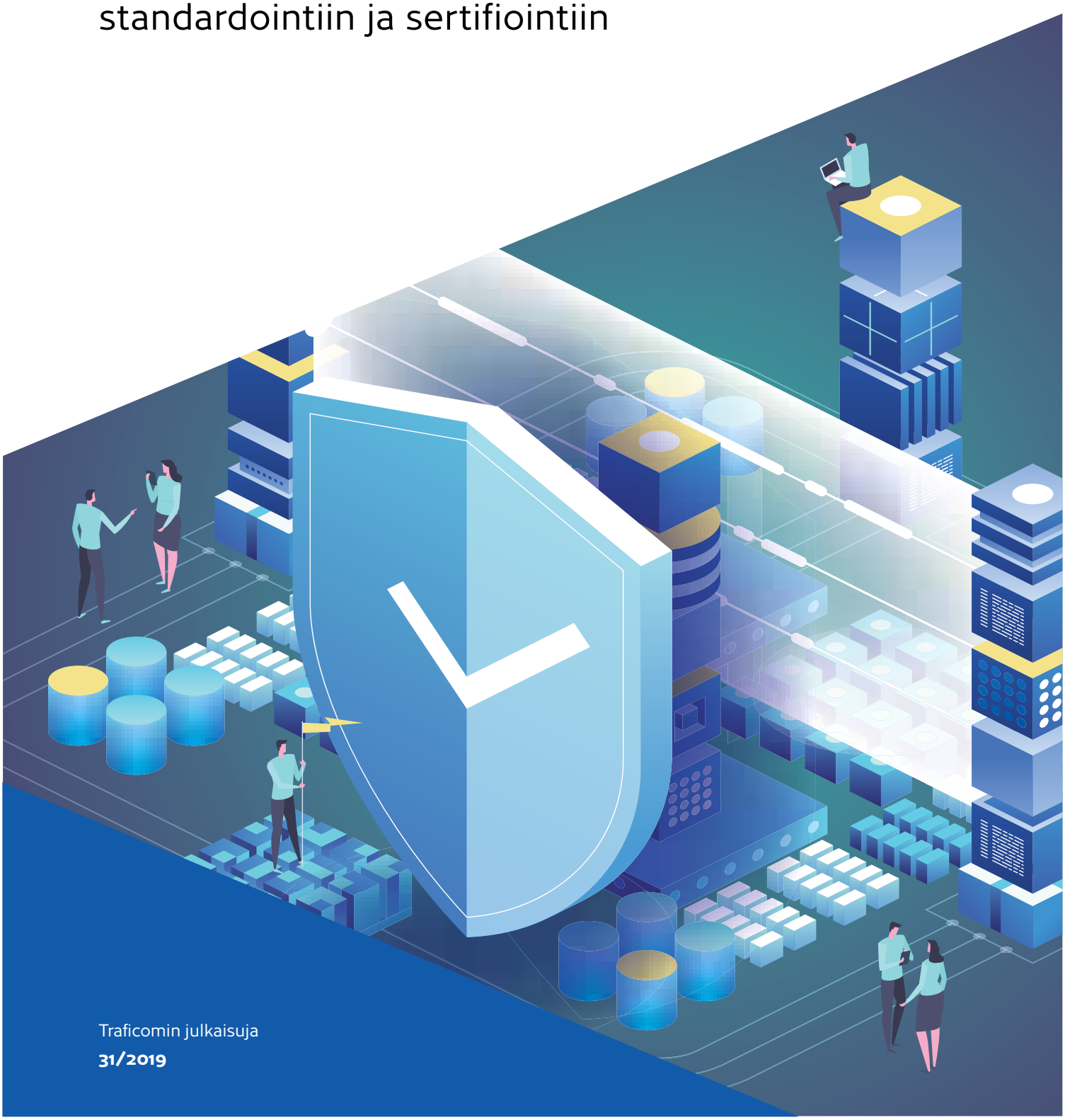
TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Luottamuksen lähteillä

Näkökulmia tietoturvan standardointiin ja sertifiointiin



Traficomin julkaisuja
31/2019

Sisältö

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
ISBN 978-952-311-354-1
31/2019

Tiivistelmä

Tässä raportissa kuvataan tietoturvallisuuden standardoinnin ja sertifioinnin nykytilaa ja tulevaisuudennäkymiä Suomen näkökulmasta. Lisäksi tarkastellaan niihin vaikuttavia tekijöitä ja käydään läpi eri toimijaryhmien näkemyksiä sekä kokemuksia aihepiiristä.

Liiketoiminta ja yhteiskunnan toiminnot tapahtuvat yhä useammin verkossa. Maailmanlaajuinen, reaaliaikainen toiminta vaatii uusia keinoja toimijoiden välisen luottamuksen rakentamiseen. Tarpeeseen vastataan muun muassa standardoinnilla, jonka avulla kehitetään toiminnan laatua, turvallisuutta ja läpinäkyvyyttä. Standardoinnin vaikutusta on mahdollista tehostaa sertifioinnilla, joka kertoo siitä, että standardissa asetetut vaatimukset täyttyvät.

Standardoinnin vaikuttavuuden kannalta keskeisessä asemassa ovat standardien kansainvälisyys, standardointiprosessin avoimuus, nopeus, ennustettavuus, joustavuus ja standardoinnin kohde. Myös saatavuus vaikuttaa standardien käytön laajuuteen ja vaikuttavuuteen. Sertifioinneilla ja auditoinneilla valvotaan vaatimusten toteutumista ja luodaan luottamusta. Auditointien laadun varmistamisessa tärkeää on myös akkreditointi eli auditointeja tekevien tahojen pätevyyden toteaminen.

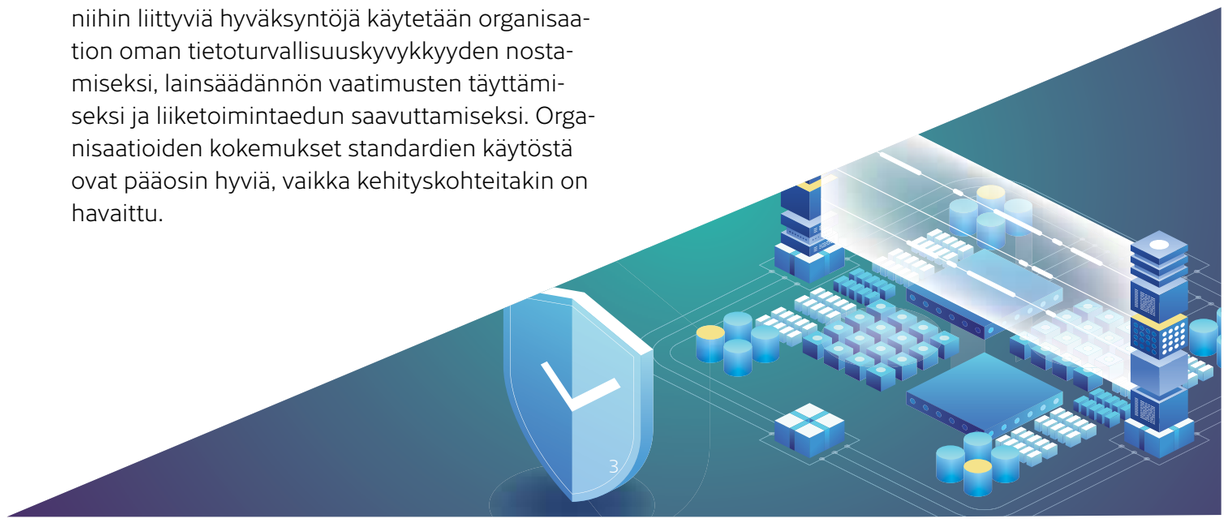
Suomessa tietoturvallisuuden standardeja ja niihin liittyviä hyväksyntöjä käytetään organisaation oman tietoturvallisuuskyvykkyyden nostamiseksi, lainsäädännön vaatimusten täyttämiseksi ja liiketoimintaedun saavuttamiseksi. Organisaatioiden kokemukset standardien käytöstä ovat pääosin hyviä, vaikka kehityskohteitakin on havaittu.

Sertifiointien hyödyntämisessä suurimpia haasteita ovat kustannukset, prosessin kesto ja sertifioinnin perusteena käytettävien vaatimusten yhdenmukainen tulkinta.

Tietoturvallisuusvaatimusten sertifiointien määrä kasvaa selvästi, mutta toistaiseksi maltillisesti. Myös kansallisten viranomaishyväksyntöjen kysyntä on niin voimakasta, että siihen ei pystytä nykyisillä resursseilla vastaamaan aina kohtuullisessa ajassa. Kesäkuussa 2019 voimaan astunut EU:n Kyberturvallisuusasetus tulee todennäköisesti kasvattamaan sertifiointien kysyntää ja käyttöä Euroopassa entisestään.

Sertifiointitoiminnan kasvaviin resurssitarpeisiin tulee varautua hyvissä ajoin. Korkea koulutustaso ja vakaa tietoturvallisuusosaaminen antavat hyvät mahdollisuudet olla edelläkävijä sertifiointitoiminnassa ja maailmanlaajuisen luottamuksen rakentamisessa.

Vuonna 2019 Liikenne ja viestintäviraston Kyberturvallisuuskeskus julkaisi Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) ja Tietoturvamerkin IoT-kuluttajalaitteille. Molemmissa julkaisuissa annetaan ohjeita tietoturvallisten laitteiden hankintaan ja niiden käyttöön. Ohjeistuksessa olemme huomioineet kansainväliset standardit, jotta globaali yhteentoimivuus voitaisiin saavuttaa mahdollisimman hyvin.



Johdanto

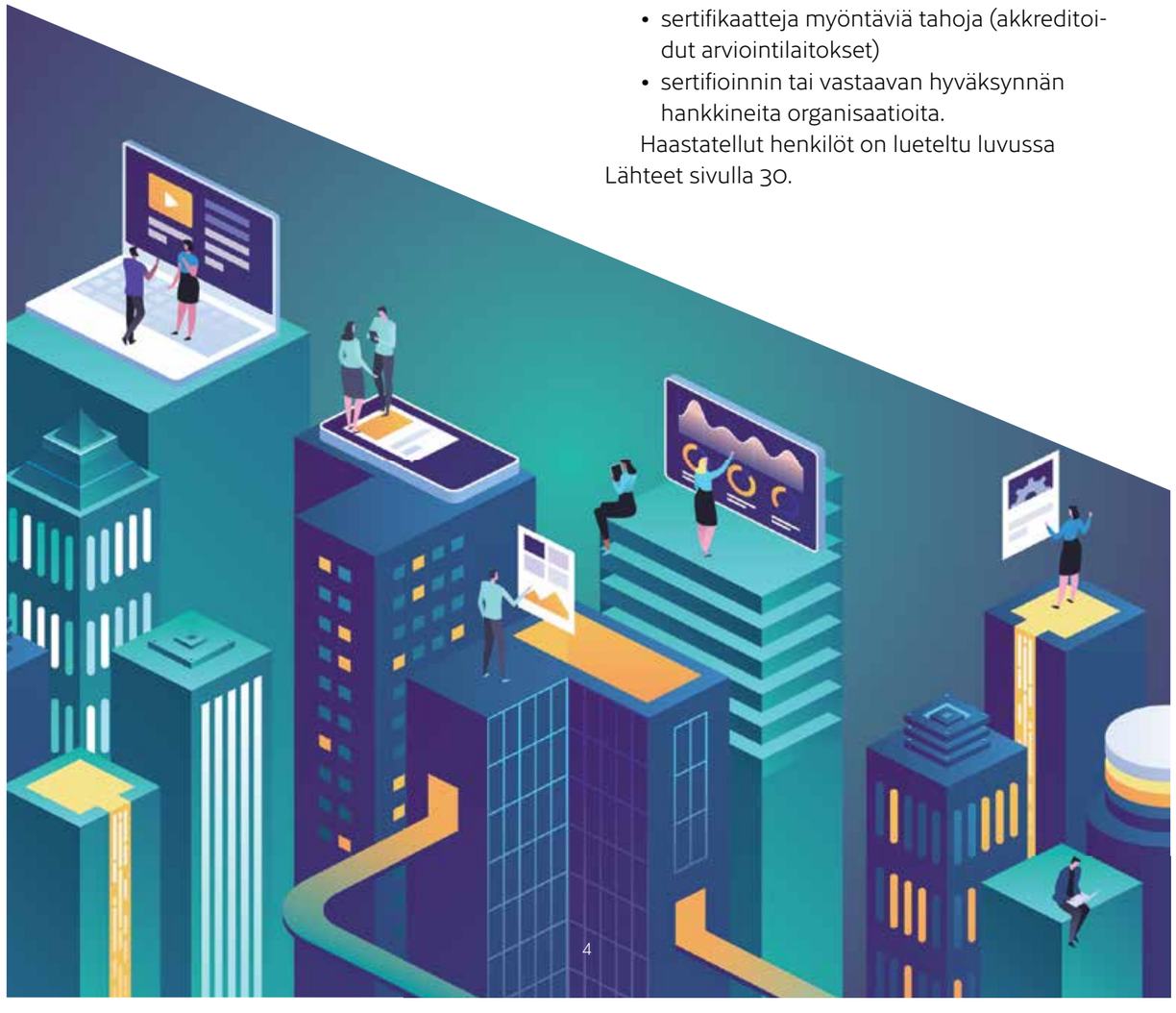
Raportissa kuvataan, kuinka tietoturvallisuus vaikuttaa luottamuksen syntymiseen ja säilyttämiseen muuttuvassa digitaalisessa toimintaympäristössä. Raportti viestii ICT-alan laite- ja palveluntuottajille sekä niiden asiakkaille tietoturvasertifiointien ja -standardoinnin merkityksellisyydestä. Lisäksi tavoitteena on lisätä tietoisuutta tietoturvasertifiointien käyttömahdollisuuksista ja edistää tarpeellisten sertifikaattien käyttöönottoa.

Seuraavissa luvuissa kuvataan aihepiiriin liittyviä taustoja, kehityskulkuja sekä vaihtoehtoisten sertifiointi- ja merkintätapojen hyötyjä ja haasteita. Raportti on kirjoitettu erityisesti organisaation johdon näkökulmasta.

Raportissa esitetyt seikat perustuvat kirjallisiin lähteisiin sekä haastatteluihin, joihin on osallistunut

- kansallisia sertifioitavia standardeja tai standardinkaltaisia ohjekokonaisuuksia laativia työryhmiä
- standardointiin osallistuvia organisaatioita
- sertifikaatteja myöntäviä tahoja (akkreditoidut arviointilaitokset)
- sertifioinnin tai vastaavan hyväksynnän hankkineita organisaatioita.

Haastatellut henkilöt on lueteltu luvussa Lähteet sivulla 30.



I OSA

1 Luottamuksen merkitys digitaalisessa liiketoimintaympäristössä

Tieto- ja viestintätekniikasta on tullut viime vuosikymmeninä kiinteä osa suomalaista yhteiskuntaa ja ihmisten arkea. Tekniikkaa sovelletaan jatkuvasti uusiin käyttökohteisiin, ja tietoa kerätään ja käsitellään tietoverkoissa valtavia määriä. Tämä edellyttää jatkuvaa luottamusta uusiin teknologioihin: tunnetta siitä, että teknologiaan voi luottaa ja että se ei aiheuta pettymystä. Luottamukseen kuuluu myös turvallisuudentunne. Kerran menetetyn luottamuksen palauttaminen on vaikeaa, minkä vuoksi pettymyksiä tulee välttää.

1.1 Digitaalinen luottamus

Luottamuksen rakentaminen ja ylläpitäminen digitaalisessa maailmassa poikkeavat monin tavoin totutusta: toiminnan eri osapuolet voivat olla toisilleen tuntemattomia ja eri kulttuureista. He voivat toimia eri puolilla maailmaa ja tieto voi silti liikkua reaaliajassa, osapuolten havaintokyvyn ulottumattomissa. Lisäksi toimijoiden määrä, toiminnan volyymi ja nopeus ovat digitaalisessa maailmassa poikkeuksellisen suuria. Omakohtainen kohteen havainnointi ja siihen tutustuminen on mahdotonta digitaalisessa maailmassa, jossa luottamus on reaalimaailmaa monimuotoisempi ja mukautuvampi käsite.

Luottamusta digitaaliseen maailmaan voidaan edistää esimerkiksi standardoinnilla ja sertifikaateilla, toisin sanoen muodostamalla yhteiset ja yleisesti tunnistetut käytännöt ja valvomalla niiden noudattamista.

1.2 Tietosuojan merkitys korostuu

Tieto- ja viestintäteknologian tietoturvallisuuden taso vaikuttaa sekä organisaatioiden että yksittäisten käyttäjien tietosuojaan ja turvallisuuteen. Näin teknologian tietoturvapuutteet vaikuttavat yhä henkilökohtaisemmalla tasolla. Samalla tietoturvallisuuden yhteys käyttäjien kokemaan luottamukseen on kasvanut. Käyttäjien kyky hallita ja ymmärtää tietoturvallisuutta ei ole kuitenkaan kasvanut vastaavasti. Sen vuoksi tarvitaan menetelmiä ja osaamista, jotka suojaavat käyttäjää ja ylläpitävät luottamusta digitaalisiin palveluihin, mikä on edellytys digitalisoituvan yhteiskunnan toiminnalle.

Kun teknologian käyttöön liittyvä osaaminen jakautuu epätasaisesti, mutta vaikutukset ovat merkittäviä ja koskettavat kaikkia, standardoinnin käyttö on erityisen perusteltua. Näin on tehty jo pitkään lähes kaikilla turvallisuuskriittisillä aloilla. Yleisesti ottaen voidaankin todeta, että mitä kriittisempää on toiminta ja tieto, johon teknologian käyttö liittyy, sitä tärkeämpää on huolehtia tiedon käsittelystä siten, että turvallisuus ja luottamus osapuolten välillä säilyvät.

1.3 Vaikutukset liiketoimintaan

Tietoturvallisuusuhat ovat lisääntyneet viime vuosina. Kiristysohjelmahyökkäykset ovat Euroopan komission mukaan kolminkertaistuneet vuosina 2015–2017. Tietoturvahyökkäysten arvioidaan maksavan vuosittain maailmantaloudelle 400 miljardia euroa. Tietoturvatietoisuus on lisääntynyt tapahtuneiden tietoturvaloukkausten myötä, joskaan ei Euroopan komission mukaan riittävästi: 69 % yrityksistä ei tiedosta riittävästi tai lainkaan altistumistaan tietoturvariskeille.

On ennustettu, että vuoteen 2020 mennessä organisaatiot, jotka toimivat aktiivisesti edistääkseen digitaalista luottamusta, osallistuvat 20 % todennäköisemmin digitaalisiin ekosysteemeihin ja houkuttelevat 40 % enemmän käyttäjiä kuin ne, jotka eivät (Gartner, 2017). Tämän vuoksi on kansallisesti ensiarvoisen tärkeää, että suomalaisyritykset ja -organisaatiot toimivat tietoturvallisesti ja myös viestivät siitä sidosryhmilleen.

2 Tietoturvallisuus ja tietoturvastandardit luottamuksen rakentamisessa

Yritykset ja julkinen hallinto käyttävät yhä enemmän digitaalisia verkkoja ja infrastruktuureja keskeisten palvelujensa tarjoamisessa. Siksi tieto- ja viestintäjärjestelmien toimivuudella on valtava vaikutus paitsi organisaatioiden myös yhteiskunnan toimintaan. Turvallisuushäiriöt heikentävät toimintavarmuutta ja kuluttajien luottamusta esimerkiksi verkkomaksujärjestelmiin sekä tieto- ja viestintäverkkoihin.

Tietoturvallisuuden standardoinnilla luodaan yhtenäiset toimintatavat ja tekniikat sähköiseen tietojen vaihtoon ja käsittelyyn. Tämä lisää parhaiden ratkaisujen käyttöä ja samalla laatua, yhteentoimivuutta ja turvallisuutta. Luottamuksen edistämisessä näistä korostuu erityisesti turvallisuus, se miten rakennetaan ja hallitaan turvallisia laitteita ja palveluita. Tärkeää on myös toteutusten läpinäkyvyys eli se, että vaatimukset ovat avoimesti saatavilla ja että niiden täyttyminen voidaan todentaa.

Tietoturvatekniikoiden avulla voidaan varmistaa, ettei tietojärjestelmissä olevia tietoja muuteta ilman valtuuksia ja että tiedot suojataan asiattomalta käytöltä. Keskeisiä standardointikohteita ovat esimerkiksi

- tietoturvallisuuden hallintajärjestelmät
- tietosuoja
- salaustekniikat
- pääsynvalvonta
- digitaalinen allekirjoitus.

Yhdessä ne auttavat rakentamaan luottamusta koko digitaalisen yhteiskunnan toimintaan.

Raporttia varten haastateltujen asiantuntijoiden mukaan on nähtävissä suuntaus, jossa lisääntyneet tietoturvavaatimukset muuttavat organisaatioiden toimintaa. Esimerkiksi Payment Card Industry Data Security Standard (PCI DSS) -standardin vuoksi moni kaupan alan toimija on luopunut maksukorttitiedon käsittelystä ja ulkoistanut sen maksupalveluntarjoajalle. Näin on vältetty huomattava määrä PCI DSS -standardin teknisiä vaatimuksia, vaikka itse standardia kauppiaat joutuvatkin noudattamaan. Sama ilmiö on nähtävillä myös kansallisten turvallisuusluokiteltujen tietojen käsittelyssä: osa organisaatioista ei halua käsitellä niitä itse vaan ulkoistaa käsittelyn.

Maailma monimutkaistuessa syntyy yhä suurempia tietoturvallisuusuhkia. Esineiden internet (Internet of Things, IoT,) on jo todellisuutta ja arvioiden mukaan vuoteen 2020 mennessä siihen on kytkettynä kymmeniä miljardeja laitteita yksin EU:ssa. IoT:n turvallisuusvaatimusten määrä kasvaa ja tietoturvallisuuden hallinta monimutkaistuu. Näin myös tietoturvallisuuden sertifioinnissa käytettävien standardien ja ohjeistusten käyttö jatkaa kasvuaan.

3 Tietoturvavaatimusten standardointi

Tietoturvallisuutta standardoidaan lukuisissa organisaatioissa monilla eri toimialoilla sekä eurooppalaisella että kansainvälisellä tasolla. Ilmiö kertoo osaltaan siitä, että tieto- ja viestintäteknologia on kietoutunut lähes kaikkiin yhteiskunnan toimintoihin. Kokonaisuuksien hallitseminen on haastavaa, mutta samalla oleellista, päällekkäisten, toistensa kanssa kilpailevien standardien välttämiseksi.

Standardien laatija ja standardointiprosessi vaikuttavat standardien tasapuolisuuteen, saatavuuteen, laatuun ja läpinäkyvyyteen sekä siihen, kuinka niitä käytetään. Seuraavassa tarkastellaan näitä tekijöitä tietoturvallisuusvaatimusten, toisin sanoen tietoturvallisuuden sertifiointiin käytettävien standardien näkökulmasta. Lisäksi esitellään lyhyesti standardointiorganisaatioiden tunnetuimpia tietoturvallisuuden vaatimusstandardeja, joita käsitellään tarkemmin selvityksen osassa II Käytännön kokemuksia.

3.1 Virallinen standardointi

Virallisella standardoinnilla tarkoitetaan kansainvälisiä, eurooppalaisia ja kansallisia standardointiorganisaatioita, joiden jäsenyys on maakohtaista. Standardointiorganisaatiot on jokaisella maantieteellisellä tasolla jaettu sähkön, televiestinnän ja yleiseen standardointiin (ks. taulukko 1). Suomessa standardoinnista vastaavat SESKO, Liikenne- ja viestintävirasto sekä Suomen Standardisoimisliitto SFS toimialayhteisöineen.

	Sähköala	**Yleinen standardointi**	**Teleala**
Maailmanlaajuinen taso	IEC International Electrotechnical Commission	ISO International Organization for Standardization	ITU International Telecommunication Union
Eurooppalainen taso	CENELEC European Committee for Electrotechnical Standardization	CEN European Committee for Standardization	ETSI European Telecommunications Standards Institute
Kansallinen taso	SESKO	SFS Suomen Standardisoimisliitto SFS toimialayhteisöineen	Liikenne- ja viestintävirasto

Viralliset standardointiorganisaatiot ovat vakiintuneita ja tunnettuja. Niiden tapa toimia yhdistämällä kansainvälisten toimijoiden näkemykset on läpinäkyvä ja laajasti hyväksytty, minkä ansiosta organisaatioihin luotetaan. Lisäksi lainsäädännössä voidaan viitata vaatimusten täyttämisen yhteydessä ainoastaan virallisiin standardeihin.

ESIMERKKI:
ISO/IEC 27001 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.
Tietoturvallisuuteen liittyviä virallisia vaatimusstandardeja on oikeastaan vain yksi: Tietoturvan hallintajärjestelmästandardi ISO/IEC 27001. Se on kansainvälisesti yksi tunnetuimmista ja käytetyimmistä organisaation tietoturvallisuuden hallinnan standardeista. Standardin laatimiseen on osallistunut peräti 25 ISOn jäsenvaltiota, ja sitä käytetään maailmanlaajuisesti laajasti sekä julkisella että yksityisellä sektorilla. Standardi koostuu perusosasta sekä esimerkkikontrollit sisältävästä liitteestä A.

3.2 Kaupallinen konsortio- ja teollisuusstandardointi

Standardeja voidaan tehdä myös teollisuudenalan tai kaupallisten toimijoiden yhteenliittymissä, kun tavoitellaan nopeutettua menettelyä. Standardoinnilla tavoitellaan tällöin tyypillisesti markkinaetua standardointiin osallistuville yrityksille. Tällaista menettelyä voidaan käyttää esimerkiksi nopeasti kehittyvällä teknisellä alalla, koska laajemman yhteisen näkemyksen muodostamisen vaativa aika merkitsisi markkinoille pääsyn viivästymistä.

3.3 Muu standardointi

Standardointityötä tehdään myös monissa voittoa tavoittelemattomissa organisaatioissa. Työskentelyyn osallistuminen on avointa kaikille, jotka ovat kiinnostuneita alan kehityksestä ja aihe liittyy esimerkiksi omiin työtehtäviin. Tällä periaatteella toimivia tietoturvallisuutta standardoivia organisaatioita ovat esimerkiksi tässäkin selvityksessä esimerkkinä käytetty Cloud Security Alliance (CSA), Open Web Application Security Project (OWASP) ja Internet Engineering Task Force (IETF).

ESIMERKKI:
Pilvipalvelutarjoajan sertifiointi CSA STAR.
CSA STAR on pilvipalveluntarjoajille kehitetty kansainvälisesti tunnustettu sertifiointi, joka perustuu amerikkalaisen Cloud Security Alliancen kehittämään Cloud Controls Matrixiin. Suomessa CSA STAR -sertifiointiauditointeja tarjoaa Nixu Certification Oy. Vaatimusmatriisi ja lista sertifioiduista toimijoista ovat Cloud Security Alliancen verkkosivuilla vapaasti saatavissa.

3.4 Julkishallinnon ohjekokonaisuudet tietoturvalainsäädännön tueksi

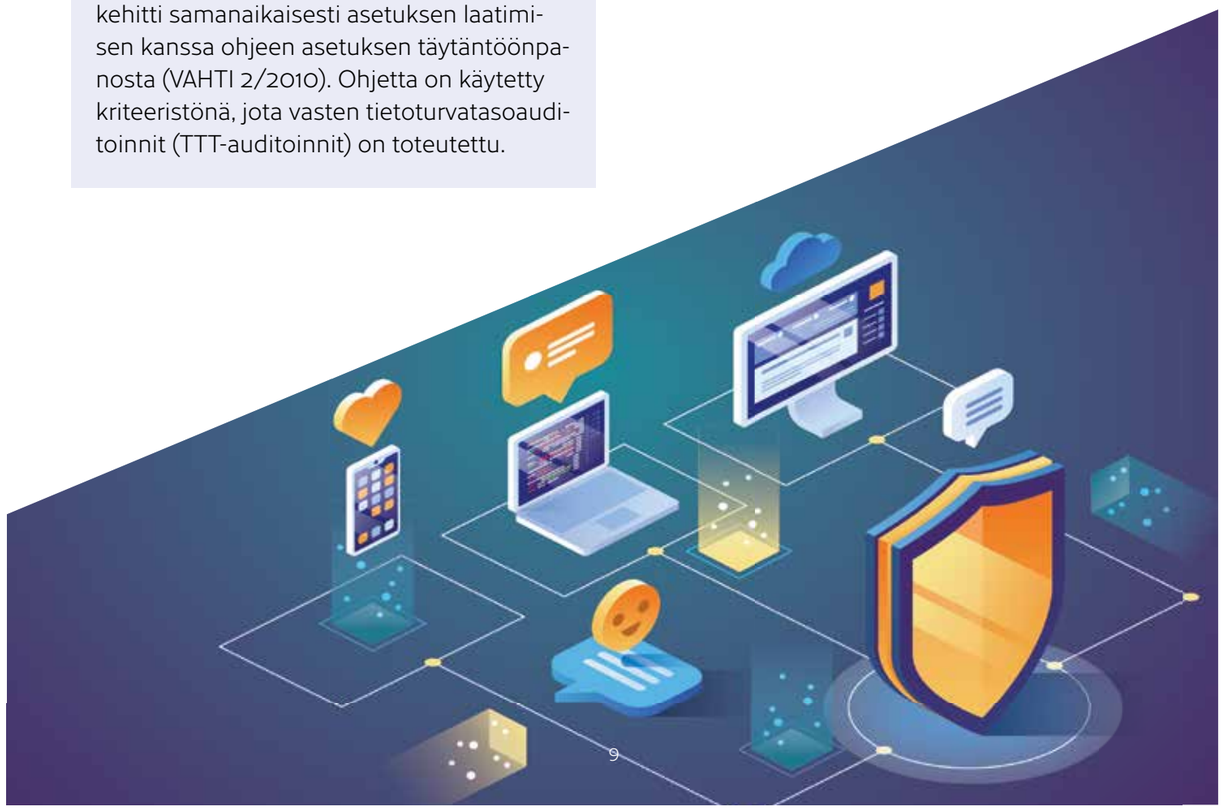
Tässä raportissa standardeiksi tulkitaan myös kansalliset, lainsäädäntöä tulkitsevat ohjekokonaisuudet, jotka ovat saavuttaneet standardinomaisen aseman. Näistä tunnetuimpia ovat valtiovarainministeriön julkishallinnon digitaalisen turvallisuuden ohjausryhmä VAHTIn antamat ohjeistukset ja tietoturvallisuuden auditointityökalu Katakri. Seuraavassa esitellään nämä ohjekokonaisuudet lyhyesti.

VAHTI-ohjeet
Valtiovarainministeriöllä on lakiin kirjattu tehtävä ohjata julkishallinnon tietoturvallisuutta, mutta sen alaisen VAHTIn luomilla tietoturvalainsäädäntöä tulkitsevilla ohjeistuksilla itsessään ei ole lakiin perustuvaa asemaa. Käytännössä ohjeistukset ovat kuitenkin muodostuneet de facto -tulkinnaksi lainsäädännöstä. Vaikka ohjeet itsessään eivät velvoita, lainsäädäntö johon ne perustuvat kylläkin.

Aikaisemmin VAHTI-ohjeet koskivat ensisijaisesti ainoastaan valtionhallintoa, mutta lainsäädäntöuudistuksen ja keväällä 2019 hyväksytyn tiedonhallintalain myötä vaatimukset ulottuvat koko julkishallintoon. Jo ennen tätä VAHTI-ohjeita on sovellettu vapaaehtoisesti myös osassa kuntia.

ESIMERKKI:
VAHTI 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta.
Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010 astui voimaan 1.10.2010. Se velvoittaa viranomaiset saattamaan toimintansa ja tietojenkäsittelynsä vastaamaan asetuksessa säädettyjä perustason tietoturvavaatimuksia.
Valtiovarainministeriön asiantuntijaryhmä kehitti samanaikaisesti asetuksen laatimisen kanssa ohjeen asetuksen täytäntöönpanosta (VAHTI 2/2010). Ohjetta on käytetty kriteeristönä, jota vasten tietoturvatasoauditoinnit (TTT-auditoinnit) on toteutettu.

ESIMERKKI:
Katakri 2015 Tietoturvallisuuden auditointityökalu viranomaisille.
Katakri 2015 on kolmas versio viranomaisten auditointityökalusta, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Katakriin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvien vähimmäisvaatimusten auditointikriteerit.
Katakri ei aseta tietoturvallisuuden toteutukselle vaatimuksia, vaan siihen kootut auditointikriteerit perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin.



4 Standardointiin ja standardeihin vaikuttavia tekijöitä

Standardointiprosessin piirteet vaikuttavat monin eri tavoin sen tuloksena syntyvään standardiin ja sen vaikuttavuuteen. Seuraavassa on kuvattu ja vertailtu lyhyesti standardointiprosesseja ja vertailtu niitä erilaisiin standardointitapoihin.

4.1 Standardointiprosessin avoimuus

Mahdollisuus osallistua standardointiprosessiin, toisin sanoen standardoinnin avoimuus, vaikuttaa suoraan siihen, kenen tarpeita valmiit standardit vastaavat.

Virallisten standardien kehittäminen on kaikille avointa ja laadinta perustuu konsensuksen hakemiseen määrämuotoista prosessia noudattaen. Tämä lisää läpinäkyvyyttä ja tasapuolisuutta. Myös standardien ajantasaisuutta ylläpidetään vakiintuneilla käytännöillä. Kansainväliseen standardisointityöhön osallistuu asiantuntijoita teollisuudesta, arviointilaitoksista ja tutkimuslaitoksista. Näin kuulluiksi tulevat vaatimusten asettajien, käyttäjien ja arvioijien äänet.

Kansalliset lainsäädäntöä tulkitsevat ohjeet, muun muassa VAHTIn julkaisut, laaditaan pääosin julkishallinnon organisaatioiden kesken. Yksityinen sektori ei näin pääse suoraan vaikuttamaan vaatimusten laadintaan tai tulkintaan, vaikka sitä saatetaan prosessin aikana kuullakin. Erityisesti arviointilaitokset toivovat mahdollisuutta osallistua julkishallinnon ohjekokonaisuuksien kehittämiseen, sillä julkishallinnon tietoturva-arviointeja tekevät yksityiset arviointilaitokset joutuvat työssään tulkitsemaan lainsäädännön vaatimuksia. Yleisesti voidaan todeta, että vaatimuksia toteuttavien ja tulkitsevien tahojen olisi hyvä osallistua vaatimusten laatimiseen. Siten tietoturvatoteutuksista saadaan mahdollisimman yhdenmukaisia ja ohjeiden kokonaisvaikuttavuus kasvaa.

Muiden kuin virallisten standardointiorganisaatioiden prosessien avoimuus vaihtelee suuresti. Konsortiostandardoinnilla voidaan esimerkiksi pyrkiä suppean joukon kaupallisen edun ajamiseen, jolloin prosessiin osallistuminen voi tarkoituksellisesti olla mahdotonta tai edellyttää suuria rahallisia investointeja. Tällainen standardointi korostaa suuryritysten vaikutusmahdollisuuksia ja heikentää samalla pienten yritysten kilpailukykyä.

Avoin standardointiprosessi edistää tasapuolisuutta, läpinäkyvyyttä ja vaatimusten tulkinnan yhdenmukaisuutta. Suljettua prosessia todennäköisemmin se myös johtaa laajaan yhteentoimivuuteen ja parantaa valmiin standardin laatua.

4.2 Standardointiprosessin nopeus

Prosessin nopeus vaikuttaa siihen, kuinka nopeasti standardointitarpeeseen pystytään vastaamaan ja kuinka laajasti ratkaisu otetaan käyttöön.

Standardoinnin on vaikeaa vastata teknisen alan tarpeisiin tehokkaasti, koska virallinen prosessi on hidas, mutta tietoturvallisuusteollisuuden kehitys nopeaa. Kansainvälisessä standardoinnissa osallistujien kansalliset erityistarpeet ovat usein ristiriidassa ja myös maanosilla on keskenään kilpailevia pyrkimyksiä. Niiden yhteensovittaminen vie aikaa, mikä pahimmillaan estää standardin syntymisen.

Epämuodollisempi ja suppeamman osallistujajoukon standardointiprosessi on usein merkittävästi nopeampi ja joustavampi toimintatapa. Tämän vuoksi erityisesti monet virallisen standardin aseman saavuttaneet tekniset standardit on tehty alun perin muissa standardointiorganisaatioissa ja myöhemmin vahvistettu erillisellä menettelyllä, jossa virallisen standardoinnin jäsenmaat pääsevät vaikuttamaan hyväksyntään.

Virallinen menettely soveltuu parhaiten sellaisten hallintajärjestelmästandardien kehittämiseen, jotka eivät sisällä muutoksille alttiita teknisiä ratkaisuja. Monet kansainvälisesti tunnetuimmista hallintajärjestelmien vaatimusstandardeista, kuten yleinen laadunhallintastandardi ISO 9001, ovatkin ISOn laatimia.

Teknologiamurroksen vaikutus standardointiin näkyy ennen kaikkea paineena nopeuttaa prosessia. Hidas prosessi sopii huonosti nopeasti kehittyviin ja leviäviin teknologioihin. Erilaisten standardointitapojen parhaita puolia pyritäänkin nyt yhdistämään virallisen standardoinnin kehittämiseksi ja nopeuttamiseksi.

4.3 Standardointiprosessin määrämuotoisuus - standardien ylläpito ja päivittäminen

Standardien kehityksen ja elinkaaren ennustettavuus vaikuttavat niiden käyttöön. Ennalta määritellyt ja määrämuotoiset prosessit voivat sitouttaa käyttäjäorganisaatiot standardeihin ja niihin liittyviin mittaviinkin investointeihin. Sen sijaan yllättävät muutokset tai standardien hylkääminen voivat haitata merkittävästi yrityksen liiketoimintaa. Virallinen standardointi tarkasti määriteltyine prosesseineen ja pysyvine organisaatioineen on vaihtoehdoista selkeästi vakain ja ennustettavin instrumentti.

4.4 Standardien saatavuus

Standardien saatavuus vaikuttaa mahdollisuuteen arvioida vaatimuksia sekä hyödyntää niitä omassa toiminnassa. Avoimesti saatavilla olevat standardit lisäävät läpinäkyvyyttä, tasapuolisuutta ja toimijoiden välistä luottamusta. Avoimet vaatimukset antavat myös mahdollisuuden arvioida standardin mukaisten toteutusten laatua.

Viralliset standardit ovat kenen tahansa hankittavissa. Telealan organisaatioita lukuun ottamatta standardit ovat pääsääntöisesti maksullisia. Yksittäisen standardin hinta ei välttämättä ole yritykselle tai organisaatiolle merkittävä toisin kuin pienelle toimijalle, oppilaitokselle tai yksittäiselle kuluttajalle. Maksullista standardia ei myöskään voi arvioida ennen hankintaa, minkä vuoksi sen soveltumista käyttötarkoitukseen ei voi ennakkoon tietää. Lisäksi huomattavan laaja standardointikatalogi vaikeuttaa tarpeeseen sopivien standardien löytämistä.

Virallisten standardien myynnillä ei tavoitella voittoa, vaan tuloilla rahoitetaan standardointiorganisaatioiden toimintaa. Käytännön avulla standardien kehittämistyöhön osallistuminen on maksutonta ja avointa, mikä edistää tasapuolisuutta ja standardin laajaa käyttöönottoa.

Suomen Standardisoimisliitto SFS on halunnut edistää maksullisten virallisten standardien käyttöä verkkopalvelulla, joka tarjoaa räätälöidyn sähköisen standardivalikoiman yksittäisten standardien ostamista edullisemmin. Samoin verkkokaupassa on mahdollista muun muassa esikatsella standardin sisällysluetteloa ja soveltamisalaa.

Esimerkiksi telealalla standardien käyttö on lisääntynyt merkittävästi maksullisuuden poistumisen jälkeen. Näistä edistysaskelista huolimatta maksullisuus on edelleen merkittävä hidaste standardien käytölle.

4.5 Standardoinnin kohteet

Standardointia voidaan soveltaa tuotteisiin, palveluihin, prosesseihin ja hallintajärjestelmiin, lähes mihin tahansa. Vaikka tavoitteena on aina parantaa laatua, yhteentoimivuutta ja turvallisuutta, standardoinnin kohde vaikuttaa standardointiprosessiin ja kohteelle asetettaviin vaatimuksiin. Seuraavaksi tarkastellaan erityisesti tietoturvallisuuden näkökulmasta keskeisiä vaatimustyyppejä.

Hallintajärjestelmävaatimukset
Hallintajärjestelmävaatimukset kohdistuvat johtamiseen menettelytapoineen. Hyvää hallintajärjestelmävaatimusta voidaan soveltaa ja käyttää eri toimialoilla ja eri kokoisissa organisaatioissa.

Menetelmästandardoinnissa sovelletaan tapauskohtaista riskien arviointia ja harkintaa, mikä vaikeuttaa vaatimusten yhtenäistä soveltamista ja tulkintaa. Kansallisessa ympäristössä on havaittu, että tulkinnan mahdollisuus johtaa helposti epäyhtenäisiin käytäntöihin ja siten toimijoiden välisen luottamuksen rapautumiseen. Tämän vuoksi tulkintojen yhtenäistämiseen tulisi kiinnittää erityistä huomiota.

Tuote- ja järjestelmävaatimukset
Tuote- ja järjestelmävaatimukset ovat usein luonteeltaan hallintajärjestelmävaatimuksia yksityiskohtaisempia ja tiukempia. Tuotteen ja järjestelmän hyvä tietoturvavaatimus on selkeä, yksiselitteinen, terminologialtaan eheä ja looginen. Tällaisten vaatimusten testaaminen perustuu usein tarkastukseen, joka ei edellytä vaatimusten tapauskohtaista tulkintaa.

Prosessivaatimukset
Myös prosesseja voidaan standardoida ja sertifioida. Tällöin pyritään vaikuttamaan lopputuotteen sijaan toiminnan laatuun ja vasta välillisesti lopputulokseen. Erityisesti henkilötietojen käsittelyprosessien sertifiointi on herättänyt kiinnostusta EU:n tietosuoja-asetuksen voimaantulon myötä.

4.6 Standardointiprosessiin osallistumisen hyödyt

Monet yritykset ja julkisyhteisöt osallistuvat standardointityöhön sekä luonnosten kommentointiin eri työryhmissä. Jos organisaatio on mukana uuden standardin luonnissa, se saa siitä kilpailuetua: Se voi vaikuttaa standardin lopulliseen sisältöön ja ymmärtää standardia nopeammin ja syvällisemmin kuin muut. Standardointityö on myös keino verkostoitua alan asiantuntijoiden kanssa. Suljettu standardointiprosessi vie tämän mahdollisuuden organisaatioilta, jotka eivät pysty osallistumaan toimintaan.

Suomen kaltaisella pienellä maalla on vähäiset mahdollisuudet synnyttää yrityksiä, jotka pystyisivät omalla vaikutusvallallaan vaikuttamaan teollisuuden kehityskulkuihin. Kansallisten ponnistusten yhdistäminen ja aktiivinen vaikuttaminen standardointiin avaavatkin kanavan kansainvälisille markkinoille ja antavat edelläkävijäaseman teknisten ratkaisujen määrittelyssä ja hyödyntämisessä.

Esimerkiksi Microsoft osallistuu aktiivisesti standardointityöhön, koska pitää sitä tehokkaana keinona varmistaa yhteentoimivuutta ja rakentaa yhteisiä pelisääntöjä. Vaikka standardointityöhön osallistumisesta koituu kuluja, työn tuottamia hyötyjä pidetään merkittävämpinä.

Microsoft osallistuu globaaliin, paikalliseen, toimialakohtaiseen sekä Yhdysvaltojen hallinnon standardointityöhön. Yritystä kiinnostaa myös muun muassa tekoälyn standardointi ja yhteisten ohjeiden luominen tekoälyn hyödyntämistä varten. Osallistumalla standardointiin se voi vaikuttaa markkinoiden kehitykseen ja yhteisten pelisääntöjen muovaamiseen.

5 Tietoturvallisuuden auditointi, akkreditointi ja sertifiointi

Tietoturvallisuusalan standardointi, akkreditointi, auditointi ja sertifiointi ovat vuorovaikutuksessa ja kytkeytyvät tiiviisti toisiinsa. Seuraavassa tarkastellaan tietoturvallisuuden todentamisen vaiheita ja niihin vaikuttavia seikkoja.

5.1 Sertifiointi

Tietoturvallisuuden vaatimustenmukaisuuden todistettavasti täyttäville toteutuksille voidaan myöntää hyväksyntä eli sertifikaatti, jonka myöntää puolueeton kolmas osapuoli. Sertifikaatteja voidaan myöntää esimerkiksi hallintajärjestelmille, liiketoiminnan jatkuvuuden hallintajärjestelmille, IT-palvelunhallintajärjestelmille, pilvipalvelun tarjoajille ja teknisille ratkaisuille (esimerkiksi tietojärjestelmätuotteille ja salaustuotteille).

Sertifioinnin taustalla on usein asiakasvaatimus. Esimerkiksi julkishallinnon tuotesertifioinneilla on lakiin perustuva liiketoimintavaatimus: asiakas edellyttää sertifiointia. Sertifikaatti on joissakin tilanteissa myös kilpailutekijä, jonka avulla voidaan erottautua kilpailijoista riskittömämpänä vaihtoehtona. Myös tietoturvatietoisuus ja esimerkiksi toistuvat tietoturvahäiriöt voivat olla syitä sertifikaatin hankinnalle.

Standardeja voidaan käyttää tietoturvallisuuden parantamiseen ilman sertifiointiakin. Sertifiointi on kuitenkin selkeä tapa viestiä standardiin sitoutumisesta. Organisaatio voi sertifikaatin avulla osoittaa asiakkailleen ja sidosryhmilleen, että jatkuva kehittäminen ja toiminnan parantaminen kuuluvat sen toimintatapoihin. Hallintajärjestelmät ja niiden sertifioinnit ovatkin usein edellytyksenä asiakkaan valitessa toimittajia tai kumppaneita, erityisesti kansainvälisessä liiketoiminnassa.

Tätä raporttia varten tehdyn selvityksen perusteella organisaatiot, jotka hakevat tietoturvallisuuden hallintajärjestelmälleen sertifiointia, kokevat sertifiointiprosessin hyödylliseksi ja valmentavaksi. Vaikka puolueettomat arvioijat eivät olekaan konsultteja, heiltä on mahdollista saada tukea ja apua hallintajärjestelmän kehittämiseen. Sertifikaattia pidetään myös kilpailuetuna, jonka avulla voidaan erottautua kilpailijoista, erityisesti pienemmistä toimijoista, jotka eivät ole hankkineet sertifiointia esimerkiksi kustannussyistä.

5.2 Arviointi ja auditointi

Suomen kielen termit ”arviointi” ja ”tarkastus” aiheuttavat usein sekaannuksia.

Arviointi sisältää tulkintamahdollisuuden, mutta tarkastus ei, koska siinä keskitytään ainoastaan vaatimusten toteutumiseen (kyllä/ei). Käsitteet menevät käytännön työssä helposti sekaisin. Myös auditointikriteeristö ja tarkastuslista rajaavat tulkinnanmahdollisuutta antamalla lisätietoa hyväksyttävistä toteutuksista. Käsitteiden huolellinen määrittely ja oikeiden termien käyttö vähentävät väärinkäsityksiä myös käytännön työssä, minkä vuoksi niihin tulisi kiinnittää huomiota.

Organisaatio voi itse arvioida, onko vaatimuksia noudatettu tai palkata työhön puolueettoman kolmannen osapuolen. Tätä pidetään luotettavimpana tapana. Kolmas osapuoli voi arvioida tai auditoida organisaation toimintaa sen dokumentteja tarkastelemalla, fyysisinä tarkastuskäynteinä tai molempien yhdistelmänä. Mitä monipuolisempia ja laajempia arviointi- tai auditointimenetelmät ovat, sitä paremmin ne osoittavat, onko vaatimuksia noudatettu. On kuitenkin hyvä huomata, että laajat arvioinnit ja auditoinnit vievät paljon aikaa ja aiheuttavat huomattavia kustannuksia.

Kolmannen osapuolen suorittamien auditointien läpimenoprosentti ei ole julkista tietoa,

mutta haastateltujen arviointilaitosten mukaan organisaatioiden kypsyystaso on noussut viime vuosina. Tämä tarkoittaa sitä, että yhä useamman organisaation käytännöt vastaavat todistetusti vaatimuksia. Tietoturvallisuuden hallintajärjestelmän kehittäminen vaikuttaa olevan työläämpi kuin ISO 9001:2015 -standardin mukaisen laadunhallintajärjestelmän kehittäminen. Standardit myös tukevat toisiaan, esimerkiksi jos jokin valtion virasto on läpäissyt ISO/IEC 27001 -sertifioinnin, se läpäisee myös todennäköisesti VAHTI 2/2010 -ohjeen mukaisen auditoinnin ilman poikkeamia.

5.3 Akkreditointi

Akkreditointi tarkoittaa pätevyyden toteamista puolueettomasti ja riippumattomasti. Eurooppalaisen lainsäädännön mukaisesti jokaisessa EU-maassa on yksi kansallinen akkreditointielin ja Suomessa tämä tehtävä on FINASilla (Finnish Accreditation Service). Turvallisuus- ja kemikaalivirasto Tukesiin kuuluva FINAS on kansainvälisen akkreditointijärjestön IAF:n (International Accreditation Forum) jäsenjärjestö. Liikenne- ja viestintävirasto puolestaan hyväksyy ja valvoo arviointilaitoksia, jotka tarjoavat viranomaisille puolueetonta tietoturvallisuuden arviointipalvelua.

Suomessa FINASin akkreditoimia ja Liikenne- ja viestintäviraston hyväksymiä virallisia tietoturvallisuuden arviointilaitoksia ovat Inspecta Sertifiointi Oy, KPMG IT Sertifiointi Oy ja Nixu Certification Oy. Lisäksi Bureau Veritas Finland, DNV GL Business Assurance Finland ja Lloyds Register tarjoavat ISO/IEC 27001 -sertifiointia Suomessa. Niiden akkreditoinnista on vastannut jokin muu IAF:n jäsenjärjestö kuin FINAS.

Viime aikoina myös akkreditoimattomat arviointilaitokset ovat alkaneet myöntää ISO/IEC 27001 -sertifikaatteja, esimerkiksi terveydenhuollon alalla. Erityisesti silloin kun kyseessä on kansainvälinen toiminta, akkreditoimaton sertifiointi tai suljettu kansallinen arviointikriteeristö on kansainväliseltä uskottavuudeltaan ja painoarvoltaan heikko. Etenkin viranomaisille tietoturva-arviointeja tekevät arviointilaitokset joutuvat käymään läpi hyväksyntäprosessin, jonka avulla varmistetaan niiden todellinen arviointikyvykkyys.

Akkreditointi viestii asiakkaille toiminnan pätevyydestä, uskottavuudesta ja luotettavuudesta sekä yhdenmukaistaa vaatimusten tulkintaa ja lisää yhteentoimivuutta. Lisäksi sillä edistetään Euroopan sisämarkkinoiden toimintaa varmistamalla, että akkreditoidun toimijan tuottamien palvelujen laatuun ja standardin tulkintaan voidaan luottaa kansainvälisesti. Näistä syistä sertifioinneissa tulisi käyttää vain akkreditoituja toimijoita.

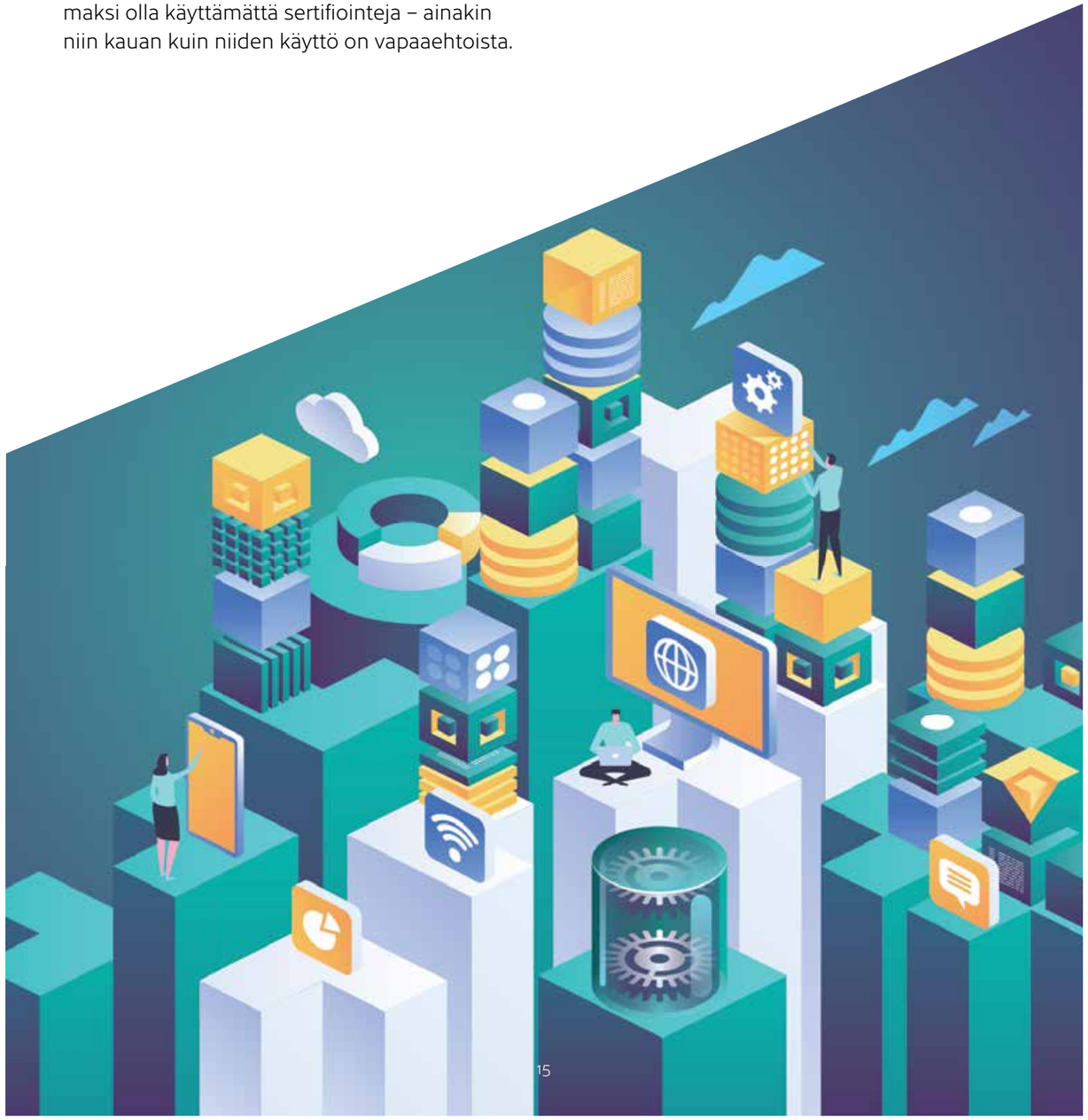
5.4 Sertifiointien merkitys liiketoiminnalle

Kustannukset vaikuttavat sertifiointien käytön laajuuteen ja vaikutukseen. Edullisten, niin sanottujen kevytsertifikaattien merkitys liiketoiminnalle voi olla vähäinen, kun taas raskaammissa vaatimuksissa ja niiden todentamisissa kustannukset voivat olla suuria. Raskaammat sertifioinnit painottuvatkin pääsääntöisesti isoihin toimijoihin ja niiden tuotteisiin.

Suomen kaikista 283 563 yrityksestä 264 519 (93,3 %) on alle 10 hengen mikroyrityksiä, minkä vuoksi uusia tai velvoittavia sertifikaatteja suunniteltaessa tulisi erityisesti huomioida, että pienet ja keskisuuret yritykset voivat hyödyntää niitä. Myös kansainvälisiin ja eurooppalaisiin sertifiointisuunnitelmiin tulisi pyrkiä vaikuttamaan niin, että ne tukisivat myös pienten ja keskisuurten yritysten kilpailukykyä.

Tieto- ja viestintäteknologia-alan nopeasti uudistuva luonne vaikuttaa myös sertifikaattien ylläpitämiseen. Käytännössä melko pienetkin muutokset voivat vaatia ainakin osittaisen uuden hyväksyntäprosessin, mikä voi aiheuttaa kohtuuttomia kustannuksia ja sitoa resursseja. Tästä syystä osa toimijoista voi nähdä paremmaksi olla käyttämättä sertifiointeja – ainakin niin kauan kuin niiden käyttö on vapaaehtoista.

Oikein tehtynä puolueettoman osapuolen tarkastus ja hyväksyntä lisäävät kuitenkin merkittävästi sidosryhmien luottamusta vaatimusten noudattamiseen.



II OSA

6 Käyttökokemuksia tietoturvastandardeista organisaatiossa

Tässä osassa käydään läpi kansallisia kokemuksia, hyötyjä ja haasteita tietoturvastandardien ja -sertifiointien käytöstä eri toimijaryhmien silmin. Lisäksi tarkastellaan standardoinnin ja sertifioinnin nykytilaa ja tulevaisuuden suuntauksia. Tiedot perustuvat johdannossa mainittuihin tietoturvallisuustoimijoiden haastatteluihin sekä lähteisiin, jotka on listattu luvussa Lähteet.

6.1 ISO/IEC 27001 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.

Tietoturvallisuuden hallintajärjestelmien kansainvälinen standardi ISO/IEC 27001 on tarkalleen ottaen hallinnan ja johtamisen standardi, ei tietoturvastandardi. Se antaa viitekehyksen ja riskiperusteisen näkymän siihen, että organisaatiossa hallitaan tietoturvallisuuteen kuuluvia asioita. Väärinymmärrykset standardin luonteesta ovat johtaneet esimerkiksi tilanteisiin, joissa on pyritty sertifioimaan tietojärjestelmä sitä vasten. Tämä ei kuitenkaan ole mahdollista – ainoastaan johtamiskäytännöt voidaan sertifioida.

Standardin uusin versio on vuodelta 2013. Siinä on otettu aiempia versioita paremmin huomioon myös sovelluspohjaiset infrastruktuurit, kuten pilvipalvelut.

ISO/IEC 27001 -standardista koetut hyödyt

ISO/IEC 27001 -standardin merkittävänä hyötynä pidetään sekä standardin että sen sertifioinnin vapaaehtoisuutta. Lisäksi standardi on riskiperusteinen: kukin organisaatio voi itse arvioida omaa toimintaansa vasten, mikä on tarpeellista ja millaisiin toimenpiteisiin se ryhtyy hallintatavoitteiden saavuttamiseksi. Näin resursseja ei tarvitse kohdentaa sellaisiin pakollisiin vaatimuksiin, joiden toteuttaminen ei tuota lisäarvoa.

Standardi koostuu joukosta vaatimuksia, jotka ovat niin yleisiä, että ne sopivat jokaiselle organisaatiolle organisaation koosta tai toimialasta riippumatta. Standardissa ei määritellä, kuinka vaatimukset tulee toteuttaa. Organisaatio voi myös jättää joitakin hallintakeinoja toteuttamatta tehtyään ja dokumentoituaan siihen liittyvän riskiarvion. Myös standardin lisäosat, joita vasten ei voi sertifioitua, mutta joita voi käyttää toiminnan kehittämisessä, on koettu hyödyllisinä.

Asiakas saattaa tarjouspyynnöissä edellyttää tarjoajaa vastaamaan laajamittaiseen tietoturvallisuuden hallintajärjestelmää koskevaan kyselyyn, mutta jos organisaatiolla on ISO-sertifikaatti, se riittää usein todisteeksi vaatimustenmukaisuudesta ja vähentää siten merkittävästi tarjouksen tekemiseen liittyvää työmäärää.

Vaikka tietoturvallisuuden hallintajärjestelmiä on kehitetty selvästi eniten ICT-alalla, myös valmistavassa teollisuudessa kansainväliset asiakkaat edellyttävät usein ISO/IEC 27001:n vaatimusten noudattamista. Tästä esimerkkinä Vaisala Oy, jonka liikevaihdosta 90 % tulee muualta kuin Suomesta ja jolle esimerkiksi kansainväliset ilmatieteen laitokset ja lääketeollisuus asettavat tiukkoja vaatimuksia. Ne voidaan osoittaa toteen vastaamalla asiakkaan lähettämään yksityiskohtaiseen tietoturvakyselyyn tai vaihtoehtoisesti toimittamalla puolueettoman kolmannen osapuolen myöntämä sertifikaatti, jolloin aikaa vievä kysely voidaan ohittaa. Vain harvoin sertifikaatti on pakollinen ja poissulkeva asiakasvaatimus.

Monet yritykset ovat valinneet ISO/IEC 27001 -standardin vaatimukset osaksi yrityksen tietoturvaa ilman sertifiointia. Nämä yritykset katselmoivat omatoimisesti hallintajärjestelmänsä ja ylläpitävät itsenäisesti tiedon eheyttä, luotettavuutta, käytettävyyttä ja alkuperää. Vuosikellomaisen toimintatavan koetaan auttavan aidosti organisaatioita toimimaan järkevästi ja tuovan systemaattisuutta johtamiseen. Standardin vaatimusten noudattamisen koetaan lisäävän sidosryhmien luottamusta siihen, että riskejä hallitaan asianmukaisesti.

> Laurean ammattikorkeakoulussa syksyllä 2016 tehdyssä opinnäytetyössä toteutettiin kysely Suomessa toimiville ICT-alan yrityksille, joilla oli ollut useamman vuoden ajan ISO/IEC 27001 -sertifikaatti. Kyselyyn vastanneet yritykset kokivat pääsääntöisesti standardin vaatimusten noudattamisen edistävän tietoturvan hallinnan jatkuvaa kehittämistä. Monissa vastauksissa oltiin tyytyväisiä toiminnan tehostumiseen: kerran luodut ohjeet oli helppo pitää ajan tasalla, eikä hyväksi havaittuja toimintatapoja tarvinnut muuttaa. Sertifikaatin koettiin tuovan etua kilpailutuksissa ja toimivan luontevana osana palveluntarjontaa. Erityisesti kansainvälisessä kaupankäynnissä ja yhteistyössä ISO/IEC 27001 -sertifikaatti on ylivoimainen osoitus vaatimustenmukaisuudesta.
>
> Opinnäytetyön tulokset tulisi ottaa huomioon myös kansallisia standardeja laadittaessa. Näin yritysten ei tarvitsisi käyttää ylimääräisiä resursseja päällekkäisten, mutta hivenen eri tavoin muotoiltujen vaatimusten toteuttamiseen ja vaatimustenmukaisuuden osoittamiseen.

Standardin soveltamisessa havaitut haasteet

Suurimmat haasteet ISO/IEC 27001 -standardin soveltamisessa liittyvät väärinymmärryksiin. Monessa organisaatiossa tulkitaan standardin liitettä A Hallintatavoitteiden ja -keinojen liiteluettelo vaatimuskokoelmaksi, jollaiseksi sitä ei ole tarkoitettu. Liite A ei sisällä vaatimuksia, vaan hyviä käytäntöjä, jotka tulee ottaa huomioon.

Päädokumentissa viitataan liitteeseen A ainoastaan luvussa 6.1.3, jossa todetaan vaatimuksena 6.1.3 c): ”Verrataan kohdassa 6.1.3 b) määritettyjä hallintakeinoja liitteessä A oleviin ja todennetaan, ettei yhtäkään tarvittavaa hallintakeinoa ole jätetty pois” sekä 6.1.3 d): ”Laaditaan soveltuvuuslausunto, joka sisältää vaaditut hallintakeinot sekä perustelut liitteessä A esitettyjen hallintakeinojen käyttämiselle tai käyttämättä jättämiselle.”

ISO/IEC 27001 -standardin heikkous on se, että liitteen A ja sovelluslausunnon merkitys eivät ole selkeitä. Liitteen A uudistaminen on standardin keskeinen kehityskohde. On jopa ehdotettu, että liite A poistettaisiin kokonaan standardista, mutta tällä hetkellä säilyttämisen puoltajia vaikuttaa olevan vastustajia enemmän.

Selvitystä varten haastateltujen mielestä osa ISO/IEC 27001 -standardin vaatimuksista on ympäripyöreitä ja hankalasti tulkittavissa. Joidenkin mielestä englanninkielistä versiota on helpompi ymmärtää kuin suomenkielistä. Lisäksi vaikuttaa siltä, että kaikki standardia käyttävät organisaatiotkaan eivät ymmärrä, että ISO/IEC 20071 on johtamisen standardi, eikä sertifikaatti itsessään kerro teknisen tietoturvan tasosta ja sen kehittymisestä. Standardi ei esimerkiksi aseta vaatimusta vaikkapa salasanan pituudelle tai seinän paksuudelle, vaikka se niihin välillisesti kantaa ottaakin (muun muassa luku 4.1 Organisaation ja sen toimintaympäristön ymmärtäminen ja 6.1.2 Tietoturvariskien arviointi).

ISO/IEC 27001:tä täydentää standardi ISO/IEC 27002, jossa on esimerkkitoteutuksia liittyen vaatimusstandardiin. Koska ISO/IEC 27002:n ohjeistus on paljon ensimmäistä osaa yksityiskohtaisempaa, toisen osan esimerkkitoteutukset tulkitaan helposti vaatimuksiksi, mitä ne eivät ole. ISO/IEC 27002:ssa esitetyt hallintakeinot ovat siis vain mahdollisia tapoja toteuttaa ISO/IEC 27001:ssä esitettyjä vaatimuksia, eivät vaatimuksia itsessään.

Ajankäytöllisistä syistä ISO/IEC 27001:n sertifiointiauditoinneissa joudutaan luottamaan paljon auditoitavan kohteen sanaan ja dokumentaatioon. Auditointi on aina luonteeltaan otokseen perustuvaa, eli kaikkea ei tarkasteta,

vaan pyritään saamaan riittävä luottamus siihen, että vaatimukset täyttyvät.

Tietoturvallisuuden hallintajärjestelmän kehittämiseen ja sen sertifiointiin liittyy merkittäviä kustannus- ja resurssikysymyksiä. Kaikkein pienimmille yrityksille ISO/IEC 27001 -sertifioinnin esteenä voivat olla erityisesti sertifioinnin kustannukset sekä tietotekniikka- ja tietoturvaosaamisen puute. Alle 10 hengen organisaatioissa ensimmäisen sertifioinnin kustannukset kolmen vuoden syklillä ovat yhteensä arviolta noin 15 000 € (sisältäen ensimmäisen arvioinnin ja sen jälkeiset vuosittaiset ylläpitokäynnit). Järjestelmän kehittämisen kustannukset ovat kuitenkin huomattavasti suuremmat kuin sertifioinnin kustannukset. Pk-yritykset voisivat hyötyä viranomaisten tuesta osaamisensa kehittämisessä. Tietoturva-alalla on kuitenkin saatavilla runsaasti kirjallisuutta, kursseja ja konsultointia, joiden hyödyntämistä ei tähän selvitykseen osallistuneiden mielestä olisi syytä tukea verovaroin. Myös maksutonta tietoa on saatavilla verkosta.

Suomessa pienetkin organisaatiot – erityisesti ne, jotka myyvät palveluitaan suuremmille toimijoille – haluavat yhä useammin osoittaa täyttävänsä tietoturvan hallintajärjestelmän vaatimukset ja hakevat tästä syystä ISO/IEC 27001 -sertifiointia.

6.2 Kansallinen FINCSC-kyberturvallisuussertifiointi

Suomessa on vuosina 2015–2016 kehitetty niin sanottu ”kevytsertifiointimenetelmä” organisaation kyberturvallisuustason mittaamiseen ja osoittamiseen: Finnish Cyber Security Certificate, eli FINCSC-menetelmä. Siinä sertifiointia hakeva yritys tekee FINCSC-portaalissa itsearvioinnin, jonka auktorisoitu arviointilaitos katselmoi.

Sertifikaatti soveltuu kustannuksiltaan ja käytettävyydeltään kaikenkokoisille organisaatioille toimialasta riippumatta. Sertifioinnin vuosihinta on 350 €. Arvioinnin uusimista suositellaan aina, kun organisaation liiketoimintaympäristö muuttuu, esimerkiksi jos ulkoistetaan palveluntuotanto tai vaihdetaan palveluntuottajaa. FINCSC-sertifiointi on ollut kaupallisessa käytössä 1.12.2016 lähtien. Sen on hyväksytysti suorittanut yrityksiä kymmeniltä eri toimialoilta.

FINCSC on kohdistettu suomalaisille markkinoille, erityisesti pienille ja keskisuurille organisaatioille niiden oman tason toteamiseksi. Yritys pystyy sertifioinnilla vakuuttamaan yhteistyöverkostolleen ymmärtävänsä kyber- ja tietoturvallisuuden perusteet ja noudattavansa hyväksi havaittuja periaatteita. Suurten yritysten ja esimerkiksi kuntasektorin toiminnassa FINCSC-sertifikaatin suorittamista vaatimalla voidaan vakuuttua kumppaniverkoston kyberturvallisuuden perustasosta ja näin ollen pienentää liiketoiminnan riskejä.

Vaikka sertifiointi on tällä hetkellä saatavissa vain suomenkielisenä, sitä ei ole sidottu maantieteellisesti ja sen käyttäjäorganisaatioilla on myös kansainvälisiä asiakkaita. FINCSC:n verkkosivuille on tuotettu myös englanninkielistä materiaalia. Sertifioinnin kansainvälisestä versiosta on suunnittelu käynnissä ja sertifioinnissa tullaan seuraamaan myös eurooppalaisen sertifioinnin toteutumista. Tavoitteena on kyetä jatkossa vastaamaan kotimaisella sertifikaatilla myös erityisesti mahdollisiin eurooppalaisiin vaatimuksiin PK-sektorin toimijoille.

FINCSC-sertifiointitason rinnalle on kehitetty FINCSC PLUS -sertifiointitaso. Tässä sertifioinnissa yrityksen toimintaa auditoidaan ulkoisesti FINCSC-itsearviointiin perustuen. Auditoinnissa arviointilaitokset tarkastelevat organisaation itsearvioinnissa kuvaamaa toimintaa asiakirjakatselmoinnein, henkilöhaastatteluin, fyysisesti havainnoiden ja tietoturvatestauksin. PLUS-tason sertifioinnilla voidaan varmistaa FINCSC-sertifioinnin todenmukaisuus, ja se on myös erittäin käyttökelpoinen valmentava väline esimerkiksi keskisuurten yritysten tiellä kohti ISO/IEC 27001 -sertifiointia tai viranomaisten Katakri-auditointeja.

FINCSC:n vaatimukset ovat peräisin useasta kansainvälisestä ja kansallisesta lähteestä, kuten ISO/IEC 27001, brittiläinen Cyber Essentials, Katakri 2015 ja EU:n tietosuoja-asetus 679/2016. Järjestelmän ovat laatineet yhdessä Elinkeinoelämän keskusliitto, Jyväskylän ammattikorkeakoulun IT-instituutti, Telia Finland Oyj, Liikenne- ja viestintävirasto ja 3DSL Isosta-Britanniasta. Pilotointiin osallistui parikymmentä pk-yritystä eri toimialoilta pääasiassa Keski-Suomen alueelta.

FINCSC:llä ei haluta vain täyttää lainsäädännön vaatimuksia. Itsearvioinnin kysymykset liittyvät yrityksen tietojen käsittelyyn, säilytykseen ja IT-palveluiden tuottamiseen käytettäviin fasiliteetteihin, prosesseihin, henkilöihin sekä teknologioihin. Arviointi perustuu yhteentoista toisiaan täydentävään osa-alueeseen. Yksittäisinä aihealueina itsearvioinnissa nousee esille muun muassa johtaminen ja riskienhallinta. Vaatimusten laatijoiden mukaan itsearviointi ei edellytä vahvaa tietoturvaosaamista. Arviointikriteeristö ei ole julkinen, mikä rajoittaa sen saatavuutta. Toisaalta on huomioitava, etteivät ISO-standarditkaan ole maksutta saatavilla ja että liiketoimintamallin valintaan vaikuttaa myös tapa, jolla sertifiointia ylläpidetään.

Sertifiointijärjestelmää ylläpitää Jyväskylän ammattikorkeakoulussa toimiva kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus JYVSECTEC, joka toimii yhteistyössä sertifiointipalveluja tarjoavien arviointilaitosten ja ohjausryhmän kanssa. FINCSC ja FINCSC PLUS -sertifiointijärjestelmän ohjausryhmä koostuu elinkeinoelämän ja julkishallinnon organisaatioista.

ESIMERKKI FINCSC-sertifikaatin käytöstä pk-yrityksessä: Case Fysio Center Jyväskylä Oy

Fysio Center Jyväskylä Oy tuottaa fysioterapia- ja kuntoutuspalveluita Jyvässeudulla ja Petäjävedellä ja se työllistää noin 20 työntekijää. Vuonna 2016 yritys liittyi kansallisen potilastiedon arkistoon Kanta-palveluihin ensimmäisenä kuntoutusalan yrityksenä, mikä toimi liikkeellepanevana voimana tietoturvallisuuden kehittämisessä. Yrityksellä ei ollut omia IT-asiantuntijoita eikä IT-osaamista, ja kuten monessa muussakin pk-yrityksessä, tietoturvaan liittyvät asiat koettiin suorastaan uhkaavina. Onkin huomioitava, että 70 % kotimaisista yrityksistä on sellaisia, joissa työtekijöitä on 1–3. Näistä vain harvalla on IT- ja tietoturvaosaamista.

Toimitusjohtaja ja muutama yrityksen työntekijä osallistuivat Jykesin järjestämään kyberturvallisuusklinikkaan, missä yhteydessä myös FINCSC-sertifiointi tuli tutuksi. Fysio Center Jyväskylä Oy haki FINCSC -sertifikaatin vuonna 2016, mutta ei ole uusinut sitä sen jälkeen. Yrityksen mukaan vaatimukset olivat tiukkoja, mutta prosessi silti hyödyllinen. Sertifikaattia käytettiin markkinoinnissa, mutta varsinaiset hyödyt nähtiin yrityksen sisäisinä – oman toiminnan tehostumisena ja määrämuotoistumisena.

6.3 VAHTI 2/2010

Valtiovarainministeriön Digitaalisen turvallisuuden johtoryhmän VAHTIn ohjekokonaisuus on kehitetty tukemaan julkishallintoa koskevan tietoturvalainsäädännön tulkintaa. Ohjeet ovat nimensä mukaisesti ohjeita tai suosituksia, eivätkä ne lain näkökulmasta velvoita toimijoita. Silti esimerkiksi VAHTI 2/2010 -ohje on usein tulkittu vaatimuskriteeristöksi ja se on ohjannut käytännössä toteutuksia voimakkaasti. Tämän vuoksi ohje rinnastetaan tässä yhteydessä standardiin.

Suuri osa VAHTI 2/2010 -ohjeen sisällöstä perustuu tai on löydettävissä suoraan ISO/IEC 27001 -standardista. Ohjeen laatimisessa on käytetty myös Open Information Security Maturity Model eli O-ISM3-kypsyysmallia, mitä on kritisoitu, sillä organisaation kyvykkyystaso ja suojattavaan kohteeseen liittyvät turvakontrollit (tietoturvatasot) ovat eri ulottuvuuksia. 2/2010 -ohjeessa on viitattu myös muihin VAHTI-ohjeisiin ja säädöksiin sekä tietosuojanäkökulmiin. Käytännössä organisaatiot, joilla on ollut hyväksytty ISO/IEC 27001 -sertifikaatti, ovat läpäisseet tietoturvatasoauditoinnin (niin sanotun TTT-auditoinnin) vaivattomasti.

Valtion IT-palvelukeskus VIP ja myöhemmin sen seuraaja Valtori kouluttivat Hanselin puitesopimukseen kuuluvien konsulttiyritysten asiantuntijoita toteuttamaan TTT- auditointeja. Nämä eivät ole täydellisiä auditointeja, vaan kyse on kertaluontoisesta avustetusta itsearvioinnista. Auditoinneissa käytetään VAHTI 2/2010 -ohjetta ja käydään läpi jopa 1200 vaatimusta, mikä on koettu varsin raskaaksi.

Kaikkia virastoja ei ole kirjoittamishetkellä auditoitu. VIPin toimeksiannoista TTT-auditointeja ryhdyttiin tekemään 2010-luvun alussa organisaatioille, jotka olivat tulossa VIPin asiakkaiksi. Myöhemmin Valtorille palvelunkäyttäjiksi siirtyi säädösperusteisesti noin 80 organisaatiota. Alkuvuosina auditointeja tehtiin paljon, myöhemmin enää satunnaisesti. Auditointien jälkeisten korjaavien toimenpiteiden seuranta on ollut Valtorin vastuulla, ei auditoivan konsultin.

Kun tietoturva-asetus astui voimaan 2010, moni virasto jätti asetuksen edellyttämän tietojen luokittelun toteuttamatta. Etenkin, jos organisaatio ei ollut VIPin/Valtorin asiakas, se jätti tyypillisesti TTT-auditoinnin tekemättä. Valtorilla on kuitenkin ollut oikeus pyytää TTT-auditointia, jotta sen olisi mahdollista saada luotettava kuva asiakkaidensa tietoturvan tasosta.

Virastoissa TTT-auditointien hyötyihin suhtaudutaan vaihtelevasti. Onnistuneimpina on pidetty auditointeja, joissa on käytetty konsultoivaa ja perustelevaa otetta. Lisäksi auditoinnit, joihin on osallistunut myös organisaation ylin johto, on koettu mielekkäiksi. VAHTI-ohjeen kattavuutta ja monipuolisuutta pidetään yleisesti hyvänä asiana, mutta myös ohjattua itsearviointia arvostetaan. Haasteiksi on koettu ohjeiden tulkinnanvaraisuus ja ICT-osuuden painottuminen ensisijaisesti hallinnolliseen ja prosessien toimivuuden tarkasteluun teknisen tietoturvan jäädessä vähemmälle.

VAHTI 2/2010 on ollut voimassa 9 vuotta. Sen työnimellä VAHTI 100 kulkeva päivitystyö on parhaillaan käynnissä vuoden 2020 alussa voimaan astuvan uuden tiedonhallintalain vuoksi. Lainsäädännön velvoittavuus laajenee tiedonhallintalain myötä, ja uusi ohjekokonaisuus tulee jatkossa koskemaan valtionhallinnon lisäksi myös kuntia ja maakuntia.

6.4 Katakri

Kansallinen auditointikriteeristö Katakri 2015 on viranomaisten auditointityökalu. Sitä käytetään arvioitaessa yrityksen turvallisuusjärjestelyjen toteutumista yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Sitä voidaan käyttää myös apuna yrityksien, yhteisöjen sekä viranomaisten muussa turvallisuustyössä ja sen kehittämisessä. Tyypillisesti Katakria on sovellettu kansainvälisessä yhteistyössä, kun suomalainen yritys tai organisaatio käsittelee jonkun toisen maan salassa pidettävää tietoa.

Katakri 2015:n Johdanto-luvussa mainitaan: ”Vaatimukset on kuvattu niin, että ne mahdollistavat erilaisia toteutustapoja. Vaatimusten yhteydessä oleviin lisätietokenttiin on kirjoitettu toteutustavoista esimerkkejä, jotka eivät kuitenkaan ole sitovia.” Katakri 2015 sisältääkin edellistä versiota enemmän tulkinnanvaraa, mikä voi aiheuttaa organisaatioissa epätietoisuutta turvallisuusjärjestelyjen riittävyydestä.

Käytännössä Katakri-auditoinnit ovat lähes syrjäyttäneet VAHTI 2/2010-tietoturvatasoauditoinnit. Asiaan vaikuttanee se, että Katakri-vaatimuksia on ainoastaan 45, kun VAHTI-auditoinneissa niitä on yli 1 000. Erityisenä haasteena VAHTIn soveltamisessa pidetään sitä, että vaatimukset eivät skaalaudu organisaation koon mukaisesti.

Katakrin auditointikriteerit on jaettu kolmeen osa-alueeseen:

1. Turvallisuusjohtamista koskeva (T) osa-alue, jossa pyritään varmistumaan siitä, että organisaatiolla on riittävät turvallisuus johtamisen valmiudet sekä kyvykkyys.
2. Fyysistä turvallisuutta koskeva (F) osa-alue, jossa kuvataan salassa pidettävien tietojen fyysistä käyttöympäristöä koske vat turvallisuusvaatimusten auditointikriteerit.
3. Teknistä tietoturvallisuutta koskeva (I) osa-alue, jossa kuvataan puolestaan tekniselle tietojenkäsittely-ympäristölle asetetut vaatimusten auditointikriteerit.

Osa-alue I jakautuu kolmeen käsiteltävän tiedon mukaiseen suojaustasoon (ST IV, ST III, ST II). Kriteerit on kuvattu siten, että toteutustavat voivat olla erilaisia. Kriteerien yhteydessä oleviin lisätietokenttiin on kirjattu toteutustapaesimerkkejä.

Arviointilaitos voi Katakria käyttäen todentaa organisaation käyttämien menetelmien turvallisuuden. Katakria sovelletaan myös kansallisesti: esimerkiksi Puolustusvoimat edellyttää kaikilta alihankkijoiltaan hyväksyttyä puolueetonta Katakri-auditointia.

Katakria ei ole tarkoitettu käytettäväksi sellaisenaan julkisen hankinnan turvallisuusvaatimuksena, mutta tällaistakin käyttöä on nähty. Julkisessa hankinnassa tarkat turvallisuusvaatimukset tulisi määrittää erikseen niin, että hankintaa koskevat riskit ja erityistarpeet otetaan huomioon.

Katakrin sisältöä tullaan todennäköisesti päivittämään tulevan lainsäädännön vaatimusten mukaisesti.

6.5 Vaatimus, ohje vai esimerkkitoteutus?

Tietoturvavaatimusten, ohjeiden ja esimerkkitoteutusten välinen suhde aiheuttaa päänvaivaa kansallisessa ympäristössä. Problematiikka näkyy VAHTI-ohjeiden, Katakrin ja ISO 27001:n tulkinnoissa.

Varsinaiset vaatimukset, tulivatpa ne sitten ylätason standardista tai lainsäädännöstä, on tyypillisesti muotoiltu melko väljästi tulkintavaraa jättäen. Käytännössä tämän tyyppiset standardit voivat jäädä vaikean hahmotettavuutensa vuoksi taka-alalle, kun taas niitä tukevissa ohjeistuksissa ja auditointikriteeristöissä esitetyt käytännön esimerkkitoteutukset nousevat vaatimusten asemaan. Tällainen tulkinta sitoo toimijoiden käsiä ja saattaa johtaa tarpeettoman kalliisiin ja kankeisiin toteutuksiin, joissa ei oteta huomioon sovelluskohteen erityispiirteitä, vaikka varsinaiset vaatimuskriteeristöt sen sallisivatkin.

Ongelma on havaittu myös ohjeistusten laatimisessa. Väestörekisterikeskuksen asiantuntijaryhmä valmistelee VAHTI 100 soveltamis- ja arviointiohjeistusta, joka tulee korvaamaan nykyisen VAHTI 2/2010 -ohjeen. VAHTI 100 -kokonaisuus kootaan verkkosivustolle, jossa vaatimukset, niitä tulkitsevat ohjeistukset ja muut tukimateriaalit erotellaan toisistaan värikoodein. Tällä pyritään välttämään aikaisempien ohjeistusten soveltamisessa ilmenneet näkemyserot vaatimusten ja niitä tulkitsevien ohjeiden välisestä suhteesta.

Raporttia varten tehtyjen haastattelujen pe-

rusteella vaikuttaa myös siltä, että tietoturvallisuuden merkitystä on vaikea viestiä organisaation johdolle riittävän selkeästi. Siksi kaivataankin konkreettista ja velvoittavaa kriteeristöä viestinnän tueksi. Näin pystyttäisiin paremmin perustelemaan johdolle, miksi tietoturvallisuuteen on syytä investoida. Myös auditoijat toivovat kriteereitä, joiden tulkinta olisi mahdollisimman yhdenmukaista auditointien tekijöistä riippumatta. Mitä konkreettisempia vaatimusten tulkintaa ohjaavat auditointikriteerit ovat, sitä helpommin tavoite saavutetaan.

Mitä yleisemmällä tasolla vaatimus ilmaistaan, sitä enemmän sen tulkintaan vaaditaan osaamista ja kokemusta tietoturvan toteuttamisesta. Liian laaja tulkinnanvara johtaa lähes poikkeuksetta siihen, että esimerkiksi eri auditoijien tulkinnat eroavat toisistaan merkittävästi. Vastaavasti, mitä yksityiskohtaisemmin ja konkreettisemmin tietoturvavaatimus ilmaistaan, sitä jäykempi ja vähemmän kokonaisuuden tarpeet huomioiva sen toteutuksesta tulee. Hyvin yksityiskohtaiset tekniset vaatimukset myös vanhenevat nopeasti ja nostavat helposti kustannuksia merkittävästi. Vaatimustason asettamiseen ja kohteen ominaispiirteisiin on siis kiinnitettävä erityistä huomiota. Tärkeää olisi myös löytää tasapaino vaatimusten ajanmukaisuuden ja yksityiskohtaisuuden välille.

7 Tuoteauditoinnit, -sertifioinnit ja viranomaishyväksynnät

Tässä luvussa tarkastellaan Suomessa käytettyjä tuotesertifiointeja ja hyväksyntöjä. Esimerkit vaihtelevat kaupallisten toimijoiden tuotteista viranomaisjärjestelmiin ja viranomaisten tekemiin tuotehyväksyntöihin.

7.1 Tietoturvallisen korttimaksamisen sertifioinnit

Kansainvälistä maksukorttialan turvallisuusstandardia, PCI DSS:ää ylläpitää ja kehittää PCI Security Standards Council. PCI DSS -standardi on viitekehys maksukorttitietojen turvallisuusprosessin kehittämiselle. Maksuturvallisuuden ylläpitämistä vaaditaan kaikilta toimijoilta, jotka varastoivat, käsittelevät tai siirtävät maksukorttitietoja. Standardi määrittää tekniset vaatimukset ja toimintamallit, joita vaaditaan maksukorttitapahtumia vastaanottavilta tai käsitteleviltä yrityksiltä sekä niissä käytettävien sovellusten ja laitteiden ohjelmistokehittäjiltä ja valmistajilta.

PCI Security Standards Council on akkreditoinut vuonna 2006 Nixu Oyj:n myöntämään PCI DSS -sertifikaatteja maksukorttitietoja käsitteleville. Sertifiointiauditointeja on tehty satoja Suomessa ja Ruotsissa ja sertifikaatteja myönnetty kaupan alalle, pankkialalle ja IT-palveluntarjoajille. Tarkat lukumäärät toimialoittain eivät ole julkista tietoa.

Osa PCI DSS -standardin vaatimuksista on jo vanhentunut ja laadittu perinteiseen toimintamalliin, jossa esimerkiksi palvelimet sijaitsevat konesalissa eivätkä pilvipalvelussa. Huoli pilvipalvelujen tarjoajien tietoturvasta on johtanut siihen, että pilvipalveluille on kehitetty viime aikoina omia täydentäviä ohjeistuksiaan.

7.2 Sähköisen tunnistuspalvelun auditoinnit

Liikenne- ja viestintävirasto on julkaissut Määräyksen 72 (M72) sähköisistä tunnistus- ja luottamuspalveluista. Nixu Certification Oy tarjoaa vahvan tunnistuspalvelun tarjoajille tämän määräyksen ja eIDAS-asetuksen edellyttämää vaatimusten mukaisuuden arviointia. Vaatimuskriteeristö on Liikenne- ja viestintäviraston laatima, mutta M72:een liittyvissä ohjeissa 211/2016 ja 215/2016 (Tunnistus- ja luottamuspalveluiden vaatimuksenmukaisuuden arvioinnit) ei ole kuvattu auditointiprosessia. Siksi esimerkiksi auditointimenetelmät ja poikkeamien luokittelu jäävät arviointilaitoksen harkinnan varaan. Vaikka asioita on jätetty auditoijan päätettäväksi, lopullisen tulkinnan hyväksyy tai hylkää Liikenne- ja viestintävirasto.

7.3 Kanta-palveluiden sertifioinnit

Suomi on kärkimaita terveyden ja hyvinvoinnin sähköisessä tiedonhallinnassa. Kansallinen terveysarkisto Kanta on sosiaali- ja terveydenhuollon digitaalisten palvelujen kokonaisuus, jota käyttävät julkisen ja yksityisen terveydenhuollon palveluntuottajat.

Liikenne- ja viestintäviraston hyväksymät arviointilaitokset arvioivat, täyttyvätkö Kanta-järjestelmään kohdistuvat vaatimukset. Vaatimukset liittyvät toiminnallisuuteen, yhteentoimivuuteen ja tietoturvaan. Sertifioinnit koskevat Kanta-palveluihin liittyviä potilastietojärjestelmiä ja niiden välissä olevia Kanta-välityspalveluita.

Sertifioinnissa käytetään Terveyden ja hyvinvoinnin laitoksen THL:n laatimaa kriteeristöä, joka perustuu määräykseen 1/2015: A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset. Vaatimukset koskevat järjestelmän kehittämistä ja ylläpitoa. Sertifiointiauditointi toteutetaan haastattelemalla henkilöstöä ja arvioimalla dokumentaatiota.

Haastateltujen arviointilaitosten edustajien mukaan Kanta-vaatimuksiin tulisi lisätä myös teknisiä testauksia. Tällä hetkellä ne eivät sisällä

esimerkiksi haavoittuvuusskannauksia.

Kanta-palveluihin ei pääse mukaan, jollei toimijalla ole voimassaolevaa sertifikaattia. Sertifiointeja on tehty useita kymmeniä ja niiden määrä näyttäisi olevan hieman vähenemään päin.

7.4 SÄHKE2-sertifioinnit

Arkistolaitoksen määräys SÄHKE2 sisältää vaatimukset ja ominaisuudet sähköisessä muodossa eri tietojärjestelmiin sisältyvien asiakirjatietojen pysyvästä säilyttämisestä. Lisäksi määräyksessä ohjeistetaan tietojärjestelmistä tuotettavan siirtokokonaisuuden muodostamisesta.

Tietojärjestelmätoimittaja voi hakea SÄHKE2-sertifikaattia tietojärjestelmätuotteelleen, joka täyttää SÄHKE2-normin vaatimukset. Sertifiointikriteerit ovat nähtävillä Kansallisarkiston verkkosivuilla.

SÄHKE2-sertifikaatti on haettavissa erikseen

- eAMS-tietojärjestelmälle (tiedonohjausjärjestelmä)
- operatiiviselle tietojärjestelmälle (asianhallintajärjestelmä)
- säilytysjärjestelmälle.

Jokaiselle järjestelmätyypille on omat sertifiointivaatimuksensa. Inspecta Sertifiointi Oy (nyk. Kiwa Inspecta) on myöntänyt noin 10:lle eri ohjelmistoyrityksen tuotteelle SÄHKE2-sertifikaatin. Markkina on pienehkö ja koskee niitä yrityksiä, jotka toimittavat tietojärjestelmiä valtionhallintoon. Kun tiedonhallintalaki uudistuu, velvoittavuus voi laajentua terveydenhuoltoon ja kuntasektorille, jolloin SÄHKE2-sertifiointien määrä voi taas lisääntyä.

7.5 Salaustuotteiden viranomaisarvioinnit ja -hyväksynnät

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen NCSA-toiminto (National Communications Security Authority) on osa Suomen turvallisuusviranomaisorganisaatiota. NCSA:n lakisääteisiin tehtäviin kuuluvat muiden muassa julkishallinnon käyttämien salaustuotteiden hyväksyntä turvaluokitellun tiedon suojaamiseksi ja turvaluokiteltua tietoa käsittelevien tietojärjestelmien hyväksyntä. Velvoitteen voimassaolon lisäehto on kuitenkin se, että kyseinen julkishallinnon organisaatio tai yritys suojaa tietoa, joka kuuluu kansainvälisten tietoturvavelvoitteiden piiriin. Hyväksynnän kohteena oleva salaustuote on fyysinen tuote tai ohjelmisto, joka käyttää kryptologisia algoritmeja.

Arviointiprosessi

Salaustuotteen arviointi- ja hyväksyntäprosessi käynnistyy salaustuotteen valmistajan, eli hyväksynnän tilaajan, yhteydenotolla ja tietojen toimittamisella Liikenne- ja viestintävirastoon, jossa laaditaan arviointisuunnitelma (mm. työmäärä, aikataulu, hinta, resurssit, arvioinnin kriteerit). Eri tuotetyypeille on omat vaatimuksensa. Osa kriteeristöistä on julkisia. Esimerkiksi ohje Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset suojaustasot on saatavilla Liikenne- ja viestintäviraston verkkosivuilla. Vaatimukset on laadittu ulkoministeriön asettamassa Liikenne- ja viestintäviraston kryptotyöryhmässä, jossa on jäseniä myös muista valtion organisaatioista sekä yliopistoista.

Joissakin EU-maissa yksi organisaatio laatii vaatimukset ja toinen toteuttaa hyväksynnät, mutta Suomessa molemmat tehtävät kuuluvat Liikenne- ja viestintävirastolle. Vaatimukset pyritään laatimaan yksiselitteisiksi ja ymmärrettäviksi. Niiden tulee myös kattaa riittävästi eri käyttötapaukset ja uhat.

Ennen arviointisuunnitelman laatimista pidetään esipalaveri, jossa käydään läpi tilaajan dokumentaatio tuotteen toiminnallisuuksista, salaustekniikasta, aikaisemmista arvioinneista, turvallisuusasioista ja viestinnästä. Arviointi voi keskeytyä esipalaveriin, jos havaitaan vaatimuksia koskevia puutteita esimerkiksi dokumentoinnissa. Tällöin tuote palautetaan takaisin tuotekehitykseen.

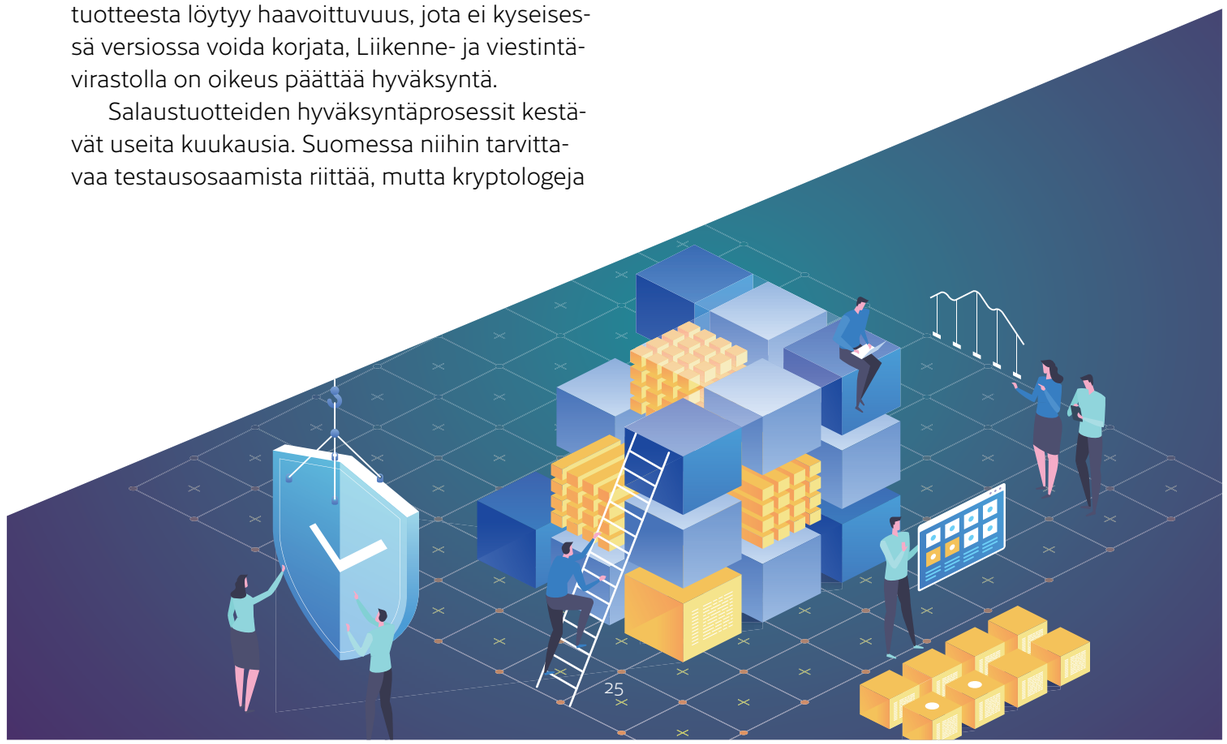
Kun arviointisuunnitelma on hyväksytty, solmitaan arviointisopimus, toteutetaan arviointi yhteistyössä tilaajan kanssa sekä laaditaan siitä loppuraportti ja käyttöpolitiikka. Valmistajalta vaaditaan myös Katakrin mukainen itsearviointi tuotekehitysprosessin suojaamisesta.

Hyväksynnän voimassaolo ja uusinta

Hyväksytyn tuotteen uusia ohjelmistoversioita ei hyväksytä automaattisesti. Kun tuotteen turvallisuuteen vaikuttavia ominaisuuksia päivitetään, hyväksyntä pitää uusia. Muuten tuote poistetaan hyväksyttyjen listalta. Valmistajat voivat tästä syystä jopa vältellä ohjelmistopäivityksiä. Joskus versio muuttuu kuitenkin niin vähän, että vanha hyväksyntä voidaan yhä katsoa päteväksi. Jos tuotteesta löytyy haavoittuvuus, jota ei kyseisessä versiossa voida korjata, Liikenne- ja viestintävirastolla on oikeus päättää hyväksyntä.

Salaustuotteiden hyväksyntäprosessit kestävät useita kuukausia. Suomessa niihin tarvittavaa testausosaamista riittää, mutta kryptologeja on saatavilla vähemmän. Kryptologia on koko EU:n alueella vain harvojen hallitsema osaamisalue, mikä huolestuttaa alan toimijoita. Koska koko tulevaisuuden tietoyhteiskunta tarvitsee kipeästi matematiikan osaajia, selvityksessä haastateltujen mielestä nuoria tulisi kannustaa aktiivisesti matematiikan opintoihin.

Salaustuotteiden hyväksynnät alkoivat Viestintävirastossa vuonna 2015. Vuodesta 2019 alkaen hyväksyntätyötä on tehty Liikenne- ja viestintäviraston voimin. Tulevaisuudessa toiminnan lisäresursoinnille ja osaamisen kehittämiselle vaikuttaa olevan tarvetta. Tietoturvatietoisuus on lisääntynyt ja arviointipyyntöjä tulee runsaasti, myös sellaisille salaustuotteille, joista virastolla ei ole aiempaa kokemusta (esimerkiksi Googlen Go-ohjelmointikielellä toteutettuja ohjelmistoja). Jos Liikenne- ja viestintävirastoa haetaan tulevaisuudessa EU:n toisen tason hyväksymisviranomaiseksi, se tulee tarvitsemaan lisäresursseja myös tähän toimintaan.



III OSA

8 Tietoturvallisuuden standardoinnin ja sertifioinnin tulevaisuudennäkymiä

Tässä luvussa käydään läpi aiemmin kuvattujen standardien ja sertifiointien kehityssuuntia sekä niihin vaikuttavia tekijöitä. Lopuksi tehdään yhteenveto ja pohditaan jatkotoimenpiteitä.

8.1 Hallintajärjestelmäsertifiointien määrän kehitys

ISO (the International Organization for Standardization) julkaisee vuosittain tilastotiedot hallintajärjestelmäsertifikaattien eli johtamisen standardien pohjalta tehtyjen sertifiointien määristä. Tiedot on kerätty ISOn jäsenmaiden akkreditoiduilta sertifiointielimiltä. Uusimman tilaston perusteella havaitaan, että standardien ja sertifiointien määrä jatkaa kasvuaan.

Suomessa ISO/IEC 27001 standardin vaatimusten mukaisia sertifiointeja oli vuoden 2017 lopussa 72 kappaletta, missä on kasvua edellisvuodesta 33 %. Maailmanlaajuisesti sertifikaatteja oli 39 501 kappaletta ja kasvua edellisvuodesta 19 %. Vaikka kansallisella tasolla absoluuttiset lukumäärät ovatkin edelleen pieniä, on kehitys merkittävää.

Suomessa eniten ISO/IEC 27001 -sertifikaatteja on ICT-alan yrityksissä, mutta myös julkishallinto on tullut vahvasti mukaan (esimerkiksi Väestörekisterikeskus, Maanmittauslaitos, Maaseutuvirasto, Valtorin TUVE-yksikkö, ELY-keskusten maataloustukien maksatus- ja valvontatoiminta).

Taulukko 2. ISO/IEC 27001-sertifikaattien kehitys Suomessa ja maailmalla.
Lähde: The ISO Survey of Management System Standard Certifications (2018).

	2006 2012	2007 2013	2008 2014	2009 2015	2010 2016	2011 2017
Suomi	1 28	14 32	13 33	18 44	23 54	27 72
Eurooppa	1 064 6 379	1 432 7 952	2 172 8 663	3 563 10 446	4 800 12 532	5 289 14 605
Maailma	5 797 18 920	7 732 21 604	9 246 23 005	12 935 27 536	15 178 33 290	16 800 39 501

Euroopassa Iso-Britannia erottuu selvästi muista suurella sertifikaattien määrällä (4503 sertifikaattia vuonna 2017, mikä on noin kolmannes kaikista Euroopan ISO/IEC 20071 -sertifikaateista). Tämä johtunee standardoinnin vahvasta asemasta maassa, minkä lisäksi monet ISO-standardit myös pohjautuvat brittiläisiin kansallisiin standardeihin. Sertifikaattien suurta määrää selittää todennäköisesti myös vahva pankkisektori: lähes kaikkien Euroopan suurten pankkien pääkonttori sijaitsee Lontoossa, ja tietoturvallisuuden hallinta korostuu tällä toimialalla. Isossa-Britanniassa käytännössä jokaisen yrityksen, joka haluaa toimia valtionhallinnon kanssa, tulee osoittaa vaatimuksenmukaisuus sertifikaatilla. Britannian jälkeen seuraavaksi suurin määrä ISO/IEC 27001 -sertifiointeja Euroopassa on Saksassa.

8.2 Julkishallinnon ohjekokonaisuuksien tulevaisuus

Uuteen tiedonhallintalakiin on keskitetty julkisen hallinnon tiedonhallintaa koskevat säädökset. Tietohallintolaki, arkistolaki, julkisuuslaki 18 §, julkisuusasetus, tietoturva-asetus ja laki sähköisestä asioinnista viranomaistoiminnassa 13 §, 21 §, 22 § yhdistyivät yhdeksi tiedonhallintalaiksi.

Uusia tietoturvallisuusvaatimuksia tulkitsevan ohjekokonaisuuden VAHTI 100:n viestintään aiotaan kiinnittää erityistä huomiota väärinymmärrysten välttämiseksi ja tulkinnan yhtenäistämiseksi. Ohjekokonaisuudesta tullaan käyttämään yleisnimitystä informaatio-ohjauksen tuki. Sama malli on otettavissa käyttöön tukemaan myös tietosuoja-asetuksen tulkintaa.

8.3 Tuotesertifioinnin tulevaisuus

EU:n kyberturvallisuusasetus astui voimaan kesäkuussa 2019 ja tulee lisäämään tietoturvasertifiointien määrää Euroopassa. Tällöin myös kuluttajalaitteet voivat tulla arvioinnin ja hyväksynnän piiriin, vaikka alustavassa suunnitelmassa sertifioinnit ja hyväksynnät ovatkin vapaaehtoisia. Tämä asettaa haasteita sertifioinnin järjestämiselle, sillä kuluttajalaitteiden kirjo on valtava ja internetiin liitetyt laitteet tulevat yleistymään kodeissa ja toimistoissa merkittävästi: arvioiden mukaan niiden määrä on kymmeniä miljardeja EU:n alueella vuoteen 2020 mennessä.

Kuluttajilla on oikeus luottaa siihen, että verkkoon liitettävät laitteet ja digitaaliset palvelut ovat luotettavia ja tietoturvallisia. EU:n kuluttajayhteisöissä on käyty keskustelua siitä, tulisiko kuluttajatuotteiden tietoturvallisuushyväksynnän olla vapaaehtoinen vai pakollinen. Esimerkiksi sähkölaitteiden ja lelujen CE-merkinnän käytöstä on havaittu, että keskivertokuluttaja ei juuri kiinnitä huomiota siihen, onko hänen ostamassaan tuotteessa CE-merkintä vai ei. On arvioitu, että tietoturvamerkintä ei kiinnittäisi suurempaa huomiota. On myös mietitty hinnan vaikutusta ostopäätökseen, jos tietoturvamerkitty kuluttajatuote on kalliimpi kuin merkitsemätön. Yhdeksi, melko radikaaliksi, ratkaisuksi on jopa ehdotettu, että kaikkiin kuluttajille suunnattuihin digilaitteisiin tulisi liittää merkintä ”unsecured”, jolloin merkinnän puuttuminen kertoisi kuluttajalle sen olevan tietoturvallinen.

Useimmat tuotesertifioinnit perustuvat lain vaatimuksiin. Kriittisen infrastruktuurin tuottajilta, esimerkiksi tietoliikenteen ja pankkiliikenteen toimijoilta, edellytetään teknisten ratkaisujen hyväksyttämistä puolueettomalla viranomaisella. Kustannuskysymykset voivat nousta esille, jos myös kuluttajatuotteet tulevat arvioinnin ja hyväksynnän piiriin. Kuluttajatuotteissa olisi perusteltua, että tuotteen valmistajalta edellytettäisiin vakuutusta EU-tasoisten tietoturvavaatimusten täyttymisestä ja määrättäisiin sanktioita mahdollisista tietoturvatapahtumista.

Selvityksessä haastateltujen toimijoiden mielestä viranomaisten (esimerkiksi Suomessa Liikenne- ja viestintäviraston) ei tulisi sertifioida kuluttajatuotteita, vaan eniten kannatusta saa selkeään ja yksinkertaiseen vaatimuskokonaisuuteen perustuva itsearviointi. Näin tuote saisi tietoturvamerkinnän valmistajan vakuuttaessa vaatimusten täyttyvän. Jos tietoturvaongelmia ilmenisi, niiden seurauksena olisi sanktio tuotteen valmistajalle. Kyseistä vaatimuslistaa voisi ylläpitää esimerkiksi EU:n verkko- ja tietoturvavirasto ENISA. Toisaalta Liikenne- ja viestintäviraston kuluttajatutkimuksissa on havaittu, että kuluttajat kokevat sertifioinnin tai erilaisten merkkien uskottavuuden kannalta olennaisena sen, että ne myöntää luotettava taho kuten viranomainen.

8.4 Tietosuojavaatimusten sertifiointi

Toukokuussa 2018 sovellettavaksi tullut EU:n yleinen tietosuoja-asetus 2016/679 (General Data Protection Regulation, GDPR) toi rekisterinpitäjille ja henkilötietojen käsittelijöille uusia velvoitteita ja vastuita. Muutos on sitonut monen organisaation kehitysresursseja parin viime vuoden ajan. Tämä on mahdollisesti viivästyttänyt muuta tietoturvallisuuteen liittyvää kehitystyötä ja sertifiointihankkeita. Vähitellen on nähtävissä, että kaikkein vilkkain vaihe GDPR:n soveltamissa alkaa laantua. Tämä jättää enemmän aikaa ja resursseja tulevaisuudessa myös muulle tietoturvatyölle ja sertifioinneille.

Ajan mittaan nähdään myös, tuleeko markkinoille erillisiä GDPR-arviointeja ja -sertifiointeja. Selvityksessä haastatellut arviointilaitokset ovat valmistautuneet tähänkin tulevaisuudennäkymään. ISOn ja IEC:n tekninen tietoturvallisuuden standardointikomitea on vastikään julkaissut standardin ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, jota voidaan käyttää arvioitaessa GDPR-vaatimustenmukaisuutta. Sertifikaatti myönnettäisiin siis standardin vaatimuksia vasten, ei tietosuoja-asetuksen. Lain vaatimuksia vasten ei voi sertifioitua, mutta laissa voidaan viitata vaatimusstandardiin, jota vasten sertifikaatti voidaan myöntää.

8.5 Kuluttajavalistus tietoturvallisuussertifioinnin tukena

Vaikka valmistaja noudattaisi hyviä tietoturvakäytäntöjä, se ei estä käyttäjää toimimasta harkitsemattomasti ja huolimattomasti. Tämän vuoksi viranomaisten salaustuotteiden hyväksynnöissä laaditaan käyttöpolitiikka hyväksynnän saaneille tuotteille. Käyttöpolitiikkaa olisi hyvä harkita myös kuluttajatuotteisiin: niihin tulisi liittää mukaan tuotteen pääasiallinen käyttötarkoitus, ja halutessaan kuluttaja voisi kytkeä tuotteen älykkäät ominaisuudet pois päältä. Esimerkiksi voidaan ottaa jääkaappi, jonka ensisijainen käyttötarkoitus on pitää elintarvikkeet viileinä, mutta joka voidaan myös liittää internetiin. Teollisuudessa ja ammattikäytössä vastaavaa käyttöpolitiikkaa ei katsota tarvittavan yhtä paljon, koska ostajan oletetaan tuntevan keskivertokuluttajaa paremmin tuotteen pääasiallinen käyttötarkoitus.

8.6 Kansallisen tietoturvaosaamisen varmistaminen

Suomessa tietoturvallisuusteollisuus koostuu pienistä ja keskisuurista yrityksistä. Omavaraisuus on noussut, mutta toisaalta suomalaista osaamista ja teknologiaa on ostettu myös ulkomaille, esimerkiksi palomuuriohjelmistaan tunnettu Stonesoft Oyj myytiin yhdysvaltaiselle McAfeelle, joka nimettiin Intel Securityksi ja myytiin edelleen asevalmistaja Raytheon-Websenselle.

Yrityskaupat tapahtuvat usein nopeasti, eikä Suomen valtio ole ehtinyt niihin aina väliin. Suomalaisen osaamisen häviämiseen ulkomaille on kuitenkin havahduttu ja valtio on ostanut mm. sähköpostin salausjärjestelmiä tekevän Deltagon Group Oy:n. Muutospyrkimyksiin omistussuhteissa on myös jatkossa hyvä varautua reagoimaan nopeasti kansallisen korkean osaamistason säilyttämiseksi ja kasvattamiseksi.

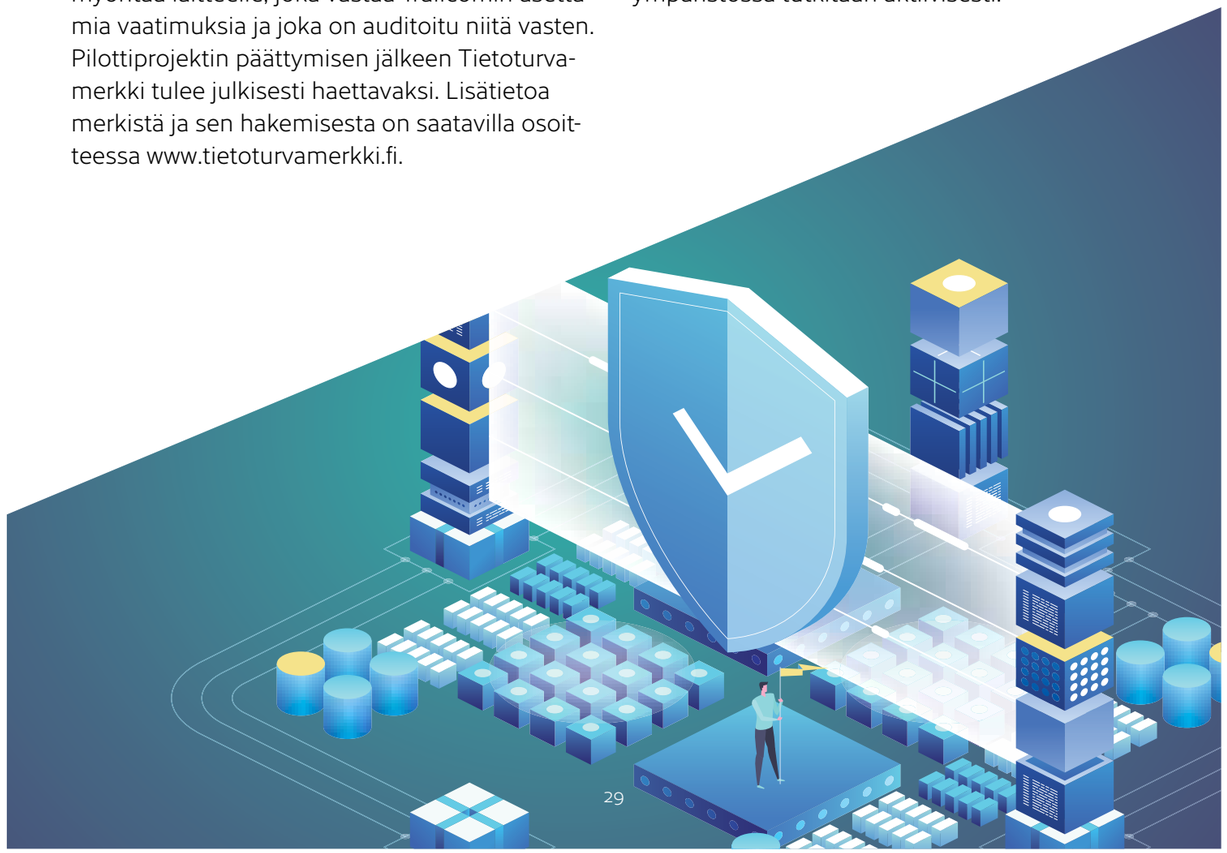
8.7 Traficomin tietoturvallisuuden arvioinnin kehitystyö

Traficomin Kyberturvallisuuskeskus kehitti vuonna 2019 kaksi uutta tapaa tietoturvallisten ratkaisujen tukemiseksi: Pilvipalvelujen turvallisuuskriteeristön (PiTuKri) ja Tietoturvamerkin IoT-kuluttajalaitteille.

PiTuKri on tarkoitettu työkaluksi pilvipalvelujen turvallisuuden arviointiin. Sen tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa. PiTuKri kokoaa pilvipalvelujen turvallisuuteen vaikuttavia hyviä käytäntöjä myös kaupallisten toimijoiden hyödynnettäviksi. Lisäksi kriteeristö sisältää tulkintoja ja ohjeistuksia pilvipalveluihin liittyvien riskien arviointiin. Tulemme julkaisemaan PiTuKrista myös pk-yritysten ja kansalaisten tarpeisiin vastaava version.

Tietoturvamerkki on Traficomin kehittämä tapa auttaa kuluttajaa tunnistamaan ja hankkimaan tietoturvallisia IoT-laitteita. Merkki voidaan myöntää laitteelle, joka vastaa Traficomin asettamia vaatimuksia ja joka on auditoitu niitä vasten. Pilottiprojektin päättymisen jälkeen Tietoturvamerkki tulee julkisesti haettavaksi. Lisätietoa merkistä ja sen hakemisesta on saatavilla osoitteessa www.tietoturvamerkki.fi.

PiTuKri ja Tietoturvamerkki ovat syntyneet vastauksena tarpeeseen arvioida uuden teknologian tietoturvallisuutta. Teknologia etenee tällä hetkellä nopeammin kuin kansainvälinen normittamistyö, minkä vuoksi valmiita kansainvälisiä standardeja ei ole saatavilla. Kehittämistyössä olemme kuitenkin huomioineet aihepiirin keskeisiksi tunnistetut jo olemassa olevat kansainväliset standardit. Uudet vaatimukset on myös haluttu harmonisoida kansainvälisten standardien kanssa parhaalla mahdollisella tavalla. Näin haluamme edistää kansainvälistä yhteentoimivuutta ja tukea suomalaisten toimijoiden siirtymistä kansainvälisille markkinoille. Sekä PiTuKri että Tietoturvamerkki ovat herättäneet myös kansainvälistä kiinnostusta. Niiden hyödyntämismahdollisuuksia kansainvälisessä ympäristössä tutkitaan aktiivisesti.



Yhteenveto

Tulevaisuudessa liikeyritysten ja yhteiskunnan toimintaympäristö monimutkaistuu entisestään: digitaaliset palvelut lisääntyvät, lait uudistuvat ja tietoturvallisuushyökkäysten uhka kasvaa. Enää ei riitä, että organisaation oma toiminta on kunnossa, vaan koko ekosysteemin tietoturvallisuutta on hallittava. Jotta monimutkaisten ja toisiinsa kietoutuvien teknologisten toteutusten tietoturvallisuudesta voidaan varmistua, niille pitää määritellä yhtenäiset vaatimukset ja tulkinnat niistä - toisin sanoen luoda standardit. Niitä tarvitaan, sillä yhdelläkään toimijalla ei ole jatkossa mahdollisuutta varmistua omakohtaisesti kaikkien sidosryhmiensä ja mahdollisten alihankkijoidensa verkostojen tietoturvallisuudesta.

Yksi suurimmista muutoksen ajureista, esineiden internet (IoT), on jo todellisuutta ja arvioiden mukaan vuoteen 2020 mennessä siihen on kytkettynä kymmeniä miljardeja digilaitteita yksin EU:ssa. IoT-laitteiden ja -järjestelmien tietoturvan puutteita pidetään yleisesti vakavana ongelmana.

Vaikka tietoturvallisuutta lähestytään usein uhkien näkökulmasta, se voidaan nähdä myös positiivisessa valossa: Laadukkaat tietoturvatoteutukset antavat mahdollisuuden nauttia uusien teknologioiden tuottamista hyödyistä huoletta.

Tietoturvallisuuden standardointi ja sertifiointi ovat yksi keskeisiä luottamuksen rakentamisen keinoja digitalisoituvassa ja verkottuvassa maailmassa. Niillä ei kuitenkaan ole itseisarvoa, vaan käyttö on aina suhteutettava käyttökohteeseen ja sen vaatimuksiin. Lisäksi on otettava huomioon sertifioinneista aiheutuva kustannus ja niistä saatava kokonaishyöty.

Suomella on teknologisen osaamisensa ja maineensa ansiosta erinomaiset edellytykset olla luomassa digitaalista luottamusta. Parhaimmillaan tietoturvallisuuden standardointi ja sertifiointi antavat mahdollisuuden uusien teknologioiden hyödyntämiseen ja kansallisen kilpailuedun luomiseen. Tämä edellyttää strategista näkemystä ja sen suunnitelmallista toteutusta. Käytännössä siis riittävää resursointia ja aktiivista vaikuttamista vaatimusstandardeihin sekä muuttuviin lakikokonaisuuksiin.

Lähteet

Lait, asetukset ja määräykset

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010, Finlex

EU:n yleinen tietosuoja-asetus 679/2016

EU:n maksupalveludirektiivi Payment Services Directive (PSD2)

Viestintäviraston määräys 72A/2018 sähköisistä tunnistus- ja uottamuspalveluista, 21.5.2018

Terveyden ja hyvinvoinnin laitoksen määräys 1/2015: A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 1406/2011, Finlex

EU:n neuvoston päätös turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi, 2013/488/EU

Standardit

ISO/IEC 27001:2013 Informaatioteknologia -- Turvallisuustekniikat -- Tietoturvallisuuden hallintajärjestelmä -- Vaatimukset / Information technology -- Security techniques -- Information security management systems -- Requirements

ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

SFS-EN ISO 22301:2014 Yhteiskunnan turvallisuus -- Liiketoiminnan jatkuvuuden hallintajärjestelmät -- Vaatimukset
ISO/IEC 20000-1:2018 Information technology -- Service management -- Part 1: Service management system requirements

ISO/IEC DIS 27552 Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines (DIS-versio Draft International Standard, ei hyväksytty)

ISO 31000:2018 Riskienhallinta

PCI DSS Payment Card Industry Data Security Standard, V3.2.1 May 2018

Haastattelut

Johtava asiantuntija Varpu Rantanen, Turvallisuus- ja kemikaalivirasto Tukesin FINAS-akkreditointipalvelu, 23.10.2018

Toimitusjohtaja Susanna Antikainen, Fysio Center Jyväskylä Oy, 25.10.2018

Konsultti, tietoturva-auditoija Arto Kangas, Netum Oy, 25.10.2018

Toimitusjohtaja Niki Klaus, Nixu Certification Oy, 26.10.2018

Liiketoimintavastaava Jarno Lötjönen, kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus Jyväskylä Security Technology (JYVSECTEC), 26.10.2018

Tietoturva-asiantuntija Päivö Lappalainen, ELY-keskusten tietohallintoyksikkö, 30.10.2018

Johtava asiantuntija Kirsi Janhunen, Väestörekisterikeskus, 31.10.2018

Advisory Senior Manager Olli Knuuti, KPMG IT Sertifiointi Oy, 1.11.2018

Tuotepäällikkö, pääarvioija Jyrki Lahnalahti, Inspecta Sertifiointi Oy, 2.11.2018

Asiantuntija Tuukka Laava, kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus Jyväskylä Security Technology (JYVSECTEC), 2.11.2018 ja 7.11.2018

Erityisasiantuntija Risto Hakala ja johtava tarkastaja Aki Tauriainen, Viestintävirasto, Kyberturvallisuuskeskus, 6.11.2018

IT Security Manager Ossi Luoma, Vaisala Oy, 7.11.2018

Teknologiajohtaja Mikko Viitaila, Microsoft Oy, 12.11.2018

Vice President Jorma Mellin, SSH Communications Security Corporation, 13.11.2018

Sähköiset lähteet

Johtamisen standardien käyttö kasvaa.
Suomen Standardisoimisliitto SFS ry:n artikkeli 12.9.2018.
https://www.sfs.fi/ajankohtaista/artikkelit

Standardit luovat kasvua ja auttavat yrityksiä menestymään.
Suomen Standardisoimisliitto SFS ry:n artikkeli 2018.
https://www.sfs.fi/ajankohtaista/artikkelit

The ISO Survey of Management System Standard Certifications.
ISO/IEC 27001 - Information Technology - Security Techniques - Information Security Management Systems – Requirements.
Data from 2006 to 2017. https://www.iso.org/the-iso-survey.html

Tilastokeskus, Yritysrekisteri.
https://www.stat.fi/tup/yritysrekisteri/index.html

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010

Katakri 2015. Tietoturvallisuuden auditointityökalu viranomaisille.
Puolustusministeriö, 26.3.2015

Arto Salonen: ISO/IEC 27001 -standardi ja tietoturvallisuuteen sitoutuminen. Opinnäytetyö Laurea ammattikorkeakoulu, 2016

Tietoturva sai uuden mittarin – suomalainen sertifikaatti osoittaa tason. Tivin artikkeli 9.5.2017.
https://www.tivi.fi/Kaikki_uutiset/tietoturva-sai-uuden-mittarin-suomalainen-sertifikaatti-osoittaa-tason-6647469

Cyber Essentials, National Cyber Security Centre.
https://www.cyberessentials.ncsc.gov.uk/

Viestintäviraston suorittamat salaustuotearvioinnit ja -hyväksynnät, Dnro: 1487/651/2017

Viestintäviraston ohje arviointikriteeristöjen tulkinnasta / Kansalliset arvioinnit, 2015

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
PL 320, 00059 TRAFICOM
p. 029 534 5000

traficom.fi

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus