



Takaavatko standardit tietoturvan? Tarkastelussa tilaturvallisuusjärjestelmät

Thomas Kotziadimos

2020 Laurea



Laurea-ammattikorkeakoulu

Takaavatko standardit tietoturvan? Tarkastelussa tilaturvallisuusjärjestelmät

Thomas Kotziadimos
Tradenomi
Opinnäytetyö
Marraskuu, 2020

Thomas Kotziadimos

Takaavatko standardit tietoturvan? Tarkastelussa tilaturvallisuusjärjestelmät

Vuosi

2020

Sivumäärä

74

Tietoturva on noussut digitalisaation myötä vuosi vuodelta tärkeämpään rooliin erilaisissa organisaatioissa. Tämä opinnäytetyö on tutkimus, joka tarkastelee tietoturvaa tilaturvallisuusjärjestelmien näkökulmasta. Sen tarkoituksena on selvittää missä määrin voimassa olevien standardien mukaisesti toteutettua tilaturvallisuusjärjestelmää voidaan standardien vaatimusten kautta pitää tietoturvallisena järjestelmänä. Tämän opinnäytetyön toimeksiantaja on Kyberturvallisuuskeskus.

Tätä tutkimusta varten kerättiin laaja joukko tietoturvallisuuteen liittyvää tietoa teoreettisen viitekehyksen hahmottamiseksi. Aineisto muodostuu tietoturvallisuuden lainsäädännöstä, kansallisista ohjeista, alan kirjallisuudesta, artikkeleista sekä muista tutkimuksista. Osa vaikeimmista kysymyksistä edellytti aiheen teknisen luonteen takia myös alan asiantuntijoiden haastattelemista.

Aineistoon sovellettiin laadullisia tutkimusmenetelmiä ja siitä pyrittiin rajaamaan käyttöön juuri tilaturvallisuusjärjestelmiä koskevat seikat. Teemoittelussa nousi esiin neljä keskeistä tilaturvallisuuden tietoturvan osatekijää: tietoliikenteen turvallisuus, ohjelmistoturvallisuus, sensoreiden ja sulautettujen järjestelmien turvallisuus sekä rakenteelliset seikat, jotka voivat vaikuttaa tietoturvan toteutumiseen. Tilaturvallisuusjärjestelmiä koskevia standardeja verrattiin teemoittain kerättyyn aineistoon, tarkoituksena paikallistaa tietoturvaan vaikuttavia puutteita standardien vaatimuksissa.

Tutkimuksen aikana löydettiin tilaturvallisuusjärjestelmiä koskevista standardeista puutteita, jotka voivat vaikuttaa valvottavan tilan tietoturvaan epäedullisella tavalla. Huomioita tehtiin kaikista tietoturvan osa-alueista. Keskeisenä havaintona tutkimuksessa oli, että tilaturvallisuusjärjestelmien tietoturvan kehittämiseksi standardeja tai vähintään kansallista ohjeistusta tulisi kehittää, jotta järjestelmien ominaisuudet pysyvät ajanmukaisina.

Asiasanat: tilaturvallisuus, tietoturva, standardi, kyberuhka, sensori

Thomas Kotziadimos

Do standards guarantee information security? Reviewing security systems

Year 2020

Pages

74

Due to the spread of digitalization, the importance of the role of information security has increased in various organizations in recent years. This thesis examines information security from the viewpoint of security systems. The purpose of the thesis is to define, to which extent a security system implemented following the requirements set by the current standards can be considered safe in terms of information security. The client for this thesis is the National Cyber Security Center.

In order to establish the theoretical framework a vast amount of data about information security was gathered. Sources include legislation, national directives, literature, articles and other studies. Due to the technical nature of the subject, some of the more difficult questions required experts in the field to be interviewed.

Qualitative research methods were applied to the information gathered, with the purpose of narrowing out the information relevant to security systems. Four main themes rose from the material: information security of telecommunications, software security, security of sensors and embedded systems and structural considerations that could affect the information security of security systems. Standards that set requirements for security systems were compared against this data to pinpoint deficiencies in the requirements of the standards.

This study was able to find such deficiencies in the standards that concern security systems. These deficiencies could have an adverse effect on the information security of the space monitored by security systems. Observations were made in all areas of information security. A key finding in this study was that in order to develop the information security of security systems, the standards or at least national directives must be developed further to meet the challenges of the day.

Keywords: security systems, information security, standards, cyber threat, sensor

Sisällys

1	Johdanto.....	6
1.1	Opinnäytetyön aihe, rajaus ja tavoite	7
1.2	Opinnäytetyön toimeksiantaja	8
1.3	Keskeiset käsitteet.....	10
2	Kirjallisuuskatsaus.....	11
2.1	Tietoturvan säännösperusta	11
2.2	Tietoliikenneturvallisuus	17
2.3	Ohjelmistoturvallisuus.....	21
2.4	Sulautettujen järjestelmien ja ilmaisimien turvallisuus.....	27
2.5	Rakenteelliset turvallisuustekijät tietoturvan näkökulmasta	32
2.6	Arvioitavat standardit	35
3	Menetelmä	38
3.1	Haastattelut	40
4	Tulokset	41
4.1	Tilaturvallisuutta säätelevien normien huomioiminen	42
4.2	Tietoliikenteeseen liittyvät turvallisuuskulmat	43
4.3	Ohjelmistoturvallisuuden huomiointi standardeissa	44
4.4	Sulautetut järjestelmät ja ilmaisimet standardeissa	48
4.4.1	Kameravalvonnan tietoturva.....	49
4.5	Rakenteelliset seikat	50
4.6	Muut huomiot	52
5	Johtopäätökset	52
6	Arviointi	57
	Lähteet.....	58
	Kuviot	71
	Taulukot	71
	Liite 1: Teemahaastattelun runko, Riku Kalinen	72
	Liite 2: Teemahaastattelun runko, Aku Pänkäläinen	74

1 Johdanto

Tilaturvallisuus on osa erilaisten organisaatioiden, yritysten ja muiden toimijoiden turvallisuuden kokonaiskuvaa. Sen tarkoitus on osaltaan varmistaa toimijan kyky suorittaa esimerkiksi liiketoimintaa tai muuta tehtävää, jota varten organisaatio tilojaan hyödyntää. Se suojaa tehokkaasti omaisuutta, jopa työtuntien ulkopuolella. Se suojaa henkilöstöä monilta erilaisilta uhilta. Tilaturvallisuus suojaa myös merkittävältä osin toimijan hallinnoimaa tietoa. (Rasmus, Rossi, Nuutinen, Hovatta, Hovinen & Arenius 2019, 11- 15.)

Luomalla, ylläpitämällä ja kehittämällä tilaturvallisuutta voidaan vastata moniin erilaisiin riskeihin. Onnettomuuksia ja vahinkoja ilmaisevat tai niiden vaikutuksia vähentävät tilaturvallisuusjärjestelmät voivat vähentää merkittävästi organisaation tappioita erilaisten tapaturmien yhteydessä ja jopa pelastaa ihmishenkiä. Tilaturvallisuus torjuu myös tahallisen toiminnan, kuten ilkivallan ja rikollisen toiminnan, riskejä ja vähentää niistä aiheutuvia kustannuksia ja haittoja. (Rasmus ym. 2019, 11 - 15.)

Alati digitalisoituvassa maailmassa tieto virtaa globaalisti nopeudella, joka vielä muutamia vuosikymmeniä sitten olisi ollut vaikea kuvitella. Tiedosta on tullut kauppatavaraa. Sitä kerätään sen itsensä takia esimerkiksi markkinoinnin kohdistamiseksi mutta sen avulla voidaan vaikuttaa jopa demokraattisten järjestelmien toimintaan. Lainsäädännön kehittämällä pyritään vastaamaan ilmiön luomiin haasteisiin, mutta pelkät säännöt eivät estä haitallisia tapahtumia. Tarvitaan järjestelmiä, jotka kykenevät suojelemaan tietoa. (Tulokas 2018.)

Verkottuva maailma on myös kiihtyvällä tahdilla havainnut kyberuhkien nousun merkittäväksi turvallisuuteen vaikuttavaksi tekijäksi. Tahallisia kyberhyökkäyksiä eivät toteuta enää vain seikkailunhaluiset, tietotekniikasta kiinnostuneet nuoret vaan yhä enemmän tehdään havainnot organisoituneista toimijoista ja suunnitelluista hyökkäyksistä (Stamps 2020). Näitä kehittyneitä hyökkäyskeinoja ovat hyödyntäneet rikollisten lisäksi myös valtiolliset toimijat (CSIS 2020).

Digitalisaatio on uusista uhkakuvista huolimatta jo vakiinnuttanut paikkansa megatrendinä, joka tulee jatkumaan. Sen kiistattomat hyödyt esimerkiksi mobiilin teknologian, tietoperustaisen päätöksenteon, pilvipalveluiden sekä sosiaalisen median hyödyntämisen muodoissa tuovat liiketoiminnallista etua ja tehostavat organisaatioiden toimintaa (Oxford Economics 2015). Uusia digitalisaatioon liittyviä riskejä ja uhkakuvia tulee kuitenkin löytymään jatkossakin. Esimerkkinä yllättävästä uudesta hyökkäyksestä käynee Black Hat 2020 -konferenssissa esitelty menetelmä, jossa kaapattujen IoT -laitteiden avulla voidaan manipuloida sähkömarkkinoita merkittävien tulojen saamiseksi rikollisin keinoin (Shekari & Bayah 2020). Uhkaa tasapainottaa

niin ikään kehittyvä osaaminen tiedon turvaamisessa. Osana tätä kehitystä kulkee tilaturvallisuus ja sen vaikutukset tietoturvalle. Kuten Brooks ym. toteaa teoksen *Cybersecurity Essentials* alussa, tietoturvaa ei voi olla ilman fyysistä turvallisuutta (Brooks ym. 2018). Mutta voivatko niin ikään digitalisoituvat ja automatisoituvat tilaturvallisuusjärjestelmät itsessään sisältää tietoturvaan kohdistuvia riskejä niiden suunnittelussa, valmistuksessa tai käyttöön-otossa? Tähän kysymykseen pyritään vastaamaan tässä tutkimuksessa.

1.1 Opinnäytetyön aihe, raja- ja tavoite

Tämä opinnäytetyö käsittelee tilaturvallisuusjärjestelmien tietoturvaa. Opinnäytetyössä tarkastellaan, tilaturvallisuusjärjestelmiä koskevia standardeja ja selvitetään, kuinka niiden vaatimukset suhtautuvat tämän hetken tietämykseen tietoturvan yleisiin toimintatapoihin, tietoturvaa koskevaan normistoon sekä toisaalta niihin ongelmiin, joita tietoturvan parissa on kohdattu.

Tilaturvallisuusjärjestelmät käsittävät laajan joukon erilaisista teknisistä laitteista rakentuvia laitekokonaisuuksia. Niitä käytetään kontrolloimaan, rajoittamaan sekä valvomaan kulkua tiettyyn tilaan. Järjestelmien monimutkaisuus voi vaihdella suuresti. Yksinkertaisimmillaan järjestelmä voi koostua esimerkiksi tietyn sisäänkäynnin valvontaan ja kontrollointiin käytetyistä ilmaisimista tai laitteista. Laajojen kokonaisuuksien valvonta taas voi käsittää jopa mitattavien tietoliikenneyhteyksien avulla hallinnoidun ja tuhansista ilmaisimista ja laitteista rakentuvan kokonaisuuden, jonka valvonnan alle voi kuulua laaja joukko kiinteistöjä ja tiloja. (Rasimus ym. 2019, 11- 15.)

Tässä työssä tarkastellaan näitä järjestelmiä sääteleviä, Suomessa käytössä olevia standardeja. Tarkoituksena on selvittää, millaisia vaatimuksia standardit asettavat laitteiden toiminnalle. Standardien asettamia vaatimuksia tarkastellaan alan kirjallisuuden sekä asiantuntija-haastatteluiden valossa. Vertailemalla järjestelmille asetettuja vaatimuksia ja asiantuntijatietoa, pyritään selvittämään, onko standardien vaatimukset riittävällä tasolla. Toisin sanoen, voidaanko standardeja noudattavaa tilaturvallisuusjärjestelmän suunnittelua, valmistusta ja käyttöönottoa pitää tietoturvan näkökulmasta ongelmattomana? Keskeistä on selvittää, millaisia turvallisuuskäsitteitä standardit tilaturvallisuusjärjestelmien tapauksessa kattavat. Koska järjestelmät rakentuvat tietoteknisten sekä toisaalta elektronisten tai mekaanisten laitteiden varaan, yhdistyy niiden erilaisten tekniikoiden, materiaalien ja toimintalogiikoiden rajapinnoissa suuri joukko järjestelmän toiminnalliseen kokonaisuuteen vaikuttavia seikkoja. Standardeja tutkimalla pyritään selvittämään, kuinka nämä eri näkökulmat huomioidaan vaatimusten muodossa ja kuinka yksityiskohtaisia ja täsmällisiä vaatimukset ovat.

Arvioitaessa tilaturvallisuusjärjestelmien tietoturvaa asiaa voidaan tarkastella kahdesta näkökulmasta. Ensimmäisen näkökulman muodostaa järjestelmän itsensä riski - standardien vaatimusten puitteissa toteutettuna - mahdollistaa ulkopuoliselle pääsy tietoon, jota tilaturvallisuusjärjestelmällä pyritään suojaamaan. Toisena näkökulmana tarkastellaan, onko standardien mukainen tilaturvallisuusjärjestelmä altis tunnetuille haavoittuvuuksille ja onko järjestelmän suojaaman tilan tieto siten ulkopuolisten saatavilla esimerkiksi vaikuttamalla tilaturvallisuusjärjestelmän toimintaan erilaisin kyberhyökkäyksin.

Tämän opinnäytetyön päätutkimuskysymys on, missä määrin tilaturvallisuusjärjestelmiä säätelevät standardit takaavat, että tilaturvallisuusjärjestelmät eivät sisällä tai aiheuta riskejä niillä valvotun tilan tietoturvalle. Koska aihe on varsin laaja käsittäen mm. tietoliikenteen, ohjelmistoturvallisuuden, sulautettujen järjestelmien ja sensoreiden sekä rakenteellisten turvallisuustekijöiden näkökulmia, tutkimuskysymys jaetaan seuraaviin alakysymyksiin:

Tietoliikennettä koskeva tutkimuskysymys on, missä määrin standardien vaatimukset takaavat tilaturvallisuusjärjestelmien tiedonsiirron eheyden, saatavuuden ja luottamuksellisuuden. Ohjelmistoturvallisuutta koskeva tutkimuskysymys on, voidaanko standardien vaatimuksia noudattamalla suojata tilaturvallisuusjärjestelmien ohjelmisto nykyaikaisia hyökkäysmenetelmiä vastaan. Sulautettujen järjestelmien ja sensoreiden osalta kysytään, ovatko standardien vaatimukset tietoturvan osalta pysyneet nopeasti kehittyvän sensorteknologian perässä. Rakenteellisten tekijöiden osalta tutkimuskysymys on, huomioivatko tilaturvallisuusjärjestelmien rakenteelliset standardit tietoturvaan kohdistuvia hyökkäyksiä, joiden vaikutusmenetelmä perustuu rakenteen läpi tapahtuvaan vaikuttamiseen.

Tämän opinnäytetyön raportin lisäksi saatujen tietojen valossa laaditaan yhteenveto, josta koostetaan esitys opinnäytetyön toimeksiantajalle koulutuskäyttöön. Esityksessä on tarkoitus välittää selkeästi keskeiset standardien asettamat, tietoturvaan vaikuttavat vaatimukset sekä erityisesti muut seikat, jotka tulee huomioida tilaturvallisuusjärjestelmien tietoturvaa pohdittaessa. Opinnäytetyön toimeksiantajalle toimitettava materiaali ei ole osa opinnäytetyötä.

1.2 Opinnäytetyön toimeksiantaja

Toimeksianto opinnäytetyön laatimiseen saatiin liikenne- ja viestintävirasto Traficomiin kuululta Kyberturvallisuuskeskukselta. Opinnäytetyön ohjaajina kyberturvallisuuskeskuksesta toimivat jatkuvuuden hallinnan yksikönpäällikkö Janne Allonen sekä erityisasiantuntija Valtteri Tohka.

Traficom aloitti uudistuneessa kokoonpanossa 1.1.2019, kun Viestintävirasto ja Trafi yhdistyivät. Sen tehtävänä on kehittää liikennejärjestelmää ja tietoyhteiskuntaa koko valtakunnan

alueella valvomalla ja edistämällä liikenteen ja viestinnän markkinoita. Yhteensä se työllistää noin 900 henkeä. (Liikenne- ja viestintäministeriö 2018.)

Kyberturvallisuuskeskus on yksi Traficomien neljästä osaamisalueesta. Sen vastuulla on viestintäverkkojen ja -palveluiden toimintavarmuus, kyberturvallisuuden kehittäminen ja valvonta sekä kyberturvallisuuden tilannekuvan tuottaminen (Traficom 2020). Kyberturvallisuuskeskuksen organisaatio on niin ikään jaettu neljään eri toimintoon. CERT-toiminto painottuu tietoturvaloukkausten ennaltaehkäisyyn sekä turva-asioista tiedottamiseen. Se esimerkiksi kerää tietoa ja selvittää verkko- ja viestintäpalveluihin kohdistuvia tietoturvaloukkauksia. Pyrkimyksenä on, että viestintäverkkojen ja -palveluiden häiriöttömällä toiminnalla turvataan yhteiskunnan elintärkeitä toimintoja. CERT-toiminto voi lisäksi avustaa vakavien tietoturvaloukkausten teknisessä selvittämisessä. Tällaisia tilanteita voivat olla esimerkiksi internetin infrastruktuuriin, kuten nimipalveluihin ja runkoverkkoon kohdistuvat hyökkäykset, televerkkoon tai laajassa mittakaavassa internetsivustoja vastaan kohdistuvat hyökkäykset ja niiden yritykset tai kun tehdään havainto täysin uuden tyyppisen hyökkäystavan käytöstä. (Kyberturvallisuuskeskus 2020a.)

Tämä opinnäytetyö laaditaan kyberturvallisuuskeskuksen NCSA-toiminnon alla. NCSA-toiminnon tehtävät liittyvät turvallisuusluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn. Lyhenne NCSA tulee sanoista *National Communications Security Authority*. Tässäkin toiminnossa pääpaino on ennaltaehkäisyssä. Toiminto hyväksyy tietojärjestelmät käytettäväksi turvallisuusluokitellun tiedon käsittelyyn. Tehtäviin kuuluu myös salaustuotteiden arviointi ja hyväksyntä sekä salausteknisen materiaalin jakeluverkoston hallinnointi ja sen turvallisen käsittelyn ohjeistaminen. (Kyberturvallisuuskeskus 2020b.)

Kyberturvallisuuskeskuksen tehtäviin kuuluu myös toimialaan kuuluvien säännösten ja määräysten noudattamisen valvonta. Valvonnan piiriin kuuluu mm. teletoiminta, digitaaliset palvelut, vahva sähköinen tunnistus sekä verkkotunnusvälitys. Määräysten, suositusten ja selvitysten avulla sekä toimijoita rekisteröimällä pyritään häiriöttömään ja turvalliseen viestintään. Myös valvonnan piiriin kuuluvan lainsäädännön soveltamista koskevia ohjeita tuotetaan viranomaisten ja yritysten käyttöön. (Kyberturvallisuuskeskus 2020c.)

Kyberturvallisuuskeskuksen vastuulla on myös toimia eurooppalaisen Galileo -paikannusjärjestelmän palveluista vastaavana tahona. Vaikka paikannusjärjestelmän paikannussignaali on avoimesti kaikkien saatavilla, on järjestelmään kehitteillä tarkkuutta parantava HAS-palvelu (*High Accuracy Service*). Muita kehitteillä olevia palveluita ovat avoin ja kaupallinen sijaintitiedon varmennuspalvelu sekä viranomaiskäyttöön suunnattu PRS-palvelu (Kyberturvallisuuskeskus 2020d.). PRS-palvelun tarkoitus on käyttöönoton jälkeen mahdollistaa avointa signaalia varmempi paikka- ja aikatietosignaali, joka sietää tahallista häirintää ja väärentämistä avointa signaalia paremmin. (Kyberturvallisuuskeskus 2020e.)

1.3 Keskeiset käsitteet

Opinnäytetyön aihepiiriin kuuluu sanastoa ja käsitteitä, joiden määrittelemine opinnäytetyön tarkoituksiin on tarkoituksenmukaista. Määriteltävät käsitteet ovat: hälytin, hälytys, hälytysjärjestelmä, ilmaisins, käyttöoikeus, tilaturvallisuusjärjestelmä sekä tietoturva.

Hälytin on laite, joka antaa hälytysmerkin.

Hälytys tarkoittaa poikkeus- tai vaaratilanteen kommunikoinniseksi sovittua tai yleisesti ymmärrettyä ääni- tai valomerkkiä, viestiä tai ilmoitusta. Hälytyksen vastaanottaja voi tilanteesta ja järjestelmästä riippuen olla tietty henkilö tai viranomainen, hälytyksen vastaanottoon tarkoitettu valvomo, hätäkeskus tai määrittelemätön julkinen yleisö.

Hälytysjärjestelmällä tarkoitetaan tämän opinnäytetyön puitteissa sähköistä järjestelmää, joka automaattisesti tai manuaalisesti aiheuttaa hälytyksen.

Ilmaisimella tarkoitetaan laitetta, joka havaitsee tapahtuman tai olosuhteiden muutoksen ja lähettää havainnosta ilmoituksen vastaanottimelle, kuten esimerkiksi hälytysjärjestelmän keskuslaitteelle. Käytetään myös termiä sensori.

Käyttöoikeus tarkoittaa oikeutta käyttää järjestelmää esimerkiksi tietokoneen, käyttöpaneelin tai etäkäyttöyhteyden avulla. Käyttöoikeudella voidaan esimerkiksi rajata murtohälytysjärjestelmän eri toimintojen käyttöä.

Tietoliikenneturvallisuus on tietoturvan osa-alue, jossa tarkastellaan tietoverkkojen ja niissä tapahtuvan tietoliikenteen suojaamiseen liittyviä asioita.

Tilaturvallisuusjärjestelmä on kokonaisuus, joka koostuu tilan turvallisuuden tason kontrolloimiseksi asennetuista ilmaisimista, käyttölaitteista, hälytysjärjestelmästä ja muista teknisistä laitteista.

Tietoturvalle tarkoitetaan järjestelmien sisältämien tietojen eheyden, luottamuksellisuuden ja saatavuuden varmistaminen. Tilaturvallisuusjärjestelmien tapauksessa tiedon eheys voi tarkoittaa esimerkiksi hälytysjärjestelmän tai siihen kuuluvien ilmaisimien tilatietojen paikkaansa pitävyyttä. Se voi tarkoittaa myös esimerkiksi ilmaisimien välittämän tiedon saatavilla oloa vain niille tahoille, joille järjestelmän omistaja on määritellyt käyttöoikeuden järjestelmään. Se voi myös tarkoittaa erilaisten tilatietojen, kuten esimerkiksi hälytysten oikea-aikaista välittymistä vastaanottajille, valvomoon tai esimerkiksi hätäkeskukseen.

2 Kirjallisuuskatsaus

Tässä luvussa tarkastellaan, mitä tietoturvan näkökulmia liittyy tilaturvallisuusjärjestelmiin. Tietoturva on yleisellä tasolla hyvin laaja aihe. Tästä syystä, tarkastelu rajataan niihin seikkoihin, jotka ovat olennaisia tilaturvallisuusjärjestelmien tapauksessa. Toisaalta kuitenkin tarkastelussa joudutaan huomioimaan esimerkiksi verkkorajapintojen osalta yleisempiäkin tietoturvaan liittyviä näkökulmia, sillä nykyisin yhä enenevässä määrin myös tilaturvallisuusjärjestelmiin halutaan etäkäyttömahdollisuus (Pänkäläinen 2020).

Kirjallisuuskatsaus on jaettu neljään pääteemaan, jotka kukin keskittyvät tilaturvallisuusjärjestelmien tietoturvan eri osa-alueisiin. Teemojen valikoitumiseen vaikutti tietoturvan jäsentely tilaturvallisuusjärjestelmien erityispiirteiden näkökulmasta. Teemoittelua myös jouduttiin muokkaamaan ja uudelleenrajaamaan prosessin edetessä, samalla kun ymmärrys ilmiöstä ja ongelmista kasvoi ja jäsenyi.

Tutkimuskysymys kohdistuu tilaturvallisuusjärjestelmiä normatiivisesti sääteleviin standardeihin. Tästä huolimatta, on myös muuta normatiivista aineistoa, jonka kautta tilaturvallisuusjärjestelmien ominaisuudet muokkautuvat. Tätä aineistoa edustaa lait, asetukset sekä kansalliset ohjeet ja juuri tästä aineistosta kirjallisuuskatsaus lähtee liikkeelle. Kirjallisuuskatsaus on tämän jälkeen jaettu neljään teemaan, jotka ovat: tietoliikenne, ohjelmistoturvallisuus, sulautetut järjestelmät ja sensorit sekä rakenteelliset turvallisuustekijät.

2.1 Tietoturvan säännösperusta

Yhteiskunnan digitalisaatio on kiihdyttänyt tarvetta huomioida tietoturva erilaisissa normistoissa kuten lainsäädännössä, asetuksissa, sopimuksissa ja ohjeissa. Lainsäädäntöä tarvitaan turvaamaan globaalissa toimintaympäristössä operoivien viranomaisten, yritysten ja elinkeinonharjoittajien toiminnan perusteet tietoturvan näkökulmasta. Laki kansainvälisistä tietoturvavelvoitteista määrittelee tietoturvalle keskeiset viranomaiset ja niiden tehtävät. Kyseisen lain neljännessä luvussa 18. pykälä kertoo siitä, kuinka tärkeää sopimusosapuolien luottamuksen näkökulmasta on, että tietoa suojellaan asianmukaisin menetelmin. Kyseinen pykälä määrittelee kansainvälisen toimielimen ja sopimusvaltion edustajien vierailut. Tässä pykälässä annetaan mahdollisuus viranomaiselle sallia kansainvälisen järjestön tai sopimusvaltion edustajalle oikeus tutustua siihen, kuinka sopimukseen liittyvien seikkojen osalta turvallisuusjärjestelyt on toteutettu (24.6.2004/588). Kuvatus kaltaisia velvoitteita voi muodostua esimerkiksi EU:n turvallisuusluokiteltujen tietojen kohdalla. EU:n neuvosto on päätöksellään 2011/292/EU määritellyt turvallisuusluokiteltujen tietojen suojaamisen. Kyseinen päätös on ratifioitu suomalaisen lainsäädäntöön vuonna 2012 ja saatettu voimaan valtioneuvoston asetuksella vuonna 2015 (224/2012, 77/2015). Myös kumppanuusyhteistyö sotilasliitto NATO:n kanssa luo

kansainvälisiä tietoturvavelvoitteita (VAHTI 2013, 18). Edellä mainittujen lisäksi Suomi on solminut myös tietoturvavelvoitteita asettavia, kahdenvälisiä sopimuksia muiden maiden kanssa, joista esimerkkinä mainittakoon laki turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta Unkarin kanssa tehdystä sopimuksesta.

Laki julkisen hallinnon tiedonhallinnasta sekä siihen läheisesti liittyvä valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtioneuvoston hallinnossa, astuivat voimaan 1.1.2020. Kyseinen laki yhdenmukaistaa viranomaisten tietoaaineistojen laadukasta hallintaa ja tietoturvaa. Sen neljäs luku käsittelee tietoturvaa. Luvussa määrätään tunnistamaan ne tehtävät, joissa toimivilta tulee edellyttää erityistä luotettavuutta. Laki myös edellyttää, että tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvan tilaa ja varmistuttava, että sen hallinnoima tieto ja tietojärjestelmät ovat turvattuja. Tähän on pyrittävä mm. testaamalla käytössä olevien järjestelmien vikasietoisuutta ja jo hankintavaiheessa on varmistuttava, että järjestelmien tietoturvatyökalut on toteutettu järjestelmässä asianmukaisesti. Lain 15. pykälä edellyttää erikseen, että viranomaisen on tarpeellisin tietoturvatyökaluin varmistuttava, että ”tietoaaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia”. Kyseisen kohdan perusteella laki luo vaatimuksia myös tilaturvallisuudelle ja samalla tilaturvallisuuden toteuttavan järjestelmän mahdollisille tietoturvaan koskeville ominaisuuksille. Kuudestoista pykälä edellyttää, että tietojärjestelmiä varten on oltava käyttöoikeusjärjestelmä, jota pidetään ajantasaisena. Lokitietojen keräämisestä säädetään 17. pykälässä, jossa todetaan, että lokia kerätään järjestelmässä olevien tietojen käytön ja luovutuksen seuraamisen lisäksi myös virhetilanteiden selvittämistä varten. (Laki julkisen hallinnon tiedonhallinnasta 906/2019.)

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtioneuvoston hallinnossa määrittelee seikkoja kuten asiakirjojen turvallisuusluokat sekä yleisellä tasolla niiden käsittelystä, siirtämisestä ja säilyttämisestä. Asetus huomioi tietojärjestelmien kohdalla näkökohtia kuten esimerkiksi käyttäjien oikeustasojen eriyttämisen, tarpeettomien toimintojen rajoittamisen sekä salauksen riittävän tason, menemättä kuitenkaan teknisiin yksityiskohtiin. (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtioneuvoston hallinnossa 1101/2019.)

Valtiohallinnon puolella ohjeistustason normistoa edustaa Valtionhallinnon tietoturvan johtoryhmän laatima Toimitilojen tietoturvaohje. On huomattava, että kyseinen ohje on julkaistu vuonna 2013, joten nopeasti kehittyvällä tietoturvan kentällä, ohjeen soveltamisessa tulee ottaa huomioon, että sen sisältämät tiedot eivät ole ajan tasalla. Toimitilojen tietoturvaohjeen tarkoituksena on tukea valtioneuvoston toimijoita toimitilaturvallisuuden kysymyksissä, kun pyrkimyksenä on suojata salassa pidettävää aineistoa. Ohje huomioi tietoturvaan liittyvät lakisääteiset velvollisuudet ja kansainvälisten toimitilaturvallisuusvaatimukset, jonkin ongel-

mallista on, että ohje on julkaistu seitsemän vuotta ennen nykyisen lain voimaan tuloa. Ohjeen ikääntyminen näkyy etenkin siinä, että nopeasti kehittyvällä tietoturvan sektorilla myös lainsäädännön kehittyminen on ollut verrattain nopeaa. Tästä syystä osa lainsäädännöstä, johon ohjeessa viitataan, on kumoutunut lainsäädännön uudistumisen myötä (esimerkiksi valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa). Lisäksi on huomioitava, että ohje keskittyy korkeintaan turvallisuusluokka II (salainen) tasoisen tietoaineiston käsittelyn asettamiin vaatimuksiin eikä näin ollen kata niitä tarpeita ja vaatimuksia, jotka kohdistuvat tiloihin, joissa muutoin kuin satunnaisesti käsitellään turvallisuusluokan I (erittäin salainen) tietoaineistoja. Tämän lisäksi osa viranomaisten turvallisuusvaatimuksista on haluttu pitää salaisina, eikä niitä siten ole käsitelty lainkaan toimitilojen tilaturvallisuusohjeessa (VAHTI 2/2013, 13, 35.)

Toimitilojen turvallisuusohjeen ajattelumalli lähtee siitä, että eri luottamuksellisuuden tasoja edustavia tietoaineistoja tulee käsitellä tiloissa, jotka vastaavat toteutukseltaan kyseisen tietoturvatason vaatimuksia. Tilojen luokittelu on tehty värikoodein, siten että julkisesta tilasta erotettu perustason tila on vihreä alue. Korotetun tason tilaa edustaa väri keltainen. Korkean tason tilaa edustaa sininen ja kaikkein korkeinta tasoa edustaa punainen väri. Perustasolta lähtien edellytetään, että asiattomilta on pääsy tiloihin estetty. Tämä edellyttää, että pääsy-oikeuden haltija on tunnistettava, kun hän saapuu tilaan. Korkeammilla tasoilla saapuminen tilaan tulee kirjautua lokitietoihin. Keltaisen ja sinisen alueen pääsyä ohje rajaa myös hätätilanteissa, kuten esimerkiksi tulipalon sattuessa. Suojattuun tilaan ei tule olla pääsyä suoraan ulkopuolisesta säilytyksestä löytyvällä ns. putkiavaimella vaan kiinteistön sisäpuolella tulee olla erillinen, valvottu putkilukko, jonka avulla suojattuihin tiloihin voidaan päästä. Kulunvalvonnassa sinisellä vyöhykkeellä edellytetään kaksoistunnistusta. Lisäksi sinisellä vyöhykkeellä kulkuoikeuksien hallinta on oltava tilan haltijalla. (VAHTI 2/2013, 18-19, 29, 41.)

Kaapeloinnista ohjeessa todetaan, että kaapelointi tulee tehdä rakenteiden pintaan. Lisäksi ohje kehottaa suosimaan kaapeloinnissa valokuidun käyttöä, koska sen salakuuntelu on teknisesti vaikea toteuttaa edellyttäen, että kaapeliin päästään käsiksi fyysisesti, koska kaapeli ei vuoda sähkömagneettista säteilyä. Näin ollen valokaapelin kautta välitetyn tietoliikenteen suojausvaatimuksia voidaan tapauskohtaisesti korvata tilan valvontatoimenpitein. Tietoliikenteestä todetaan yleisemmin, että korkean turvatason tapauksessa tietoliikenneyhteydet on rakennettava kahdennettuna). (VAHTI 2/2013, 68 - 69.)

Suomessa on käytössä myös kansallinen turvallisuusauditointikriteeristö, joka tunnetaan yleisesti nimellä Katakri. Sen ensimmäinen versio julkaistiin vuonna 2009 ja sitä on sen jälkeen kehitetty edelleen erilaisissa työryhmäkokoontumissa, joissa on ollut edustettuna niin viranomaista kuin elinkeinoelämäkin. Katakriin viimeisin versio on julkaistu vuonna 2015, ja nopeasti kehittyvän tietoturva-alan näkökulmasta on jo hieman vanhentunut. Katakri on kehitetty työkaluksi, jonka avulla voidaan arvioida organisaation kykyä suojata tietoa. Sen sisältö

pohjautuu lainsäädäntöön ja kansainvälisten sitoumusten myötä syntyville tietoturva vaatimuksille. (Puolustusministeriö 2015, 2 - 3.)

Katakri jakautuu varsinaisen sisällön osalta kolmeen pääotsikkoon: turvallisuusjohtaminen, fyysinen turvallisuus sekä tekninen turvallisuus. Näistä kolmesta osasta kaksi viimeksi mainittua liittyvät näkökulmiltaan tilaturvallisuusjärjestelmien tietoturvaan kiinteästi. Fyysisen turvallisuuden vaatimuksissa korostuu suojattavien tilojen kulunvalvonta ja lukitus, sisältäen kuitenkin jonkin verran tulkinnanvaraisia ilmaisuja kuten: ”asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja”. Katakri jakaa tilat hallinnollisiin tiloihin, turva-alueisiin sekä teknisiin turva-alueisiin. Sisällöltään Katakri:n vaatimukset vastaavat edellä käsiteltyä toimitilojen turvallisuusohjetta ollen kuitenkin paikoin kattavammin ilmaistu. Esimerkiksi teknisellä turva-alueella ei vaatimuksen F 02 mukaan saa olla ”luvattomia tietoliikennesyhteyskäytöksiä tai laitteita”. (Puolustusministeriö 2015, 18 - 20.)

Katakrin vaatimuksessa F 03 edellytetään, että kulunvalvontaan, murtohälytyksen ilmaisuun sekä muuhun valvontaan käytetty laitteisto on ”hyväksytyjen teknisten standardien tai vähimmäisvaatimusten mukaisia”. Kyseiset, vaatimuksessa spesifioidut, standardit ovat tämän opinnäytetyön tarkastelun kohteena. Vaatimukset F 06 ja F 07 käsittelevät salakatselun- ja kuuntelun mahdollisuutta, joskaan mitään teknisiä määreitä vaatimuksiin ei liity. (Puolustusministeriö 2015, 23 - 28.)

Tekniseen tietoturvaan keskittyvässä Katakrin viidennessä luvussa on kansallisista ohjeista ja säädöksistä kaikkein täsmällisimmin otettu kantaa tietoturvan teknisiin vaatimuksiin. Se on jaoteltu osiin, jotka ovat: tietoliikenneturvallisuus, tietojärjestelmäturvallisuus, tietoaineistoturvallisuus sekä käyttöturvallisuus. Tietojenkäsittely-ympäristöjen suojattua yhteenliittämistä käsittelevässä vaatimuksessa I 01 edellytetään, että jo alkaen suojaustasolta IV, ”tietojenkäsittely-ympäristö on erotettu muista ympäristöistä”. Eri suojaustasojen tietoa käsittelevien järjestelmien välille edellytetään hyväksytyn yhdyskäytäväratkaisun hyödyntämistä. Vaatimuksen esimerkeissä tuodaan myös esiin, että suojattavan tiedon määrällä voi olla merkitystä tietovarannon luokitukseen. Esimerkiksi suuri määrä IV-tason tietoa voi edellyttää, että tietovarantoa käsitellään III-tason vaatimusten mukaisesti. Periaatteesta käytetään nimeä ka-
sautumisvaikutus. (Puolustusministeriö 2015, 30 - 32.)

Katakrin vaatimuksessa I 02 todetaan, että kaikkiin tietotekniikkajärjestelmiin tulisi suhtautua siten, että niiden oletetaan olevan epäluotettavia. Tästä syystä mitään tarpeettomia toiminnallisuuksia ei tulisi olla päällä ja kaikille päällä oleville toiminnallisuuksille tulee löytyä toiminnallinen tarve. Sama periaate koskee myös tietoliikenneprotokollia, joka tarkoittaa sitä, että vain toiminnallisen tarpeen edellyttämät protokollia pidetään käytössä järjestelmän muodostavissa laitteissa. Vaatimus sisältää myös huomion palvelunestohyökkäyksiin varautumisesta. (Puolustusministeriö 2015, 33.)

Etäyhteyksiä koskeva vaatimus I 04 vaikuttaisi olevan laadittu puhtaasti varsinaista tiedonkäsittely-ympäristön muodostavan tietotekniikan näkökulmasta. Vaatimuksessa luetellaan sen koskevan ensisijaisesti laitteita kuten palomuurit, reitittimet, kytkimet, palvelimet sekä työasemat. Siinä kuitenkin mainitaan tilaturvallisuusjärjestelmien tietoturvaan liittyen tärkeä seikka, sillä vaatimus edellyttää, että hallintayhteyksien suojauksien arvioinnissa tulee huomioida se, ”miltä osin ko. hallintayhteyden kautta pystytään vaarantamaan salassa pidettävät tiedot”. Esimerkkinä epäsuorasta tietoon pääsystä on mainittu mahdollisuus palomuurisääntöjen muokkaamiseen hallintayhteyden kautta. Etäyhteyksiin liittyviä näkökulmia täydentää vaatimus I 05, jossa todetaan, että kaikkiin langattomiin rajapintoihin tulee suhtautua kuten avoimeen verkkoon. Tämän lisäksi vaatimuksessa I 08 edellytetään, että hallintayhteyksien kirjautumisessa on oltava käytössä aikakatkaistu ja että kaikki järjestelmän päivitykset haetaan vain tietyistä lähteistä. (Puolustusministeriö 2015, 35 - 37, 42.)

Toimijoiden tunnistamisesta vaatimus I 07 edellyttää jo suojaustasolla IV, että jokaisella käyttäjällä on yksilöllinen, henkilökohtainen tunnistus. Vähintään salanasuojausta edellytetään jo tällä tasolla, kun taas suojaustasosta III eteenpäin edellytetään vahvaa, vähintään kahteen tekijään perustuvaa tunnistautumista. Lisäksi edellytetään, että päätelaite, jolta kirjautuminen suoritetaan, on tunnistettu teknisin menetelmin ennen sen pääsyä verkkoon. Kirjautumismenetelmä tulee lisäksi olla suojattu ns. *brute force* sekä *man-in-the-middle* -hyökkäyksiä vastaan ja että kaikki kirjautumisessa käytetty, verkon yli välitetty tieto kulkee salattuna. (Puolustusministeriö 2015, 40 - 41.)

Katakri:n vaatimus I 10 määrittelee, että suojaustasolla IV tallenteet, joita voidaan hyödyntää tietomurtojen selvittämisessä, on säilytettävä vähintään kuusi kuukautta. Tasoilla II - III edellytetään vähintään kahden tai viiden vuoden säilytysaikaa ja lisäksi lokitiedot on varmuuskopioitava. Vaatimus I 11 taas edellyttää, että on olemassa menetelmiä, joilla poikkeuksellinen verkkoliikenne voidaan havaita. Tämän tarkoituksena on tunnistaa mahdollisimman nopeasti esimerkiksi tekeillä oleva tietomurto. Vaatimuksessa I 13 otetaan kantaa ohjelmistoilla toteutettaviin pääsynhallintaratkaisuihin. Vaatimus edellyttää turvallisen ohjelmoinnin periaatteiden täyttämistä ja että rajapintojen on kestävä yleiset hyökkäysmenetelmät. Vaatimus luettelee käytännön toimenpiteitä turvallisen ohjelmiston takaamiseksi seuraavasti:

1. Ohjelmistokehittäjän riittävä tietoturvatietous on varmistettu.
2. Ohjelmistokehityksen aikana on suoritettu tietoturvaus-analyysi ja havaitut riskit on joko kontrolloitu tai nimenomaisesti hyväksytty.
3. Rajapinnat (ainakin ulkoiset) on testattu viallisilla syötteillä sekä suurilla syötemäärillä.
4. Riippuen ohjelmointiympäristöstä, helposti ongelmia aiheuttavien funktioiden ja rajapintojen käyttöön on määritelty politiikka ja sitä valvotaan.
5. Arkkitehtuuri ja lähdekoodi on katselmoitu.

6. Ohjelmakoodi on tarkastettu automatisoidulla staattisella analyysillä.
7. Ohjelmakoodin versionhallinnan ja kehitystyökalujen eheys on varmistettu.
(Puolustusministeriö 2015.)

Hajasäteilyyn liittyvä vaatimus I 14 toteaa, että suojaustasolla III - II suojautuminen toteutetaan Viestintäviraston NCSA-toiminnon hyväksymin menetelmin (Puolustusministeriö 2015, 51). Vaatimuksessa I 21 käsitellään fyysistä turvallisuutta pitkälti toimitilojen turvallisuusohjeen kanssa samalla tasolla, joskin vaatimus täsmentää tilanteita, joissa turvallisuusluokkien III tai II aineistoa joudutaan tilapäisesti käsittelemään alemman tason tilassa (Puolustusministeriö 2015, 61). Vaatimus I 23 puolestaan täsmentää aikaisempia ohjelmistojen haavoittuvuuteen liittyviä seikkoja määrittelemällä, kuinka palvelimia ja verkkolaitteita tulee testata säännöllisesti tunnistettujen haavoittuvuuksien varalta. (Puolustusministeriö 2015, 64.)

Laki yksityisistä turvallisuuspalveluista määrittelee, että rakenteellisen suojauksen tai sähköisten valvontajärjestelmien suunnitteleminen, asentaminen, korjaaminen sekä muuttaminen ovat turvasuojaustehtäviä. Lain kuudessakymmenes pykälä määrittelee nämä tehtävät luvanvaraisiksi siten, että niitä saa suorittaa vain turvallisuusalan elinkeinoluvan haltija. Poliisi julkaisee sivuillaan luetteloa turvallisuusalan elinkeinoluvan haltijoista. Tällä hetkellä tuoreimmassa luettelossa (päivätty 13.11.2020) on 771 sellaista turvallisuusalan elinkeinoluvan haltijaa, joiden kohdalla on hyväksyntä turvasuojaustehtäviin (Poliisi 2020).

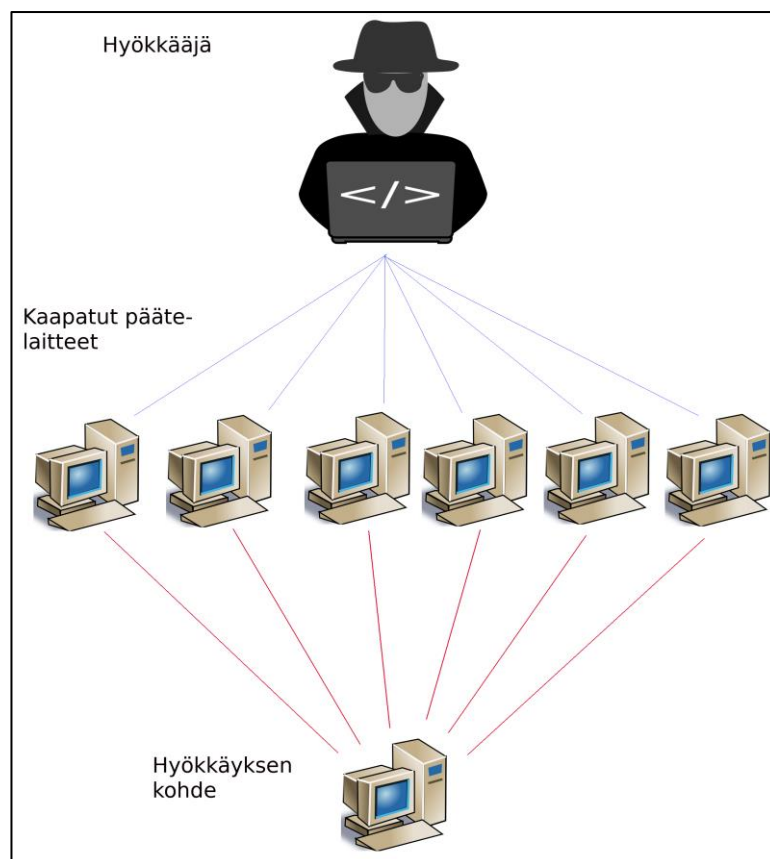
Finanssiala ry julkaisee luetteloa murtohälytysjärjestelmiä toimittavista liikkeistä (Finanssiala 2020). Tällä hetkellä kyseissä luettelossa on 198 yritystä. Tullakseen listatuksi kyseiseen luetteloon, murtohälytysjärjestelmiä toimittavan tahon on täytettävä Finanssiala ry:n vaatimukset, jotka on lueteltu Finanssiala ry:n julkaisemassa ”Murtohälytinsuunnittelun ja asennusliikkeiden vaatimukset”. Kyseisissä vaatimuksissa kohta 5.4 edellyttää, että asennuksissa on käytettävä ”hyväksyttyjä järjestelmän osia”, määrittelemättä asiaa tarkemmin. Muilta osin vaatimukset eivät käsittele tietoturvaan liittyviä asioita.

Turva-alan yrittäjät ry on julkaissut kesällä 2020 uusimman painoksen kameravalvontaoppaasta. Oppaan tarkoituksena on kehittää ja yhtenäistää kameravalvontaa käytännönläheisin ohjein. Se ei ole velvoittava asiakirja itsessään, mutta pyrkii selventämään asiaan liittyvää lainsäädäntöä. Muutama oppaan yli sadasta sivusta on omistettu tietoturvalle, ja ne käsittelevät asioita kuten kameravalvontajärjestelmän suunnittelu, yhteyksien suojaaminen, salasanoja, etäkäyttöä sekä ohjelmistopäivityksiä. Vaikka luetellut aiheet ovat tärkeitä, toimii kameravalvontaopas kuitenkin lähinnä yleisen tason katsauksena, menemättä kovin tarkasti tietoturvaa koskeviin yksityiskohtiin. (Turva-alan yrittäjät ry 2020.)

2.2 Tietoliikenneturvallisuus

Avoimesta verkosta tulevien tietoteknisten uhkien määrä on jatkuvassa kasvussa ja uusia, yhä kehittyneempiä hyökkäystapoja tulee esiin enemmän kuin koskaan aikaisemmin (Rerup ja Aslaner 2018, 250). Kun tilaturvallisuusjärjestelmä altistetaan etäkäytön myötä avoimen verkon turvallisuusriskeille, tulee suojautumisessa ottaa huomioon monia seikkoja.

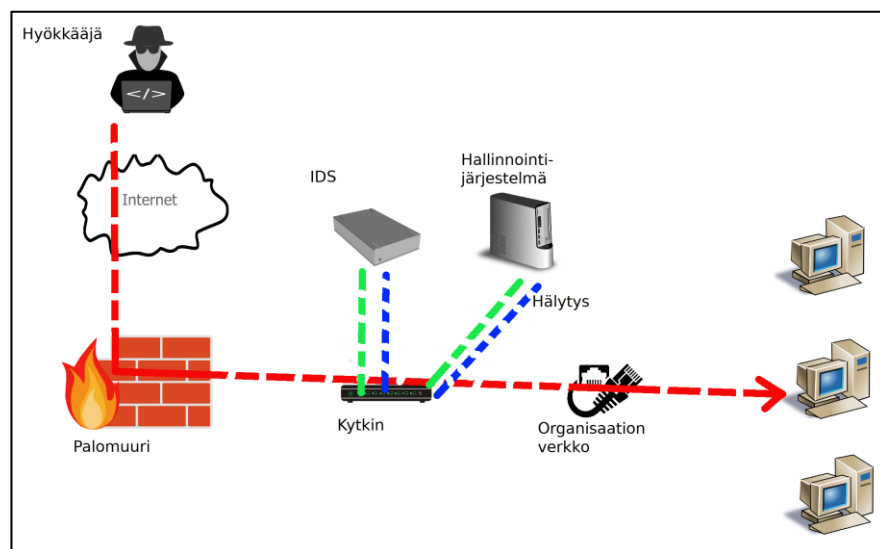
Yleisimpiä verkkoon kytkettyjen palveluiden haitaksi koituvia hyökkäyksiä ovat hajautetut palvelunestohyökkäykset (DDOS, *Distributed Denial Of Service*). Hyökkäys toteutetaan tyypillisesti kaapattujen, verkkoon kytkettyjen päätelaitteiden avulla ja tarkoituksena on lähettää hyökkäyksen kohteena olevalle palvelulle erittäin suuri määrä pyyntöjä verkkopalvelun toiminnan lamaannuttamiseksi. Toisinaan DDOS -hyökkäyksiä käytetään pohjustamaan jonkin toisen hyökkäysmenetelmän käyttöä tai sitä voidaan käyttää hämäysmielessä, pyrkimyksenä kiinnittää kohdeorganisaation tietoturvasta huolehtivan tahon huomio toisaalle. (Rerup & Aslaner 2018, 251.)



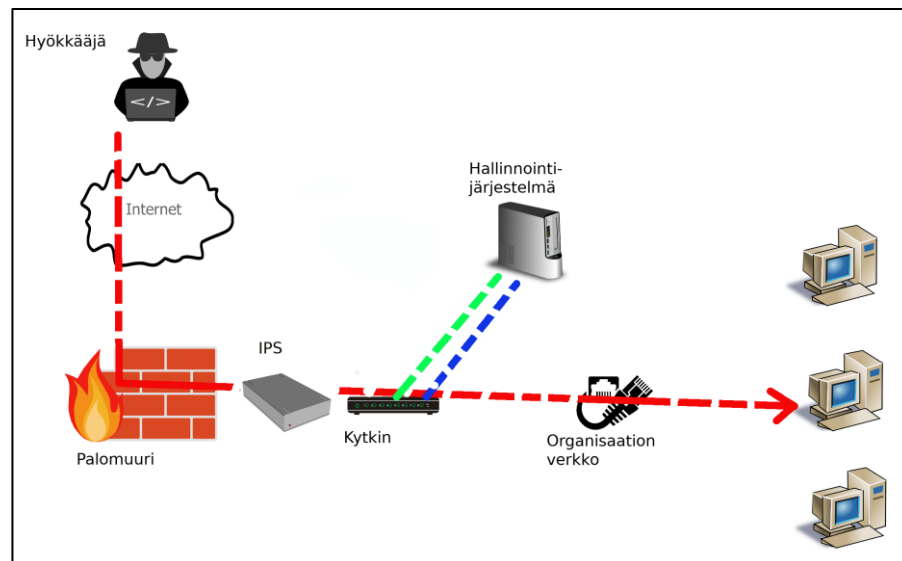
Kuva 1: Hajautettu palvelunestohyökkäys. Hyökkääjä käyttää suurta määrää kaapattuja päätelaitteita luodakseen niin paljon verkkoliikennettä hyökkäyksen kohteen suuntaan, että palvelun normaali toiminta estyy.

Rerupin ja Anslanerin mukaan varsinaiset tietomurrot liittyvät yleensä sellaisiin tapauksiin, joissa pyrkimyksenä on teollisuusvakoilu (2018). Tarkoituksena on tällöin päästä käsiksi organisaation salaisiin tietoihin ja käyttää niitä oman kilpailuaseman parantamiseen. Tietomurroissa yleisenä toimintatapana on hyödyntää ns. käyttäjän manipulointimenetelmiä (*Social Engineering*) käyttäjätunnusten hankkimiseen. Eräs tehokas ja yleinen menetelmä tunnetaan nimellä *Spear Phishing*. Siinä hyökkääjä hankkii etukäteen tietoa kohteesta ja räätälöi tiedonkalastelun kohteeseen sopivaksi (Sillanpää 2019, 20). Suojautumiskeinoina suositellaan tietosuuden lisäämistä yleisimmistä käyttäjän manipulointimenetelmistä, verkkoliikenteen valvomista turvallisuusohjelmistojen avulla sekä verkon suojaamista palomuurin avulla. Perinteinen palomuri ei välttämättä tarjoa enää nykyisin kovin hyvää suojaa kehittyneimpiä DDOS-hyökkäyksiä vastaan, mutta niin sanotut älykkäät palomuurit, jotka voidaan opettaa tunnistamaan uusia hyökkäystapoja, antavat paremman suojan. (Rerup & Aslaner 2018, 254 - 255.)

Verkon turvallisuus edellyttää valvontaa, jolla pyritään tunnistamaan tunkeutumisen tai sen yrityksen merkkejä kuten epätavallista tietoliikennettä tai epätavallista aktiiviteettia korkeimpien oikeustasojen käyttäjätunnuksilla (Mooney 2020, 28). Organisaation omaan verkkoon kytkettyjen päätelaitteiden suojaamiseksi verkon ulkopuolelta tulevia hyökkäyksiä vastaan voidaan käyttää erilaisia teknologioita. Hännisen (2019, 11 - 12) mukaan nämä palomuurista erilliset järjestelmät jakautuvat tunkeutumisen havaitseviin järjestelmiin (*Intrusion Detection System*, IDS), sekä järjestelmiin, jotka pyrkivät estämään tunkeutumisen (*Intrusion Prevention System*, IPS). Siinä missä IDS parantaa verkon turvallisuutta tunnistamalla tunkeutumisen ja ilmoittamalla siitä, toteuttaa IPS näiden lisäksi vastatoimia, joilla tunkeutuminen pyritään estämään tai rajaamaan (Hänninen 2019, 11 - 12).



Kuva 2: Intrusion Detection System. IDS valvoo verkkoliikennettä ja pyrkii tunnistamaan tunkeutumisen. (Hänninen 2019.)



Kuva 3: Intrusion Prevention System. IPS estää verkkoliikenteen, jonka se tunnistaa tunkeutumisiksi järjestelmään. (Hänninen 2019.)

Kun edellä esitetystä Hännisen (2019) kuvauksesta voisi tehdä johtopäätöksen IPS -tyyppisen laitteen eduksi, kuvailee kuitenkin Narwal ja Mohapatra (2020) IDS -tyyppisten ratkaisujen etuja mm. arkaluontoista tietoa sisältävissä, langattomissa potilastietojärjestelmissä (Narwal & Mohapatra 2020, 12 - 13). Heidän mukaansa IDS -järjestelmä voi tunnettujen hyökkäysten piireteiden lisäksi toimia siten, että se reagoi kaikkeen tavanomaisesta verkkoliikenteestä poikkeavaan tietoliikenteeseen. Tässä lähestymistavassa on kuitenkin riskinä väärät hälytykset, sillä oppiva järjestelmä adaptoituu verkkoliikenteen määriin viiveellä (Narwal & Mohapatra 2020, 13).

Edellä mainittuja näkemyksiä tukee myös Crawley (2016, 13), jonka mukaan paras päivittäisessä käytössä oleva verkon tietoliikenteen turvamenetelmä on aina päällä oleva, automatisoitu tunnistus ja torjunta. Singh, Singh ja Kaur (2018, 32) tekemän selvityksen johtopäätökset tukevat tätä näkemystä tuoden esiin mm. mahdollisuuden tunnistaa haittaohjelmien saastuttamia laitteita analysoimalla verkon DNS-tietoliikennettä. Heidän mukaansa juuri verkkoliikenteen tyyppillisen käyttäytymisen analysointi on tehokkaampi menetelmä kuin pyrkimys löytää itse haittaohjelma sen ennalta tiedettyjen tai oletettujen tuntomerkkien perusteella, sillä haittaohjelmat kehittyvät ja muuttuvat nopeasti (Singh, Singh & Kaur 2020, 32).

Mikäli hyökkääjä pääsee käsiksi verkkoon, voi hän käyttää verkkoliikenteen salakuunteluun erilaisia ohjelmia. Näitä verkkoliikenteen seurantaan tarkoitettuja ohjelmia kutsutaan *Sniffereiksi*. Verkkoliikenteen salakuuntelu voi olla luonteeltaan jatkuvaa, jolloin verkossa liikkuvat paketit ovat hyökkääjän saatavilla reaaliaikaisesti. Kuuntelua voidaan toteuttaa myös verkkoliikennettä tallentamalla. Tällöin hyökkääjä voi satunnaisesti ottaa yhteyden verkkoon ja ladata käyttöönsä tallenteen, joka sisältää kopion verossa tapahtuneesta tiedonsiirrosta. Perinteisten, päätelaitteita ja palvelimia yhdistävässä paikallisverkossa voidaan toteuttaa myös erilaisia välimieshyökkäyksiä (*Man-in-the-middle-attack*). Hyökkääjä voi esimerkiksi muuttaa verkossa salaamattomana kulkevan sähköpostin sisältöä ennen sen päätymistä vastaanottajalle. Mikäli hyökkääjä kuitenkin ainoastaan kuuntelee verkkoliikennettä, voi hyökkääjän toimia olla hyvin vaikea havaita. Salakuuntelua voidaan vaikeuttaa huomattavasti salaamalla verkon tietoliikenne. Verkko voidaan myös jakaa eri segmentteihin, jolloin yhteen verkon osaan päästyään, hyökkääjä ei pysty kuuntelemaan koko verkon liikennettä. Yksittäiset verkon käyttäjät voivat parantaa turvallisuutta käyttämällä eri verkoissa ja palveluissa eri salasanoja ja vaihtamalla salasanoja riittävän säännöllisesti. (Rerup & Aslaner 2018, 253 - 254.)

Eräs tapa etäyhteyden luomiselle on tilanne, jossa etäyhteys avataan vain tarvittaessa järjestelmän haltijan toimesta esimerkiksi sovittuna aikana. Tämä toimintamalli sopii etenkin etänä suoritettavien päivitysten ja muiden ylläpitotoimenpiteiden suorittamiseen. (Pänkäläinen 2020.)

Rerupin ja Anslanerin (2018) mukaan VPN-tekniikan käyttö on jossain määrin korvannut edellä mainittuja, tarkoitusta varten avattuja tiedonsiirtoyhteyksiä. Lyhenne VPN (Virtual Private Network) tarkoittaa virtuaalista erillisverkkoa, jonka kautta verkkoliikenne kulkee yleensä salattuna. Suojelupoliisin järjestelmäasiantuntijan Riku Kalisen (2020) mukaan edellä mainituista ominaisuuksista johtuen juuri VPN, yhdessä vahvan, kahteen tekijään pohjautuvan tunnistautumisen kanssa, on suositeltava tapa etäyhteyden muodostamiseen. Rerup ja Anslaner (2018) kuitenkin toteavat, että VPN on mahdollisesti korvautumassa SSL-pohjaisten, salatun verkkoliikenteen mahdollistavien, julkisen verkon protokollien hyödyntämisen yleistyessä.

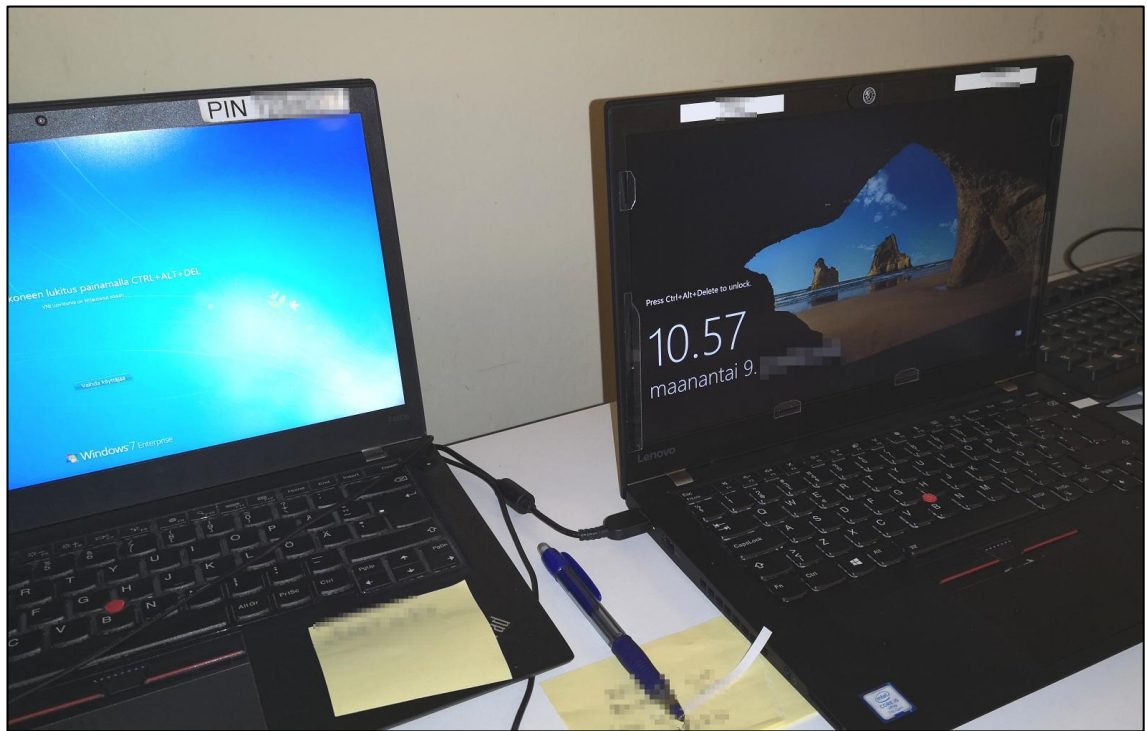
Mm. Kalinen (2020) mainitsee, että verkon turvallisuutta voidaan parantaa kytkemällä pois sellaisia palveluita ja protokollia, jotka eivät ole välttämättömiä järjestelmän toiminnan kannalta. Samalla kannalla on myös Katakri. Mansfield-Devine (2017, 15) kuitenkin tuo esiin, että joissain tapauksissa toiminnallisuuden rajaaminen voi johtaa uusien haavoittuvuuksien syntymiseen, joten järjestelmän toiminnallisuutta on ajateltava kokonaisuutena. Esimerkkinä Mansfield-Devine mainitsee Mirai -bottiverkon kohteena olleet laitteet, joiden BusyBox -käyttöjärjestelmän ominaisuuksia karsimalla, ohjelmiston kehityksestä vastannut XiongMai -niminen yritys, oli käytännössä luonut haavoittuvuuden, joka oli edellytys Mirai -bottiverkon syntymiselle.

2.3 Ohjelmistoturvallisuus

Kaikki tietoverkossa toimivat päätelaitteet sisältävät ohjelmiston. Päätelaitteilla tarkoitetaan laitteita kuten pöytätietokoneet, kannettavat tietokoneet, mobiililaitteet sekä palvelimet. Näihin laitteisiin liittyy riski siitä, että niihin pääsee tunkeutumaan sellainen henkilö, jolla ei pitäisi olla pääsyä kyseiseen laitteeseen. Hänninen (2019, 9 - 10) käyttää omassa tutkimuksessaan Shell:n ja Martin:n vuonna 2006 teoksessa *Webster's New World Hacker Dictionary* esittämää määritelmää tunkeutumisesta: ”vaarantaa järjestelmä ohittamalla sitä suojaavat turvatekijät tai aiheuttamalla sen joutuminen turvattomaan tilaan”. Mooney:n (2020, 9) mukaan iso osa päätelaitteiden aiheuttamista ongelmista on perinteisesti johtunut laitteiden vikaantumisesta, kuten esimerkiksi kiintolevyn rikkoutumisesta, mutta jatkuvasti suurempi osa ongelmista johtuu tahallisista tietoturvaan kohdistuvista hyökkäyksistä. Tästä johtuen, siinä missä kyberturvallisuus oli aikaisemmin vain harvojen organisaatioiden ongelma, on tänä päivänä kaikkien organisaatioiden panostettava luottamuksellista tietoa sisältävien päätelaitteidensa suojaamiseen. Päätelaitteiden tietoturvaan liittyvät tekijät jakautuvat kolmeen ryhmään: ohjelmistojen turvallisuus, tietovarantojen turvallisuus sekä verkon turvallisuus. (Mooney 2020, 9-11.)

Virheet ohjelmistojen toteutuksessa ja suunnittelussa voivat vaarantaa päätelaitteen tietoturvan, kuten käy ilmi Mooney:n (2020) esimerkissä. Tietoturvan parissa työskennellyt testaa pystyi löytämään tutkimastaan järjestelmästä ensin virheen, jonka avulla hän pääsi näkemään järjestelmän sisäisiä tiedostoja. Näistä hän löysi edelleen toisen virheen, jonka avulla hän pystyi saamaan järjestelmän suorittamaan mitä tahansa syöttämäänsä koodia, asettaen järjestelmän ja kaiken sen sisältämän tiedon vakavaan vaaraan väärissä käsissä. (Mooney 2020, 39.)

Ohjelmistojen turvallisuuden puutteet eivät aina johdu pelkästään virheistä ohjelman toteutuksessa vaan kyse voi olla tilanteesta, jossa järjestelmän käytettävyyttä painotetaan sen turvallisuuden kustannuksella. Esimerkkejä näistä tapauksista ovat vaikkapa jaetut kansiot sekä kaksisuuntainen tiedonsiirto tulostimen ja työaseman välillä. Joissain tapauksissa vaakakuppi voi kallistua turvallisuuden asemasta käytettävyyden suuntaan, jos ajatellaan, että kyseisessä päätelaitteessa ei ole kriittisiä tietoja. Tietomurron suunnittelijalle kuitenkin monet sinänsä viattoman oloiset tiedot voivat toimia osana esimerkiksi käyttäjän manipulointiin tähtäävän hyökkäyksen räätälöintiin juuri kohdeorganisaatiota varten. Tällaisia tietoja ovat esimerkiksi käyttäjän koko nimi sekä asema organisaatiossa. (Bradley & Carvey 2006, 5 - 6.)



Kuva 4: Tietoturva vastaan käytettävyys. Kuvan tietokoneissa on organisaation korkean turvatason johdosta salattu kiintolevy sekä salasanalla suojatut käyttäjätilit. Salasanat löytyvät kuitenkin tarralapuilta, jolloin käytettävyyden helpottuminen samalla mitätöi tekniset turvajärjestelyt. (Kirjoittajan oma arkisto.)

Työasemien ohjelmistojen turvallisuutta parantavia tekijöitä on lukuisia. Perustana voidaan pitää työaseman kiintolevyn salausta sekä riittävän turvallisten salasanojen edellyttämistä järjestelmään kirjautumisen yhteydessä. Kirjautumisen ei tule olla mahdollista muistiin tallennetun salasanan avulla. Käyttäjillä tulee olla yksilölliset käyttäjätilit ja ylläpitotehtäviä varten tulee olla luotuna mahdollisimman rajallinen määrä ylläpitotehtäviin käytettäviä käyttäjätilejä. Käyttäjätilien oikeustasojen avulla rajoitetaan käyttäjien pääsyä eri tietoihin. Käyttäjätilien tulee lukittua itsestään tietyn ajan kuluessa, jos laite ei ole käytössä. Jokaisessa päätelaitteessa tulee olla ohjelmisto, joka pyrkii tunnistamaan erilaisia haittaohjelmia ja estämään niiden toiminnan. (Bosworth, Kabay, & Whyne 2014, 17.)

Tietovarantojen turvallisuuden keskeinen tekijä tietojen salauksen käyttäminen (Mooney 2020, 28). Tilanteessa, jossa hyökkääjä onnistuu tietomurron seurauksena saamaan haltuunsa organisaation tietovarannon sisältämän tiedon, voi tieto olla hyödytöntä hyökkääjälle, jos se on asianmukaisesti salattu. Salauksen hyödyntäminen on ollut avuksi todellisissa tapauksissa, kuten esimerkiksi vuoden 2013 Adobeen kohdistuneen tietomurron yhteydessä. Vaikka hyökkääjä sai käsiinsä paljon arkaluonteista tietoa, ei hyökkääjä päässyt salauksen takia käsiksi

Adoben asiakkaiden luottokorttitietoihin. Toisaalta tunnetaan tapauksia, joissa tietomurron seurauksena esimerkiksi erittäin arkaluonteisia, mielenterveyspotilaiden terapiamuistiinpanoja on päätyntä julkisuuteen yhdessä potilaat yksilöivien henkilötietojen kanssa. Psykoterapiakeskus Vastaamon tapauksessa toimittajan tavoittama tietomurron toteuttanut taho syytti psykoterapiakeskusta huonosta tietoturvasta. (Mooney 2020, 60 sekä Rimpiläinen 2020.)

Monet hyökkäykset tietojärjestelmiä vastaan edellyttävät käyttäjältä aktiivisia toimia. Tyypillinen keino on lähettää hyökkäyksen kohteelle sähköposti, jonka liitetiedostoon on upotettu haittaohjelma. Erästä variaatiota kutsutaan nimellä RAT (*Remote Access Trojan*), jollaisen avulla hyökkääjä pääsee käsiksi kohdetietokoneeseen ja voi mm. ottaa kuvaruutukaappauksia ja tallentaa kaikki näppäimistön painallukset (Salmon, Levesque, & McLafferty 2017, 84 - 86.). Salmon ym. (2017, 87 - 94) mukaan ilmaiseksi saatavilla olevan Metasploit -ohjelman avulla RAT voidaan piilottaa esimerkiksi PDF- tai MS Word -tiedostoon, jolloin taitavasti kohdeorganisaatiota varten räätälöity sähköposti voi herättää riittävästi luottamusta, jotta käyttäjä avaa tiedoston ja haittaohjelma pääsee asentumaan. Toisaalta jo aikaisemmin Okamoto on esittänyt tavan, jolla kaikki Metasploit -työkalun hyökkäykset voidaan vähintään tunnistaa (Okamoto 2015, 691 - 698).

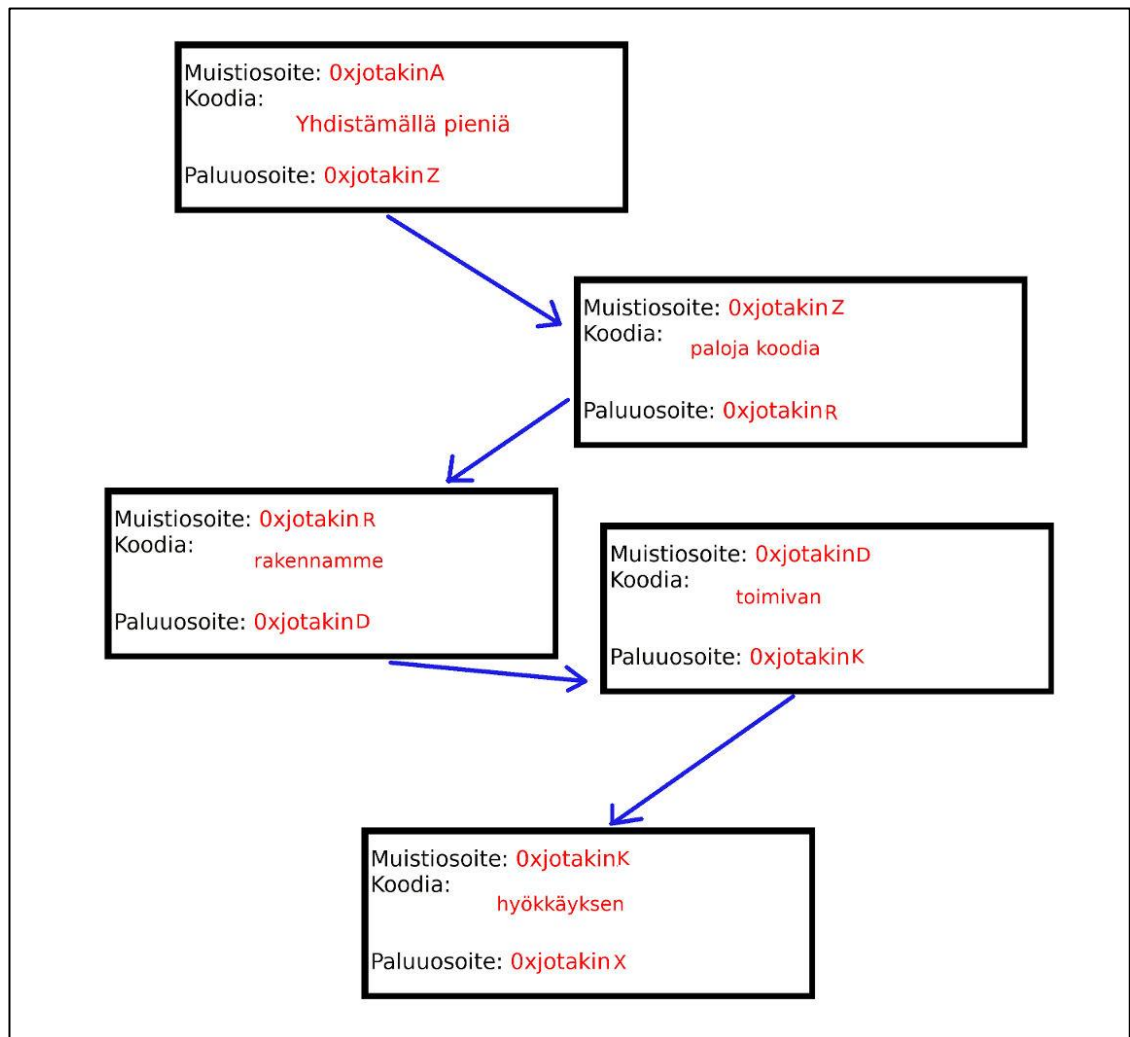
Tietoteknisten järjestelmien turvallisuus on jatkuvaa kilpajuoksua hyökkäysmenetelmien kehityksen kanssa. Ohjelmistoista löytyvät viat ja haavoittuvuudet näyttävät mahdollistavan käytännössä ehtymättömän keinovalikoiman toinen toistaan erikoisempia tekniikoita, jotka vain odottavat löytäjänsä. Esimerkiksi vuonna 2019 Windows10 -käyttöjärjestelmästä paljastui vika sen DACL-järjestelmästä (*Discretionary Access Control List*). Vian ansiosta hyökkääjä saattoi tiedostojen rakennetta muokkaamalla onnistua saamaan ylläpitäjätason oikeudet käyttöjärjestelmään. Toinen, edellistä mielikuvituksellisempi ja oikeuksia ylläpitotasolle laajentava, Windows -käyttöjärjestelmistä löydetty haavoittuvuus edellytti valikon luomista ja sen poistamista heti kun ohjelma oli kutsunut kyseistä valikkoa. (Diogenes & Ozkaya 2019, 182.)

Joitakin vuosia sitten ohjelmistojen turvallisuudelle aiheutti ongelmia ns. puskurinylivuotoa hyödyntävät hyökkäykset. Näissä hyökkääjä tutki järjestelmän käyttämää koodia etukäteen, pyrkien löytämään esimerkiksi funktioita, joiden ohjelmoinnissa ei varauduttu riittävästi huomioimaan, mitä syötteitä funktio voi saada. Kun esimerkiksi merkkijonon kopiointiin tarkoitettulle *strcpy()* -funktioille annettiin riittävän pitkä syöte, voitiin löytää kohta, jossa funktion syötteen tarvitsema muisti ylitti sillä käytössä olevan muistin määrän. Tämän tiedon pohjalta voitiin takaisinlaskemalla selvittää kaksi asiaa: missä tarkassa muistin kohdassa on tallennettuna paluusoite funktiota kutsuneelle ohjelmakoodille ja miten pitkä syöte mahtuu muistitilaan ennen tätä paluusoitetta. Näitä kahta tietoa hyödyntäen hyökkääjä saattoi laatia syötteen, jolla ohjelman suoritus voitiin ohjata hyökkääjän luoman koodiin. Puskurinylivuotohaavoittuvuuksia vastaan alettiin etsimään erilaisia suojautumistapoja. Yksi lähestymistapa oli

tietenkin korjata olemassa olevia ohjelmia ja kirjastotiedostoja siten, että syötteiden käsittelyssä varmistuttiin, että syötetty tieto oli turvallista käsiteltäväksi. Tämän lisäksi tulivat järjestelmien muistia suojaavat tekniikat, kuten DEP (*Data Execution Prevention*) sekä ASLR (*Address Space Layout Randomization*) joilla pyrittiin estämään muun kuin suoritettavaksi tarkoitettavan tiedon ajamista ohjelmana sekä vaikeuttamaan paluusoitteiden ja funktioiden muistipuskurien muistiosoitteiden selvittämistä. Koska DEP esti hyökkääjän oman koodin suorittamisen, kun koodi ei sijainnut suorittamista sallivalla muistialueella, alkoivat hyökkääjät nopeasti hyödyntämään järjestelmässä jo sisällä olevaa ohjelmakoodia hyökkäyksen rakentamiseen. Käytännössä tämä tarkoitti paluusoitteiden osoittamista *libc*-kirjastotiedostoon, jonka sisäisen toiminnallisuuden varaan erittäin monet ohjelmat rakentuvat. ASLR kuitenkin vaikeutti *libc*:n sisältämän koodin paikallistamista muistissa. (Bramwell 2018, 268 - 284.)

Myös Bhattacharjee (2018) on tehnyt havaintoja, joiden mukaan varsinkin heikomman suorituskyvyn omaavissa laitteissa, kuten IOT-laitteissa, varautuminen puskurinylivuotohaavoittuvuuksiin ja väärän laisiin syötteisiin perustuviin hyökkäyksiin on puutteellista. Lisäksi näissä laitteissa ohjelmistoalustojen mahdollistamia turvallisuutta parantavia tekijöitä ei ole yleensä oletusasetuksissa otettu käyttöön. Laitteet eivät myöskään usein ylläpidä lokia tapahtumista. Verkkorajapintojen puolella on usein käytössä haavoittuvia tiedonsiirtoprotokollia eikä fyysisiä portteja ole välttämättä suojattu mitenkään. (Bhattacharjee 2018, 32.)

Kun tietokonejärjestelmien suojaaminen puskurinylivuotoa hyödyntäviin hyökkäyksiin kehittyi, Bramwellin (2018, 268 - 284) mukaan hyökkääjät siirtyivät seuraavaksi rakentamaan hyökkäyksen suoraan hyökkäyksen kohteena olevan ohjelman sisältämistä, konekielisestä koodista. Menetelmä tunnetaan nimellä ROP (*Return Oriented Programming*). Bramwell nimeää hyökkääjillä käytössään olevia, ilmaisia ja helposti saatavia työkaluja hyökkäysten räätälöintiin, kuten esimerkiksi MSFrop ja ROPgadget. Eräs suojautumiskeino tätä tekniikkaa hyödyntäviltä hyökkäyksiltä on ROP -hyökkäyksen ajonaikainen tunnistaminen, kuten Das, Chen, Chandramohan, Liu & Zhang (2018, 374) esittävät. Das ym. esittelevät tutkimuksessaan ROPSentry -nimisen, adaptoituvan menetelmän, jonka ROP-hyökkäyksen tunnistus perustuu matalan tason tapahtumien analysointiin.



Kuva 5: ROP-hyökkäysmenetelmä. Hyökkäys rakennetaan yhdistelemällä suoritettavan koodin paloja, jotka peräkkäin suoritettuna toteuttavat hyökkääjän haluaman toiminnallisuuden. (Bramwell 2018, 268 - 284.)

Bramwellin edellä kuvailemiin hyökkäysmenetelmiin nähden toista ääripäätä edustaa Mishran, Agarwalin ja Sumanin (2018) tutkimuksen näkökulma, joka painottuu päätelaitteiden haavoittuvuuksiin, jotka luodaan asentamalla laitteeseen valmistusvaiheessa hyökkäyksen mahdollistava elektroniikkakomponentti. Mishran ym. mukaan näitä tapauksia tunnetaan ja ne ovat mahdollisia kaikissa eri päätelaitetyypeissä. Nämä uhat jakautuvat kahteen ryhmään: jatkuvasti päällä oleviin, haitallisiin komponentteihin, joiden pääasiallinen tehtävä on tapahtumien ja tietojen seuranta sekä toisaalta ns. laukaistaviin haitallisiin komponentteihin, joiden pääasiallinen tarkoitus on mahdollistaa hyökkääjän pääsy päätelaitteeseen tarvittaessa. Haitallisen komponentin tunnistaminen voi olla erittäin vaikeaa ja on siksi erittäin kallista. (Mishra, Agarwal & Suman 2018, 69 - 70.)

Mobiililaitteiden kohdalla kehitys on siinä pisteessä, että ne ovat tiedonkäsittelykyvyiltään ja verkottuneisuudeltaan vähintään perinteisten työasematietokoneiden veroisia. Tästä syystä myös niiden ongelmat tietoturvan suhteen ovat rakenteeltaan hyvin saman kaltaisia. Android -ekosysteemissä mobiililaitteen käyttöjärjestelmäytimenä toimii Linux -kernel. Linux on vuosien saatossa kehittynyt voimakkaasti tietoturvaominaisuuksissaan ja se tarjoaa käyttöjärjestelmän ytimenä tietoturvaan monia etuja, joita ei varsinkaan vanhemmissa Windows -käyttöjärjestelmän versioissa ollut mukana. Näitä ovat mm. käyttäjäkohtainen oikeuksien hallinta sekä suoritettavien prosessien eriyttäminen. Näiden perusrakenteiden avulla niin käyttäjät kuin ohjelmatkin voidaan rajata toimimaan vain niillä oikeuksilla, joita niille on myönnetty. Lisäksi alkaen Android -versiosta 4.3, Android on tukenut tietoturvaominaisuuksiltaan vahvistetun, SELinux -kernelin käyttöä (Security-Enhanced Linux). (Skulkin, Tindall & Tamma 2018, 21-26.)

Näistä turvatekijöistä huolimatta, mobiililaitteita vaivaa monet tietoturvaongelmat. Esimerkiksi kuuluisa Pegasus -niminen, mobiililaitteisiin suunnattu vakoiluohjelma käyttää kolme eri haavoittuvuutta tai virhettä ohjelmistossa asentuaakseen ja toimiakseen. IOS-ekosysteemissä käytetyssä Safari -internetselaimessa olleen haavoittuvuuden ansiosta Pegasus-vakoiluohjelman asentuminen käynnistyy haittaohjelman sisältävää linkkiä seurattaessa. IOS:n käyttöjärjestelmäytimessä olleen haavoittuvuuden ansiosta käyttöjärjestelmäytimen sijainti laitteen muistissa oli mahdollista selvittää. Lisäksi toisen käyttöjärjestelmäytimessä olevan, muistin korruptoitumiseen liittyvän haavoittuvuuden avulla Pegasuksen on mahdollista päästä valvomaan laitteen kaikkia toimintoja, kuten esimerkiksi kameran ja mikrofonin kautta tulevaa informaatiota sekä mitä käyttäjä kirjoittaa laitteella. (Citizen Lab 2016.)

Mobiililaitteiden ongelmiin on kaksi perimmäistä syytä, joista merkittävämpi on niiden yleisyys ja laaja levinneisyys. Kun teknologialla on riittävä peitto, muodostuu se pelkästään yleisyytensä johdosta tärkeäksi kohteeksi tietomurtoja ja haittaohjelmia suunniteleville tekijöille. Toinen merkittävä tekijä on käyttäjien laiskuus laitteidensa suojaamisen suhteen. (Diogenes & Ozkaya 2019, 163.)

Mobiililaitteilla on myös heikkoutena se, että käyttäjät on totutettu ottamaan käyttöön uusia applikaatioita heti tuoreeltaan ja soveltamaan niitä tarpeisiinsa viipymättä. Tästä syystä monissa laajassakin käytössä olevissa ohjelmissa paljastuu verrattain usein täysin uusia haavoittuvuuksia. Esimerkiksi toukokuussa 2019 paljastui, että aikaisemmin mainitun Pegasus-vakoiluohjelman pystyi asentamaan käyttäjän mobiililaitteeseen WhatsApp -ohjelmassa olleen haavoittuvuuden avulla. Riitti, että soitettiin WhatsApp -puhelu hyökkäyksen kohteena olevaan laitteeseen. Puheluun ei tarvinnut edes vastata, sillä haittaohjelman asentamiseen riitti puhelun muodostamiseen tarkoitetun datavirran muokkaaminen. (Diogenes. & Ozkaya 2019, 180.)

Toinen, uusia ominaisuuksia hyödyntävä keino, jolla haittaohjelma on voitu asentaa mobiililaitteeseen, on ns. Tap'n Ghost -tekniikka. Tässä tekniikassa hyödynnetään mobiililaitteen NFC-lukijaa. Pinta, jonka läheisyydessä käyttäjän mobiililaitte tulee olemaan, voidaan käsitellä siten, että sen sisällä on piilossa NFC-kortti. Kortin avulla mobiililaitteen internetselain saadaan lataamaan haittaohjelman asentumiseen johtavan sivun. (Diogenes & Ozkaya 2019, 211 - 212.)

Farrell (2015, 8) tuo esiin mobiililaittevarkauksiin keskittyvässä artikkelissaan myös sen näkökulman, että jossa mobiililaitteen avulla käyttäjällä on joko fyysinen pääsy tai mahdollisuus etäyhteyden käyttöön esimerkiksi suljettuun tilaan tai järjestelmään, voi hyökkääjä saada pääsyn yksinkertaisesti varastamalla mobiililaitteen käyttäjältä. Vastatoimeksi hän ehdottaa käytänteitä, jotka automaattisesti lukitsevat mobiililaitteen sen päätyessä väärin käsiin ja estävät pääsyn sen sisältämään tietoon. (Farrell 2015, 8.)

2.4 Sulautettujen järjestelmien ja ilmaisimien turvallisuus

Heathin (2002, 2) määritelmän mukaan sulautetuilla järjestelmissä tarkoitetaan mikrokontrollerin tai prosessorin toimintaan perustuvaa järjestelmää, jonka tarkoitus on kontrolloida määriteltä toimintoa tai toimintoja ja jota loppukäyttäjän ei ole tarkoitus ohjelmoida. Kuvaus sopii moniin tilaturvallisuusjärjestelmän komponentteihin, kuten valvontakameroihin, ilmoitinlaitteisiin ja joihinkin monimutkaisempiin ilmaisimiin.

Muutaman vuoden aikana yleistyneet IOT-laitteet ovat yksi esimerkki sulautetuista järjestelmistä ja kasvava trendi sensoriteknologiassa. IOT on lyhenne sanoista Internet Of Things, esi-neiden internet. Termillä tarkoitetaan laajaa kirjoa erilaisia laitteita, jotka on mahdollista liittää osaksi tietoverkkoa. Rerupin ja Aslanerin mukaan IOT-laitteet alkoivat tulla laajemmin saataville 2015 ja yleistyivät kovalla vauhdilla. Niiden laaja käyttöönotto tapahtui nopeasti, että laitteiden tietoturvaominaisuudet eivät pysyneet laitteiden kaupallisen suosion vauhdissa. Myös Mansfield-Devine (2017, 13) pitää liian nopeaa yleistymistä osasyynä tietoturvaongelmiin mainitessaan, että markkinoille tulee jatkuvasti laitteita, joissa on uusia haavoittuvuuksia. Tämän seurauksena, jo seuraavana vuonna nähtiin Mirai -nimisen, kaapatuista IOT-laitteista koostuvan bottiverkon toteuttamia DDOS-hyökkäyksiä. IOT-laitteet ovat usein melko halpoja, eikä niiden tietoturvaominaisuuksiin panosteta kovin paljon. Tästä syystä ne muodostavat edelleen suosittu rajapinnan erilaisille tietoturvaloukkauksille. Tietoturvayhtiö Symantecin mukaan, on olemassa IOT-laitteita, jotka avoimeen verkkoon liitettynä joutuvat kaapatuiksi noin kahdessa minuutissa. Hyvin yksinkertaisetkin IOT-laitteet voivat toimia verkkohyökkäyksen välineenä. Esimerkiksi kouluun asennettu, verkosta käsin ohjattavissa ollut valaistusjärjestelmä valjastettiin toteuttamaan DDOS-hyökkäys samaista koulua vastaan vain joitakin kuukausia valaistusjärjestelmän asentamisen jälkeen. (Rerup & Aslaner 2018, 267 - 268.)

Bhattacharjee (2018, 12) avaa IOT-laitteiden merkitystä termillä CPS, *Cyber-Physical System*. Tällä tarkoitetaan verkkoon kytkettävää laitetta, jolla on kuitenkin vuorovaikutusta reaali-maailman kanssa. Esimerkkinä hän mainitsee tietoverkkoon kytketyn termostaatin. Tämänkaltaisten järjestelmien rooli on kasvanut myös teollisuudessa, jossa teollisten prosessien valvonta- ja hallintajärjestelmät kytkeytyvät yhä useammin verkkoon. Lisäksi nämä järjestelmät voivat hyödyntää niin ikään verkkoon kytkettyjen sensoreiden tarjoamia tietoja. Näissä järjestelmissä puutteellinen tietoturva voi johtaa mittaviin vahinkoihin ja jopa vaaratilanteisiin. (Bhattacharjee 2018, 12 - 13.)

Rerup ja Aslaner totetavat IOT-laitteiden suurimpien ongelmien johtuvan käyttäjien ja niitä asentavien henkilöiden laiskuudesta sillä väärinkäytösten helppous perustuu usein siihen, että asennuksen yhteydessä laitteiden oletussalasanoja ei ole vaihdettu (Rerup & Aslaner 2018, 268). Bhattacharjee (2018, 32) näkee ongelman vakavana, koska erilaiset uhat voivat vaikuttaa laitteiden tuottamaan informaatioon tai siihen fyysiseen ympäristöön, jota laite mahdollisesti säätelee toiminnallaan, jolloin esimerkiksi laitteen välittämä tieto voi vääristyä tai jäädä saapumatta, joka taas voi vaikuttaa suoraan esimerkiksi venttiilin säätöön.

Käyttäjien toimintatavat eivät kuitenkaan ole ainoa heikko kohta IOT-laitteiden tietoturvassa. Rerupin ja Aslanerin mukaan (2018, 268 - 269) pienien ja halpojen laitteiden muistia ei ole yleensä suojattu, joten salasanat on mahdollista lukea suoraan laitteen muistista eikä niissä myöskään usein ole eroteltu erilaisia pääsyoikeustasoja joka tarkoittaa käytännössä sitä, että jos IOT-laitteeseen päästään kirjautumaan sisälle, on samalla mahdollista muokata kaikkea sen toimintaan liittyviä asetuksia. Rerup ja Aslaner (2018, 268) tuovat esiin, että IOT-laitteiden kohdalla on myös yleistä heikkojen salasanojen käyttö. Käytöksen taustalla vaikuttaa se, että IOT-laitteita on usein käytössä suuri määrä, jolloin yksilöllisten, riittävän vaikeiden salasanojen hallinnointi lisää työkuormaa. Bhattacharjee (2018, 32) jakaa näkemyksen ja käytännössä toteaa samat huomiot kuin Rerup ja Aslaner.

IOT-laitteiden tietoturvaominaisuuksien parantamiseksi olisi tulisi kiinnittää huomiota kirjautumiseen ja käyttöoikeuksien saamiseen liittyviin seikkoihin. Mansfield-Devine kritisoi (2017, 13), että markkinoilla on jopa laitteita, joissa on konfigurointia varten käytössä vanhentunut ja haavoittuva Telnet-protokolla sekä järjestelmään kiinteästi koodatut ylläpitotilit ja salasanat. Rerupin ja Aslanerin (2018, 268 - 269) mukaan valmistajien tulisi toimittaa laitteen kertakäyttöisin aloitussalasinoin, joka pakottaisi käyttäjän vaihtamaan laitteen salasana käyttöönoton yhteydessä. Lisäksi laitteiden tulisi varmistaa, että käyttäjän syöttämä salasana on tietoturvamielessä järkevällä tasolla. Toisaalta Narwal ja Mohapatra (2020, 38) luettelevat monia muitakin vaihtoehtoja autentikointimenetelmiksi todeten samalla, että salasanoihin perustuvia järjestelmiä kehitetään yhä koska ratkaisu on yksinkertainen mutta tulevaisuudessa esimerkiksi lohkoketjuteknologiaan ja monivaiheiseen tunnistautumiseen perustuvat menetelmän tulevat yleistymään (Narwal & Mohapatra 2020, 38). Myös Anand ja Sharma

(2020, 9) jakavat näkemyksen lohkoketjuteknologian hyödyntämisessä mutta tuovat esiin myös ns. *Fog*- ja *Edge* -teknologiat sekä koneoppimisen käytön, erityisesti tilanteissa, joissa IOT-laitteisiin perustuvaa järjestelmää halutaan suojata rakentamalla turvallisuutta parantava välikerros järjestelmän ja dataa hyödyntävän tason väliin.

Narwal ja Mohapatra (2020, 38) myös mainitsevat salattujen protokollien käytön mahdollisuuden. Tähän vaihtoehtoon on ottanut aikaisemmin kantaa Devi, Kumar sekä Sethumadhavan (2017, 674) toteamalla, että esimerkiksi salattuun WEP-protokollaan (*Wired Equivalent Privacy*) ei voi nykyisin turvautua sen sisältämien heikkouksien vuoksi. He suosittelevat WPA2 -protokollan käyttöä, joskin varauksella, sillä myös kyseistä protokollaa vastaan on olemassa hyökkäysmenetelmiä (Devi, Kumar & Sethumadhavan 2017, 674). Devi ym. (2017, 682) suosittelevatkin automatisoimaan WPA2 -protokollaa hyödyntävän verkon turvallisuuden valvonnan, jotta riksi uusien haavoittuvuuksien hyödyntämiselle pienenee.

Rerup ja Aslaner tuovat esiin, että laitteissa tulisi olla eroteltuna vähintään kaksi eri tasoista käyttöoikeutta, eli niin sanottu peruskäyttäjän oikeustaso rajoitetuin oikeuksin sekä laajempi, ylläpitotehtäviin tarkoitettu käyttöoikeustaso. Myös salasanojen säilytys laitteen muistissa olisi syytä tehdä turvallisemmin, esimerkiksi salauksen avulla, jotta niitä ei voi suoraan lukea laitteen muistipiiriltä. Lisäksi laitteiden tulisi sisältää kirjautumisen aikakatkaisu, jolloin niiden hyödyntäminen esimerkiksi DDOS-hyökkäyksen toteuttamiseksi vaikeutuisi. (Rerup & Aslaner 2018, 268 - 269.)

Valvontakameroiden osalta Halkosaari (2014) on tunnistanut tietoturvan osalta yleisiä ongelmia, joissa on paljon yhtäläisyyksiä IOT-laitteissa havaittujen ongelmien kanssa. Niitä ovat esimerkiksi heikot salasanat sekä oletusarvoihin jätetyt salasanat. Lisäksi ohjelmistot ovat usein vanhentuneita. Ongelmien voidaan katsoa juontuvan siitä, että julkisuudessa ei ole käsitelty riittävästi tapauksia, joissa kameravalvonnan riskeistä liittyvät ongelmat ja vastuut olisivat tulleet esiin. (Halkosaari 2014, 43.)

Kameroita on käytetty hyväksi joissakin julkisuuteenkin nousseissa tapauksissa. Mirai -niminen bottiverkko perustui kaapattuihin, verkkoon kytkettyihin kameroihin ja niiden avulla pystyttiin luomaan massiivisia DDOS-hyökkäyksiä. Kameroista paljastuneiden haavoittuvuuksien ja takaovien myötä niihin liittyviä riskejä on ryhdytty analysoimaan ja jo vuonna 2016 englantilaiset tiedusteluviranomaiset toivat julki huolen, joka liittyi maassa eniten käytettyihin, Hikvision -merkkisiin valvontakameroihin. Kyseiset kamerat valmistetaan Kiinassa. Myös muiden valmistajien kameroista on paljastunut yllättäviä takaovia. Vaikka osassa tapauksia laitteisiin ja ohjelmistoihin jätetyt takaovat onkin toteutettu lähinnä valmistajan huolto- ja hallinnointitoimenpiteiden helpottamiseksi, ovat ne silti mahdollistaneet ja helpottaneet myös hyökkääjien pääsyä kameroihin. (Wickes 2018.)

Kameroiden heikot tietoturvaominaisuudet eivät ainoastaan aseta kameran sensoriteknikan saatavilla olevaa tietoa (kuva ja joissain tapauksissa ääni) vaaraan vaan hyökkääjän päästessä käsiksi kameraan voi kamera tarjota keinon päästä murtautumaan verkon muihinkin laitteisiin (Wickes 2015). Samaa tulokseen ovat tulleet jo aikaisemmin myös Park ja Kim (2015, 3).

Samoja ongelmia luettelee myös Crawley (2016, 14), jonka mukaan heikosti suojatuista kame-roista tekee houkuttelevan maalin myös helposti verkosta ladattavat hyökkäysohjelmat. Rikol-lisesta toiminnasta tulee houkuttelevaa, kun pienellä vaivalla voidaan kaapata joukko lait-teita ja käyttää niitä kiristämiseen. Park ja Kim (2015, 2) pitävät myös ongelmallisena, että verkkoon kytkettyjen kameroiden ohjelmisto on helppo tunnistaa verkkoliikennettä seuraa-malla, jolloin hyökkääjän on mahdollista etsiä juuri kyseisiin laitteisiin tehovia hyökkäysme-netelmiä. Myös Anandin ja Sharmanin (2020, 6) ajatukset ovat samoilla linjoilla ja heidän mu-kaan laitteiden ohjelmistoissa tulisi myös kiinnittää huomiota tietoturvaseikkoihin kun kamera on vasta käynnistymisvaiheessa, sillä käynnistymisvaiheessa käytettävissä olevien haavoittu-vuuksien hyödyntäminen voidaan mahdollistaa katkaisemalla hetkeksi laitteen virransyöttö. Crawley näkeekin tärkeänä osaavan henkilöstön palkkaamisen, jotta järjestelmien haavoittu-vuuksia pystytään paikkaamaan ja hyökkäyksiin varautumaan ennalta (Crawley 2016, 14 - 15). Park ja Kim (2015, 3 - 9) sitä vastoin ehdottavat itse laitteiden turvaominaisuuksien tehosta-mista esimerkiksi hyödyntämällä kameroiden kuvavirtaa steganografisin keinoin vahvan auten-tikoinnin ja salauksen toteuttamiseksi.

Yhtenä kameravalvonnan ongelmana on, että se usein jää kiinteistön muun tietoverkon ulko-puolelle, eikä sen ylläpidosta huolehdi tietoturvaan perehtynyt taho. Vaikka Katakri ottaa kantaa kameroiden sijoitteluun, se ei kuitenkaan huomioi useiden kameroiden kykyä tallentaa myös ääntä. Wickes'n mukaan tallennusominaisuuksiensa puolesta valvontakamera saattaa joissain tapauksissa olla oletettua laajemman lainsäädännön piirissä, jos asiaa tarkasteltaisiin tietoturvan näkökulmasta. Tähän yhdistyy myös ongelma, jonka Park ja Kim (2015, 3) tuovat esiin, joka syntyy, kun kamerat lähettävät tallenteensa salaamattomana. Park ja Kim argu-mentoivat, että pääsy itse kameran läheteeseen ei ole ainoa keino päästä käsiksi arkaluon-toiseen tietoon vaan pääsy salaamattomaan tallenteeseen riittää. Halkosaari (2014) mainit-see, että kameravalvontaan liittyvissä vastuukysymyksissä on epäselvyyttä siitäkin syystä, ettei asiaa koskevia oikeustapauksia juurikaan ole.

Yleisellä tasolla tilaturvallisuusjärjestelmien ilmaisimien turvallisuutta voi lähestyä kahdesta näkökulmasta. Ensinnäkin voiko sensoria harhauttaa tai estää sitä toimimasta, jolloin sensorin valvoman tilan tietoturva vaarantuu. Toinen näkökulma puolestaan on se, voiko hyökkääjä käyttää sensorin mittauskykyä saadakseen tietoa valvotusta tilasta tai voiko sensorin tietolii-kenne mahdollistaa pääsyn järjestelmään, jonka osana sensori toimii. (Narwal & Mohapatra, 10.)

Ilmaisimia, eli sensoreita, on olemassa laaja joukko eri käyttötarkoituksiin ja jopa samoihin käyttötarkoituksiin löytyy eri mittaustekniikkaan perustuvia ratkaisuja. Esimerkiksi jos halutaan mitata ja ilmaista sensorin avulla liikkuuko tietyllä alueella joku, voidaan tähän tarkoitukseen käyttää mm. mikroaaltosensoreita, aktiivisia infrapuna- tai laserilmaisimia, passiivisia infrapunailmaisimia tai erilaisia maan alle upotettavia ratkaisuja kuten seismisiä sensoreita, magneettikenttää mittaavia sensoreita, valokuidun taipumiseen perustuvia OTDR-sensoreita tai piezo-sähköilmiöön perustuvia painesensoreita. Sensoreilla on niiden toteutustavan sanele- mat rajoitukset sille, mitä ne voivat havaita. Toinen tärkeä seikka sensorin valinnassa tiettyyn ympäristöön on sen herkkyys aiheuttaa vääriä hälytyksiä juuri kyseisessä ympäristössä. Toistuvat väärät hälytykset johtavat siihen, että sensorin ilmaisua ei voida käyttää osana järjestelmän toimintaa, joka puolestaan johtaa koko järjestelmän turvatason heikkenemiseen. Tästä syystä esimerkiksi seisminen ilmaisin ei ole hyvä valinta alueella, jonka läheisyydessä on normaalioloissa runsaasti raskasta liikennettä. (Pearson 2007, 97 - 102.)

Pearsonin mukaan sisätiloissa tavalliset sensorytyypit ovat liiketunnistimet, lasinrikkoilmaisimet sekä ns. ovikytkimet, jotka useimmiten toimivat magneetilla (Pearson 2007, 103). Osa sensoreista voi toimia langattomasti, mutta Finogeevin (2017) mukaan langattomissa sensoreissa on puutteita mm. viestinnän salauksessa, ja sielläkin missä salaus on toteutettu, on avaintenhallinta usein puutteellista (Finogeev 2017).

Allsoppin (2009) mukaan joitakin sensoreita voidaan ohittaa laukaisematta niiden hälytystä. Esimerkiksi joidenkin liikkeeseen reagoivien sensoreiden kohdalla riittää, että liikkuu riittävän hitaasti sensorin tarkkailemalla alueella, jolloin sensori ei rekisteröi liikettä lainkaan. Edelleen Allsopp mainitsee, että sijoittamalla sensorin huonosti, voi valvottavalle alueelle jäädä katvealueita. Katvealueilla sensorin havaintokyky ei riitä, jos tunkeutuja käyttää jotain epätavallista etenemismuotoa, kuten ryömimistä. Lisäksi Allsopp tuo esiin, että joissakin sensoreissa voi olla näkyvillä painike, jonka avulla sensorin toiminta voidaan estää. Myös Pearson mainitsee eri tasoista sensoreista magneettikytkimien yhteydessä. Pearsonin vertaa yhden magneetin ja Reed-kytkimen muodostamaa sensoria korkeamman turvatason sensoriin, jonka sisällä on useita magneetteja ja Reed-kytkimiä. Tobias (2015) osoittaa, kuinka yksinkertaista on sabotoida yhdestä magneetista ja Reed-kytkimestä koostuvan sensorin toiminta. Kun joukko magneetteja sijoitellaan kytkimen sisälle eri päin, voidaan muodostaa magneettikytkin pareja, joiden harhauttaminen ulkoisin keinoin on huomattavasti vaikeampaa kuin sellaisen kytkimen harhauttaminen, jossa on sisällä vain yksi magneetti (Pearson 2007, 97 - 102). Toisaalta Magnasphere Corp (2012) on jo aikaisemmin näyttänyt toteen, että myös useista magneeteista koostuvan sensorin harhauttaminen on mahdollista.

Sensorit voivat myös kadotessaan muodostaa erilaisia uhkia, toteavat Li, Wang, Kim, Zhang & Dai (2018, 44). Lin ym. mukaan sensorien sisältämä data voi päätyä hyökkääjän käyttöön, jos hyökkääjä saa sensorin haltuunsa ja esimerkiksi pääsee lukemaan laitteen muistin. Li ym.

mainitsevat, että jo sensorin sisältämä mittausdata voi olla vahingollista mutta sensorin sisältämät tiedot voivat auttaa myös muodostamaan hyökkäyksen verkkoa vastaan. Tätä ongelmaa vastaan voisi suojautua käyttämällä salausta siten, että sensorin säilyttämät tiedot ovat oletusarvoisesti salattuja ja niiden avaamiseen tarvitaan salausavain, joka on saatavilla vain silloin, kun sensori on kytketty ja autentikoitu verkkoonsa. Muussa verkossa tai irrallaan ollessaan sensorin muistista voidaan tiedot lukea vain salatussa formaatissa (Li, Wang, Kim, Zhang & Dai 2018, 46). Dodangehin ja Jahangirin mukaan kuitenkin sensoreissa voi lähinnä tulla kyseeseen symmetrisen avaimen menetelmät, jotka eivät ole yhtä turvallisia kuin asymmetriset salausmenetelmät, mutta ovat toteutettavissa myös vaatimattomamman laskentatehon omaavissa sensoreissa (Dodangeh & Jahangir 2018, 63). Artikkelissaan Dodangeh ja Jahangir (2018, 68) esittävät yhdeksi vaihtoehdoksi protokollaa, jossa autentikointivaiheen yhteydessä sensori saa salausavaimen verkosta ja vaikka selväkielinen autentikointi on riski tietoturvalle, puolustavat he tätä lähestymistapaa riittävän hyvänä ratkaisuna, kun autentikointi obfuskoidaan, jolloin näkemys on pääpiirteiltään yhteneväinen Li ym. (2018, 46) esittämän kanssa. Eriävän näkemyksen esittävät Anand ja Sharma (2020, 6), jotka tuovat esiin ns. *Booting Attack* -menetelmän, jossa hyökkääjä nimenomaan pyrkii hyödyntämään laitteiden käynnistyksen aikana alentuneita tietoturvaominaisuuksia.

2.5 Rakenteelliset turvallisuustekijät tietoturvan näkökulmasta

Finanssialan (2017) julkaisema Rakenteellisen murtosuojauksen ohje käsittelee mm. ovia, ikkunoita sekä kiinteistöjen kiinteitä rakenteita kuten karmeja, kattoa ja lattiaa. Lisäksi se käsittelee lukitusta. Kaikki nämä seikat liittyvät tilaturvallisuuteen ja myös välillisesti suojatun tilan tietoturvaan. Tila, jonka pääsyä ei ole rajoitettu estämällä pääsy rakenteellisin keinoin, ei voi olla tietoturvallinen. Opinnäytetyön näkökulman johdosta tarkastelun ulkopuolelle rajataan kuitenkin ne rakenteelliset seikat, jotka suoraan käsittelevät rakenteiden lujuutta tai niiden murtosuojauksista fyysistä voimaa edellyttäviä keinoja vastaan. Finanssialan murtosuojauksen ohje ottaa kantaa mm. lukkojen telkiin, niiden rakenteeseen sekä etäisyyteen toisistaan niissä lukoissa, joissa on useampia telkiä. Sähköisiin lukkoihin se ei kuitenkaan ota kantaa, eikä yleisemmän tason rakenteellisiin ratkaisuihin, kuten tilaturvallisuusjärjestelmien kaapelointiin ja sen suojaamiseen.

Sähköinen kulunhallinta tarkoittaa yleisellä tasolla yhtä tai useampaa, elektronisesti ohjattua lukkoa tai muuta pääsynhallintaan soveltuvaa laitetta. Usein näihin yhdistyy ominaisuuksia, jota voidaan käyttää muodostamaan hälytys, jos tilaan yritetään tunkeutua ilman pääsy oikeutta. Järjestelmää kontrolloidaan tyypillisesti hallintapaneelin tai tietokoneen avulla. Järjestelmän osat ovat yhteydessä palvelimeen TCP/IP -verkon välityksellä. Yksi keskeinen osa

järjestelmää on myös lukulaite, joka kykenee tunnistamaan kulkuoikeuden osoittavan avainkortin tai vastaavan. (Norman 2012, 37 - 40.)

Sähköllä ohjattuja lukkoja on erilaisia. Niillä on kuitenkin yksi yhdistävä tekijä. Normanin (2012) mukaan lähes kaikissa tapauksissa sähköllä ohjatun lukon edellytetään päästävän ihmiset suojatusta tilasta pois esimerkiksi sähköjen katketessa. Yleinen tällaisten lukkojen toimintaperiaate on, että lukitussa asennossa pysyäkseen lukon sisällä oleva magneetti tarvitsee virtaa. Jos kiinteistön sähkönsyöttö ei pysty antamaan lukolle virtaa, lukon telki vapautuu magneetin voimasta ja lukko avautuu. Jotta voidaan varautua tilanteeseen, jossa sähkölukon omaava ovi murrettaisiin väkisin auki, tulisi ovelle sähkölukon lisäksi sensori, jolla voidaan havaita, onko ovi kiinni vai auki. Tilanteessa, jossa kulkuoikeutta ei ole osoitettu esimerkiksi avainkortin, numerokoodin tai biometrisen tunnisteiden avulla ja jossa ovi avataan muilla keinoilla, tulisi järjestelmän osana muodostaa hälytys. (Norman 2012, 80 - 87.)

Järjestelmän kaapelointi on sen toiminnan kannalta keskeinen tekijä. Kaapelointi voidaan jakaa yleisellä tasolla kahteen pääluokkaan: optiseen ja sähköiseen kaapelointiin. Katakriin mukaan optista kaapelointia tulisi suosia sen tietoturvan kannalta edullisten ominaisuuksien takia. Tämä ei kuitenkaan ole useimmiten mahdollista tilaturvallisuusjärjestelmien komponenttien kohdalla. Norman suosittelee (2012, 341) suojaamaan tilaturvallisuusjärjestelmien kaapelit suojaavalla rakenteella siten, että ne eivät kulje vapaana rakenteiden, kuten sisäkattojen ritilöiden päällä. Suojaamattomat kaapelit ovat alttiita esimerkiksi ilkivallalle. Suojaavien rakenteiden tulisi olla materiaaliltaan kestäviä, mieluiten metallisia. (Norman 2012, 341 - 342.)

Valvontakameroiden tiedonsiirtoon suositellaan käytettäväksi kaapelointia langattoman tiedonsiirron asemasta. Kaapelin etuja ovat mm. pienempi riski häiriöille sekä paremmat tietoturvaominaisuudet. Kaapelointi voidaan toteuttaa monella eri tavalla riippuen valittujen kameroiden teknisistä ominaisuuksista. Nykyisin on voimakkaasti yleistynyt ns. IP-kameroiden käyttö, jolloin kameroiden tiedonsiirtoon, toisinaan myös sähkönsyöttöön, käytetään tavantomaista verkkokaapelia. Tämä tekniikka on helppokäyttöistä ja kustannustehokasta, joskin verkko-ominaisuuksiin liittyy riskejä tietoturvan näkökulmasta. (Homeland Security 2013, 36 - 42.)



Kuva 6: Huolimaton asennus. Erään kiinteistön riskikartoituksessa havaittu kamera-asennus. Kameran verkkoliitin on jäänyt rakenteen ulkopuolelle näkyviin (ympyröity punaisella), jolloin kameran johdon irrottaminen tai kameran tietoliikenteen taltioiminen on erittäin helppoa. Kamera oli myös suunnattu siten, että kiinteistön alueella oli helppo liikkua kameran havaitsematta, jos kameran sijainti ja suunta oli etukäteen tiedossa. (Kirjoittajan oma arkisto.)

Tilaturvallisuusjärjestelmien rakenteellisten ominaisuuksien puutteita avaa myös Jim Stickley'n demonstraatiot turvajärjestelmien ohittamisesta. On tavallista, että tilaturvallisuusjärjestelmällä suojatun tilan oven avaamisesta käynnistyy aika, jonka kuluessa saapujan on esimerkiksi koodin avulla poistettava hälytysjärjestelmä viritetystä tilasta. Jos koodia ei anneta määritellyn ajan sisällä, järjestelmä käynnistää hälytyksen. Jim Stickley on demonstroinut, kuinka näissä tapauksissa hälytys voidaan ohittaa murtamalla nopeasti auki tilaturvallisuusjärjestelmän keskuslaitteen kuori ja irrottamalla laitteen tietoliikenneyhteydet ja virransyöttö. (Stickley, J. 2011.)

2.6 Arvioitavat standardit

Opinnäytetyön tarkastelun kohteena on joukko standardeja, jotka määrittelevät tilaturvallisuusjärjestelmien ominaisuuksia, rakennetta ja toiminnallisuutta. Standardit ovat tiettyjen yhteistyöperiaatteiden mukaan laadittuja asiakirjoja, jotka määrittelevät tietyn asian ominaisuudet. Asiantuntijat ja standardisoimisjärjestöt laativat nämä asiakirjat, usein teollisuuden edustajan aloitteesta. EU:ssa noin viidesosa standardeista laaditaan EU:n toimeksiannosta. Standardien keskeinen tarkoitus on parantaa turvallisuutta ja yhteensopivuutta. (SFS 2018.)

Standardin luominen on aikaa vievä prosessi. Prosessi on harvoin valmis alusta loppuun alle kolmessa vuodessa. Prosessin alussa määritellään tarve, johon standardi vastaa. Standardin laatimista varten kerätään laaja ryhmä, jossa on hyvä edustus valmistavasta teollisuudesta. Merkittävä osa ajasta, vähintään puoli vuotta, kuluu lausuntokierrosten läpikäymiseen. (Pänkäläinen 2020.)

Opinnäytetyöhän valittiin tarkasteltavaksi Suomessa käytössä olevia standardeja. Nämä standardit on lueteltu Finanssiala ry:n julkaisussa ”Murtohälytysjärjestelmät ja -palvelut”. Finanssiala ry luetteloi Suomessa toimivat, murtohälytysjärjestelmiä toimittavat liikkeet omien vaatimustensa perusteella. Listalle päästäkseen, yrityksen on osoitettava kelpoisuus sertifiointilaitoksen myöntämällä sertifikaatilla tai lausunnolla, joka osoittaa toiminnan täyttävän listatun standardin vaatimukset. (Finanssiala 2020.)

Seuraavat standardit valittiin opinnäytetyössä tarkastelun kohteeksi:

Standardin tunnistus	Standardin otsikko
SFS-EN50131-1 2007+A1+A2 2017	HÄLYTYSJÄRJESTELMÄT. MURTO- JA RYÖSTÖILMAISUJÄRJESTELMÄT. OSA 1: JÄRJESTELMÄVAATIMUKSET
SFS-CLC TS 50131-7	HÄLYTYSJÄRJESTELMÄT. MURTO- JA RYÖSTÖILMAISUJÄRJESTELMÄT. OSA 7: SOVELTAMISOHJEET
SFS-EN 54-21	PALOILMOITTIMET. OSA 21: PALO- JA VIKAILMOITUSTEN VÄLITINLAITTEET
SFS-EN 50131-2-2	Alarm systems. Intrusion and hold-up systems. Part 2-2: Intrusion detectors. Passive infrared detectors
SFS-EN 50131-2-4	ALARM SYSTEMS - INTRUSION AND HOLD-UP SYSTEMS. PART 2-4: REQUIREMENTS FOR COMBINED PASSIVE INFRARED AND MICROWAVE DETECTORS

SFS-EN 50131-2-6	ALARM SYSTEMS - INTRUSION AND HOLD-UP SYSTEMS - - PART 2-6: OPENING CONTACTS (MAGNETIC)
SFS-EN 50131-3	ALARM SYSTEMS - INTRUSION AND HOLD-UP SYSTEMS. PART 3: CONTROL AND INDICATING EQUIPMENT
SFS-EN 50132-1	HÄLYTYSJÄRJESTELMÄT. TURVASOVELLUKSISSA KÄYTETTÄVÄT KAMERAVALVONTAJÄRJESTELMÄT. OSA 1: JÄRJESTELMÄVAATIMUKSET
SFS-EN 50133-1 + A1	HÄLYTYSJÄRJESTELMÄT. TURVALLISUUSSOVELLUKSISSA KÄYTETTÄVÄT KULUNVALVONTAJÄRJESTELMÄT. OSA 1: JÄRJESTELMÄVAATIMUKSET
SFS-EN 50133-2-1	HÄLYTYSJÄRJESTELMÄT. TURVALLISUUSSOVELLUKSISSA KÄYTETTÄVÄT KULUNVALVONTAJÄRJESTELMÄT. OSA 2-1 YLEISET VAATIMUKSET KOMPONENTEILLE
SFS-EN 50136-1	Hälytysjärjestelmät. Ilmoituksensiirtojärjestelmät ja -laitteet. Osa 1: Yleiset vaatimukset ilmoituksensiirtojärjestelmille
SFS-EN 62676-1-1	TURVASOVELLUKSISSA KÄYTETTÄVÄT KAMERAVALVONTAJÄRJESTELMÄT. OSA 1-1: JÄRJESTELMÄVAATIMUKSET. YLEISET VAATIMUKSET
SFS-EN 62676-1-2	TURVASOVELLUKSISSA KÄYTETTÄVÄT KAMERAVALVONTAJÄRJESTELMÄT. OSA 1-2: JÄRJESTELMÄVAATIMUKSET. VIDEOSIIRTOA KOSKEVAT SUORITUSKYKYVAATIMUKSET
SFS-EN 1627 en	PEDESTRIAN DOORSETS, WINDOWS, CURTAIN WALLING, GRILLES AND SHUTTERS. BURGLAR RESISTANCE. REQUIREMENTS AND CLASSIFICATION
SFS-EN 1628 + A1 en	PEDESTRIAN DOORSETS, WINDOWS, CURTAIN WALLING, GRILLES AND SHUTTERS. BURGLAR RESISTANCE. TEST METHOD FOR THE DETERMINATION OF RESISTANCE UNDER STATIC LOADING

SFS-EN 1629 + A1 en	Pedestrian doorsets, windows, curtain walling, grilles and shutters. Burglar resistance. Test method for the determination of resistance under dynamic loading
SFS-EN 1630 + A1 en	Pedestrian doorsets, windows, curtain walling, grilles and shutters. Burglar resistance. Test method for the determination of resistance to manual burglary attempts

Taulukko 1: Tilaturvallisuusjärjestelmien standardit.

Tilaturvallisuusjärjestelmiä käsittelevät standardit jakavat tilaturvallisuusjärjestelmät neljään turvallisuusluokkaan. Heikoin turvallisuusluokka on taso 1, eli matalan riskin taso. Sen kuvauksen mukaan hyökkääjän oletetaan olevan heikosti perillä tilaturvallisuusjärjestelmistä eikä hänellä oleteta olevan käytössään kuin suppea valikoima työkaluja. Tason 2 järjestelmät on suunnattu matalasta keskimääräisen riskin kohteisiin. Siinä hyökkääjällä oletetaan olevan vähän tietoa suojaavista järjestelmistä ja yleisluonteinen valikoima työkaluja käytössään. Kuvauksessa on erikseen mainittu yleismittari, joten tekijän voidaan olettaa kykenevän mittaamaan vähintään virtoja ja jännitteitä sekä esimerkiksi komponenttien tai silmukoiden vastusarvoja. Keskimääräisestä korkean riskin kohteita varten on tarkoitettu tason 3 tilaturvallisuusjärjestelmät. Tällä tasolla hyökkääjien oletetaan olevan perehtyneitä tilaturvallisuusjärjestelmien toimintaan sekä omaavan kattavan valikoiman työkaluja ja kannettavia elektronisia laitteita. Vaikka standardi ei asiaa tarkemmin avaa, on huomattava, että yleismittari oletettiin kuuluvaksi yleisluontoisiin työkaluihin. Tästä voidaan päätellä, että kolmosluokassa kuvatut, kannettavat elektroniset laitteen pitävät sisällään välineitä, joilla voidaan päästä käsiksi esimerkiksi langattomien tai langallisten tiedonsiirtotapojen signaalin sisältöön. Tällaisia välineitä voisivat olla esimerkiksi oskilloskooppi, vektoripiirianalysaattori tai kannettava tietokone verkkoliikennettä analysoivine ohjelmistoineen. Korkeimmalla tasolla, eli tasolla 4, suojataan kohteita, joissa turvallisuus on tärkeämpää kuin muut tekijät. Hyökkääjällä oletetaan olevan kyky suunnitella toiminta yksityiskohtaisesti. Lisäksi hyökkääjän käytössä oletetaan olevan täysi valikoima laitteita ja keinoja, kuten esimerkiksi kyky korvata keskeisiä tilaturvallisuusjärjestelmän komponentteja. Koko järjestelmän luokitus muodostetaan alimman luokitellun komponentin luokan mukaisesti. (SFS-CLC/TS 50131-7, 20 - 21, 26)

3 Menetelmä

Tämä opinnäytetyö on laadullinen tutkimus. Laadullinen tutkimus on yleensä vailla hypoteesia ja näin on myös tässä opinnäytetyössä. Tässä opinnäytetyössä ei siis lähestytä ennalta muotoiltua oletusta sitä koetellen. Laadullisen tutkimuksen voidaan katsoa käsittelevän aineistoa ilman esioletuksia ja sitä kautta mahdollisesti auttaa luomaan pohjaa myöhemmin tehtävälle määrälliselle tutkimukselle (Hirsjärvi, Remes & Sajavaara 1997, 159). Tässä työssä mainittu näkökulma konkretisoituu, kun tarkastellaan tilaturvallisuusjärjestelmiä käsitteleviä standardeja tietoturvan näkökulmasta ja verrataan niiden sisältöä alan vallitsevaan tietämykseen.

Opinnäytetyön menetelmä on toteutettu sisällönanalyysinä vertaillen eri aineistoja. Aineistoina tässä opinnäytetyössä ovat tilaturvallisuusjärjestelmiä käsittelevät standardit, tieto- ja kyberturvallisuuteen liittyvä kirjallisuus sekä asiantuntijahaastattelut. Sisällönanalyysillä pyritään sisällön systemaattiseen ja objektiiviseen tarkasteluun ja se etsii aineistosta merkityksiä, joiden avulla aineistoista pyritään löytämään tiivistetty ja yleisessä muodossa oleva kuvaus tutkittavasta ilmiöstä. (Tuomi & Sarajärvi 2018, 116 - 118.) Tässä opinnäytetyössä ilmiön muodostaa tietoturva ja siihen kohdistuvat uhat sekä toisaalta mahdollisuus tai keinot varautua kyseisiin uhkiin. Kuvaus ilmiöstä kiteytyy, kun aineistosta haetaan vastausta alatutkimuskysymysten kautta, jotta lopulta kyetään vastaamaan päätutkimuskysymykseen, joka arvioi tilaturvallisuusjärjestelmiä laadullisessa mielessä.

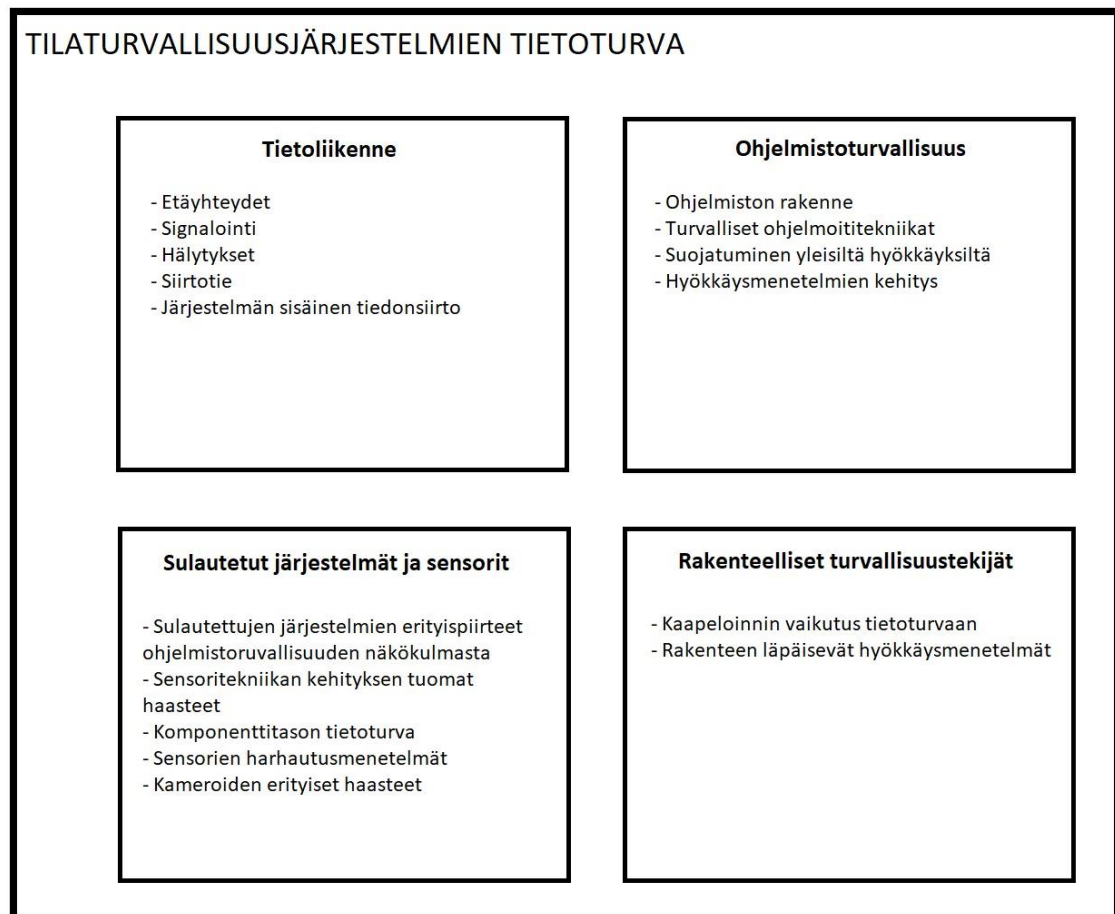
Sisällönanalyysi alkaa aineiston läpikäymisellä. Aineisto pelkistetään ja pilkotaan, jonka jälkeen aineisto ryhmitellään tavoitteena kokoavan käsitteen muodostaminen (Tuomi & Sarajärvi 2018, 104). Päämääränä on tuottaa tietoa tiivistämällä aineisto selkeäksi kokonaisuudeksi (Eskola & Suoranta 2014, 175 - 176).

Kun aineisto on pelkistämisen avulla saatu jaettua teemoihin, päästään aineistosta erottamaan tutkimuksen kannalta olennainen tieto. Tämän tiedon perusteella voidaan muodostaa teoreettisia käsitteitä. Käsitteiden tarkasteleminen, yhdistäminen ja vertailu tuottaa vastaukset tutkimuskysymyksiin. (Tuomi & Sarajärvi 2018, 123 - 125.)

Tässä työssä edettiin niin, että tilaturvallisuusjärjestelmiä käsittelevien standardien pohjalta etsittiin toistuvia teemoja. Nämä teemat muodostivat pohjan tiedonetsinnälle, sillä erittäin tekninen aihe vaati tiedonhaun kohdistamista oikeisiin osa-alueisiin pelkän yleisen tietoturvaan liittyvän aineiston asemasta. Aineistoksi valikoitui tietoturvan liittyvää lainsäädäntöä, kansallisia ohjeita, kirjallisuutta, tutkimusartikkeleita ja tutkimuksia. Kirjallisuuskatsaukseen kerättiin tästä aineistosta niitä tietoja, jotka liittyivät keskeisellä tavalla standardien katselmoinnista esiin nousseisiin teemoihin. Kirjallisuuskatsauksesta saatuja tietoja täydennettiin valikoiduilla asiantuntijahaastatteluilla. Lopuksi tuloksiin kerättiin ikään kuin kulminaatiopisteeksi tietoturvan näkökulman kautta valikoituneita kohtia tilaturvallisuusjärjestelmien stan-

dardeista ja tuotiin nämä seikat vastakkain sen tiedon kanssa, joka oli saatavilla muista lähteistä. Tarkoituksena oli osoittaa, mitä puutteita standardeista oli löydettävissä sekä toisaalta arvioida viimeistään johtopäätöksiä muodostettaessa, miten vakavia kyseiset puutteet olivat.

Tutkimus eteni iteratiivisesti, sillä tarvittavan teknisen tiedon määrä oli melko mittava. Kun standardeja tarkastelemalla nousi esiin tietoturvaan liittyviä seikkoja, oli niihin etsittävä ymmärrystä alan kirjallisuudesta. Tämä puolestaan tarkensi ja jäsensi standardin tekstin pohjalta syntyneitä käsityksiä ja jalostui edelleen. Prosessin aikana laajentunut tietämys vaikutti mm. teemoittelun lopulliseen muotoon. Seuraava kaavio kuvaa sitä, miten standardien läpikäymisen ja toisaalta teoreettisen viitekehyksen pohjalta muodostui lopulta tilaturvallisuusjärjestelmien tietoturvan jako neljään erilliseen teemaan.



Kuva 7: Pääteemat. Tilaturvallisuusjärjestelmien tietoturva jäsentyi eri lähteitä tarkastelemalla neljään eri pääteemaan.

3.1 Haastattelut

Haastattelut tiedonkeruumenetelmänä vievät paljon aikaa, kun huomioidaan valmistautumiseen, itse haastatteluun sekä kertyneen aineiston jälkikäsittelyyn kulunut aika kokonaisuutena (Hirsjärvi, Remes & Sajavaara 1997, 201). Haastattelun käyttöä tiedonkeruuseen tässä opinnäytetyössä kuitenkin puolsi se, että joustavan luonteensa johdosta tällä tiedonkeruumenetelmällä saatiin kohdennettua tiedonhankintaa opinnäytetyön kannalta olennaisiin kysymyksiin syventäen siten aiemmin hankittua tietoa (Hirsjärvi ym. 1997, 200).

Opinnäytetyössä käytetty haastattelumenetelmä on puolistrukturoitu teemahaastattelu. Haastattelut suunniteltiin teemoittain ja niihin valittiin sopivat asiantuntijat. Teemahaastattelun käyttö soveltuu tilanteeseen, jossa tutkitaan esimerkiksi haastateltavan ajatuksia ja kokemuksia tutkittavasta ilmiöstä (Hirsjärvi & Hurme 2004, 47-48). Haastattelut toteutettiin yksilöhaastatteluina. Myös ryhmä- ja parihaastatteluita pohdittiin mahdollisena menetelmänä. Etuna olisi voinut olla esimerkiksi se, että haastateltavat olisivat voineen täydentää toistensa vastauksia ja tuottaa siten enemmän tietoa tutkittavasta ilmiöstä (Hirsjärvi & Hurme 2004, 61). Käytännön aikataulusyistä yksilöhaastatteluiden järjestäminen osoittautui kuitenkin huomattavasti sujuvammaksi työskentelytavaksi. Puolistrukturoitu haastattelu edellyttää, että haastattelua varten laaditaan etukäteen kysymykset. Etukäteen laaditut kysymykset eivät kuitenkaan täysin sido haastattelun kulkua, vaan kysymyksiä voidaan esittää etukäteen suunnitellusta poikkeavassa järjestyksessä, joitain kysymyksiä voidaan jättää kysymättä ja tilanteen niin vaatiessa, haastattelija voi täydentää etukäteen laadittuja kysymyksiä keskustelun myötä heräävin, uusin kysymyksin (Hirsjärvi & Hurme 2004, 47).

Opinnäytetyötä varten haastateltiin seuraavat asiantuntijat:

Kalinen Riku, järjestelmäasiantuntia, Suojelupoliisi

Teema: Tilaturvallisuusjärjestelmien tietoteknisten laitteiden haavoittuvuudet ja kyberturvallisuus suhteessa valtiollisten toimijoiden suorituskykyyn.

Pänkäläinen Aku, turvallisuusasiantuntija, Finanssiala Ry

Teema: Tilaturvallisuuslaitteita koskevat standardit, standardien laatiminen, standardien kehittäminen ja päivittäminen.

Haastateltavien valinnassa keskityttiin toimeksiantajan suositteluihin henkilöihin, tai muuten pitkään kyseiseen teemaan liittyvissä asiantuntijatehtävissä työskennelleitä henkilöitä. Kaikki henkilöt, joilta tiedusteltiin mahdollisuutta osallistua haastatteluun, suostuivat haastateltaviksi. Yksi haastateltavaksi pyydetty asiantuntija suostui haastateltavaksi, mutta haastattelun järjestäminen ei haastateltavan aikataulusyistä onnistunut.

Riku Kalisen haastattelu toteutettiin Suojelupoliisin tiloissa. Haastattelu kesti yhteensä hieman yli tunnin. Etukäteen suunnitellussa kysymysrungossa oli huomioitu haastateltavan asiantuntijuuden alue. Vaikka haastattelu noudatti jossain määrin kysymysrunkoa, siitä kuitenkin poikettiin tarvittaessa esimerkiksi toiston välttämiseksi ja enemmän keskustelumaisemman ilmapiirin luomiseksi. Haastattelun aikana tehtiin muistiinpanoja ja muistiinpanot kirjoitettiin puhtaaksi välittömästi haastattelun jälkeen. Haastattelussa käytetty runko on esitetty opinnäytetyön liitteessä yksi.

Aku Pänkäläisen haastattelu järjestettiin etäyhteyden avulla, hyödyntäen Microsoft Teams -alustaa. Haastattelu kesti noin viisikymmentä minuuttia. Tässäkin haastattelussa keskustelun kulku ohjautui etukäteen laadittujen kysymysten kautta, jättäen kuitenkin tilaa avoimelle keskustelulle ja erityistä huomiota vaativille yksityiskohdille. Muistiinpanot haastattelusta laadittiin keskustelun aikana ja ne kirjoitettiin puhtaaksi välittömästi haastattelun jälkeen. Haastattelussa käytetty runko on esitetty opinnäytetyön liitteessä kaksi.

4 Tulokset

Tässä luvussa tarkastellaan tilaturvallisuusjärjestelmiä koskevien standardien sisältöä. Standardien vaatimuksia verrataan kirjallisuuslähteistä sekä haastatteluiden avulla saatuja tietoja vasten. Tarkastelukulma kohdistuu tilaturvallisuusjärjestelmien tietoturvaan. Tarkoituksena on tarkastella erityisesti neljää osa-aluetta, jotka ovat nousseet sekä kirjallisuuskatsauksen että haastatteluiden myötä keskiöön. Nämä osa-alueet ovat tilaturvallisuusjärjestelmien etäkäyttöön liittyvät tietoturvakysymykset, niiden ohjelmistojen haavoittuvuudet, sensorien ja langattomien laitteiden haavoittuvuudet sekä rakenteellisista seikoista johtuvat riskit tietoturvalle.

4.1 Tilaturvallisuutta säätelevien normien huomioiminen

Tilaturvallisuusjärjestelmiä määrittelevät standardit ovat melko hyvin linjassa asiaan liittyvän lainsäädännön ja kansallisen ohjeistuksen kanssa. Tätä selittää osittain se, että kansallisen ohjeistuksen laatimisessa on käytetty tukena alaa koskevia standardeja.

Merkittävimmät ongelmat ovat löydettävissä kameravalvonnan alueelta. Kuten Halkosaari (2014) tuo esiin, kameravalvonnan problematiikkaa ei ole koeteltu tuomioistuimissa. Myöskään ulkomailta kuuluvia, varoittavia ääniä ei ole vielä noteerattu esimerkiksi kameroiden komponenttitason ongelmiin liittyen tai niiden tietoliikenteeseen liittyviin epäselvyyksien osalta. Siinä missä yksittäisten kameroiden epämääräiset pyrkimykset kommunikoida internetiin on helppo estää ja ongelmat sitä kautta sivuuttaa, voivat piirilevyllä piilevät mikrofonit tai langattoman tiedonsiirron yhteydet edellyttää laajemman huomion kohteeksi tullessaan muutoksia vähintään kansallisen tason ohjeistukseen. Vaikka Turva-alan yrittäjien julkaisema kameravalvontaopas ottaa asiaan kantaa, olisivat standardit tehokkaampi paikka näille määritelmille, joskin standardoinnin keinoin asiaan vaikuttaminen on vaikeaa ja aikaa vievää (Pänkäläinen, 2020).

Eräs huomiota herättävä seikka on, että Finanssiala ry:n julkaisemassa luettelossa murtohälytysjärjestelmiä toimitavista liikkeistä on huomattavasti vähemmän toimijoita kuin poliisin luettelossa on turvallisuusalan elinkeinoluvan haltijoita, joilla on oikeus suorittaa turvasuojaustehtäviä. Osaltaan ilmiötä voi selittää se, että osa poliisin hyväksymistä yrityksistä on toimeksiantojen kautta keskittynyt liiketoiminnassaan muuhun toimintaan, eikä hyväksyntää Finanssiala ry:n luetteloon ole siksi haettu. Kuitenkin luetteloiden eron ollessa lähes nelinkertainen, lienee syytä olettaa, että kaikki tilaturvallisuusjärjestelmiä toimittavat tahot eivät ehkä ole jostain syystä hakeneet Finanssiala ry:n luettelointia, vaikka mahdollisesti suorittavat turvasuojaustehtäviä. On kuitenkin todettava, että Finanssiala ry:n luetteloimiseen edellytetyt vaatimukset keskittyvät pääasiassa yrityksen laadullisiin ja ammattitaidollisiin seikkoihin, eivätkä suoranaisesti vaikuta tilaturvallisuusjärjestelmän tietoturvaan.

Yleisenä niin lainsäädäntöä kuin kansallisen tason ohjeistustakin koskevana huomiona voidaan todeta, että pääsuunta, johon ne ohjaavat tietoturvan toteutumista, on kohti vähintään hyväksyttävää tasoa. Havaintoa osittain tukee myös Pänkäläisen (2020) toteamus, että olemassa oleva tilaturvallisuusjärjestelmin luokittelujärjestelmä ei sovellu esimerkiksi sellaiseen viranomaiskäyttöön, jossa edellytetään erittäin korkeaa turvatasoa. On kuitenkin todettava, että tutkimuksessa käytettiin kansallisen tason ohjeistuksen arviointiin tutkimusta laadittaessa voimassa olleita versioita ohjeistuksesta. Esimerkiksi Katakrista on uusi, vuoden 2020 versio tätä kirjoitettaessa lausuntokierroksella. Ajantasaisemman version arviointi olisi ollut luonnollisesti toivottava asia mutta uuden version julkaisuajankohta ei toteutunut tämän tutkimuksen aikahaarukassa.

4.2 Tietoliikenteeseen liittyvät turvallisuuskäsitteet

Standardi SFS-EN 50131-1:2007 + A1 + A2:2017 käsittelee kohdassa 8.3.1 pääsyoikeuksia tilaturvallisuusjärjestelmien keskuslaitteisiin. Se määrittelee oikeustasot, sekä kriteerit, joilla eri oikeustasoille on mahdollista kirjautua. Kriteerit ovat samat riippumatta siitä, käytetäänkö järjestelmää paikanpäältä vai etäkäyttöyhteyden yli. (SFS-EN 50131-1:2007 + A1 + A2:2017, 22.)

Erilaiset käyttäjän manipulointiin perustuvat riskit kasvavat ja korostuvat erityisesti silloin, kun käyttöoikeus tapahtuu etäkäyttöyhteyden yli. Haastattelussa Pänkäläinen kuvaa tämän tilanteen, jossa asetusten muuttamiseksi muodostetaan etäkäyttöyhteys alemman tason käyttöoikeuden omaavan henkilön suostumuksella. Kysymykseksi voi jäädä, mistä suostumuksen antava, alemman käyttöoikeustason haltija voi olla varma, että etäyhteyttä pyytää asianmukainen taho?

Tiedonsiirtoa käsitellään standardin SFS-CLC/TS 50131-7 liitteen H kohdassa 1.2, jossa todetaan, että mikäli tilaturvallisuusjärjestelmän signaalien välitykseen käytetään lankajärjestelmää, jota käyttävät myös muut laitteet tai järjestelmät, tulee varmistua, että tilaturvallisuusjärjestelmän signalointi ei vaarannu edes näiden muiden laitteiden vikatilanteissa. (SFS-CLC/TS 50131-7, 66)

Standardin SFS-CLC/TS 50131-7 kohta 7.3.3.3 käsittelee langattomia yhteyksiä. Siinä, ja sitä täydentävässä liitteen H kohdassa 1.3, edellytetään mm. huomioimaan muiden langattomien laitteiden sekä suurien metalliesineiden aiheuttamat ongelmat langattomalle tiedonsiirrolle. Tärkeimpänä seikkana voidaan kuitenkin pitää sen vaatimusta, joka koskee langattomien laitteiden antennin sijoittamista. Standardin määritelmän mukaan huomioon tulee ottaa: ”Antennin sijoittaminen luotettavan viestinnän aikaansaamiseksi järjestelmän komponenttien välille”. Pänkäläinen (2020) ottaa haastattelussa kantaa erityisesti tapauksiin, joissa tilaturvallisuusjärjestelmien viestintä murtohälytystapauksessa esimerkiksi vartioimisliikkeen suuntaan perustuu ainoastaan langattomiin yhteyksiin. Pänkäläinen toteaa, että useissa murtohälytystapauksissa hälytys tilaturvallisuusjärjestelmältä on lähtenyt vasta käytännössä siinä vaiheessa, kun murtomiehet ovat poistuneet paikalta. Tapausten tutkimuksessa saatujen tietojen pohjalta vaikuttaa siltä, että rikollisilla on ollut käytössään häirintälaitteita, joilla langattoman tiedonsiirron signaali on saatu estettyä siksi aikaa, kun murtoa ollaan toteuttamassa. (SFS-CLC/TS 50131-7, 30 sekä Pänkäläinen 2020.)

Standardi SFS-EN 50136-1:2012 + A1:2018 käsittelee tilaturvallisuusjärjestelmien ilmoituksen siirtoa. Sen kohdassa 6.2.5 käsitellään varautumista palvelunestohyökkäykseen. Vaatimus käytännössä määrittelee, että palvelunestohyökkäys ei saa haitata ilmoituksensiirtoa niin kauan kun se ei siirtotien kapasiteetin tukkimalla estä signaalin lähettämistä. Vaatimuksen tekee erikoiseksi se, että juuri siirtotien kapasiteetin tukkiminen on usein palvelunestohyökkäyksen

tarkoituskkin. Saman standardin kohta 6.3.3.3.2 käsittelee tilannetta, jossa ilmoituksensiirtojärjestelmä käyttää kahta tai useampaa siirtotietä. Standardi edellyttää, että ensisijaisen siirtotien toiminnan valvomisen lisäksi myös muiden siirtoteiden toimintaa on seurattava ja että järjestelmän on ilmoitettava niidenkin vikaantumisesta. Vikasignaalin tulee standardin mukaan näkyä myös hälytyksen vastaanottopäässä. (SFS-EN 50136-1:2012 + A1:2018, 15 - 19.)

Standardin SFS-EN 50136-1:2012 + A1:2018 kohdassa 6.8.1 käsitellään ilmoituksensiirtojärjestelmän yleisiä turvallisuusvaatimuksia. Standardi määrittelee, että ilmoituksensiirtojärjestelmän on käytettävä vähintään 128-bittistä, symmetriseen avaimeen perustuvaa salausta kaikissa ilmoituksensiirtojärjestelmän data- ja hallinnointitoimissa.

Kameravalvonnan suorituskkyä määrittelevän standardin SFS-EN 62676-1-2, kohta 12.1 toteaa, että korkeimmassa turvallisuusluokassa kaikki suojattujen teknisten tilojen ulkopuolinen dataviestintä on salattava ja sallitut salaustavat ovat symmetrisessä salauksessa 128-bittinen AES tai vaihtoehtoisesti 1024-bittinen RSA. Standardi erikseen kieltää käyttämästä ”natiivisalausta”, jolla tarkoitettaneen laitevalmistajan tarjoamia, omia salausmenetelmiä (SFS-EN 62676-1-2, 106).

4.3 Ohjelmistoturvallisuuden huomiointi standardeissa

Standardi SFS-EN 50131-1:2007 + A1 + A2:2017 kohta 11 on otsikoitu ”toimintavarmuus”. Ohjelmiston turvallisuuteen otetaan tässä asiakirjassa kantaa melko suuripiirteisesti toteamalla, että tilaturvallisuusjärjestelmässä on oltava ”hyvin suunniteltu ohjelmisto”. Vaikka tämä ei ole ainoa kohta tilaturvallisuusjärjestelmiä määrittelevissä standardeissa, on määritelmä niin avoin ja tulkinnanvarainen, ettei se ohjaa järjestelmien ohjelmistokehitystä tehokkaasti. Pänkäläisen (2020) mukaan standardi on laadittava avoimeksi. Kuitenkin ohjelmistoja vastaan suunnattuja hyökkäysmenetelmiä ja keinoja niiltä suojautumiseksi tunnetaan ja on dokumentoitu siinä laajuudessa, että tulisikin punnita, voitaisiinko tilaturvallisuusjärjestelmien ohjelmistoilta edellyttää, että niissä hyödynnettäisiin Bramwell:n (2018) mainitsemia suojautumisen keinoja kuten DEP ja ASLR vähintään korkeammilla turvatasoilla.

Standardi SFS-EN 50131-1:2007 + A1 + A2:2017 käsittelee kohdassa 8.3.1 tilaturvallisuusjärjestelmien käyttäjätasoja. Standardi jakaa käyttäjätasot neljään eri oikeuksia käsittävään tasoon, joista Taso 1 edustaa toimintoja, joihin kenellä tahansa on pääsy, kun taas puolestaan Taso 4 edustaa laitteen valmistajan pääsyä ja vaikutusmahdollisuuksia laitteen toimintaan ja konfiguraatioon (SFS-EN 50131-1:2007 + A1 + A2:2017, 22). Samantyyppinen käyttöoikeustasojen erittely mainitaan myös standardissa SFS-EN 54-21, joka käsittelee paloilmoittimia.

Edellä mainitussa standardissa SFS-EN 50131-1:2007 + A1 + A2:2017 käsitellään sitä, mitkä ovat edellytykset pääsyn saamiseen eri käyttöoikeustasolle. Standardi mainitsee, että tasojen kaksi ja kolme pääsyoikeudet on varattu käyttäjille, joskaan tasojen välisiä eroja ei käsitellä juurikaan. Standardi sisältää vain esimerkit tasolle, siten että tason kaksi yhteydessä mainitaan ”esim. operaattoreille” ja tason kolme yhteydessä mainitaan ”esim. hälytysliikkeen henkilökunta”. Ilmeistä on, että ristiriita näiden esimerkkien välillä on helppo löytää vaikkapa tilanteessa, jossa sama yritys on toimittanut kohteeseen sekä hälytysjärjestelmän että henkilöstön, joka miehittää turvavalvomon. Pääsyoikeuden erona mainitaan tasojen välillä, että korkeammalla tasolla käyttäjän oikeuksiin kuuluu: ” Kaikki I&HAS-järjestelmän rakenteeseen vaikuttavat toiminnot. (Muuttamatta laitteiston rakennetta)”. Epäselvän ilmaisun taustalla on ongelma standardin suomennoksessa. Kyseisen kohdan englanninkielinen ja samalla virallinen tekstiasu on: *”All functions affecting an I&HAS configuration (without changing equipment design)”*. Toisin sanoen, kolmannella käyttöoikeustasolla käyttäjän on sallittua muuttaa laitteen asetuksia, mutta ei itse laitetta. (SFS-EN 50131-1:2007 + A1 + A2:2017, 22.)

Edelleen standardin sama kohta määrittelee, että pääsy eri turvatasoille on suojattava avaimella, koodilla tai vastaavalla menetelmällä. Tasolle kolme on lisäksi käyttäjän tasolla kaksi sallittava ylemmän tason pääsyoikeuden avaaminen. Vastaavasti tason neljä pääsyoikeuden avaaminen edellyttää oikeutusta sekä tason kaksi että tason kolme pääsyoikeuden haltijoilta. Näihin sääntöihin muodostaa kuitenkin poikkeuksen esimerkiksi se, jos laitetta ollaan asentamassa ensi kertaa tai jos pääsy laitteeseen tapahtuu suojaetuista tiloista. Pääsy korkeammalle tasolle voidaan myös sallia, jos samaan aikaan sallitaan hälytyksen tai varoituksen muodostuminen. Samat määritelmät koskevat myös tilannetta, jossa pääsy muodostetaan etäkäyttöyhteyden yli. (SFS-EN 50131-1:2007 + A1 + A2:2017, 22.)

Hyvänä asiana edellä käsitellyn standardin kohdalla voidaan pitää sitä, että se erittelee käyttöoikeustasot, kuten edellyttävät esimerkiksi Rerup ja Aslaner (2018, 268-269.). Sanamuodoiltaan ja selkeydeltään standardi, ja varsinkin sen suomennos, jättävät kuitenkin toivomisen varaa, kuten edellä on tuotu esiin. Mitä standardi ei kuitenkaan edellytä millään pääsyoikeustasolla, on kahteen tekijään perustuva oikeuden myöntäminen, jota suosittaa mm. Kalinen (2020). Standardissa SFS-EN 50131-3 mainitaan (SFS-EN 50131-3, 15), että kahteen tekijään perustuva autentikointi on sallittua mutta sitä ei vaadita miltään turvallisuusluokalta. Myöskään standardi SFS-EN 50133-1 + A1. 2003, joka käsittelee kulunvalvontajärjestelmien toiminnallisia vaatimuksia, ei ota tässä asiassa kantaa kuin lähinnä vaadittavien koodien pituuksiin (SFS-EN 50133-1 + A1. 2003, 22). Vaikka standardi edellyttää korkeammille käyttäjätasolle pääsemiseksi hyväksyntää alemman tason käyttäjiltä, jättää tämä yhteen tekijään perustuvassa autentikoinnissa kuitenkin mahdollisuuksia erityyppisille väärinkäytöksille. Esimerkiksi samassa tilassa työskentelevät työntekijät voivat nähdä toistensa pääsykoodeja tai jos pääsy on rajattu vain avaimella, voi avaimiin olla mahdollista päästä käsiksi muidenkin samassa tilassa työskentelevien, kuin niiden virallisen haltijan.

SFS-EN 50131-1:2007 + A1 + A2:2017 standardin kohta 8.10 määrittelee, kuinka tilaturvallisuusjärjestelmän tulee käsitellä ns. lokitietoja. Siinä määritellään, kuinka monta erillistä tapahtumaa vähintään järjestelmän tulee kyetä säilyttämään ja mikä on minimisäilytysaika siinä tapauksessa, että järjestelmän tehonsyöttö katkeaa. Lisäksi luetellaan 28 erilaista tapahtumaa, sekä määritellään tasotyypeittäin, kuuluuko kyseinen tapahtuma tallennettavien tapahtumien joukkoon kyseisen turvatason tilaturvallisuusjärjestelmissä. Määrittelyä voidaan pitää yksityiskohtaisuudessaan ja täsmällisyydessään onnistuneena. Ongelmaksi voi kuitenkin nousta se, että kaikkein suurimmankin turvallisuustason järjestelmiltä edellytetty, tietojen tallennuksen minimiaika on 30 päivää. Kalinen (2020) toi haastattelussa esiin, että usein erilaiset tietoturvaloukkaukset tulevat esiin vasta useiden kuukausien kuluttua varsinaisesta tapahtumasta. Kalisen mukaan on tavallista, että tapahtuman paljastuttua, lokitiedot ovat ehtineet jo kadota ja tämä tyypillisesti vaikeuttaa tutkintaa huomattavasti. On huomattava, että standardin minimisäilytysaikavaatimus koskee tilannetta, jossa järjestelmän virransyöttö on katkennut. Tämän johdosta keskeiseen rooliin nousee ne toimenpiteet, joita järjestelmän käyttäjät suorittavat tilanteessa, jossa järjestelmän virransyöttö katkeaa. (SFS-EN 50131-1:2007 + A1 + A2:2017, 40.)

Standardissa SFS-EN 54-21 on kohdassa 7.10.2.1 esitetty mitä laitteen ohjelmistoa koskevaa dokumentaatiota valmistajan tulee toimittaa laitteen sertifiointia varten. Dokumentaation edellytetään kattavan ohjelmiston yleisen kuvauksen, funktionaalisen kuvauksen sekä kuvailevan kaikki moduulit lyhyine selvityksineen kunkin toiminnasta ja keskinäisestä vuorovaikutuksesta funktiokutsuineen ja keskeytyskäsitteilyineen. Lisäksi dokumentaation edellytetään selvittävän mille muistialueille eri tiedot, kuten itse suoritettava ohjelma, sen konfiguraatiot ja ajon aikaiset muuttujat tallennetaan. Dynaamisen muistinhallinnan ollessa käytössä edellytetään, että kyseisiä tietoja pidetään eri muistialueilla ja tämän tulee käydä ilmi ohjelmiston dokumentaatiosta. Tällä ei kuitenkaan ilmeisesti pyritä niinkään suojautumaan tarkoituksellisia hyökkäyksiä vastaan menetelmillä, joita Bramwell (2018, 268) mainitsee, vaan paremmin rajoittamaan mahdollisten ohjelmointivirheistä johtuvien vikojen laajuutta.

Kohta 7.10.2.2 edelleen täsmentää ohjelmiston dokumentaatioon kohdistuvia vaatimuksia. Kyseisen kohdan edellyttämää dokumentaatiota ei ole tarve toimittaa hyväksyntäprosessiin mutta se on oltava olemassa mahdollista tarkastusta varten. Vaatimukset ovat linjassa sen kanssa mitä ohjelmiston dokumentaatiolta voidaan edellyttää. Kohta 7.10.2.3 määrittelee ohjelmiston toteuttamisen päälinjoja toteamalla mm., että ohjelmiston tulee olla modulaarinen. Kyseistä vaatimusta käsiteltiin yksityiskohtaisesti haastattelussa Kalisen kanssa (2020). Kalisen mukaan ohjelmiston modulaarisuus on suurimmassa osassa tapauksia erittäin tärkeä ominaisuus ohjelmiston turvallisuuden kannalta. Kalisen mukaan tärkein modulaarisuuden etu on se, että mikäli tilaturvallisuusjärjestelmästä paljastuu vikoja tai haavoittuvuuksia tai sitä tarvitsee päivittää jostain muusta syystä, voidaan päivittäminen kohdistaa tiettyyn järjestelmän osaan ilman että muiden osien toiminnallisuus vaarantuu. Kalinen mainitsee esimerkkinä

todellisen tapauksen, jossa hotellihuoneiden kortinlukijoista paljastui vakava haavoittuvuus. Tällaisessa tapauksessa päivitys voidaan tehdä kortinlukijalaitteiden ohjelmistolle ilman, että järjestelmän toiminta muuten häiriintyy. Kalinen korostaa, että tämänkaltaisissa tapauksissa ohjelmiston ja yleisemmin koko järjestelmän komponenttien rajapintojen määrittelyllä on suuri merkitys. Standardi myös toteaa, että rajapintojen toteutuksessa on varauduttava virheellisiin syötteisiin. Kohdassa 7.10.4.4 edellytetään ohjelman suorituksen tarkkailua järjestelmän ylläpitämään perusaikaan perustuen. Kohdat 7.10.5 ja 7.10.6 määrittelevät suoritettavan ohjelman tallentamisesta pysyvään muistiin, johon on pääsy ainoastaan käyttöoikeustasolla 4 ja että käyttöpaikkakohtaisia tietoja voidaan päästä muuttamaan myös käyttöoikeustasolla 3. Lisäksi määritellään, että järjestelmän tulee tarkastaa käyttöpaikkakohtaisten tietojen oikeellisuus korkeintaan tunnin välein. Kalisen mukaan vaatimukset ovat linjassa järkevien käytänteiden kanssa. (SFS-EN 54-21, 18 - 20 sekä Kalinen 2020.)

Ohjelmistojen turvallisuudesta on erikseen todettava, että mikään tilaturvallisuusjärjestelmiä käsittelevä standardi ei edellytä laitteiden lähdekoodin tarkastamista sertifiointivaiheessa. Standardi SFS-EN 54-21 edellyttää kohdassa 7.10.2.2, että valmistajan on dokumentoitava lähdekoodin lisäksi myös kehitysvälineet, joista mainitaan erikseen kääntäjät. Kääntäjä on ohjelma, joka muuttaa ohjelman lähdekoodin prosessorin ymmärtämäksi ohjelmaksi, eli binääritiedostoksi. Jos myöhemmin ilmenisi tarve tarkastella ohjelmiston toimintaa tarkemmin, on periaatteessa mahdollista verrata laitteeseen tallennettua ja lähdekoodista samalla kääntäjäohjelman versiolla tehtyä suoritettavaa ohjelmaa, ja todeta, että kyseistä lähdekoodilistausta on käytetty järjestelmän ohjelmiston tuottamiseen. Kalinen kuitenkin kritisoi menetelmän luotettavuutta kahdesta syystä. Ensinnäkin samasta lähdekoodista samalla kääntäjällä käännetty ohjelma ei välttämättä ole identtinen käännöskerrasta toiseen. Tämä johtuu Kalisen mukaan siitä, että osa kääntäjistä pyrkii parantamaan ohjelmiston turvallisuutta muuttamalla käännettyjen ohjelman osien sijaintia binääritiedoston sisällä. Erityisesti tämä koskee ohjelman käyttämiä kirjastotiedostoja, joiden sijaintia muuttamalla pyritään estämään kirjastotiedostojen hyödyntämistä hyökkäysmenetelmissä, joita Bramwell (2018, 268) mainitsee. Vaikka kääntäjässä ei olisi käytössä kuvatus kaltaisia tietoturvaominaisuuksia, on Kalisen mukaan mahdollista, että jo pelkästään kääntäjän optimointiasetusten muutokset voivat muuttaa identtisistä lähdekoodeista muodostuvaa binääritiedostoa. Toinen Kalisen mainitsema syy sille, miksi standardin edellyttämä dokumentaatio ei riitä takaamaan ohjelmiston turvallisuutta on se, että on täysin mahdollista, että järjestelmän binääritiedoston muodostamiseen käytetty kääntäjä itsessään on tehty niin, että se automaattisesti sisällyttää kaikkiin ohjelmiin tietyn haavoittuvuuden tai takaoven. Kalisen mukaan, kyseinen tekniikka voidaan käytännössä toteuttaa niin, että jopa itse kääntäjäohjelman kääntäminen lähdekoodista tuottaa kääntäjästä version, joka asentaa muihin käännettäviin ohjelmiin haavoittuvuuden. Kalinen mainitsee, että edellä kuvatus, monimutkaisesta ongelmasta johtuen, korkeaa tietoturvaa

edellyttävissä sovelluksissa on yleistä, että niitä kehittävät organisaatiot ylläpitävät turvallisuusyistä itse omaa versiota kääntäjäohjelmista. (Kallinen 2020.)

4.4 Sulautetut järjestelmät ja ilmaisimet standardeissa

Standardi SFS-CLC/TS 50131-7 käsittelee kohdassa 7.3.1 millaisia komponentteja tilaturvallisuusjärjestelmän tulee sisältää. Se määrittelee yleisellä tasolla, että järjestelmän komponenttien tulisi vastata vaadittua turvatasoa ja ympäristöolosuhdeluokkaa. Sanamuoto ei kuitenkaan ole velvoittava. Standardi määrittää, että koko järjestelmän turvatasoksi tulee sen alimman turvataso komponentin taso. Standardi antaa kuitenkin mahdollisuuden käyttää myös komponentteja, joilla ei ole olemassa turvataso luokitusta, jossa tapauksessa järjestelmän taso määräytyy alimman luokitellun komponentin mukaisesti. Tämä jättää olennaisen riskin tietoturvalle, erityisesti tapauksessa, jossa suojattava kohde edellyttäisi korkean turvataso komponenttien käyttämistä, mutta toteutuksen osata käytetään komponentteja, joiden tietoturvaominaisuuksia ei esimerkiksi puutteellisen luokittelun johdosta tunneta. (SFS-CLC/TS 50131-7, 26.)

Standardi SFS-EN 50131-1:2007 + A1 + A2:2017 käsittelee kohdassa 8.7.3 sitä, miten tilaturvallisuusjärjestelmän tulee huomioida, jos joku siihen liitetystä sensoreista pyritään korvaamaan jollain muulla laitteella. Käytännössä standardin vaatimus on, että vain ylimmän tason, eli tason 4 laitteilta edellytetään, että järjestelmä huomaa, jos joku komponentti, viesti tai signaali korvataan. Muilla tasoilla kyseessä on vapaaehtoinen ominaisuus. Tämä on huolestuttavaa, kun otetaan huomioon, että Pankäläisen mukaan (2020) markkinoilla ei ole tason neljä vaatimuksia toteuttavia järjestelmiä ja toisaalta Kalisen (2020) mukaan vapaaehtoisia ominaisuuksia ei laitteissa juurikaan toteuteta. Tästä voidaan päätellä, että saatavilla olevissa tilaturvallisuusjärjestelmissä on mahdollisesti melko heikot valmiudet havaita, onko jokin signaali tai komponentti korvattu. Saman standardin kohdalla 8.83 määritellään aikaviiveet, joiden puitteissa eri tasoissa järjestelmissä tulee reagoida signaaliyhteyksien menetykseen. Korkeimmalla tasolla viiveen maksimiaika on kymmenen sekuntia, kun alemmilla tasoilla se on sata sekuntia. Kohta 8.9.1 standardissa lisää tähän, että murto-, ryöstö- ja sabotaasisignaalit, jotka ovat aktiivisina yli 400 millisekuntia, on käsiteltävä. (SFS-EN 50131-1:2007 + A1 + A2:2017, 36.)

Standardi SFS-EN 50131-2-2:2017 käsittelee PIR-liiketunnistimia. Standardin kohdan 4.1 mukaan, kolmannen ja neljännen turvallisuusluokan sensorien tulee reagoida, jos ne peitetään mutta ainoastaan korkeimman turvallisuusluokan ilmaisimien edellytetään tuottavan hälytyksestä kertovan signaalin tilanteessa, jossa niiden näkymä on rajoitettu kauempaa. Käytännössä tämä tarkoittaa, että alemman turvallisuusluokan laitteiden havaintoalueelle voi sijoittaa IR-valoa läpäisemättömän esineen eikä sensori reagoi sen takana tapahtuvaan liikkeeseen.

Kohta 6.4.7 määrittelee kyseisen ominaisuuden testimenetelmän korkeimman luokan ilmaisimille ja protokollan mukaan korkeimmassakin luokassa havaintoalan peittymisen tulee aiheuttaa signaali, jos havaintoala lyhenee alle puoleen ja este on paikoillaan yli kolmen minuutin ajan. Saman kohdan taulukossa kaksi määritellään erilaiset sensorin tilat sekä niihin liittyvä signaali. Erikoisena voidaan pitää linjausta, jossa standardi kieltää ilmaisimen signaaloinnin tilanteessa, jossa sensori ei havaitse liikettä. Tämä tuntuisi olevan ristiriidassa sen kanssa, mitä edellä on kuvattu standardin SFS-EN 50131-1:2007 + A1 + A2:2017 vaatimuksesta pystyä reagoimaan tilanteeseen, jossa menetetään signaaliyhteys sensoriin. (SFS-EN 50131-2:2017, 7 - 8.)

Myös PIR- ja mikroaaltotekniikkaa yhdistäviä liikeilmaisimia koskevassa standardissa EN 50131-2-4:2008 on havaittavissa puutteelliseksi luonnehdittavia yksityiskohtia. Standardin liitteessä I määritellään työkalut, joita testauksessa käytetään, kun tutkitaan ilmaisimen kykyä havaita tunkeutuminen sensorin kuoren sisäpuolelle. Työkalulistauksessa ei kuitenkaan huomioida esimerkiksi akkuporakonetta lainkaan. Jos hyökkääjä tuntee laitteen rakenteen ennalta, on poraamalla melko helppoa välttää yleisimmät kuoren murtamisen havaitsemiseksi käytetyt menetelmät ja päästä vaikuttamaan laitteen toimintaan. (EN 50131-2-4:2008, 38.)

Standardi EN 50131-2-6:2008 käsittelee magneetilla toimivia ilmaisimia, joita käytetään esimerkiksi tunnistamaan oven avautuminen. Kohdassa 4.1 on taulukko, jossa määritellään eri turvatasojen ilmaisimien toiminta eri tilanteissa. Ensimmäisen kahden turvallisuusluokan ilmaisimilta ei edellytetä useita erillisiä magneetteja kontaktiparin sisällä eikä magneettisen häirinnän tunnistamista. Kuten ovat osoittaneet esimerkiksi Tobias (2015) sekä Magnasphere Corp (2012), magneettisen häirinnän avulla on mahdollista ohittaa niin yhdestä kuin useammastakin magneettista koostuva ilmaisin, jos ilmaisimessa ei ole magneettisen häirinnän tunnistusta. Magneettisen häirinnän tunnistuksen puute voi myös aiheuttaa ongelmia kiinnitysalustasta irrottamisen tunnistukselle, kuten Magnasphere Corp (2012) osoittaa, joka on ominaisuus, jota standardi edellyttää jo toisen turvallisuusluokan laitteilta. Toisen turvallisuusluokan laitteilta ei kuitenkaan edellytetä magneettisen häirinnän tunnistamista (EN 50131-2-6:2008, 9).

4.4.1 Kameravalvonnan tietoturva

Standardi SFS-EN 50132-1 määrittelee tilaturvallisuusjärjestelmissä käytettävien kameroiden järjestelmävaatimukset. Standardi huomioi sangen yksityiskohtaisesti kuvatallenteiden kelpoisuuden todisteena, painottaen mm. seikkoja, kuten kuvan alkuperäisyyden osoittaminen jälkikäteen. Standardin kohdassa 6.3.2.4.2 määritelty vaatimus käyttöoikeustasoista on linjassa sen kanssa mitä mm. Rerup ja Aslaner (2018, 268-269) edellyttävät. Standardin kohdan 6.3.3.3 vaatimus datan suojaamisesta edellyttää kameran tallenteiden salaumahdollisuutta

vasta korkeimman turvallisuusluokan järjestelmiltä. Standardin kohdassa 6.3.2.3 määritellään, että korkeimmassa turvallisuusluokassa järjestelmän on havaittava kuvalähteen korvaaminen kuvayhteydessä tai käsittelyssä, joskin tämän vaatimuksen verifiointi lienee haasteellista, ottaen huomioon lukuisat turvallisuuspuutteet, joita kamerajärjestelmissä on löytynyt (SFS-EN 50132-1, 64).

Standardin kohdassa 8.3 käsitellään kameravalvontajärjestelmän komponenttien dokumentaatiota. Vaikka standardi puhuu komponenteista, selviää asiayhteydestä, että sanalla tarkoitetaan järjestelmäkomponentteja eikä esimerkiksi piirilevyllä olevia yksittäisiä komponentteja. Näin ollen, kameran dokumentaatiosta ei välttämättä käy ilmi laitteen elektroniikkakomponenttitason yksityiskohdat. Mm. Kalinen (2020) toi esiin laitteiden ja järjestelmien laajennettavuuden modulaaristen ohjelmistojen avulla ja totesi, että laitteissa on nykyisin usein samat komponentit huolimatta siitä, millä ominaisuuksilla se on hankittu. Näin ollen on mahdollista, että esimerkiksi tilassa, jossa käydään luottamuksellisia keskusteluja, saattaa olla asennettuna kamera, jossa on myös mikrofoni, jonka olemassaolo ei käy ilmi järjestelmän dokumentaatiosta. Myös standardi SFS-EN 62676-1-1 sisältää samoja määritelmiä ilman esiin tuotuja ongelmia koskevia tarkennuksia (SFS-EN 62676-1-1, 100). Jäljempänä mainittu standardi sisältää myös liitteen B, jossa on erillisiä vaatimuksia sovellettavaksi ”kansalliseen turvallisuuteen liittyvissä järjestelmissä”. Nämä vaatimukset eivät kuitenkaan liity tietoturvaan vaan tallenteen yhteensopivuuteen ja käytettyihin videoformaatteihin (SFS-EN 62676-1-1, 104).

Teoreettisessa viitekehyksessä käsiteltiin tapauksia, kameroihin oli kohdistunut erilaisia hyökkäyksiä (esim. Mirai -bottiverkko). Standardit ei kuitenkaan käytännössä huomioi kovin kattavasti niitä seikkoja, joita alan kirjallisuus ja toisaalta viimeaikaiset tutkimukset ovat havainneet ongelmalliseksi kameroiden tietoturvassa. Esimerkiksi standardissa SP108390123FI, joka käsittelee videonsiirron suorituskykyä, todetaan että kaikkein korkeimmassa turvallisuusluokassa järjestelmän on muodostettava vika- tai sabotaasisignaali, jos kamera ei ole saatavissa 30 sekunnin ajan (SP108390123FI, 64). Sama kohta toteaa suoran signaalin puuttumisen havaintoajaksi kaksi sekuntia korkeimmassa turvallisuusluokassa, neljä sekuntia luokassa kolme ja kahdeksan sekuntia toisessa turvallisuusluokassa. Voidaankin kysyä, kauanko hyökkääjältä kestäisi irrottaa valmiiksi rakenteiden sisältä esiin vedetty IP-kameran johto RJ45 liittimestä ja kiinnittää väliin hyökkääjän oma laite, kuten kytkin? Tuskin montaa sekuntia.

4.5 Rakenteelliset seikat

Standardi SFS-EN 50131-1:2007 + A1 + A2:2017 käsittelee kohdassa 8.7 tilaturvallisuusjärjestelmän keskuslaitteen suojaamista sabotaasilta. Kuten kirjallisuuskatsauksessa tuotiin esiin, Norman (2012) suosittelee kaapeloinnin suojaamista. Standardissa SFS-CLC/TS 50131-7 annetaan esimerkin omainen suositus metallisen asennusputken, johtokanavan tai kaapelikourun

käyttämistä etenkin silloin, kun kaapelointi kulkee valvotun tilan ulkopuolella. Keskuslaitteita käsittelevän standardin osalta johtojen suojaus laitteen sisällä toteutetaan käytännössä keskuslaitteen koteloinnin avulla. Standardi edellyttää, että keskuslaitteen sisälle pääsyyn on oltava käytössä siihen tarkoitettu työkalu ja että asiaton pääsy ei tule olla mahdollista ilman että siitä jää jälkiä. (SFS-EN 50131-1:2007 + A1 + A2:2017, 34)

Standardi määrittelee kotelon rakenteen tulkinnanvaraisesti kuvaten, että kotelon on oltava ”vankkarakenteinen ja mekaanisesti turvattu” (SFS-EN 50131-1:2007 + A1 + A2:2017, 34). TraceSecurity -nimiselle yritykselle työskennellyt Jim Stickley on mm. TV:ssä demonstroinut, kuinka hälytysjärjestelmän koteloointi voidaan avata nopeasti murtamalla ja täten estää järjestelmän normaali toiminta. Standardin tulisi tässä yhteydessä määritellä vankkarakenteisuus jollakin mitattavissa olevalla määritelmällä, joka estäisi mm. Stickley:n esiintuoman menetelmän käytön tilaturvallisuusjärjestelmän toiminnan estämiseen. (Stickley 2011.)

Sabotaasin ilmaisen muotoja on avattu saman standardin taulukossa numero 12, jossa yhtenä kohtana on eritelty ”tunkeutuminen komponentteihin”. Laajasti tulkiten, komponentilla voidaan tässä yhteydessä tarkoittaa kaikkia tilaturvallisuusjärjestelmän laitteita. Sabotaasin ilmaisuus on kuitenkin komponenttiin tunkeutumisen kohdalla määritelty standardissa SFS-EN 50131-1:2007 + A1 + A2:2017 pakolliseksi ominaisuudeksi vasta tason 4 tilaturvallisuusjärjestelmien kohdalla (SFS-EN 50131-1:2007 + A1 + A2:2017, 35). Samoin standardi EN 50131-3:2009, joka käsittelee tilaturvallisuusjärjestelmien keskuslaitteita, määrittelee kuoren sisällä tunkeutumisen tunnistamisen pakolliseksi vasta korkeimmassa turvallisuusluokassa. Samoin standardi SFS-EN 50133-2-1 joka käsittelee komponenttien yleisiä vaatimuksia, määrittelee että komponentin avaaminen on tunnistettava kun ”kotelo avataan normaalisti”, jättäen mahdolliseksi esimerkiksi kotelon poraamisen (SFS-EN 50133-2-1, 12).

Standardit SFS-EN 1627, SFS-EN 1628 + A1, SFS-EN 1629 + A1 sekä SFS-EN 1630 + A1 käsittelevät erilaisia ovia ja niiden kestävyyttä erilaisissa kuormissa ja erilaisia murtoyrityksiä vastaan. On silmiinpistävää, että nämä rakenteellista turvallisuutta käsittelevät standardit vaikuttavat kypsemmiltä ja varsinkin testien osalta kattavammilta, kuin elektronista tietoturva käsittelevät standardit. Esimerkiksi standardin SFS-EN 1630 + A1 kohta 7.1 sallii erilaisten sähkökäyttöisten työkalujen käytön rakenteen murtosuojaamisen testauksessa, kun taas elektronisten komponenttien testeissä tulokset voisivat olla erilaisia, jos hyökkääjän voitaisiin olettaa tuntevan komponentin rakenteen ja käyttävän poraa päästäkseen käsiksi sen kriittisiin kohtiin (SFS-EN 1630 + A1, 11- 14).

4.6 Muut huomiot

Kalinen (2020) tuo esiin standardeissa esiintyviin, vapaaehtoiisiin toiminnallisuuksiin liittyvän näkemyksen. Hänen mukaansa järjestelmiin harvoin toteutetaan mitään sellaisia toimintoja, joiden toteuttaminen ei ole tarpeellista. Tähän hän mainitsee kaksi syytä: 1. kaikkien ominaisuuksien testaaminen aiheuttaa kustannuksia, sekä 2. valmistajat mieluummin saavat maksun lisätoiminnallisuuksista, joita voidaan nykyisin myydä esimerkiksi verkkoyhteyden yli tapahtuvien ohjelmistopäivitysten avulla. Näin ollen voidaan kysyä, onko standardien tapa kirjata ominaisuudet jollain tietyllä tasolla vapaaehtoisiksi tarkoituksenmukaisin merkintätapa?

5 Johtopäätökset

Tämän tutkimuksen tutkimuskysymyksenä oli, kuinka hyvin tilaturvallisuusjärjestelmiä määrittävät standardit pystyvät takaamaan, että tilaturvallisuusjärjestelmät ovat turvallisia tietoturvan näkökulmasta. Aiheen laajuuden pakottamana kysymys jaettiin teemojen mukaisiin alatutkimuskysymyksiin. Tässä kappaleessa vastaamme tutkimuksen kysymyksiin saatujen tulosten ja havaintojen pohjalta.

Standardin SFS-CLC/TS 50131-7 vaatimukset langattomalle tiedonsiirrolle ovat tiukasti tulkittuna riittävät. Kuitenkin mm. Pänkäläisen (2020) esiin tuomat havainnot signaalinhäirintälaitteiden yleistymisestä murtojen yhteydessä herättävät ajatuksen siitä, tulisiko ainakin korkeampia turvatasoja ajatellen olla ohjeistus tai peräti vaatimus tietoliikenneyhteyksien varmistamiseksi ja siirtoteiden vikaantumisesta seuraavien toimenpiteiden tarkemmasta määrittelemisestä. Vaikka standardi SFS-EN 50136-1:2012 + A1:2018 vaatii, että hälytyksen vastaanottopäässäkin tulee näkyä vikasignaali tapauksessa, jossa tilaturvallisuusjärjestelmän siirtotie on vikaantunut, kertoo Pänkäläisen (2020) kuvaus tilanteesta, jossa toimintatavat eivät ole riittävällä tasolla vastaamaan siirtotien toimintaa häiritsevään hyökkäysmenetelmään. Riittävän tason määrittäminen on luonnollisesti tämän työn rajausten ulkopuolella, mutta harkittavaksi voisi tulla esimerkiksi kahdennettujen tietoliikenneyhteyksien edellyttämistä tai langattoman antennin sijoittamista koskevia vaatimuksia, joilla antenni saataisiin sijoitettua paremmin turvaan signaalinhäirinnältä. Vaatimusta ei voitane pitää liian rajoittavana, sillä jo voimassa olevissa standardeissa on vaatimuksia kahdennetuista siirtoteistä välitinlaitteen virransyötölle (SFS-EN 54-21, 16). Lisäksi voitaisiin määritellä tiukemmin ne toimenpiteet, joita edellytetään tilanteessa, jossa hälytyksen vastaanottopäässä havaitaan siirtotien vikaantuminen.

Sekä ohjelmistoturvallisuuteen että tietoliikenteen turvallisuuteen liittyvänä havaintona todetaan, että tilaturvallisuusjärjestelmiä käsittelevät standardit eivät millään turvatasolla, taikka siellä missä eri käyttöoikeustasoja on eritelty, edellytä järjestelmiltä kahteen tekijään

perustuvaa autentikointia. Tämän asian tärkeyttä kuitenkin painottivat haastatellut asiantuntijat (Kalinen 2020, Pänkäläinen 2020) erityisesti etäyhteyksien tapauksessa.

Julkisuudessakin esillä olleessa keskustelussa on sivuttu esimerkiksi Kiinassa valmistettujen laitteiden ohjelmistojen turvallisuutta siitä näkökulmasta, että on olemassa tahoja, jotka voivat haluta luoda ohjelmistoihin haavoittuvuuksia tai ns. takaovia tarkoituksellisesti. Pänkäläinen huomauttaa (2020), että Kiinan lisäksi myös monilla muilla valtiollisilla toimijoilla voi olla samankaltaisia intressejä joissakin tilanteissa. Näkemyksen jakaa myös turvallisuusasiantuntija Jerker Hellström Yleisradion tekemässä haastattelussa (YLE 2020). Tätä taustaa vasten tarkasteltuna standardien edellyttämää tasoa ohjelmiston dokumentoimisesta ei voida pitää riittävänä kaikkein korkeimman turvatason edellyttämiin sovelluksiin. Kalisen (2020) mukaan turvallinen lähdekoodi ei riitä takaamaan ohjelmiston turvallisuutta, sillä kääntäjä, jolla lähdekoodi muutetaan prosessorin ymmärtämäksi binäärikoodiksi, voi olla viritetty asentamaan ohjelmistoon haavoittuvuus. Tästä syystä ohjelmiston turvallisuuden takaamiseksi olisi vähintään korkeimman turvallisuusluokan laitteita koskevia vaatimuksia kehitettävä. Vaatimusten tulisi edellyttää lähdekoodin katselmointia sekä sellaisen kääntäjäversion käyttöä binääritiedoston luomisessa, jonka turvallisuudesta voitaisiin varmistua. Nämä ongelmat eivät rajoitu ainoistaan sensoreihin ja kameroihin vaan laajemmassa mielessä koskevat myös ohjelmistoturvallisuutta tilaturvallisuusjärjestelmien kaikilla komponenttitasoilla.

Valvontakameroiden osalta on huomattava, että standardien mukaan vasta korkeimmassa turvallisuusluokassa edellytetään mahdollisuutta tallenteiden salaamiseen. Kun otetaan huomioon, että Pänkäläisen (2020) mukaan korkeimman turvallisuusluokan järjestelmän toteuttaminen ei tätä kirjoitettaessa ole edes mahdollista ja kun huomioidaan mitä Park ja Kim (2015, 3) toteavat salauksen tärkeydestä, tulisikin pohtia, olisiko syytä ulottaa kyseinen vaatimus koskemaan myös vähintään kolmannen turvallisuusluokan järjestelmiä. Standardin vaatimuksia tulisi myös täsmentää vähintään korkeimmissa turvallisuusluokissa siten, että valmistaja edellyttäisi luettelemaan kaikki järjestelmässä olevat, kuvan, äänen tai muun vastaavan tiedon tallentamiseen kykenevät komponentit. Kuten on käynyt ilmi, myös sellaisia komponentteja, joita ei ole tarkoitettu ensisijaisesti äänen tallentamiseen (esim. kiihtyvyysanturi), on voitu käyttää salakuuntelussa hyödyksi. Näin ollen järjestelmän tilaajan tulisi pystyä valitsemaan tiloihin tarvittaessa sellaisia laitteita, joiden sensoreita ei ole mahdollista käyttää tilan salakuunteluun. Kun standardiin SFS-EN 62676-1-1 on voitu lisätä liite, jossa määritellään erityisiä vaatimuksia valvontakamerajärjestelmälle silloin, kun sen käyttö on yhteydessä kansallisen turvallisuuteen, olisi ehkä syytä tarkastella mahdollisuutta määritellä liitteessä videotalenteiden yhteensopivuusvaatimusten lisäksi myös vaatimuksia, jotka koskevat edellä esiin tuotuja tietoturvaongelmia.

Ilmaisiin liittyen, myös liiketunnistimina usein tavattujen PIR-sensoreiden standardit jättävät siinä määrin keinoja sensorin harhauttamiselle ja ohittamiselle, että alimpaa turvallisuusluokkaa lukuun ottamatta niiden käyttöön asemasta tulisi miettiä muita vaihtoehtoisia sensoreita. Myös magneetilla toimivien ovenavaussensorien standardi kaipaasi vähintään tarkennuksia, sillä nykyisellään standardi mahdollistaa vielä turvallisuusluokassa kaksi sellaisten sensoreiden käytön, joiden ohittaminen on verrattain helppoa yksinkertaisin menetelmin.

Esiin on syytä nostaa myös, että käytännössä tilaturvallisuusjärjestelmiä säätelevät standardit edellyttävät vasta turvatason neljä laitteilta kykyä huomata, jos järjestelmään kuuluva sensori tai sensorin lähettämä signaali on korvattu. Tätä seikkaa tulisi tarkastella kahdesta näkökulmasta. Nykyisin on saatavilla monia helposti ohjelmoitavia ja vähän energiaa kuluttavia mikrokontrollereita ja pieniä tietokoneita, kuten esimerkiksi kehitysalustaperheisiin Arduino ja Raspberry Pi kuuluvia tuotteita. Hyödyntämällä näitä halpoja ja yleisesti saatavilla olevia laitteita, on verrattain yksinkertaista rakentaa paristolla tai akulla toimiva laite, joka voidaan yhdistää tilaturvallisuusjärjestelmään hyökkääjän toimesta. Hyökkääjä voisi käyttää tätä lähestymistapaa kahteen tarkoitukseen. Hän voisi ensinnäkin käyttää laitetta tilaturvallisuusjärjestelmän signaalien tutkimiseen. Toinen vaihtoehto on rakentaa laite, jonka lähettämä signaalointi muistuttaa järjestelmässä normaalitilassa liikkuvaa signalointia ja täten harhauttaa järjestelmän sensorien normaalia toimintaa esimerkiksi korvaamalla jonkin sensorin tai kokonaisen sensoreiden muodostaman silmukan. Kun otetaan huomioon mitä Bhattacharjee (2018) sekä Rerup ja Aslaner (2018) tuovat esiin IOT-laitteiden turvallisuuden parantamisesta, voitaisiin samaa hyödyntää sensorien yhteydessä. Liittämällä sensorien signalointiin esimerkiksi järjestelmän keskuslaitteen ylläpitämästä ajasta johdetun, vaihtuvan komponentin ja käyttämällä edes yksinkertaista salausta jonkin haavoittuvaksi tiedetyn tietoliikenneprotokollan asemasta, olisi sensorien korvaamisen havaitseminen toteutettavissa tavalla, joka olennaisesti vaikeuttaisi signaalien tai komponenttien korvaamiseen perustuvia hyökkäysmenetelmiä. Vaatimusta ei voitane pitää teknisesti haastavana, sillä standardin SFS-EN 54-21 kohdan 7.10.4.4 perusteella jo tilaturvallisuusjärjestelmän ohjelmiston suorituksen valvonta edellyttää perusajan ylläpitoa ((SFS-EN 54-21, 18). Aikakomponentin mukana pito mahdollistaa myös varautumisen tilanteeseen, jossa hyökkääjä pyrkii syöttämään verkkoon esimerkiksi aikaisemmin tallennettua dataa (Dodangeh & Jahangir 2018, 68). Laskentatehon ollessa ongelmana voitaisiin sensoreissa edellyttää esimerkiksi Lin ym. (2018, 46) sekä Dodangeh:n ja Jahangir:n (2018, 68) esittämää lähestymistapaa, jossa yksinkertaisen autentikoinnin jälkeen sensori saa käyttöönsä salausavaimen, jota ilman sensorin data ei olisi käytettävissä tai laitteesta luettavissa edes, jos sensori joutuisi väärin käsiin.

Standardien ja toisaalta muun aineiston vertaaminen toi esiin tekijöitä, joissa tilaturvallisuusjärjestelmien asentajien, ylläpitäjien ja käyttäjien toiminta voi vaikuttaa tilaturvallisuuden kokonaistilaan. Toimivan ohjeistuksen ja vakioitujen käytänteiden avulla voidaan joitakin

puutteita korjata ilman, että järjestelmien teknisiä vaatimuksia muutetaan. Esimerkiksi luomalla uusia järjestelmiä, komponentteja ja sensoreita koskeva käyttöönotto-ohjeistus, voidaan vaikuttaa siihen, että järjestelmään ei jää sellaisia osia, joissa on käytössä oletussalasanoja. Käyttäjiä tulisi myös edellyttää muodostamaan myös tilaturvallisuusjärjestelmien tapahtumalokista varmuuskopio säännöllisin väliajoin, ja erityisesti tilanteissa, joissa järjestelmän toiminnassa havaitaan jotain tavallisuudesta poikkeavaa. Näin menetellen voidaan turvata tutkintatoimien suorittamista tapauksissa, joissa tietoturvapoikkeaman ja varsinaisen tapahtuman välillä olisi kulunut enemmän aikaa, kuin järjestelmien tekniset vaatimukset edellyttävät tapahtumalokien säilytysajoiksi. Koska kattavan ohjeistuksen laatiminen edellyttää melko syvällistä, tietoturvan problematiikkaan liittyvää ymmärrystä, ei riittävää osaamista välttämättä ole käytössä esimiestasolla kaikissa organisaatioissa. Johtamisen ja esimiestyön tukemiseksi ja toisaalta organisaatioiden turvallisuuskulttuurin kehittämiseksi sopiva ohjeistus ja kuvaus hyvistä käytänteistä voisi osaltaan auttaa organisaatioita kehittämään tilaturvallisuuden liittyvien järjestelmiensä tietoturvaa ja sen mahdollisiin loukkauksiin varautumista. Kumpaakin tässä mainittua esimerkkiä koskevia ohjeita löytyy standardin SFS-CLC/TS 50131-7 vaatimuksista (kohdat 11.1 sekä 11.2) mutta standardin sisältämä tieto ei jalkaudu tilaturvallisuusjärjestelmien käyttäjille, mikäli asioita ei ohjeisteta osana työpaikan käytänteitä.

Yleisenä huomiona voitaneen tuoda esiin, että standardien määritelmät eivät kaikissa tapauksissa ole ehkä selkeimpiä mahdollisia. Dokumenttien yleistä rakennetta ja jäsentelyä olisi ehkä mahdollista kehittää mm. muodostamalla dokumentti, jossa määritellään hierarkia, jonka kautta lukijan on helppo löytää sen standardi, jonka juuri hän tarvitsee. Lisäksi etenkin standardien suomennosten laadussa olisi kehittämistä. Suomennos, jonka pohjalta oikean käsityksen muodostaminen edellyttää lisäksi virallisen, englanninkielisen tekstin lukemisen, ei lähtökohtaisesti toteuta tehtäväänsä onnistuneesti. Standardeissa myös näkyy, että niitä on laadittu eri aikoina. Osa vanhemmista standardeista jättää melkoisesti toivomisen varaa tietoturvan nykyaikasteiden näkökulmasta, kun taas esimerkiksi 2018 hyväksytty standardi ilmoituksensiirtojärjestelmistä edellyttää kaikelta ilmoituksensiirtoon käytetyltä tietoliikenteeltä jo salauksen käyttämistä.

Edellä esitellyn perusteella voidaan todeta, että tilaturvallisuusjärjestelmiä määrittelevät standardit sisältävät tietoturvaan haitallisesti vaikuttavia puutteita tietoliikenteen, ohjelmistoturvallisuuden, sensoreiden ja sulautettujen järjestelmien sekä rakenteellisten seikkojen kohdalla. Tehtyjen havaintojen perusteella suurimmat puutteet painottuvat tilanteisiin, joissa tietoteknisiin keinoin pyritään vaikuttamaan tilaturvallisuusjärjestelmän toimintaan. Löydettyjen puutteiden joukossa on kuitenkin myös sellaisia tekijöitä, jotka voivat mahdollistaa hyökkäyksen, joka kohdistuu suoraan suojatun tilan tietoturvaan tilaturvallisuusjärjestelmän haavoittuvuuksien kautta. Myös joidenkin, ehkä jo vanhentuneiden sensoriratkaisujen käyttö sekä toisaalta uusimpien, vielä riittävästi kehittymättömien sensorien käyttö standardien sallimissa rajoissa voi osaltaan luoda haavoittuvuuksia suojatun kohteen tietoturvalle. Eri teemojen

puutteissa tavattujen puutteiden priorisointi tai arvottaminen on kuitenkin tämän tutkimuksen rajauksen ulkopuolella ja vaatisi luultavasti myös kohdekohtaista arviointia, jotta painoarvo olisi mahdollista asettaa oikein. On kuitenkin todettava, että vaikka nykyisellään tilaturvallisuusjärjestelmien standardit ovat pääsääntöisesti melko hyvällä tasolla, eivät ne kuitenkaan takaa suojatun tilan tietoturvaa tapauksissa, joissa hyökkääjällä on käytössään tietoteknistä osaamista sekä mahdollisuus suunnitelmalliseen työskentelyyn (mm. kohteen tiedustelu). Tämän tyyppiset, tietoturvaan kohdistuvat hyökkäykset tulevat etenkin kyseeseen valtiollisten toimijoiden tapauksessa, mutta myös liikesalaisuuksiin liittyvissä tapauksissa sekä yhä enenevissä määrin myös rikollisten toiminnassa.

Tutkimuksen aikana esiin tulleiden puutteiden pohjalta voidaan suositella joitakin toimenpiteitä nykytilan kehittämiseksi. Haastatteluissa (mm. Pänkäläinen 2020) tuli esiin, ettei nykyisiä standardeja laadittaessa ole huomioitu esimerkiksi etäkäyttöyhteyksien nopeaa kehittymistä tai IOT-tekniikan yleistymistä osana erilaisia kiinteistöautomaatioon ja tilaturvallisuuden liittyviä järjestelmiä. Näiden seikkojen ottaminen huomioon tulevaisuuden standardien kehitysversioneissa on toteutettavissa joidenkin vuosien aikajänteellä. Kansallisella tasolla tulisi pohtia, voitaisiinko tilaturvallisuusjärjestelmille kehittää jonkinlainen menettely, jolla järjestelmän tietoturvan taso voitaisiin arvioida ja sertifioida. Tämä voisi olla erillinen tietoturvahyväksyntä, joka myönnettäisiin järjestelmien osille kuten sensoreille ja päätelaitteille, silloin kun voitaisiin todeta, että niissä ei ole ilmeisiä puutteita tietoturvan näkökulmasta. Erillisellä tietoturvahyväksynnällä olisi ehkä mahdollista puuttua tietoturvan näkökulmasta kyseenalaisiin tilanteisiin, joita voi syntyä silloin, kun tilaturvallisuusjärjestelmän toteuttamiseen käytetään muita kuin luokiteltuja komponentteja, kuten standardi SFS-CLC/TS 50131-7 mahdollistaa.

Ohjelmistoturvallisuuden kehittämiseksi tulisi standardeissa tarkemmin huomioida, kuinka voidaan osoittaa, että tuotantoympäristöön asennetun laitteen ohjelmisto on sama, kuin lähdekoodin perusteella voisi olettaa. Vastaavasti, vähintään korkeimpien turvallisuusluokkien laitteiden sisältämien komponenttien dokumentointi tulisi standardeissa huomioida nykyistä tarkemmin. Tietoliikenteen osalta todetaan, että useissa tuoreissa tutkimuksissa on saatu lupaavia tuloksia erilaisten hyökkäysten tunnistamisesta menetelmillä, jotka ovat perustuneet reaaliaikaisen analyysin käyttämiseen. Näitä ovat mm. Dasin ym. esittelemä keino ROP-hyökkäyksen tunnistamiseksi.

Tulevaisuudessa olisikin syytä tutkia, voisiko tilaturvallisuusjärjestelmien moninaiseen hyökkäysvektorien kirjoon suhtautua kokonaisvaltaisesti, painottaen erilaisia reaaliaikaisen tunnistamisen menetelmiä. Standardien kehittämiseksi tulisi esimerkiksi hyödyntää penetraatiotestauksen, eli ns. eettisten tietomurtojen oppeja ja ajattelumalleja. Tulevaisuuden uhkiin varautumiseksi tulisi myös ottaa huomioon alati kasvava, mobiilin laskentatehon vaikutus salauksen ja esimerkiksi *brute force* -hyökkäyksiin varautumisen kohdalla.

Lisäksi jatkossa olisi syytä selvittää tarkemmin erillisen tutkimuksen avulla, millainen vaikutus tilaturvallisuusjärjestelmien tietoturvalle muodostuu niitä asentavien ja toimittavien yritysten toiminnasta. Nykyinen säätely perustuu poliisin myöntämään hyväksyntään, jonka keskeisin näkökulma on toimijan nuhteeton tausta, sekä toisaalta Finanssiala ry:n luettelointiin, joka keskittyy etupäässä yrityksen laadulliseen arviointiin. Koska tilaturvallisuusjärjestelmien asennukseen liittyvillä yksityiskohdilla ja asennusta koskevilla tiedoilla on laaja vaikutus järjestelmän tietoturvaan, tulisikin selvittää, kuinka tietoturvaa koskevia edellytyksiä olisi mahdollista ulottaa järjestelmiä asentaviin toimijoihin.

6 Arviointi

Tämä tutkimus koostui suuresta määrästä tietoturvaluuteen liittyvää tietoa. Tietoa käsiteltiin sisällönanalyysin keinoin. Menetelmän valintaa voidaan pitää onnistuneena, sillä sen avulla tietomäärä oli helpompi jäsentää osakokonaisuuksiin, jotka auttoivat hahmottamaan asioiden merkityksiä. Eri teemojen kautta syntyi kokonaiskäsitys tietoturvaan vaikuttavista, keskeisistä asioista, kun tarkastelu kohdistuu nimenomaan tilaturvallisuusjärjestelmien tietoturvaan. Aineistojen vertailu tilaturvallisuusjärjestelmiä käsitteleviin standardeihin tuntui niin ikään toimivalta valinnalta. Kun tilaturvallisuusjärjestelmien tietoturvaan vaikuttavat teemat yleisestä tietoturvasta käsittelevästä aineistosta oli hahmotettu, oli standardien vaatimukset helpompi mieltää näiden teemojen kautta ja verrata niitä siten alan ajankohtaiseen tietoon.

Asiantuntijahaastatteluissa puolistrukturoitu teemahaastattelu osoittautui tehokkaaksi tavaksi hankkia tutkimuksen kannalta keskeistä tietoa. Haastattelurunko voitiin suunnitella asiantuntijan osaamisaluetta ajatellen, mutta menetelmä toisaalta mahdollisti asiasta keskustelun myös laajemminkin. Menetelmän käyttöä edesauttoi myös haastateltavien korkea asiantuntemuksen taso.

Kokonaisuutena valitut menetelmät mahdollistivat aineistojen riittävän tarkan vertailun, jolloin oli mahdollista löytää standardeista tietoturvaan vaikuttavia puutteita. Olennaista oli, että kyseessä olivat seikat, jotka ovat tilaturvallisuusjärjestelmissä jääneet huomiotta, mutta joita on jo opittu huomioimaan muissa teknologian sovelluksissa, joissa tietoturva on osa järjestelmän keskeisiä ominaisuuksia. On kuitenkin huomattava, että tilaturvallisuusjärjestelmiin kuuluvan teknologian kirjo on mittava ja aihetta voi lähestyä useista eri näkökulmista. Vaikka mainituilla menetelmillä onnistuttiin selvittämään tietoturvaluuteen vaikuttavien puutteiden olemassaolo, tulisi mahdollista jatkotutkimusta ajatellen pohtia, voisiko aihetta pilkkoa erillisiin osiin, jotta kunkin näkökulman tarkempaan analysointiin olisi löydettävissä parhaiten sopivimmat tutkimusmenetelmät.

Lähteet

Painetut

224/2012. Laki Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta neuvostossa kokoontuneiden Euroopan unionin jäsenvaltioiden välillä tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.

24.6.2004/588. Laki kansainvälisistä tietoturvallisuusvelvoitteista.

77/2015. Valtioneuvoston asetus Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta neuvostossa kokoontuneiden Euroopan unionin jäsenvaltioiden välillä tehdyn sopimuksen voimaansaattamisesta sekä sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain voimaantulosta.

Allsopp, W. 2009. Unauthorized Accesss - Physical Penetration Testing For IT Security Teams. Chichester, Iso-Britannia: John Wiley & Sons.

Balapure, A. 2013. Learning Metasploit Exploitation and Development. Birmingham, Iso-Britannia: Packt Publishing.

Bhattacharjee, S. 2018. Practical Industrial Internet of Things Security. Birmingham, Iso-Britannia: Packt Publishing.

Bosworth, S., Kabay, M. & Whyne, E. 2014. Computer Security Handbook. Hoboken, New Jersey, USA: Wiley.

Bradley, T. & Carvey, H. 2006. Essential Computer Security. USA: O'Reilly Media.

- Bramwell, P. 2018. Hands-On Penetration Testing on Windows: Unleash Kali Linux, PowerShell, and Windows Debugging Tools for Security Testing and Analysis. Birmingham, Iso-Britannia: Packt Publishing.
- Brooks, C., Grow, C., Craig, P. & Short D. 2018. Cybersecurity Essentials. Yhdysvallat: Sybex.
- Diogenes, Y. & Ozkaya, E. 2019. Cybersecurity - Attack and Defence Strategies. Birmingham, Iso-Britannia: Packt Publishing.
- Eskola, J. & Suoranta, J. 2014. Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino.
- Hirsjärvi, S & Hurme, H. 2004. Tutkimushaastattelu -teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.
- Hirsjärvi, S., Remes, P & Sajavaara, P. 1997. Tutki ja kirjoita. 13., osin uudistettu laitos. Keuruu: Otavan Kirjapaino Oy.
- Makan, K. 2014. Penetration Testing with the Bash shell. Birmingham, Iso-Britannia: Packt Publishing.
- Mooney, C. 2020. Using Computer Science in High-Tech Security Careers. New York, USA: The Rosen Publishign Group.
- Norman, T. 2012. Electronic Access Control. Waltham, MA, USA: Elsevier.

Pearson, R. 2007. Electronic Security Systems - A Manager's Guide to Evaluating and Selecting System Solutions. Burlington, MA, USA: Elsevier.

Rasimus, T., Rossi, A., Nuutinen, A., Hovatta, T., Hovinen, R. & Arenius, K., 2019. Turvaa oikein -opas - Turvallisuusjärjestelmien hankinnan sekä turvallisuussuunnittelun ja -urakoinnin hyvät käytännöt. Espoo. Turva-alan yrittäjät ry.

Rerup, N & Aslaner, M. 2018. Hands-On Cybersecurity for Architects - Plan and design robust security architectures. Birmingham, Iso-Britannia: Packt Publishing.

Salmon, A, Levesque, W. & McLafferty, M. 2017. Applied Network Security. Birmingham, Iso-Britannia: Packt Publishing.

SFS-CLC/TS 50131-7. 2009. Hälytysjärjestelmät. Murto- ja ryöstönilmaisujärjestelmät. Osa 7: Soveltamisohjeet. Helsinki: Suomen Standardoimisliitto.

SFS-EN 1627. 2012. Pedestrian doorsetts, windows, curtain wallings, grilles and shutter. Burglar resistance. Requirements and classification. Helsinki: Suomen Standardoimisliitto.

SFS-EN 1628 + A1. 2015. Pedestrian doorsetts, windows, curtain wallings, grilles and shutter. Burglar resistance test method for the determination of resistance under static loading. Helsinki: Suomen Standardoimisliitto.

SFS-EN 1629 + A1. 2015. Pedestrian doorsetts, windows, curtain wallings, grilles and shutter. Burglar resistance test method for the determination of resistance under dynamic loading. Helsinki: Suomen Standardoimisliitto.

SFS-EN 1630 + A1. 2015. Pedestrian doorsetts, windows, curtain wallings, grilles and shutter. Burglar resistance test method for the determination of resistance to manual burglary attempts. Helsinki: Suomen Standardoimisliitto.

SFS-EN 50131-1:2007 + A1 + A2:2017. 2017. Hälytysjärjestelmät. Murjo- ja ryöstönilmaisujärjestelmät. Osa 1: Järjestelmävaatimukset. Helsinki: Suomen Standardoimisliitto.

SFS-EN 50131-2-2:2017. 2017. Alarm systems. Intrusion and hold-up systems. Part 2-2: Intrusion detectors. Passive infrared detectors. Helsinki: Suomen Standardoimisliitto.

SFS-EN 50131-3. 2009. Alarm systems. Intrusion and hold-up systems. Part 3. Control and indicating equipment. Helsinki: Suomen Standardoimisliitto.

EN 50131-2-6:2008. 2009. Alarm Systems - Intrusion and Hold-Up Systems - Part 2-6: Opening Contacts (Magnetic). Helsinki: Suomen Standardoimisliitto.

SFS-EN 50132-1. 2010. Hälytysjärjestelmät. Turvasovelluksissa käytettävät kameravalvontajärjestelmät. Osa 1: Järjestelmävaatimukset. Helsinki: Suomen Standardoimisliitto.

SFS-EN 50133-1 + A1. 2003. Hälytysjärjestelmät. Turvallisuussovelluksissa käytettävät kuluvalvontajärjestelmät. Osa 1: Järjestelmävaatimukset. Helsinki: Suomen Standardoimisliitto.

SFS-EN 50133-2-1. 2001. Hälytysjärjestelmät. Turvallisuussovelluksissa käytettävät kuluvalvontajärjestelmät. Osa 2: Yleiset vaatimukset komponenteille. Helsinki: Suomen Standardoimisliitto.

SFS-EN 50136-1:2012 + A1:2018. 2018. Hälytysjärjestelmät. Ilmoituksensiirtojärjestelmät ja -laitteet. Osa 1: Yleiset vaatimukset ilmoituksensiirtojärjestelmille. Helsinki: Suomen Standardoimisliitto.

SFS-EN 54-21. 2006. Paloilmoittimet. Osa 21: Palo- ja vikailmoitusten välitinlaitteet. Helsinki: Suomen Standardoimisliitto.

SFS-EN 62676-1-1. 2014. Turvasovelluksissa käytettävät kameravalvontajärjestelmät. Osa 1-1: Järjestelmävaatimukset. Yleiset vaatimukset. Helsinki: Suomen Standardoimisliitto.

SFS-EN 62676-1-2. 2014. Turvasovelluksissa käytettävät kameravalvontajärjestelmät. Osa 1-2: Järjestelmävaatimukset. Videon siirtoa koskevat suorituskyykyvaatimukset. Helsinki: Suomen Standardoimisliitto.

Skulkin, O., Tindall, D & Tamma, R. 2018. Learning Android Forensics. Birmingham, Iso-Britannia: Packt Publishing.

VAHTI 2/2013. Toimitilojen tietoturvaohje. Valtiohallinnon tietoturvallisuuden johtoryhmä. Valtiovarainministeriö.

Sähköiset

Anand, S. & Sharma, A. 2020. Assessment of security threats on IoT based applications. Viitattu 7.11.2020. Aineisto saatavana osoitteessa: <https://www.sciencedirect-com.nelli.laurea.fi/science/article/pii/S2214785320370607>

Citizen Lab 2016. Sophisticated, persistent mobile attack against high-value targets on iOS. Viitattu 23.10.2020. Aineisto saatavana osoitteessa: <https://blog.lookout.com/trident-pegasus>

Crawley, A. 2016. Hiring Hackers. Network Security. Viitattu 8.11.2020. Aineisto saatavana osoitteessa: <https://www.sciencedirect-com.nelli.laurea.fi/science/article/pii/S1353485816300885>

CSIS 2020. Significant Cyber Incidents. Central for Strategic & International Studies:n ylläpitämä lista merkittävistä kyberhyökkäyksistä. Viitattu 15.8.2020. Aineisto saatavilla osoitteessa: <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>

Das, S., Chen, B, Chandramohan, M., Liu, Y. & Zhang, W. 2018. ROPSentry: Runtime defence against ROP attacks using hardware performance counters. Computers & Security. Viitattu 7.11.2020. Aineisto saatavana osoitteessa: <https://www.sciencedirect.com/science/article/pii/S0167404817302481>

Devi A., Mohan A., Sethumadhavan, M. 2017. Wireless Security Auditing: Attack Vectors and Mitigation Strategies. Viitattu 8.11.2020. Aineisto saatavana osoitteesta: <https://www.sciencedirect-com.nelli.laurea.fi/science/article/pii/S1877050917319853>

Dodangeh, P. & Jahangir, A. 2018. A biometric security scheme for wireless body area networks. *Journal of Information Security and Applications*. Viitattu 8.11.2020. Aineisto saatavana osoitteessa: <https://www-sciencedirect-com.nelli.laurea.fi/science/article/pii/S221421261730621X>

Farrell, G. 2015. Preventing phone theft and robbery: the need for government action and international coordination. *Crime Science*. Viitattu 8.11.2020. Aineisto saatavana osoitteessa: <https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-014-0015-0>

Finanssiala 2017a. Rakenteellinen murtosuojausohje I. Finanssiala ry. Viitattu 1.10.2020. Aineisto saatavana osoitteessa: <https://www.finanssiala.fi/vahingontorjunta/dokumentit/Rakenteellinen%20murtosuojaus%20I.pdf>

Finanssiala 2017b. Murtohälytysjärjestelmien suunnittelu- ja asennusliikkeiden vaatimukset. Viitattu 16.11.2020. Aineisto saatavana osoitteessa: https://www.finanssiala.fi/vahingontorjunta/dokumentit/Turvallisuusjarjestelmien_suunnitteluliike_vaatimukset.pdf

Finanssiala 2020. Murtohälytysjärjestelmiä toimittavat liikkeet. Finanssiala ry. Viitattu 16.8.2020. Aineisto saatavana osoitteessa: https://www.finanssiala.fi/vahingontorjunta/dokumentit/Murtohalytysjarjestelmia_toimittavat_liikkeet.pdf#search=murtoh%C3%A4lytys

Finogeev, A. 2017. Information attacks and security in wireless sensor networks of industrial SCADA systems. *Journal of Industrial Information Integration*. Viitattu 23.10.2020. Aineisto saatavana osoitteessa: <https://www-sciencedirect-com.nelli.laurea.fi/science/article/pii/S2452414X16301029>

Halkosaari, A. 2014. Kameravalvonnan nykytila. Laurea. Viitattu 23.10.2020. Aineisto saatavana osoitteessa: https://www.theseus.fi/bitstream/handle/10024/82935/Halkosaari_Antti.pdf?sequence=1&isAllowed=y

Heath, S. 2002. Embedded Systems Design. Elsevier Science & Technology. Viitattu 12.11.2020. Aineisto saatavana osoitteessa: <http://ebookcentral.proquest.com/lib/laurea/detail.action?docID=294113>.

Homeland Security 2013. CCTV Technology Handbook. U.S. Department of Homeland Security, Science and Technology Directorate. Viitattu 20.10.2020. Aineisto saatavana osoitteessa: https://www.dhs.gov/sites/default/files/publications/CCTV-Tech-HBK_0713-508.pdf

Hänninen, M. 2019. Open source intrusion detection systems evaluation for small and medium-sized enterprise environments. Viitattu 21.10.2020. Aineisto saatavilla osoitteessa: <https://www.theseus.fi/bitstream/handle/10024/265554/Markku%20H%c3%a4nninen%20thesis.pdf?sequence=2&isAllowed=y>

Kyberturvallisuuskeskus 2020a. CERT. Kyberturvallisuuskeskuksen CERT-toiminnon esittely internetissä. Viitattu 16.8.2020. Aineisto saatavilla osoitteessa: <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/cert>

Kyberturvallisuuskeskus 2020b. NCSA. Kyberturvallisuuskeskuksen NCSA-toiminnon esittely internetissä. Viitattu 16.8.2020. Aineisto saatavilla osoitteessa: <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa>

Kyberturvallisuuskeskus 2020c. Sääntely ja valvonta. Kyberturvallisuuskeskuksen Sääntely ja valvonta -toiminnon esittely internetissä. Viitattu 16.8.2020. Aineisto saatavilla osoitteessa: <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta>

Kyberturvallisuuskeskus 2020d. Satelliittipaikannus. Satelliittipaikannus -toiminnon esittely internetissä. Viitattu 16.8.2020. Aineisto saatavilla osoitteessa: <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/satelliittipaikannus>

Kyberturvallisuuskeskus 2020e. Galileon viranomaispalvelu PRS. PRS-palvelun esittely internetissä. Viitattu 16.8.2020. Aineisto saatavilla osoitteessa: <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/satelliittipaikannus/galileon-viranomaispalvelu-prs>

Laki julkisen hallinnon tiedonhallinnasta 906/2019. Viitattu 1.9.2020. <https://www.finlex.fi/fi/laki/ajantasa/2019/20190906>

Laki yksityisistä turvallisuuspalveluista 1085/2015. Viitattu 16.11.2020. <https://www.finlex.fi/fi/laki/ajantasa/2015/20151085>

Li, Y., Wang, X., Kim, D., Zhang, D. & Dai, R. 2018. Designing self-destructing wireless sensors with security and performance assurance. Computer Networks. Viitattu 7.11.2020. Aineisto saatavana osoitteessa: <https://www-sciencedirect-com.nelli.laurea.fi/science/article/pii/S1389128618302299>

Liikenne- ja viestintäministeriö 2018. Viestintävirasto ja Trafi yhdistyvät Liikenne- ja viestintävirastoksi - Liikennevirastosta tulee Väylävirasto. Liikenne- ja viestintäministeriön tiedote. Viitattu 15.8.2020. Aineisto saatavilla osoitteessa: <https://www.lvm.fi/-/viestintavirasto-ja-trafi-yhdistyvat-liikenne-ja-viestintavirastoksi-liikennevirastosta-tulee-vaylavirasto-987823>

Magnasphere Corp. 2012. Magnetic defeat of GE Sentrol 2707A. Viitattu 7.11.2020. Aineisto saatavana osoitteessa: <https://www.youtube.com/watch?v=N9N7zrW-qPA>

Mansfield-Devine, S. 2017. Weaponising the Internet of Things. Viitattu 8.11.2020. Aineisto saatavana osoitteessa: <https://www-sciencedirect-com.nelli.laurea.fi/science/article/pii/S1353485817301046>

Misra, R., Agarwal, K. & Suman, P. 2018. Hardware Trojans in IOT Devices: A Survey. International Journal of Advanced Research in Computer Science. Viitattu 7.11.2020. Aineisto saatavana osoitteessa: <https://search.proquest.com/docview/2101236604?pq-origsite=gscholar&fromopenview=true>

Narwal, B. & Mohapatra, A. 2020. A survey on security and authentication in wireless body area networks. Journal of Systems Architecture. Viitattu 7.11.2020. Aineisto saatavana osoitteessa: <https://www.sciencedirect.com/neli.laurea.fi/science/article/pii/S1383762120301600/pdf?md5=4cee275cad054581ac045b0befb4b158&pid=1-s2.0-S1383762120301600-main.pdf>

Okamoto, T. 2015. SecondDEP: Resilient Computing that Prevents Shellcode Execution in Cyber-Attacks. Procedia Computer Science. Viitattu 8.11.2020. Aineisto saatavana osoitteessa: <https://www.sciencedirect.com/science/article/pii/S1877050915023388>

Oxford Economics 2015. Digital Megatrends 2015 - The Role of Technology in the New Normal Market. Viitattu 15.8.2020. Aineisto saatavilla osoitteessa: https://www.oxford-economics.com/Media/Default/Thought%20Leadership/advisory-panels/Digital_Megatrends.pdf

Park, J., Kim, S. 2015. Study on Strengthening Plan of Safety Network CCTV Monitoring by Steganography and User Authentication. Advances in Multimedia. Viitattu 8.11.2020. Aineisto saatavana osoitteessa: <https://www.hindawi.com/journals/am/2015/960416/>

Poliisi 2020. Luettelo turvallisuusalan elinkeinoluvan haltijoista 13.11.2020. Viitattu 16.11.2020. https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/94640_Turvallisuusalan_elinkeinoluvat_13.11.2020_tau-lukko.pdf?b52d38a0b087d888

Puolustusministeriö 2015. Katakri 2015 -Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 16.10.2020. Aineisto saatavana osoitteessa: https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Rimpiläinen, T. 2020. Psykoterapiakeskus Vastaamon kiristäjä julkaisi yöllä lisää erittäin arkaluontoisia potilaskertomuksia. Viitattu 22.10.2020. Aineisto saatavana osoitteessa: <https://yle.fi/uutiset/3-11606925>

SFS 2018. Miniopas standardeista. Suomen Standardisoimisliitto SFS ry. Viitattu 16.8.2020. Aineisto saatavana osoitteessa: https://www.sfsedu.fi/files/345/miniopas_2018_web.pdf

Shekari, T. & Bayah, R. 2020. IoT Skimmer: Energy Market Manipulation through High-Wattage IoT Botnets. Esitelmä Black Hat 2020 -conferenssissa. Viitattu 15.8.2020. Aineisto saatavilla osoitteessa: <https://i.blackhat.com/USA-20/Wednesday/us-20-Shekari-IoT-Skimmer-Energy-Market-Manipulation-Through-High-Wattage-IoT-Botnets.pdf>

Sillanpää, M. 2019. Social engineering against security policyHow to infiltrate company's premises using social engineering? Viitattu 16.10.2020. Aineisto saatavilla osoitteessa: https://www.theseus.fi/bitstream/handle/10024/265555/sillanpaa_miika_thesis.pdf?sequence=2&isAllowed=y

Singh, M., Singh, M. & Kaur, S. 2018. Detecting bot-infected machines using DNS fingerprinting. Digital Investigation. Viitattu 7.11.2020. Aineisto saatavana osoitteessa: <https://www-sciencedirect-com.nelli.laurea.fi/science/article/pii/S174228761830272X>

Stamps, M. 2020. The Evolution of the Hacker. Techguard Security. Viitattu 15.8.2020. Aineisto saatavilla osoitteessa: <https://blog.techguard.com/the-evolution-of-the-hacker>

Stickley, J. 2011. Jim Stickley Demonstrates How to Bypass Home Alarms. Viitattu 23.10.2020. Aineisto saatavana osoitteessa: <https://www.youtube.com/watch?v=6bRWJVul2yM>.

Tobias, M. 2015. Simplisafe Bypass of Magnetic Trips. Viitattu 7.11.2020. Aineisto saatavana osoitteessa: <https://www.youtube.com/watch?v=9c1-t3QLs3k>

Traficom 2020. Traficomin organisaation 1.6.2020. Traficomin esittely internetissä. Viitattu 16.8.2020. Aineisto saatavilla osoitteessa: <https://www.traficom.fi/fi/traficom/tietoa-traficomista/organisaatio?toggle=Kyberturvallisuuskeskus%20>

Tulokas, J. 2018. Digitalisaatio edellyttää ennakoivaa tietoturvaa - reaktiivisuus ei enää riitä. F-Secure & Talouselämä. Viitattu 15.8.2020. Aineisto saatavilla osoitteessa: <https://www.talouselama.fi/kumppaniblogit/f-secure-oyj/digitalisaatio-edellyttaa-ennakoivaa-tietoturvaa-reaktiivisuus-ei-ena-riita/3d2c1d11-ad00-3f5b-8857-b7e37840df49>

Turva-alan yrittäjät ry 2020. Kameravalvontaopas. Viitattu 17.11.2020. Aineisto saatavana osoitteessa: <https://www.finanssiala.fi/vahingontorjunta/dokumentit/Kameravalvonta-opas.pdf>

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019. Viitattu 17.11.2020. <https://www.finlex.fi/fi/laki/alkup/2019/20191101>

Wickes, J. 2018. CCTV: an open door into enterprise and national infrastructure. ScienceDirect. Viitattu 23.10.2020. Aineisto saatavana osoitteessa: <https://www.sciencedirect.com/elli.laurea.fi/science/article/pii/S135348581830014X>

YLE 2020. "Kiina on kuin anakonda kattokruunussa" - kysimme tutkijalta ja turvallisuuspoliisilta kiistelyn kohteena olevasta Ruotsin 5G-päätöksestä. YLE 10.11.2020. Viitattu 10.11.2020. Aineisto saatavana osoitteessa: <https://yle.fi/uutiset/3-11640966>

Julkaisemattomat

Kalinen, R. 2020. Järjestelmäasiantuntijan haastattelu 18.9.2020. Suojelupoliisi. Helsinki.

Pänkäläinen, A. 2020. Turvallisuusasiantuntijan haastattelu 30.9.2020. Finanssiala ry. Helsinki.

Kuviot

Kuva 1: Hajautettu palvelunestohyökkäys.	17
Kuva 2: Intrusion Detection System.	18
Kuva 3: Intrusion Prevention System.	19
Kuva 4: Tietoturva vastaan käytettävyys.	22
Kuva 5: ROP-hyökkäysmenetelmä.	25
Kuva 6: Huolimaton asennus.	34
Kuva 7: Pääteemat.	39

Taulukot

Taulukko 1: Tilaturvallisuusjärjestelmien standardit.	37
--	----

Liite 1: Teemahaastattelun runko, Riku Kalinen

Kysymykset:

1. Millaiset hyökkäysmenetelmät tulevat kyseeseen tilaturvallisuusjärjestelmien tapauksessa?
2. Millainen rakenteellinen tai muu pääsy järjestelmään tarvitaan hyökkäyksen toteuttamiseen?
3. Mitä asioita tulisi ottaa huomioon hyökkäykseltä suojautumiseksi?
4. Millaisia resursseja ja osaamista hyökkäyksen toteuttaminen edellyttää?
5. Onko tiedossa tilaturvallisuusjärjestelmiin kohdistuneita kyberhyökkäyksiä Suomessa tai muualla? Onko tiedossa, kuka niiden takana on ollut? Voitko kertoa tapauksesta tarkemmin?
6. Jos hyökkäystä ei voi täysin estää, miten voi minimoida vahinkoja, jos halutaan varautua siihen, että hyökkäys tai tunkeutuminen järjestelmään tapahtuu joskus tulevaisuudessa?
7. Millaisia ohjelmointitekniikoita tulisi välttää tai suosia hyökkäyksiltä suojautumiseksi?
8. Nykyisin on myynnissä tilaturvallisuusjärjestelmien laitteita, joiden toiminnallisuutta voidaan muuttaa ostamalla laitteisiin uusia toimintoja ohjelmistomoduleina (esim. Axorin kamerat). Onko ohjelmiston muokausmahdollisuudessa riskejä tietoturvan näkökulmasta?
9. Joissakin tilaturvallisuusjärjestelmiinkin mahdollisesti kytkettävissä laitteissa voi olla valmistusteknisistä syistä sellaisia sensoreita, joita ei kyseisessä kaupallisessa tuotteessa hyödynnetä. Voiko ylimääräiset sensorit vaarantaa valvotun tilan tietoturvaa?
10. Markkinoilla on esimerkiksi valvontakameroita, jotka voidaan kytkeä suoraan internet-yhteyteen. Voidaanko tällaista kameratoteutusta pitää turallisena?

11. Mikä olisi oikea tapa toteuttaa turvallinen etäkäyttö tilaturvallisuusjärjestelmään?
12. Onko inhimillisillä tekijöillä tai käyttäjän toiminnalla merkitystä kyberhyökkäyksen näkökulmasta pitkälti automaattisesti toimivien tilaturvallisuusjärjestelmien tapauksessa?
13. Tilaturvallisuusjärjestelmiä käsittelevät standardit ottavat kantaa järjestelmien ja sensoreiden suunnitteluun, valmistukseen ja asentamiseen. Onko joku näistä vaiheista tietoturvan näkökulmasta kriittisempi kuin joku muu? Miksi? Mihin vaiheeseen itse kohdistaisit hyökkäyksen, jos tarkoitus olisi saada tietoja suojatun kohteen sisältä?
14. Nykyiset standardit käsittävät neljä tasoa, joista tiukin on ”korka riski”. Sen määritelmä on: ”Käytettävä kun turvallisuus on etusijalla yli kaikkien muiden tekijöiden. Murtautujalla tai ryöstäjällä oletetaan olevan kyky ja resurssit suunnitella murtautuminen tai ryöstö yksityiskohtaisesti ja omaavan täyden valikoiman laitteita, mukaan lukien keinot korvata keskeisiä murto- ja ryöstöilmaisujärjestelmän komponentteja”. Onko mielestäsi jotain sellaisia seikkoja, joita korkeimmalla turvatasolla tulisi huomioida, joita ei tyypillisesti voi kattaa standardoinnin keinoin? (Esimerkiksi laitteiden valmistajaan tai alkuperämaahan liittyen)
15. Mitä mieltä olet standardien vaatimuksista koskien ohjelmistojen ja tietoliikenteen turvallisuutta?
16. Mitä parannuksia standardeihin ehdottaisit?

Liite 2: Teemahaastattelun runko, Aku Pänkäläinen

Kysymykset:

1. Kertoisitko, kuinka tyypillinen tilaturvallisuusjärjestelmää käsittelevä standardi syntyy? Ketkä vaikuttavat sen sisältöön, kauanko prosessi kestää ja kuinka usein ja millaisista syistä standardeja päivitetään?
2. Kun tuodaan markkinoille uusi tilaturvallisuusjärjestelmä tai sen komponentti, minkälainen on vaadittu hyväksyntäprosessi? Kuinka paljon tämä prosessi maksaa yritykselle?
3. Kuinka usein tulee vastaan tilanteita, joissa hyväksyntäprosessi ei mene läpi? Millaisia ovat tyypilliset puutteet tai ongelmat?
4. Standardeissa luokitellaan tilaturvallisuusjärjestelmiä neljään eri tasoon. Mitkä ovat tyypilliset käyttötapaukset eri tasoille suojauksille? Mitkä ovat eri tasojen erot mielestänne tietoturvan näkökulmasta?
5. Onko olemassa käyttötapauksia, joihin luokitusjärjestelmä ei toimi tai sovi?
6. Viime aikoina on julkisuudessa esiintynyt keskustelut esimerkiksi tietyissä maissa valmistettujen teknologiatuotteiden tietoturvaominaisuuksista. Onko mielestänne tässä keskustelussa tuotu esiin jotain sellaista, joka pitäisi huomioida tilaturvallisuusjärjestelmien suhteen?
7. Voisiko mahdollisten esim. valmistusmaasta johtuvien riskien käsittelemiseksi standardeissa olla vielä korkeampi taso? Jos sellainen olisi, mitä lisä seikkoja se voisi edellyttää laitteilta, niiden komponenteilta tai ohjelmistolta?
8. Mitkä ominaisuudet ovat kriittisimmät tilaturvallisuusjärjestelmissä tietoturvan kannalta?
9. Onko tilaturvallisuusjärjestelmiä koskeviin standardeihin tiedossa muutoksia lähitulevaisuudessa? Jos ei, tuleeko mieleen minkä osa-alueen kehittämistä niissä tulisi priorisoida tai onko jossain selkeitä puutteita?
10. Onko tiedossanne sellaista tapausta, jossa tilaturvallisuusjärjestelmiin olisi tarkoituksellisesti jätetty tietoturvallisuudelle riskialttiita ominaisuuksia tai puutteita?
11. Standardit eivät rajoita ”ylimääräisten” komponenttien olemassaoloa. Tulisiko asia huomioida korkeimmalla tasolla?