiheutetaan taloudellista vahinkoa tai vähäistä suurempaa haittaa sille henkilölle, joita tiedot koskevat.

Tietotekniikkaa hyödyntäviä muita rikosmuotoja on paljon, vaikka kysymys ei olisikaan varsinaisesta verkkorikollisuudesta. Esimerkkeinä ovat tekijänoikeusrikokset. Lainsäädäntö (*tekijänoikeuslaki 404/1961*) siitä, että verkkosivuille ei saa laittaa tekijänoikeuden suojaamaa aineistoa ilman lupaa. Tietoverkosta ei saisi myöskään kopioida vapaasti tietoaineistoja ansiotarkoituksiin tai edes omaan käyttöön silloin, jos aineistossa on tietomurron estävä suojaus. Lisäksi tiedostojen jakelu verkossa on kiellettyä ilman tekijänoikeuden haltijan lupaa.

Tietoverkossa tapahtuvan toiminnan oikeudelliseen kehykseen kuuluvat EU:n verkko- ja tietoturvadirektiivi (NIS-direktiivi), EU:n yleinen tietosuoja-asetus ja kansallinen *tietosuojalaki (1050/2018)*. NIS-direktiivillä on pyritty varmistamaan korkeatasoinen verkko- ja tietojärjestelmien turvallisuus koko EU:n alueella, sillä direktii-

vissä on säädetty tietoturvavelvollisuuksista ja häiriöraportoinnista. Direktiivi velvoittaa muun muassa keskeiset digitaalisten palvelujen tarjoajat kattavaan verkko- ja tietoturvallisuusriskien hallintaan.

EU:n yleisessä tietosuoja-asetuksessa[15] on sen sijaan asetettu yrityksille ja organisaatioille vaatimuksia henkilötietojen keruuta, säilytystä ja hallintoa varten. Kansallinen henkilötietojen käsittelyä koskeva tietosuojalaki puolestaan täsmentää ja täydentää EU:n tietosuoja-asetusta, vaikka se ei muodosta itsenäistä ja kattavaa sääntelykokonaisuutta, vaan sitä sovelletaan rinnakkain tietosuoja-asetuksen kanssa. Myös *laissa sähköisen viestinnän palveluista (917/2014*) on säädetty tietoturvaan ja luottamuksellisen viestinnän suojaan liittyvistä asioista.

Keskeisenä viranomaistoimijana tietoturva-asioissa toimii liikenne- ja viestintävirasto (Traficom) **Kyberturvallisuuskeskus**, joka kerää tietoa tietoturvaloukkauksista, tiedottaa tietoturva-asioista, selvittää verkko- ja viestintäpalveluihin kohdistuvia uhkia, suorittaa järjestelmien ja verkkojen tarkastuksia sekä valvoo teleyritysten toimintaa ja sähköisen viestinnän yksityisyyden suojaa koskevien velvoitteiden täyttymistä. Tietoverkkorikosten osalta toimijoita ovat paikallispoliisi, koko valtakunnan osalta keskusrikospoliisi ja suojelupoliisi.

Verkkorikosten määrä ja tilastointi

Varsinaisten tietoturvarikosten määrästä ei ole olemassa kattavia tilastotietoa. Satunnaisten hyökkäysten määrästä on ollut saatavilla jotain tilastoja Viestintäviraston Kyberturvallisuuskeskuksen yhteydenottotiedoista. Tilastokeskuksen oikeustilastot kuvaavat sen sijaan poliisin tietoon tulleita rikoksia. Yhteensä poliisin tietoon tuli noin 6 030 tietoturvarikosta (ml. datavahingonteot) vuonna 2020. Niistä 71 prosenttia oli identiteettivarkauksia. Ilman identiteettivarkauksia poliisin tietoon tulleita verkkorikoksia oli 1 740 vuonna 2020 (Taulukko 2).

Vuosina 2016-20 verkkorikosten määrä lisääntyi peräti 50 prosentilla, jos identiteettivarkauksia ei oteta tilastossa huomioon. Suhteellisesti eniten lisääntyivät tietomurrot ja tietomurron yritykset. Sen sijaan datavahingonteot, viestintäsalaisuuden loukkaukset, tietojärjestelmien häirintään liittyvät rikokset ja tietosuojarikokset vähenivät. Tosin kaikki tietoturvarikokset eivät tule poliisin tietoon ja myös poliisin hallinnollisesti tilastoimiin tietoverkkorikoksiin liittyy useita ongelmia, sillä rikostilastointi suoritetaan rikosnimikkeittäin.[16]

Yrityksiin kohdistuvien kyberturvallisuuden uhkista antaa käsityksen se, että Helsingin seudun kauppakamarin vuonna 2019 tekemän kyselytutkimuksen mukaan yli 60 prosenttia piti phishing- ja haittaohjelmahyökkäyksiä suurimpina tietoturvauhkinaan. Toiseksi eniten pelätään yrityksen luottamuksellisen tiedon vuotamista. Kolmanneksi suurimpina tietoturvauhkina olivat palvelunestohyökkäykset. Selvitys antaa kuitenkin lohduttoman käsityksen kyberuhkiin varautumisesta ja siinä tapahtuneesta kehityksestä viime vuosina.

Selvityksen mukaan yritysten joukossa on suuri määrä helppoja kyberturvattomia kohteita, jotka eivät ole pitäneet huolta digitaalisesta yritysvastuustaan osana tieto-

[15] Euroopan parlamentin ja neuvoston asetus 679/2016.

[16] Yhtenä esimerkkinä näistä ovat tietomurrot. Jos rikoksen tekijä on onnistunut teossaan, täyttyvät jonkin muun rikosnimikkeen edellytykset ja tietomurto muuttuu tilastoissa toiseksi rikosnimikkeeksi jo esitutkinnan aikana.

verkkojen yhdistämää yhteiskuntaa. Luotettavan tiedon saanti tietoturvauhista ja niihin varautumisesta on ensiarvoisen tärkeää, mutta esimerkiksi viranomaisten tuottama tieto ei tavoita yrityksiä riittävästi. Ongelmat ovat suurimpia pk-yrityksissä, mutta verkottuneessa yhteiskunnassa koolla ei ole väliä. Syynä on, että alihankintaketjut on valittu tietoisesti kyberhyökkäysten kohteiksi.

Taulukko 2 Poliisin tietoon tulleet verkkorikokset 2020 (Lähde: Oikeustilastot, Tilastokeskus).

	Lkm 2020[17]	Kasvu 2016-20, lkm	Kasvu 2016-20, %	Osuus (ml. idenditeetti-rikokset), %	Osuus (pl. identideetti-rikokset), %
Datavahingonteko	15	-2	-11,8	0,2	0,9
Salassapitorikos ja -rikkomus	73	12	19,7	1,2	4,2
Viestintäsalaisuuden loukkaus	312	-97	-23,7	5,2	17,9
Tietoliikenteen häirintä	88	2	2,3	1,5	5,1
Tietojärjestelmän häirintä	22	-32	-59,3	0,4	1,3
Tietomurron yritys	66	53	407,7	1,1	3,8
Tietomurto	1083	665	159,1	18,0	62,2
Tietosuojarikos	83	-20	-19,4	1,4	4,8
Identiteettivarkaus	4284	976	29,5	71,1	-
Yhteensä	**6026**	**1557**	**34,8**	**100,0**	**100,0**

3.2 Tietoturvallisuuden kehittämistarpeet

Tietoturvallisuuden merkitys ja siihen liittyvät uhkakuvat ovat korostuneet kaikissa turvallisuusalan selvityksissä 2010-luvulla ja tietoturvatuotteiden ja –palvelujen kysyntä on pysynyt korkealla tasolla suhdannetilanteesta riippumatta. Elinkeinoelämässä tietoturva on kiinteä osa yritysten kokonaisturvallisuutta, jolla taataan liiketoiminnan häiriötön jatkuvuus. Organisaatioille tieto on tärkeää, mutta sen merkitys ymmärretään useimmiten vasta sitten, kun tieto ei ole saatavilla, se on virheellistä, tai tieto on vuotanut organisaation ulkopuolelle.

Vaatimukset tietoturvasta ovat kasvaneet verkkoliiketoiminnan lisääntymisen myötä. Yksinkertaistettuna tietoturvallisuudesta huolehtiminen on arjen toimintaa, jolla ylläpidetään paitsi tietojen eheyttä, jäljitettävyyttä, oikea-aikaista saatavuutta ja käytettävyyttä sekä yrityksen prosessiohjaus-, tietoliikenne- ja palvelujärjestelmiä, joista koko yritystoiminta voi olla riippuvaista. Tietoturvallisuus on tärkeä osa myös julkisyhteisöjen toimintaa. Julkisyhteisöillä on tietoja, joiden turvaaminen on välttämätöntä jo lainsäädännössä määrättyjen velvoitteiden vuoksi.

Valtiovallalla on muutoinkin laajempi vastuu yleisen toimintaympäristön turvallisuudesta, johon kuuluu olennaisena osana *kyberturvallisuus*.[18] Tästä on osoituksena kyberturvallisuusstrategia ja kyberturvallisuuskeskuksen olemassaolo Liikenne- ja viestintävirasto Traficomissa. Varsinaisesti *kyberturvallisuus* on tavoitetilaa, jossa kyberympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberympäristöön kohdistuvat uhkat ovat tietoturvauhkia, jotka toteutuessaan vaarantavat tietojärjestelmien oikeanlaisen tai tarkoitetun toiminnan.

[17] Sisältää myös rikosten törkeät muodot.

[18] **Kyberympäristö** koostuu yhdestä tai useammasta tietojärjestelmästä (atk- ja tiedonsiirtolaitteista, ohjelmista ja ihmistä koostuva järjestelmä).

Asiantuntijoiden mukaan verkkorikollisuudesta aiheutuvia vahinkoja ennaltaehkäistään perusasioista huolehtimalla ja siten, että rikos havaitaan mahdollisimman pian. Panostukset tietoturvallisuuteen takaavat toiminnan häiriöttömän jatkuvuuden. Tosin lisääntynyt monimutkaisuus edellyttää tietoturvalta toimintamalleja, joiden avulla kokonaisuus on hallittavissa. Tietoturvariskeihin varautuminen ja ennaltaehkäiseminen maksavat, mutta se on pitkässä juoksussa kannattavaa, ja sitä ei minkään yrityksen tai julkisyhteisön ole varaa laiminlyödä

Varsinkin pk-yritykset ja yrittäjät saattavat keskittyä tietoturvassa korkeintaan vain ostettuun tekniikkaan. Tunne turvallisuudesta ostetaan palomuurilla ja virustorjunnalla, vaikka uhkakuvat ovat muuttuneet. Oma tietoturva koetaan hyväksi, vaikka yritykseltä puuttuisi kokonaan tietoturvastrategia ja -politiikka. Osasyynä on, että tietoturvaan liittyvä tietämys ei ole jokamiehen osaamisaluetta. Pienyrityksissä tietoturvauhat ovat silti samoja kuin suurissa organisaatioissa ja tietoturvan edellyttämä hallinnointi voi olla yhtä haastavaa.

Kaikissa yrityksissä ja muissa yhteisöissä on tärkeä ratkaista tietoturvan kysymykset riittävän yksinkertaisella ja kustannustehokkaalla tavalla. Tietoturvan rakentaminen lähtee pitkälti siitä, että organisaatiossa kaikki työntekijät tunnistavat sen, mikä on salassa pidettävää tai luottamuksellista tietoa, ja mikä tieto ei saisi päätyä ulkopuolisille tahoille. Toinen tapa on rajata tiedon ja tietojärjestelmän käyttöoikeuksia ja tiedon käyttäjien määrää. Asiantuntijoiden mukaan entistä useampi organisaatio onkin laatinut tietojen luokittelu- ja käsittelyohjeet.

Toisaalta monia tietoturvariskejä voidaan vähentää, kun kiinnitetään huomiota perusasioihin. Niitä ovat salasanojen vaihto ja tietoliikenteen salauksen tarkistus verkkosivustoilla ja varmuuskopioinnista huolehtiminen. Organisaatiossa on myös tiedettävä, miten toteutuneissa tietoturvaloukkauksissa toimitaan ja asiasta viestitään. Työyhteisöissä tietoturvaa voidaan lisätä koulutuksella, henkilöstövalinnalla ja töiden uudelleenorganisoinnilla. Ennen kaikkea tietoturvallisuuden kehittämisessä on kyse henkilöiden toimintatapojen muuttamisesta.

Yrityksissä tietoturvakustannusten muuttaminen rahaksi on haastava tehtävä. Tietoverkkorikollisuus voi näkyä pienenä resurssikuormituksena, mainevahinkona tai koko yrityksen toiminnan vaarantavana tapahtumana. Tietoturvan pettäessä suorat kustannukset on helppo arvioida, sillä ne koostuvat erilaisista selvittelykustannuksista, korjaavista toimenpiteistä, vaikutuksesta myyntiin, vahingonkorvauksista ja vaihtoehtoisten toimintamallien aiheuttamasta lisätyöstä. Taloudellisilta vahingoilta voi suojautua osittain myös vakuutuksin.

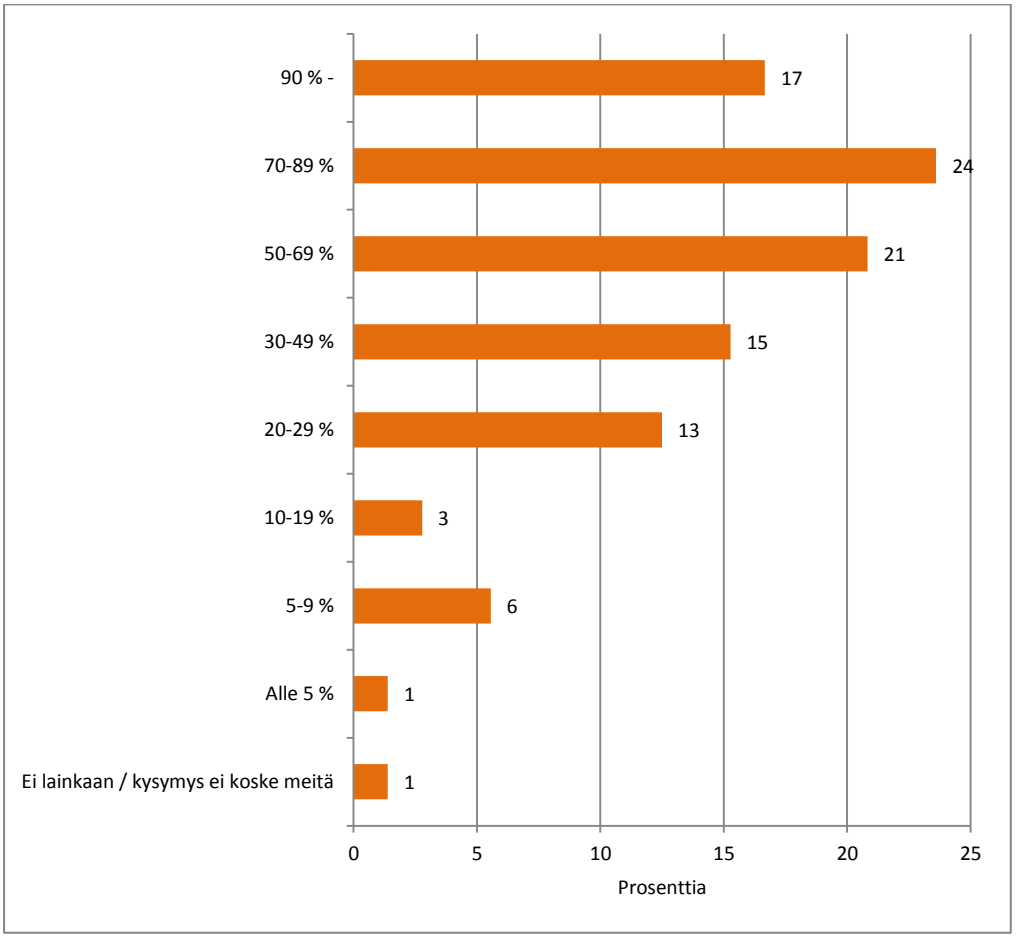
Piilokustannusten arviointi on paljon vaikeampaa. Pienessä yrityksessä turvallisuusriskin toteutuminen voi merkitä toiminnan loppumista. Esimerkiksi verkkokaupassa asiakassuhteet eivät kauan säily, ellei tietoliikenneympäristö ole riittävän luotettava. Merkittävä osa tietoverkkorikollisuudesta on lisäksi piilorikollisuutta, joten kaapatun tiedon rahallista arvoa on mahdotonta määrittää. Imagollisista syistä ja asiakaskadon pelon vuoksi rikosten uhreiksi joutuneet yritykset eivät ole myöskään usein halukkaita viemään asioita julkiseen käsittelyyn.

3.3 Hyvinvointialat ja toimintojen digitalisointi

Hyvinvointialoilla tietoturvallisuuden merkitystä ovat korostaneet *toimintojen digitalisoituminen*, sillä alan yritykset ja järjestömuotoiset palveluntuottajat hyödyntävät toiminnassaan koko ajan enemmän digitaalista ympäristöä (pilvipalvelut, esineiden ja asioiden Internet, asiakaspalvelujen digitaalinen tarjonta, keinoäly, verkkokauppa, yms.). Tosin yksityisesti tuotetuissa sosiaali- ja terveyspalveluissa sekä varhaiskasvatusalalla yritysten ja järjestöjen toiminnan digitalisointiaste voi poiketa yritys- ja toimialakohtaisesti toisistaan hyvin paljon.

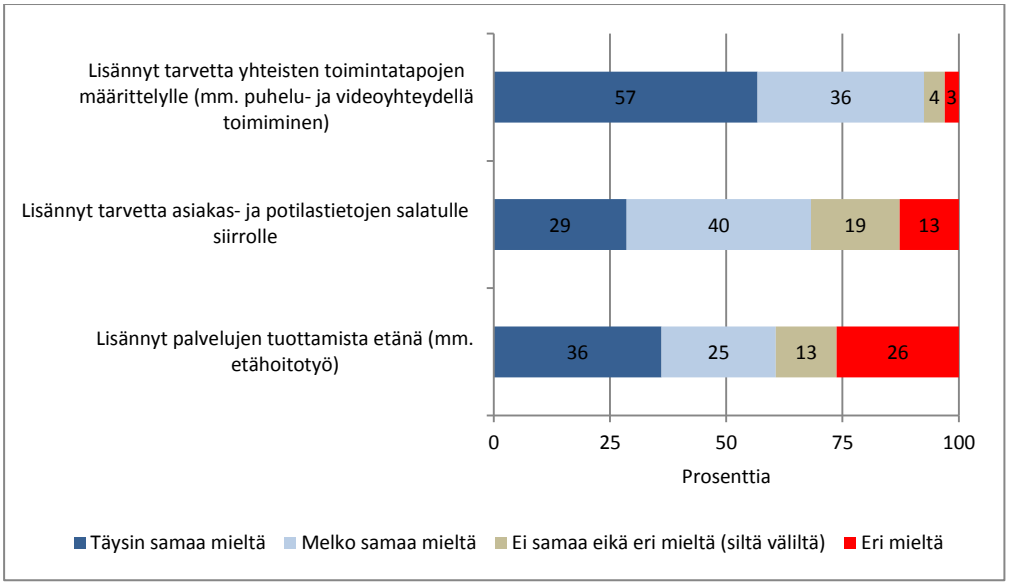
Hyvinvointialoilla vuonna 2021 tehtyjen turvallisuusalan kyselyjen mukaan toimintojen digitalisointiaste kohoaa silti yllättävän korkealle. Kyselyyn vastanneista peräti runsaat 60 prosenttia ilmoitti, että yrityksen tai järjestön liiketoiminnan prosesseista ja palveluista vähintään 50 prosenttia nojautuu digitaalisiin laitteisiin, ohjelmistoihin ja dataan tällä hetkellä (Kuvio 7). Epidemiakriisi on vauhdittanut kehitystä edelleen, sillä yli 60 prosenttia kyselyyn vastanneista kertoi, että palvelujen etätuottaminen on lisääntynyt (etähoitotyö, yms.).

Kuvio 7 *Hyvinvointialojen turvallisuusalan kyselyyn vastanneiden yritysten ja järjestöjen näkemys liiketoiminnan prosessien ja palvelujen digitalisointiasteesta, prosenttia vastanneista (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



Toteutunut kehitys on johtanut siihen, että tarve asiakas- ja potilastietojen salatulle siirrolle on lisääntynyt. Asiasta ilmoitti lähes 70 prosenttia kyselyyn vastanneista. Edelleen yli 90 prosenttia vastasi, että tarve yhteisten toimintatapojen määrittelylle (mm. puhelu- ja videoyhteydellä toimiminen) on kasvanut (Kuvio 8). Monien palveluntuottajien osalta suurimmat muutokset koskevat työkollegojen kanssa käytäviä kokouksia, jotka ovat siirtyneet enenevässä määrin verkkoon.[19] Eli kysymys on sisäisen viestinnän digitalisoitumisesta.

Kuvio 8 *Hyvinvointialojen turvallisuusalan kyselyyn vastanneiden yritysten ja järjestöjen näkemys epidemiakriisin vaikutuksista liiketoiminnan prosessien ja palvelujen digitalisointiin, prosenttia vastanneista (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



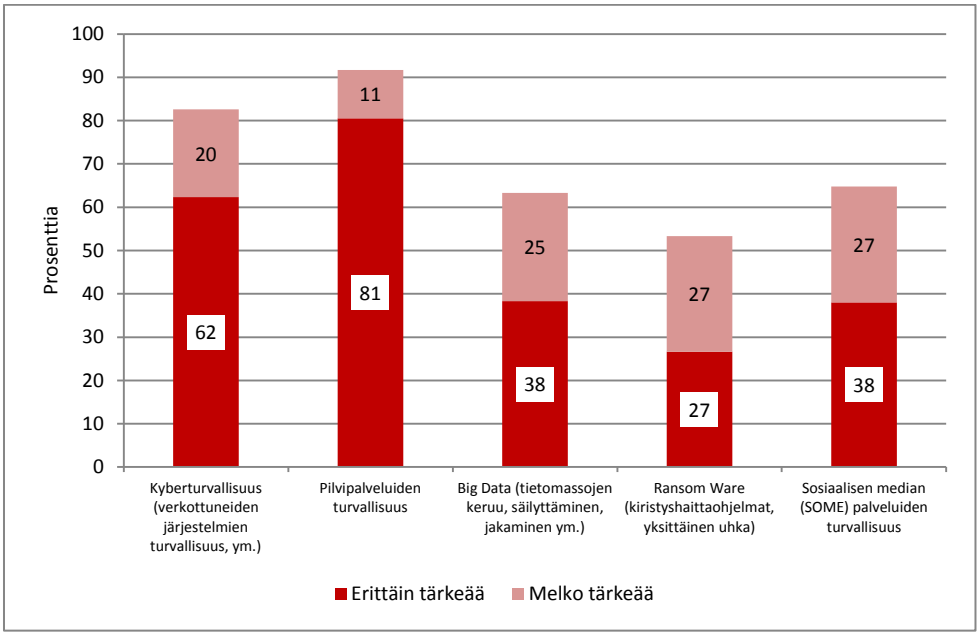
3.4 Tietoturvan painopistealueet hyvinvointialoilla

Hyvinvointialojen kyselyssä yrityksiltä ja järjestöiltä tiedusteltiin ensimmäistä kertaa tärkeimmistä tietoturvallisuuden kehittämisen painopistealueista kesällä 2021. Asiakokonaisuudet jaettiin neljään pääryhmään, joita olivat *tietoturvallisuuden ajankohtaiset uhkakuvat ja riskit, hallinnollisen tietoturvallisuuden asiat, teknisen tietoturvallisuuden asiat ja tietoturvallisuutta koskevien riskien arviointi.* Samat kysymykset esitettiin vuonna 2020 eri toimialoja edustaville Suomen Yrittäjien ja Helsingin seudun kauppakamarin jäsenyrityksille.

Kyselyjen mukaan asiakasorganisaatiot pitävät pilvipalvelujen turvallisuutta ja kyberturvallisuutta[20] tärkeimpinä tietoturvallisuuteen liittyvinä *ajankohtaisina teemoina.* Big Dataan[21], sosiaalimedian turvallisuuteen ja kiristyshaittaohjelmiin (*Ransom Ware*) liittyvät kysymykset ovat hieman vähemmän tärkeitä, mikä näkyy vastausten saldoluvuissa. Saldoluvut saadaan, kun asiaa tärkeänä pitäneiden vastanneiden prosenttiosuudesta vähennetään niiden vastanneiden prosenttiosuus, jotka eivät pidä asiaa kovin tai lainkaan tärkeänä (Kuvio 9).

[19] Sama koskee etäkoulutusta yleistymistä.
[20] Verkottuneiden järjestelmien turvallisuus, yms.
[21] Tietomassojen keruu, säilyttäminen ja jakaminen, yms.

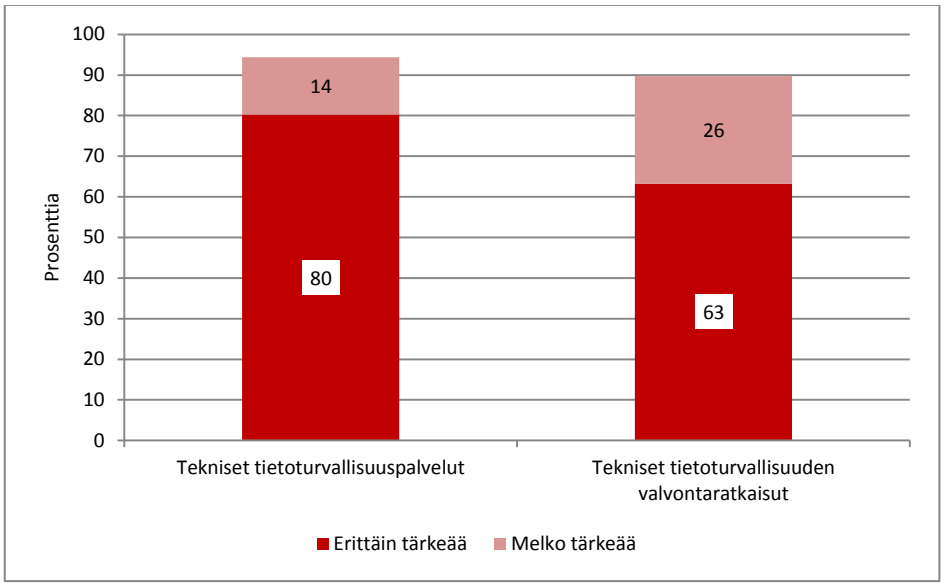
Kuvio 9 *Tietoturvallisuuden ajankohtaiset teemat hyvinvointialojen yrityksissä ja järjestöissä, asiaa tärkeänä pitävien prosenttiosuus (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



Tekninen tietoturvallisuus

Noin 90-94 prosenttia hyvinvointialojen palveluntuottajista piti *teknisten tietoturvallisuuden* asioita erittäin tai melko tärkeinä (Kuvio 10). Teknistä tietoturvallisuutta ovat virussuojaukset (AV, antivirus) ja palomuurit (FM, firewall), jotka vähentävät haittaohjelmatartuntoja, tietokoneen ohjelmistojen tietoturva-aukkojen hyödyntämistä ja valjastusta palvelunestohyökkäykseen. Tekniseen tietoturvallisuuteen kuuluvat periaatteessa myös tietojen ja tietoliikenteen salausratkaisut sekä erilaiset tunkeutumisen havaitsemisjärjestelmät.

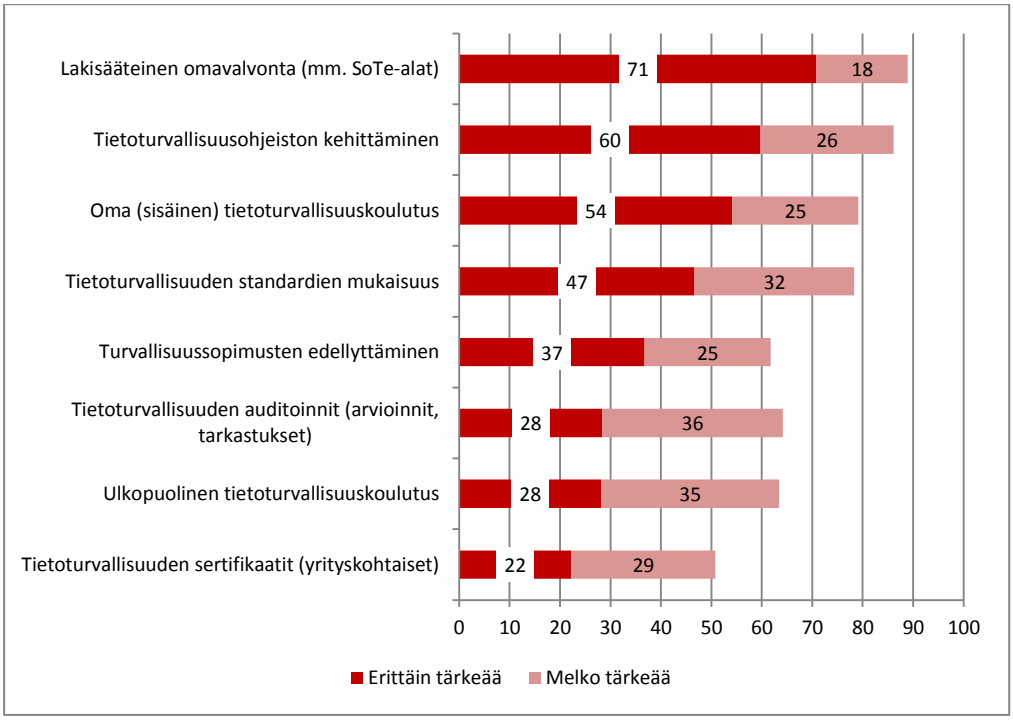
Kuvio 10 *Tekniset tietoturvallisuuden asiat hyvinvointialojen yrityksissä ja järjestöissä, asiaa tärkeänä pitävien prosenttiosuus (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



Hallinnollinen tietoturvallisuus

Hallinnollisen tietoturvallisuuden osalta yritykset ja järjestöt korostivat lakisääteistä SoTe-alojen omavalvontaa, tietoturvaohjeiston kehittämistä, oman organisaation sisäistä tietoturvakoulutusta sekä tietoturvallisuuden standardien mukaisuutta (Kuvio 11). Näiden jälkeen tuli turvallisuussopimusten edellyttäminen. Sen sijaan tietoturvallisuuteen liittyvät auditoinnit (tarkastukset, arvioinnit), ulkopuolisen tahon järjestämä tietoturvakoulutus ja erityisesti tietoturvallisuuden yrityskohtaisiin sertifikaatteihin suhtauduttiin pidättyväisemmin.

Kuvio 11 *Hallinnolliset tietoturvallisuuden asiat hyvinvointialojen yrityksissä ja järjestöissä, asiaa tärkeänä pitävien prosenttiosuus (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



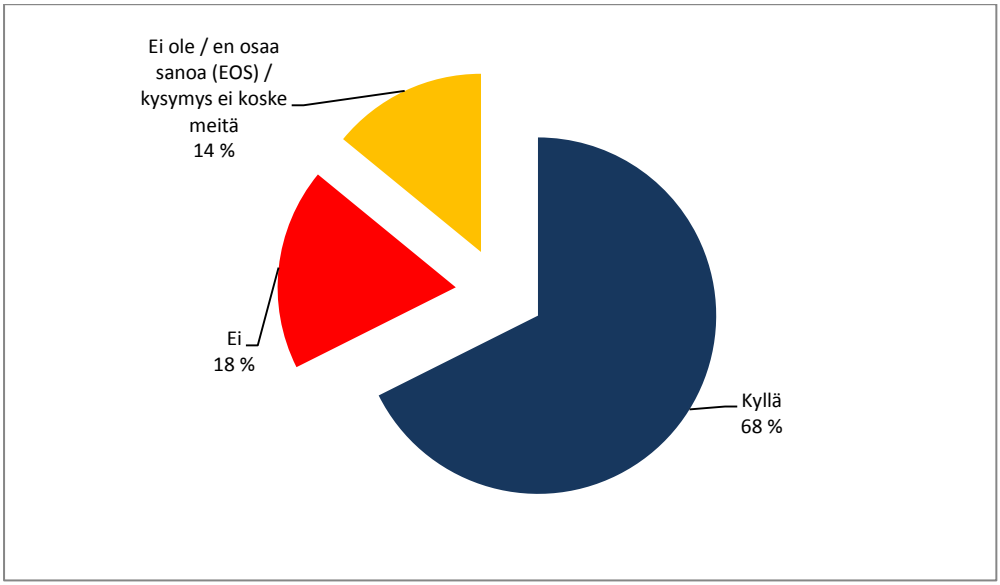
Hallinnolliseen tietoturvallisuuteen kuuluu se, että noin 30 prosentilla hyvinvointialojen turvallisuusalan kyselyyn vastanneista oli laadittuna oma erillinen tietoturvastrategia kesäkuussa 2021. Noin 60 prosentilla tietoturvallisuusasiat oli sisällytetty organisaation (yritys tai järjestö) yleiseen strategiaan (Kuvio 13). Edelleen kaksi kolmasosaa vastanneista totesi, että heidän edustamansa organisaatio on määrittänyt varautumissuunnitelmissaan ne kriittiset toiminnot[22], joiden tietoturva ja toiminta on varmistettava kaikissa tilanteissa (Kuvio 12).

Huomionarvoista on, että turvallisuusalan kyselyyn vastanneista 65 prosenttia oli samaa mieltä siinä, että sosiaali- ja terveydenhuollossa yhteisten tietoturvan minimivaatimusten määrittelyllä voidaan tehokkaasti parantaa potilas- ja asiakastietojen tietoturvan tasoa ja selkeyttää sitä, millaisia toimenpiteitä kaikilta sosiaali- ja terveydenhuollon toimijoilta edellytetään tietojen suojaamiseksi. Tämä olisi tärkeää muun

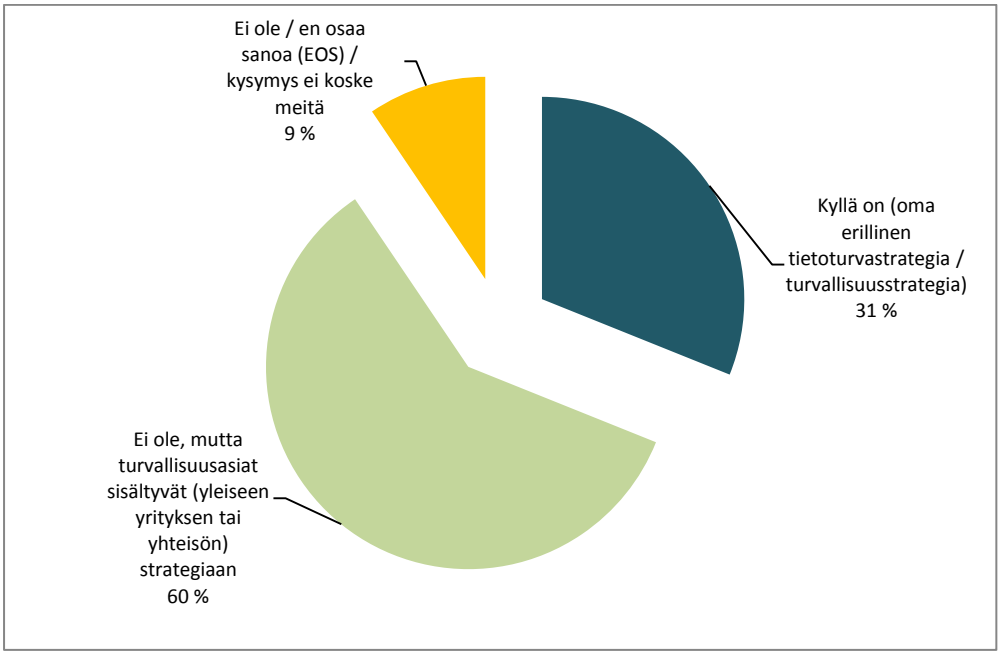
[22] Tuotetut palvelut ja niihin liittyvät järjestelmät, kuten laitteet ja ohjelmistot.

muassa kanta-palveluissa. Tosin vain runsas neljännes yrityksistä ja yhteisöistä oli mukana kanta-palveluissa kesäkuussa 2021.[23]

Kuvio 12 *Tietoturvan kannalta kriittisten toimintojen määrittely hyvinvointialojen turvallisuusalan kyselyyn vastanneissa yrityksissä ja järjestöissä, prosenttia vastanneista (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*

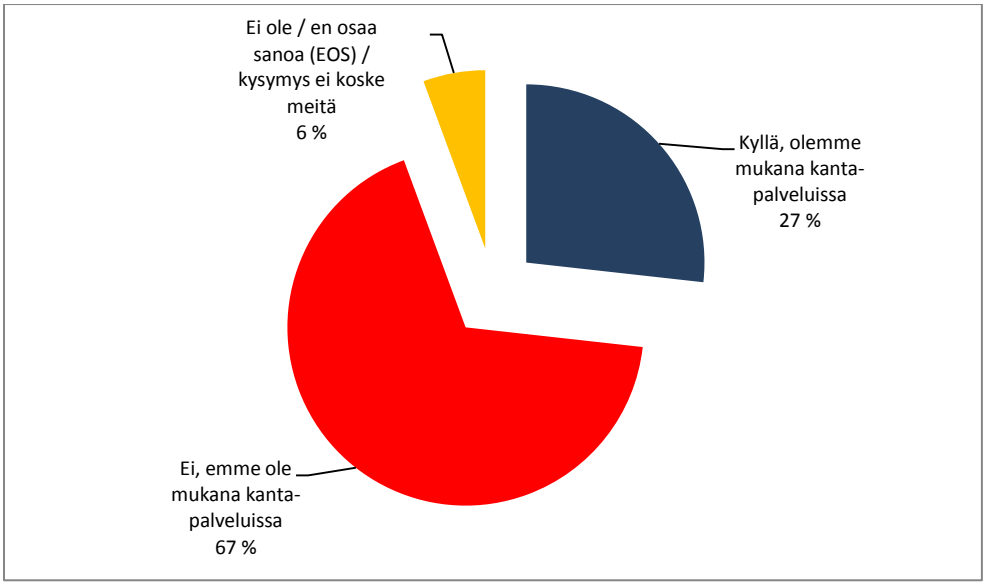


Kuvio 13 *Tietoturvastrategiat hyvinvointialojen turvallisuusalan kyselyyn vastanneissa yrityksissä ja järjestöissä, prosenttia vastanneista (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



[23] Kanta tuottaa digitaalisia sosiaali- ja terveydenhuollon palveluja, jotka hyödyttävät kansalaisia sekä sosiaali- ja terveydenhuollon toimijoita. Kantapalveluja ovat omakanta, lääketietokanta, resepti-palvelu, potilastiedon arkisto, vanhojen potilastietojen arkisto, terveydenhuollon todistusten välitys, kelain, kanta-asiakastestipalvelu ja sosiaalihuollon asiakastiedon arkisto. Kantapalveluihin liittyminen edellyttää sertifioituja tietojärjestelmiä.

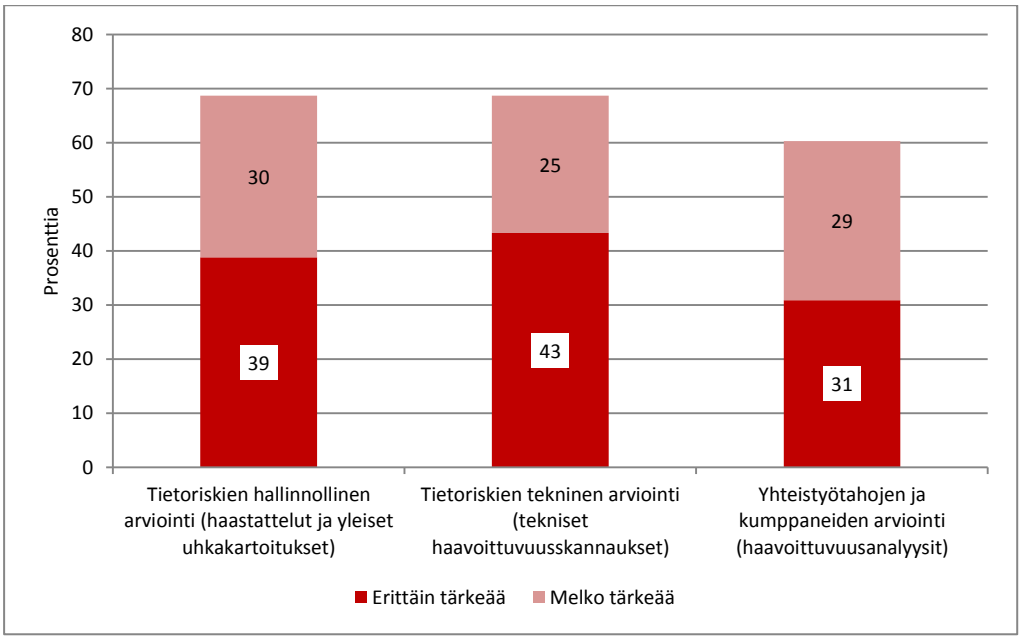
Kuvio 14 *Hyvinvointialojen turvallisuusalan kyselyyn vastanneiden yritysten ja järjestöjen mukanaolo kanta-palveluissa, prosenttia vastanneista (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



Tietoriskien arviointi ja kartoitus

Tietoriskien arviointi ja kartoitus ovat tärkeitä työvälineitä, kun tavoitellaan kustannustehokasta tietoturvaa sekä uhkien ja väärinkäytösten ennaltaehkäisyä. Oma henkilöstö ei pysty aina tekemään riskikartoitusta, vaan siihen tarvitaan ulkopuolista apua. Riskikartoitus on jaettavissa tekniseen arviointiin (tekniset haavoittuvuusskannaukset, yms.), hallinnolliseen arviointiin (haastattelut, yleiset uhkakartoitukset, yms.) ja yhteistyötahojen ja -kumppaneiden arviointiin. Riskejä voidaan pienentää varmistamalla myös omien työntekijöiden luotettavuus.

Kuvio 15 *Tietoturvallisuuden riskeihin liittyvät asiat hyvinvointialojen yrityksissä ja järjestöissä, asiaa tärkeänä pitävien prosenttiosuus (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



Tietoturva ja sähköiset turvajärjestelmät

Tietoturvalla on suuri merkitys myös muissa turvallisuusjärjestelmissä, joilla valvotaan kiinteistöjä ja niissä olevia toimitiloja, tuotantoprosessia tai työntekijöiden liikkumista. Sähköiset valvontajärjestelmät hyödyntävät lisääntyvässä määrin ITC- ja mobiiliteknologiaa, mikä on korostanut järjestelmien tietoturvallisuutta. Asiaa ei kysytty hyvinvointialojen kyselytutkimuksessa, mutta aiempien selvitysten mukaan tietoturva korostuu kameravalvontajärjestelmissä, kulunvalvonta- ja työajanseurantajärjestelmissä sekä vartiointipalveluissa.[24]

[24] Tietoturvallisuuden merkitys ja vaikutus tulisi ottaa huomioon erilaisten turvallisuusalan tuotteiden, palveluiden ja järjestelmien hankinnoissa (Lähde: Finnsecurity ry ja Suunnittelu- ja tutkimuspalvelut Pekka Lith / Lith Consulting Group: Turvallisuusalan yritysten suhdanne- ja toimialaraportti 2020).

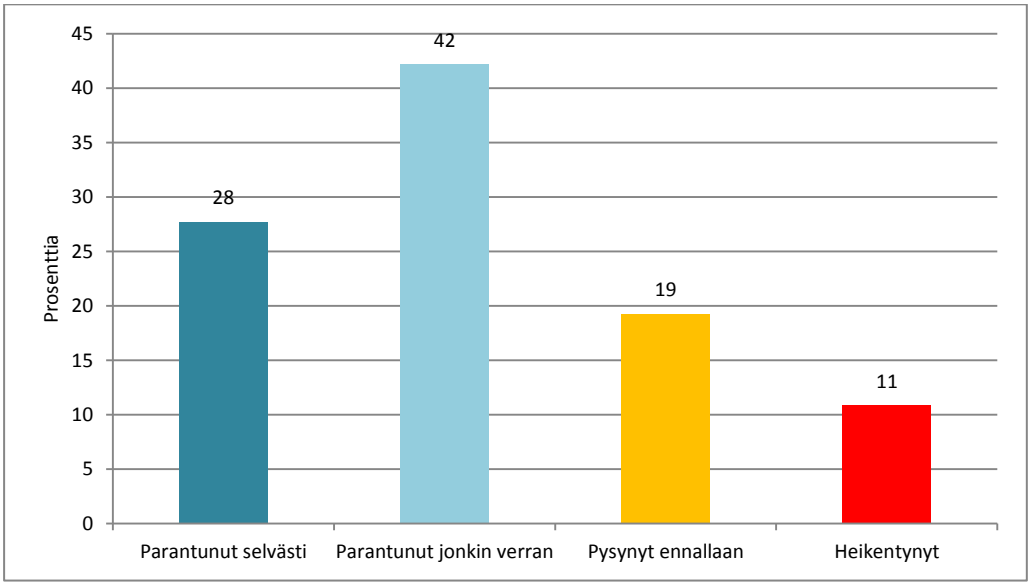
Yhteenveto

Turvallisuusalan kyselyihin vastanneista 80 prosenttia piti *tietoturvallisuutt*a koskeviin uhkiin varautumista tärkeänä. Toiseksi ja kolmanneksi keskeisimpinä turvallisuus- ja onnettomuusuhkina *pidettiin toimitilojen paloturvallisuutta sekä vesi- ja kosteusvahinkoja*. Seuraavilla sijoilla olivat henkilöstöön kohdistuva uhkailu, häirintä ja väkivalta sekä työnteon terveydelliset haitat ja vaaratilanteet ja ympäristösuojeluun liittyvät onnettomuusuhat. Vähiten pelättiin oman henkilöstön rikoksia ja väärinkäytöksiä sekä alihankkijoihin kohdistuvia uhkia.

Uhkakuvista ja riskeistä huolimatta 70 prosenttia kyselyihin vastanneista yrityksistä ja järjestöistä totesi, että yleinen turvallisuustilanne on parantunut vuosina 2016-21. Vajaa viidennes katsoi, että tilanne on pysynyt ennallaan. Ainostaan runsaat kymmenen prosenttia vastanneista ilmoitti, että turvallisuustilanne olisi heikentynyt. Suhteellisen hyvän turvallisuustilanteen taustalla ovat turvallisuusuhkiin ja –vaaroihin liittyvän tietoisuuden lisääntyminen ja turvallisuusasioiden merkityksen parempi tunnustaminen kaikessa toiminnassa.

Lisäksi voidaan todeta, että pääosa asiakaskyselyihin vastanneista suhtautuu turvallisuustilanteen kehitykseen varsin luottavaisesti edustamansa yrityksen tai yhteisön näkökulmasta katsoen seuraavan 1-2 vuoden aikana. Noin 61 prosenttia ennakoi turvallisuustilanteen paranevan, mitä uudet toimintatavat ja teknologian kehitys edesauttavat. Tosin taloudellisen tilanteen heikkeneminen voi hidastaa toivottua kehitystä. Vain yksi prosentti ennusti turvallisuustilanteen huonontuvan, joten asiaa koskeva saldoluku oli plus 60.

Kuvio 1 *Hyvinvointialojen turvallisuusalan kyselyyn vastanneiden yritysten ja järjestöjen näkemys yleisen turvallisuustilanteen kehityksestä 2016-21, prosenttia vastanneista (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



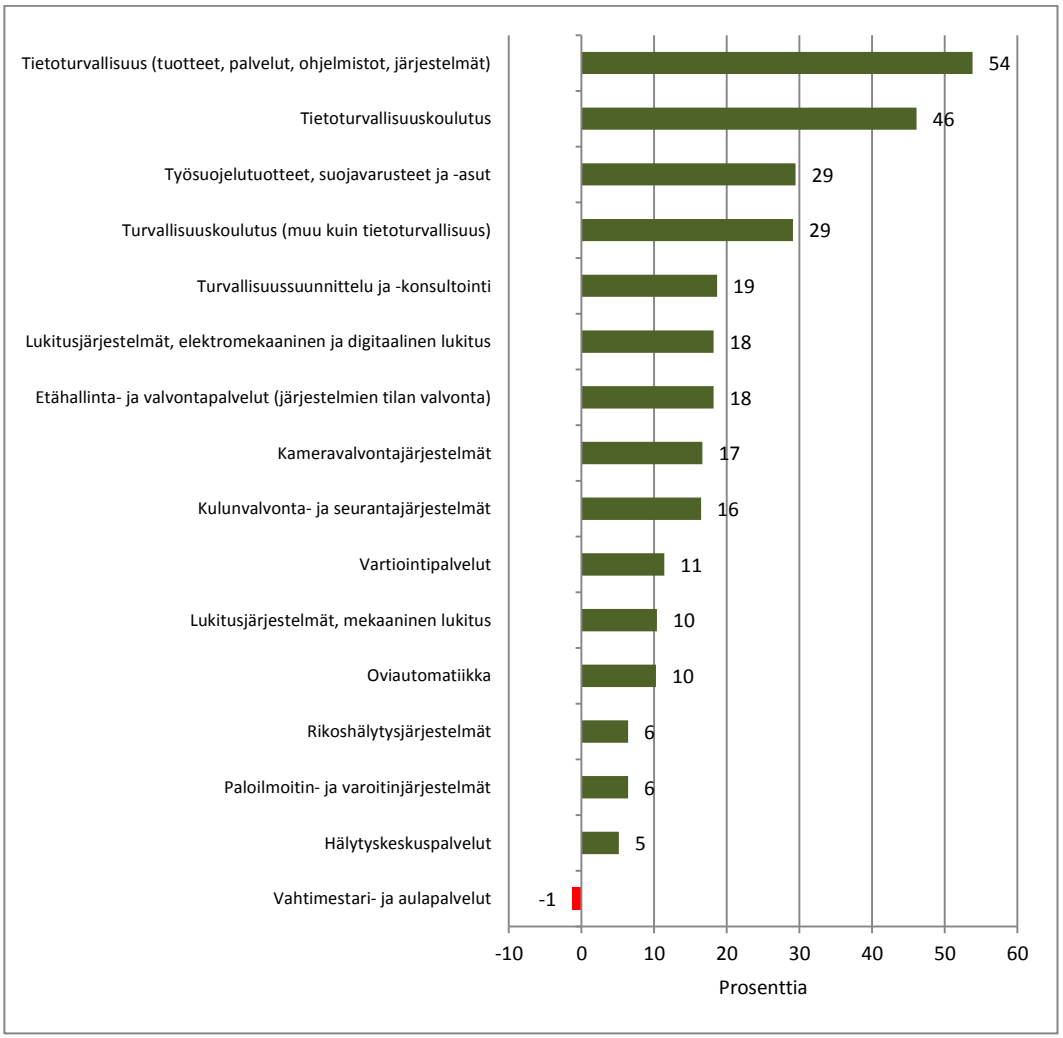
Ulkoa ostettujen turvallisuushyödykkeiden kysyntä

Hyvinvointialan turvallisuuskyselyihin vastanneista 90 prosenttia ilmoitti hankkineensa tietoturvallisuustuotteita, palveluja ja järjestelmiä. Paloilmoitus- ja varoitin-

järjestelmiä oli hankkinut 86 prosenttia. Vähintään 80 prosenttia oli ostanut tietoturvallisuuskoulutusta ja muuta turvallisuuskoulutusta omalle henkilöstölleen, mitä voidaan pitää myönteisenä asiana. Nämä turvallisuustuotteet ja -palvelut kohdistuvat sellaisiin asioihin, joilla voidaan pienentää yksityisten hyvinvointialojen keskeisiä turvallisuusuhkia ja onnettomuusriskejä.

Alan tuotteiden, palvelujen ja järjestelmien kysyntänäkemykset säilyvät hyvinvointialoilla varsin hyvinä lähivuosina. Kysyntänäkymien saldoluvut ovat plussalla kaikkien hyödykeryhmien osalta lukuun ottamatta vahtimestari- ja aulapalveluja, joita hyödynnetään muutoinkin varsin vähän. Saldoluku saadaan, kun kysynnän kasvua ennakoivien prosenttiosuudesta vähennetään kysynnän laskua ennakoivien prosenttiosuus. Parhaimmat ne ovat tietoturvallisuustuotteissa, palveluissa ja järjestelmissä sekä tietoturvallisuuskoulutuksessa.

Kuvio 2 *Hyvinvointialojen turvallisuusalan kyselyyn vastanneiden yritysten ja järjestöjen näkemys turvallisuusalan tuotteiden, palvelujen ja järjestelmien kysyntänäkemyksistä lähivuosina saldolukuina, prosenttia (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



Erityisteema: tietoturvallisuus

Tietoturvallisuutta on määritelmällisesti tietojen, järjestelmien ja palvelujen suojaus hallinnollisten ja teknisten toimenpiteiden avulla. Tietoturva rakentuu tiedon *luotta-*

mukselliSuuden, *eheyden* ja *käytettävyyden* pohjalle. Luottamuksellisuudella tarkoitetaan, että tietoa voivat käsitellä vain henkilöt, joilla on siihen oikeus. Tiedon eheydellä ymmärretään sitä, että tieto ei saisi muuttua tahattomasti tai tahallisesti, tai muutokset pitäisi ainakin havaita. Käytettävyys tarkoittaa, että tarvittava tieto on saatavilla silloin kuin sitä tarvitaan.[25]

Tilastokeskuksen oikeustilastojen mukaan poliisin tietoon tuli noin 6 030 tietoturvarikosta (ml. datavahingonteot) vuonna 2020. Niistä 71 prosenttia oli identiteettivarkauksia. Ilman identiteettivarkauksia poliisin tietoon tulleita verkkorikoksia oli 1 740 vuonna 2020. Verkkorikosten määrä lisääntyi vuosina 2016-20 noin 50 prosentilla (pl. identiteettivarkaudet). Suhteellisesti eniten kasvoivat tietomurrot ja tietomurron yritykset. Tosin kaikki tietoturvarikokset eivät tule poliisin tietoon ja rikoksia koskeviin tilastoihin sisältyy monia ongelmia.

Hyvinvointialoilla tietoturvallisuusasiat ovat ajankohtaistuneet sitä mukaa, kun toimintojen digitalisointi on edennyt. Epidemiakriisi on vauhdittanut kehitystä, kun palvelujen etätuottaminen on lisääntynyt ja tarve asiakas- ja potilastietojen salatulle siirrolle on kasvanut. Alan turvallisuuskyselyssä tietoturvallisuuden ajankohtaisten uhkakuvien ja riskien puolella tärkeimmäksi nousi pilvipalvelujen turvallisuus. Palvelujen ja niissä olevan tiedon siirto yrityksen oman verkon ja hallinnan ulkopuolelle voivat aiheuttaa huolta tietoturvallisuudesta.[26]

Hallinnollisen tietoturvallisuuden osalta yritykset ja järjestöt korostivat lakisääteistä SoTe-alojen omavalvontaa, tietoturvaohjeiston kehittämistä, oman organisaation sisäistä tietoturvakoulutusta sekä tietoturvallisuuden standardien mukaisuutta (Kuvio 11). Näiden jälkeen tuli turvallisuussopimusten edellyttäminen. Sen sijaan tietoturvallisuuteen liittyvät auditoinnit (tarkastukset, arvioinnit), ulkopuolisen tahon järjestämä tietoturvakoulutus ja erityisesti tietoturvallisuuden yrityskohtaisiin sertifikaatteihin suhtauduttiin pidättyväisemmin.

Tekniset tietoturvallisuuden asiat on koettu kaikenlaisissa organisaatioissa jossain määrin tärkeämmiksi kuin muut tietoturvallisuuteen liittyvät asiat. Teknistä tietoturvallisuutta ovat virussuojaukset (AV, antivirus) ja palomuurit (FM, firewall), jotka vähentävät haittaohjelmatartuntoja, tietokoneen ohjelmiston tietoturva-aukkojen hyödyntämistä ja valjastusta palvelunestohyökkäykseen. Tekniseen tietoturvallisuuteen kuuluvat periaatteessa myös tietojen ja tietoliikenteen salausratkaisut sekä erilaiset tunkeutumisen havaitsemisjärjestelmät.

Tietoriskien arviointi ja kartoitus ovat tärkeitä työvälineitä, kun tavoitellaan kustannustehokasta tietoturvaa sekä uhkien ja väärinkäytösten ennaltaehkäisyä. Riskikartoitus on jaettavissa tekniseen arviointiin (tekniset haavoittuvuusskannaukset, yms.), hallinnolliseen arviointiin (haastattelut, yleiset uhkakartoitukset, yms.) ja yhteistyötahojen ja -kumppaneiden arviointiin. Riskejä voidaan pienentää varmistamalla

[25] Tietoturvallisuuden tavoitteena on yksinkertaistettuna sellainen asiantila, joissa tiedon käytettävyyteen, eheyteen ja käytettävyyteen ei kohdistu suuria riskejä.

[26] Pilvipalvelujen riskit liittyvät tietojen yksityisyyteen, kun tiedot ja sovellukset on hajautettu ympäri maailmaa ja samat palvelut on useamman eri tahon käytössä. Myös pilvipalvelun tarjoajien henkilöstöllä saattaa olla pääsy tärkeisiin tietoihin.

myös omien työntekijöiden luotettavuus. Lisäksi huomiota kannattaa kiinnittää sähköisten turvajärjestelmien tietoturvaan.[27]

Taulukko 1 Kooste turvallisuusalan vuoden 2021 kyselyyn vastanneiden hyvinvointialojen yritysten ja järjestöjen näkemyksistä koskien tietoturvallisuuden ajankohtaisia teemoja ja toiminnan kehittämistarpeita, prosenttia vastanneista (ml. saldoluvut) (Lähde: Hyvinvointialojen turvallisuuskysely 2021).

	Asiaa tärkeänä pitävien osuus, %	Siltä väliltä suhtautuvien osuus, %	Asia vähemmän tärkeänä pitävien osuus, %	**Saldoluku[28], %**
Ajankohtaiset tietoturvateemat:				
Pilvipalvelujen turvallisuus	92	7	1	**90**
Kyberturvallisuus[29]	83	14	3	**80**
Ransom Ware[30]	53	30	17	**37**
Big Data[31]	63	17	20	**43**
SOME-palvelujen turvallisuus	65	27	8	**56**
Hallinnollisen tietoturvallisuuden asiat:				
Lakisääteinen omavalvonta	89	7	4	**85**
Tietoturvallisuusohjeiston kehittäminen	86	7	4	**82**
Tietoturvallisuuden standardien mukaisuus	78	18	3	**75**
Oma sisäinen tietoturvakoulutus	79	19	1	**78**
Turvallisuussopimusten vaatiminen	62	26	12	**50**
Tietoturvallisuuden auditoinnit[32]	64	27	9	**55**
Ulkopuolinen tietoturvakoulutus	63	28	8	**55**
Tietoturvallisuuden yrityskohtaiset sertifikaatit	51	21	29	**22**
Teknisen tietoturvallisuuden asiat:				
Tekniset tietoturvallisuuspalvelut	94	6	0	**94**
Tietoturvallisuuden valvontaratkaisut	90	6	4	**85**
Riskien arviointi:				
Tietoriskien tekninen arviointi	69	22	9	**60**
Yhteistyötahojen ja –kumppaneiden arviointi	60	24	16	**44**
Tietoriskien hallinnollinen arviointi	60	22	9	**60**

Tietoturvallisuusasioiden nykytila

Hyvinvointialan turvallisuuskyselystä välittyy käsitys, että tietoturvallissuutta koskevat asiat ja haasteet on tunnustettu ja varotoimenpiteitä riskien pienentämiseksi on tehty. Arviolta 90 prosentilla kyselyyn vastanneista oli laadittuna oma erillinen tietoturvastrategia tai tietoturvallisuusasiat oli sisällytetty organisaation yleiseen strategiaan. Kaksi kolmasosaa kertoi myös, että heidän edustamansa organisaatio on määrittänyt varautumissuunnitelmissaan ne kriittiset toiminnot, joiden tietoturva ja toiminta on varmistettava kaikissa tilanteissa

Lähitulevaisuuden näkymät tuntuvat olevan yksityisillä hyvinvointialoilla tältä osin myönteisemmät kuin esimerkiksi Suomen yrityskentässä keskimäärin, sillä Helsin-

[27] Kameravalvontajärjestelmät, kulunvalvonta- ja työajanseurantajärjestelmät ja vartiointipalvelut.
[28] Asiaa tärkeänä pitävien prosenttiosuus miinus asiaa vähemmän tärkeänä pitävien prosenttiosuus.
[29] Verkottuneiden järjestelmien turvallisuus, yms.
[30] Kiristyshaittaohjelmat, yksittäinen turvallisuusuhka
[31] Tietomassojen keruu, säilyttäminen, jakaminen, yms.
[32] Arvioinnit, tarkastukset

gin seudun kauppakamarin selvitysten mukaan kaikkia toimialoja edustavien yritysten joukossa on suuri joukko kyberturvattomia kohteita, jotka eivät ole pitäneet huolta digitaalisesta yritysvastuustaan. Selvityksessä todettiin myös, että luotettavan tiedon saanti tietoturvauhista ja niihin varautumisesta on tärkeää, mutta viranomaisten tuottama tieto ei tavoita yrityksiä riittävästi.

Kaikissa organisaatioissa on kuitenkin tärkeää ratkaista tietoturvan kysymykset riittävän yksinkertaisella ja kustannustehokkaalla tavalla. Tietoturvan rakentaminen lähtee pitkälti siitä, että organisaation työntekijät tunnistavat sen, mikä on salassa pidettävää tai luottamuksellista tietoa, ja mikä tieto ei saisi päätyä ulkopuolisille tahoille. Toinen tapa on rajata tiedon ja tietojärjestelmän käyttöoikeuksia ja tiedon käyttäjien määrää. Asiasta tehtyjen selvitysten mukaan entistä useampi yritys onkin laatinut tietojen luokittelu- ja käsittelyohjeet.

Toisaalta monia tietoturvariskejä voidaan vähentää, kun kiinnitetään huomiota perusasioihin. Niitä ovat salasanojen vaihto ja tietoliikenteen salauksen tarkistus verkkosivustoilla ja varmuuskopioinnista huolehtiminen. Organisaatiossa on myös tiedettävä, miten toteutuneissa tietoturvaloukkauksissa toimitaan ja asiasta viestitään. Työyhteisöissä tietoturvaa voidaan lisätä koulutuksella, henkilöstövalinnalla ja töiden uudelleenorganisoinnilla. Ennen kaikkea tietoturvallisuuden kehittämisessä on kyse työntekijöiden toimintatapojen muuttamisesta.

Lähteitä

Muun muassa

EU:n komissio: Komission tiedonanto neuvostolle, Euroopan parlamentille ja alueiden komitealle, Tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi, Bryssel 22/05/2007.

Finnsecurity ry ja Suunnittelu- ja tutkimuspalvelut Pekka Lith / Lith Consulting Group: Turvallisuusalan yritysten suhdanne- ja toimialaraportti 2020. (www.finnsecurity.fi)

Helsingin seudun kauppakamari: Yrityksiin kohdistuvat kyberuhat, Helsinki 2019. (www.helsinki.chamber.fi)

Keskuskauppakamari ja Helsingin seudun kauppakamari: Yritysten rikosturvallisuus 2017, Riskit ja niiden hallinta, tutkimus 2017. (www.chamber.fi)

Liikenne- ja viestintävirasto: Kyberturvallisuus ja yrityksen hallituksen vastuu, Traficomin julkaisuja 2/2020, Helsinki 2020 (www.traficom.fi).

Lith, Pekka: Kiinteistöala Suomen kansantaloudessa. Suunnittelu- ja tutkimuspalvelut Pekka Lith, Vantaa 2021. (www.kiinteistotyonantajat.fi)

Tilastokeskus: Oikeustilastot. (www.stat.fi)

Tilastokeskus: Toimialaluokitus TOL 2008, käsikirjoja 4, Helsinki 2008.

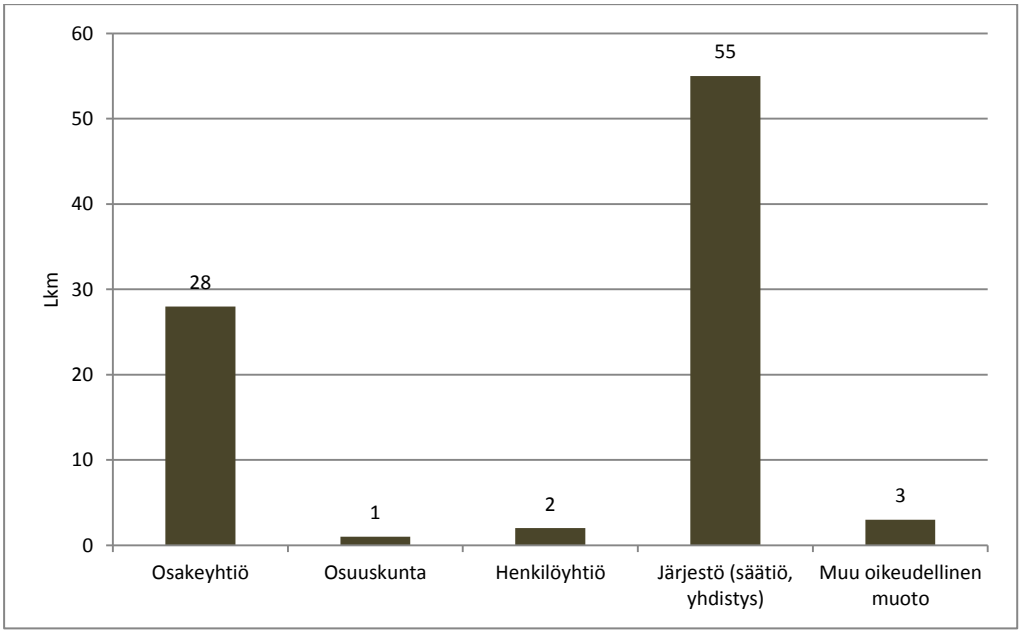
Liite 1: Hyvinvointialojen 2021 turvallisuuskyselyyn vastanneet

Hyvinvointiala HALI ry:n ja Lääkäripalveluyritykset LPY ry:n turvallisuusalan kyselyihin vastasi hyväksyttävästi 90 *yksityistä* palveluntuottajaa, jotka edustavat turvallisuusalan tuotteiden, palvelujen ja järjestelmien hyödyntäjiä ja turvallisuusalan asiakasorganisaatioita. Tosin hyvinvointialojen palveluntuottajilla voi olla omaa turvallisuusalan henkilöstöä.[33] Kyselyyn oli vastannut puutteellisesti kymmenkunta palveluntuottajaa, mutta näitä vastauksia ei ole otettu huomioon. Lisäksi kyselyn oli avannut vastaamatta kymmeniä palveluntuottajia.

Kyselyt suoritettiin kesäkuussa 2021 ja ne kohdennettiin HALI ry:n ja LPY ry:n jäsenille avoimen kyselylinkin avulla, joka toimitettiin vastaajille liittojen toimesta erillisen lähetekirjelmän mukana. Vastaajat koostuivat turvallisuusjohtajista ja –päälliköistä, riskinhallintapäälliköistä ja muista turvallisuusalan asiantuntijoista. Pienissä organisaatioissa vastaajat voivat olla toimitusjohtajia, toiminnanjohtajia ja muita vastuuhenkilöitä, sillä pienten yritysten ja järjestöjen palkkalistoilla on vain harvoin turvallisuusalan ammattilaisia.[34]

Kyselyyn vastanneista yritysmuotoisia palveluntuottajia oli 35 prosenttia. Kolmannen alan yhteisöjä (säätiöt, yhdistykset: jatkossa järjestöt) oli 62 prosenttia. Muita oikeudellisia muotoja edustivat kolme prosenttia vastanneista. Näyttää siltä, että nuppiluvulla mitattuna järjestömuotoiset palveluntuottajat ovat osallistuneet kyselyyn ahkerammin kuin yritykset (Kuvio 1). Henkilöstön kokoluokittain tarkasteltuna 47 prosenttia vastanneista edusti pieniä 10-49 henkilöä työllistäviä yrityksiä ja järjestömuotoisia palveluntuottajia (Kuvio 2).

Kuvio 1 *Hyvinvointialojen turvallisuuskyselyyn vastanneet (yksityiset) palveluntuottajat oikeudellisen muodon mukaan, lkm (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*

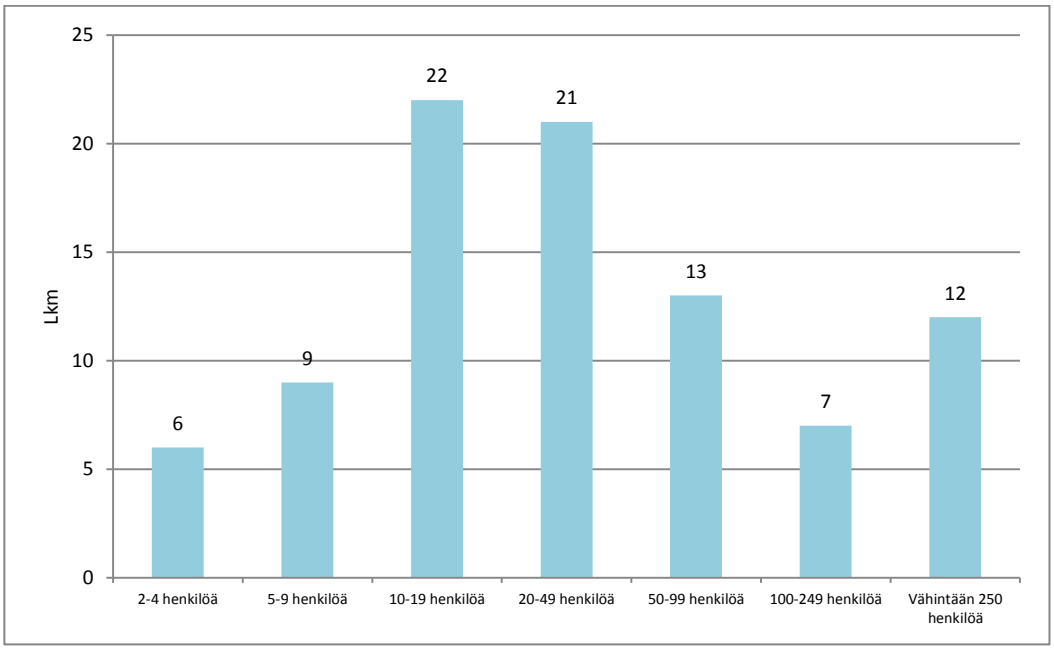


[33] Hyvinvointialoilla tarkoitetaan tässä sosiaali- ja terveydenhuoltoa sekä varhaiskasvatusta, joka luettiin aiemmin takavuosikymmeninä osaksi sosiaalipalveluja.
[34] Vastaajien taustoja ei selvitetty kuitenkaan tarkemmin kyselytutkimuksessa.

Keskisuuria 50-249 henkilön organisaatioita oli 22 prosenttia ja suuria vähintään 250 henkilöä työllistäviä organisaatioita kolmetoista prosenttia vastanneista.[35] Alle kymmenen henkilön palveluntuottajia oli 17 prosenttia. Suuret ja keskisuuret yritykset ja järjestöt organisaatiot poikkeavat pienistä organisaatioista siten, että ne ostavat monipuolisesti turvallisuushyödykkeitä eri tarkoituksiin ja niillä voi olla palkkalistoillaan hankintojen tekemiseen koulutettua ja ammattitaitoista väkeä, jotka vastaavat organisaation turvallisuustoiminnoista.

Pienissä organisaatioissa ei ole yleensä turvallisuusalan koulutuksen saaneita ammattilaisia, ja niiden turvallisuustarpeet ovat rajoitetumpia kuin suurissa organisaatioissa lukuun ottamatta tietoturvallisuutta, mitä minkään kokoisen organisaation ei ole varaa laiminlyödä. Toimialakohtaiset erot voivat olla luonnollisesti suuria hyvinvointialojen välillä. Päätoimialoittain tarkasteltuna kyselyyn vastanneista noin 70 prosenttia edusti sosiaalipalvelualaa, noin 25 prosenttia terveyspalvelualaa ja viisi prosenttia varhaiskasvatuksen toimialaa.

Kuvio 2 *Hyvinvointialojen turvallisuuskyselyyn vastanneet yritykset ja järjestöt henkilöstön suuruusluokittain, lkm (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*

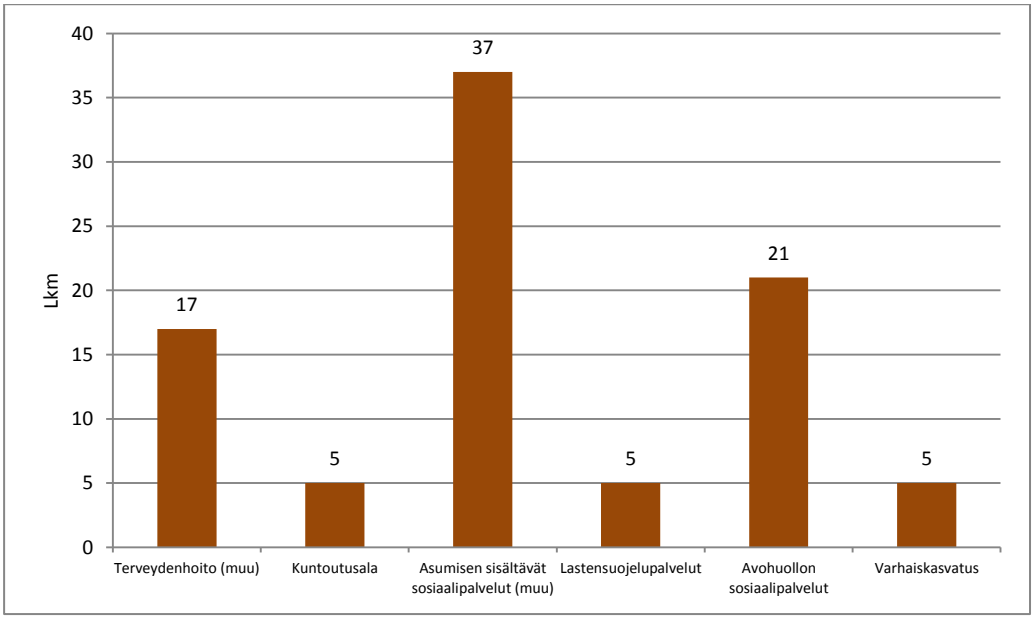


[35] Se, että kyselyyn vastanneiden joukossa on suhteellisen paljon suuria ja keskisuuria yksityisiä palvelujen tuottajia, nostaa kyselytutkimuksen painoarvoa. Suurten palveluntuottajien toiminnan laajuus on tuotoksella mitattuna paljon suurempaa kuin vastaavanlainen palvelutuotanto (ikääntyneiden ja erityisryhmien palveluasuminen, perusterveydenhuollon tasoiset palvelut, yms.) on esimerkiksi useimmissa Suomen kunnissa.

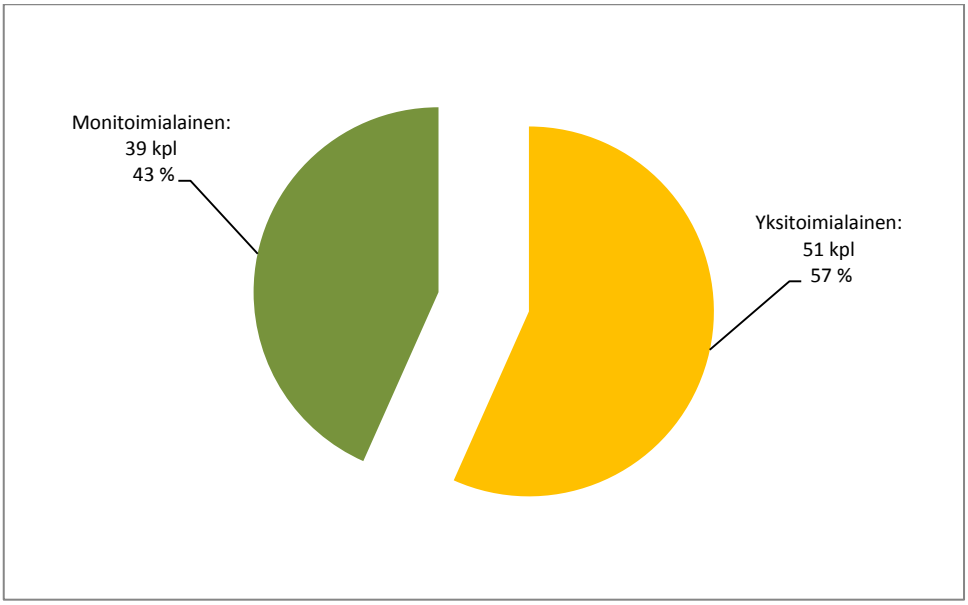
Vastanneiden toimialat ja tuottamat palvelut

Sosiaalipalvelujen tuottajista 47 prosenttiyksikköä tuottaa päätoimialanaan asumisen sisältäviä sosiaalipalveluja ja 23 prosenttiyksikköä avohuollon sosiaalipalveluja. Terveyspalvelualalla kuusi prosenttiyksikköä on päätoimialaltaan kuntoutusalan palvelutuottajia. Käytännössä yli 40 prosenttia vastanneista ja etenkin pääosa keskisuurista ja suurista toimijoista on monialaisia palveluntuottajia, jotka tarjoavat markkinoilla erilaisia sosiaali- ja terveyspalveluja. Yleisimpiä palveluja ovat ikääntyneiden ja erityisryhmien asumispalvelut (Kuvio 5).

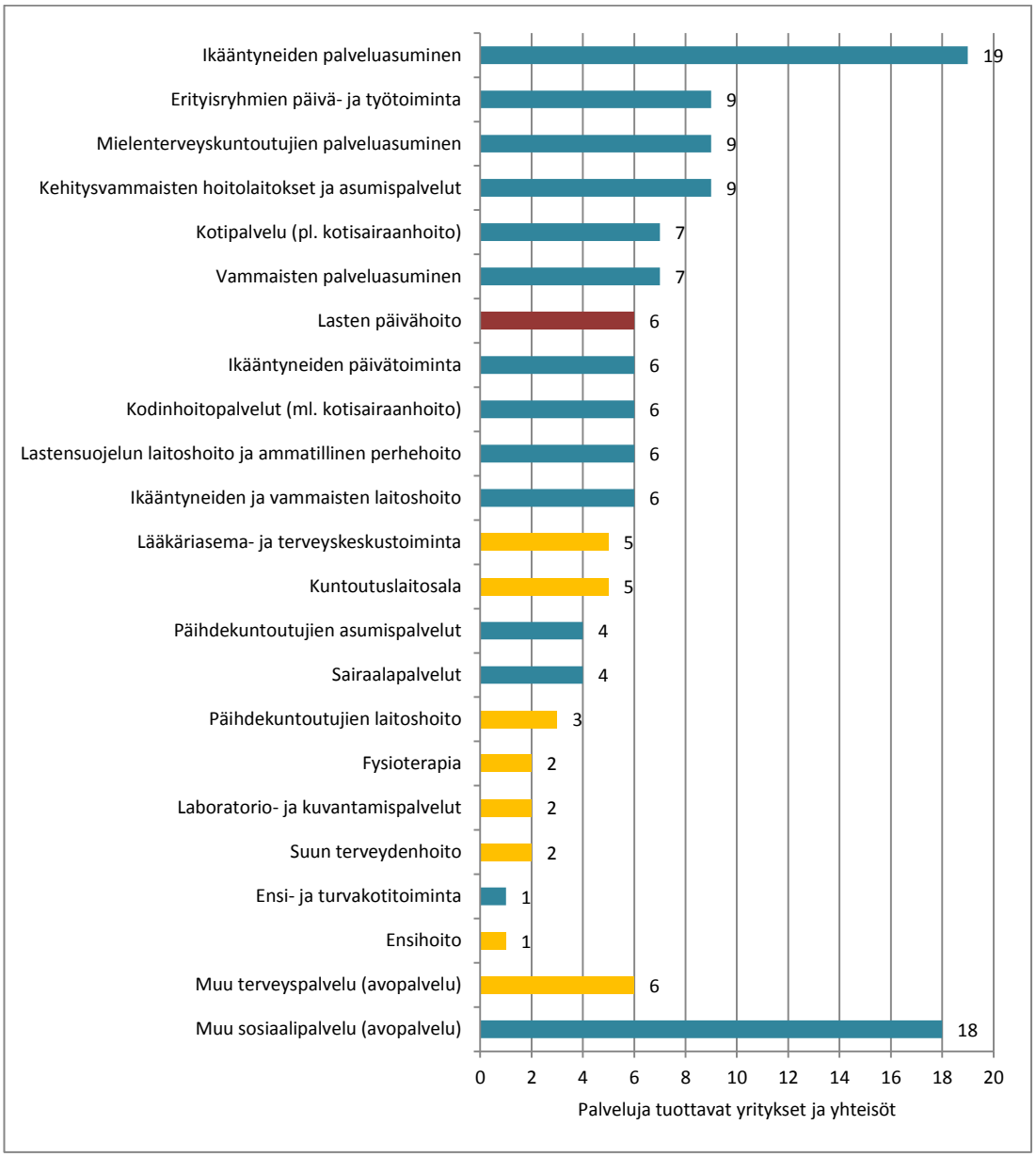
Kuvio 3 *Hyvinvointialojen turvallisuuskyselyyn vastanneet yritykset ja järjestöt henkilöstön ”päätoimialoittain”, lkm (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



Kuvio 4 *Hyvinvointialojen turvallisuuskyselyyn vastanneet yritykset ja järjestöt palvelutuotannon monialaisuuden mukaan, lkm (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



Kuvio 5 *Hyvinvointialojen turvallisuuskyselyyn vastanneet yritykset ja järjestöt niiden tuottamien yksittäisten SoTe- ja varhaiskasvatuksen palvelujen mukaan, lkm (Lähde: Hyvinvointialojen turvallisuuskysely 2021).*



Kysymysrunko

Vastaajien perustietoja olivat oikeudellinen muoto, henkilöstön koko ja toimiala (palveluvalikoima). Kyselyssä paneuduttiin ensiksi organisaation kokemiin keskeisiin uhkakuviin ja onnettomuusriskeihin. Toiseksi vastaajia pyydettiin kuvaamaan turvallisuustilanteen kehitystä sekä siihen vaikuttaneita tekijöitä viiden viime vuoden aikana sekä ennakoimaan turvallisuustilanteen kehitystä ja haasteita lähivuosina. Seuraavaksi kysyttiin, millaisia turvallisuusalan tuotteisiin, palveluihin ja järjestelmiin organisaatiot ovat hankkineet.

Erityisen mielenkiinnon kohteena olivat tietoturvallisuutta koskevat asiat. Hyvinvointialojen edustajilta tiedusteltiin, mitkä ovat heidän mielestään tärkeimmät tietoturvallisuuteen liittyvät uhkakuvat ja haasteet sekä sitä, miten niihin on varauduttu. Jälkimmäinen on jaettu kyselyssä teknisen ja hallinnollisen tietoturvallisuuden asioi-

hin sekä tietoturvallisuuden riskien arviointiin. Tietoturvallisuutta korostavat myös lainsäädännölliset vaatimukset ja se, kuinka suuri osa yrityksen tai järjestön liiketoiminnan prosesseista ja palveluista on digitalisoitu.

Erillisiin kysymyskohtiin kuuluivat, kuinka epidemiakriisi on vauhdittanut liiketoimintojen digitalisointia, onko organisaatio määrittänyt ne kriittiset tuotetut palvelut ja niihin liittyvät järjestelmät, joiden tietoturva ja toiminta tulee varmistaa kaikissa tilanteissa. SoTe-palvelujen tuottajilta tiedusteltiin lisäksi, onko palvelutuottaja mukana kanta-palveluissa sekä tarvitaanko sosiaali- ja terveydenhuoltoon kaikkia palveluntuottajia koskevat tietoturvan minimivaatimukset, joilla parannettaisiin potilas- ja asiakastietojen tietoturvan tasoa.