Opinnäytetyö (AMK)

Tieto- ja viestintätekniikan koulutus

2020

Jere Kalliomäki

TIETOTURVAKARTOITUS PK-YRITYKSELLE

- case Jimm’s PC-Store Oy

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikan koulutus

Kevät 2020 | 40 sivua, 14 liitesivua

Jere Kalliomäki

TIETOTURVAKARTOITUS PK-YRITYKSELLE

- case Jimm’s PC-Store Oy

Digitalisaation mukanaan tuomat innovaatiot, kerätyn tiedon määrän kasvu ja tiedon kehittyneet käyttämisen mallit ovat tuoneet mukanaan myös uusia uhkia, minkä takia tietoturvatyöskentelyn on täytynyt kehittyä sen mukana. Lisäksi myös uudet asetukset ja lainsäädäntö ohjaavat tietoturvallisuuden toteuttamista.

Opinnäytetyön tavoitteena oli tehdä toimeksiantajalle tietoturvakartoitus ja laatia sen pohjalta raportti yrityksen omaan käyttöön. Tietoturvakartoituksen avulla saadaan selville yrityksen tämän hetkinen tietoturvan taso ja havaitaan mahdolliset puutteet, joiden perusteella voidaan tehdä kehitysehdotuksia yrityksen tietoturvallisuuden kehittämiseksi ja havaittujen puutteiden korjaamiseksi.

Tämän opinnäytetyön tarkoituksena oli perehtyä tietoturvallisuuteen, sen tärkeyteen sekä siihen, mistä se koostuu. Lisäksi tutkittiin tietoturvallisuutta ohjaavia tekijöitä sekä tietoturvakartoitukseen liittyviä prosesseja ja menetelmiä. Siinä käytiin läpi tietoturvallisuuden termistöä ja periaatteita, jonka jälkeen opittua tietoa hyödynnettiin toimeksiantajan kanssa sovitun työn toteuttamiseksi.

ASIASANAT:

tietoturva, tietoturvakartoitus, tietosuoja, luottamuksellisuus, riskienhallinta

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and communications technology

2020 | 40 pages, 14 appendix

Jere Kalliomäki

INFORMATION SECURITY ASSESSMENT FOR A BUSINESS

- case Jimm’s PC-Store Oy

The innovations brought about by digitalization, the increase in the amount of information collected and the advanced use cases of information have also brought new threats with them. The information security work has had to evolve too because of this. In addition, new regulations and legislation guide the implementation of information security.

The goal of this thesis was to create an information security assessment for the client, and to compose a report based on the results for the organization’s own use. The security assessment helps determine the company’s current level of information security along with possible weaknesses. Improvements to the information security and to clear the found weaknesses are made based on the gained results.

The purpose of this thesis was tot get acquainted with information security, its importance and what is consists of. In addition, the factors guiding information security and the processes and methods related to information security mapping were studied. It reviewed the terminology and principles of information security, after which the information accumulated was utilized to carry out the work agreed with the client.

KEYWORDS:

Information security, information security assessment, data protection, confidentiality, risk management

SISÄLTÖ

LIITTEET

KUVAT

KUVIOT

SANASTO

CIA triad	Tietoturvallisuuden kolme tavoitetta: luottamuksellisuus, eheys ja saatavuus (engl. Confidentiality, Integrity and Availability)
DDoS	hajautettu palvelunestohyökkäys (engl. Distributed Denial of Service)
DoS	palvelunestohyökkäys (engl. Denial of Service)
Katakri	Kansallinen turvallisuusauditointikriteeristö
PDCA	PDCA-sykli: suunnittele, toteuta, arvio ja toimi (engl. Plan, Do, Check, Act) on ongelman ratkaisumalli ja kehittämismenetelmä.
SaaS	SaaS-palvelulla tarkoitetaan pilvessä sijaitsevaa ohjelmistoa, jota ylläpidetään palveluntarjoajan toimesta (engl. Software as a Service)
SLA	Palvelutasosopimus on asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot. (engl. Service Level Agreement)
Tietoturva	Tietoturvallisuuden synonyymi, erityisesti yhdyssanoissa käytettävä termi
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä

1 JOHDANTO

Maailma elää suurta digitalisoitumisen aikakautta ICT-teknologian kehittyessä nopeammin kuin koskaan. Tämän kehityksen keskiössä ovat tietokoneet, tietoliikenne ja internet sekä näihin liittyvät uudet innovaatiot. Näiden kehitys vaikuttaa niin yksilöiden kuin myös organisaatioiden toiminta- ja käyttäytymismalleihin liittyen tiedon käyttämiseen, liikuttamiseen sekä jalostamiseen. Digitalisaation aikakausi ja ICT-teknologian kehitys aiheuttavat tiedon määrän räjähdysmäisen kasvun sekä sen, että tietoa on käytettävissä aina vain enemmän. Tiedon määrän kasvu tuo mukanaan sekä mahdollisuuksia että uhkia. Yritysten omista palvelimista ja itse tuotetuista palveluista on siirrytty ulkoisen toimijan tarjoamiin kokonaisratkaisuihin (SaaS), joiden lisäksi myös pilvipalveluiden käyttäminen on yleistynyt merkittävästi. Digitalisoituminen sekä teknologian kehittyminen kiinnostavat myös rikollisia tahoja, ja verkkorikollisuus sen eri muodoissa onkin yleistymässä. Edellä mainituista syistä tietoturvallisuudesta onkin tullut keskeinen, kaikkien toimintaan vaikuttava osa-alue. Digitalisaation takia myös tietoturvatyö on muuttunut ja on tuleva muuttumaan. Siinä missä aikaisemmin on suojattu eniten verkkoja, suojataan nykyään laitteita ja tulevaisuudessa pyrittäneen suojaamaan itse tietoa.

Tietoturvallisuuden toteutuminen eri yritysten välillä vaihtelee. Valtaosassa isoista organisaatioista on selkeät ajantasaiset toimintamallit, ohjeistukset sekä standardit tietoturvan toteuttamiselle liiketoiminnan jatkuvuuden varmistamiseksi. Sen sijaan pienissä sekä keskisuurissa yrityksissä tilanne saattaa olla täysin toinen. EU:n asettamat tietosuoja-asetukset sekä tietoriskien välttämiseen liittyvät ohjeistukset koskevat kuitenkin kaikkia yrityksen koosta ja liikevaihdosta riippumatta.

Opinnäytetyön tavoitteena on luoda toimeksiantajalle tietoturvakartoitus, jonka tulokset myös raportoidaan. Tietoturvakartoituksen toteuttamiseksi perehdytään ensin tietoturvaan, sen perusteisiin, sitä sääteleviin lakeihin sekä ohjeistuksiin. Lisäksi tutustutaan tietoturvakartoituksen työkaluihin, joista valitaan käyttötarkoitusta varten sopivin. Valitulla työkalulla luodaan tietoturvakartoituksen kysymykset toimeksiantajan vastattavaksi. Tämän jälkeen vastaukset analysoidaan, ja niiden perusteella laaditaan raportti yrityksen tietoturvan tasosta. Tietoturvakartoituksen tulokset ja raportti jätetään työstä pois salassapidettävänä materiaalina.

Opinnäytetyön toimeksiantaja on vuodesta 2001 tietotekniikan alalla toiminut Jimm’s PC-Store Oy. Yritys on asiantuntevaa palvelua tarjoava tietotekniikan, komponenttien ja

viihde-elektroniikan verkkokauppa. Yrityksen toimipiste sijaitsee Turussa ja se työllistää tällä hetkellä noin 50 henkilöä. Yritys tarjoaa myös mahdollisuuden asioida noutopalvelumyymälässä Turussa (Jimm's PC-Store -verkkosivut). Toimeksiantajalle on aikoinaan tehty tietoturvakartoitus, mutta tästä on kulunut jo aikaa. Tämän jälkeen yrityksen toiminta on kasvanut huomattavasti entisestä, minkä lisäksi se on myös kokenut suuren organisaatiomuutoksen. Opinnäytetyön avulla yritys saa tietoa tämänhetkisestä tietoturvan tilastaan. Toimeksiantajan toiveena olisi myös julkaista kartoituksen pohjalta laadittu tietoturvaraportti yrityksen sisäiseen jakeluun.

Opinnäytetyön julkaistu osa on hyvin teoriapainoitteinen, koska kaikki yritysspesifinen tieto on jätetty työstä pois salassapidettävänä materiaalina. Työ on jaoteltu siten, että luvussa 2 tutustutaan tietoturvallisuuteen käsitteenä sen periaatteet huomioon ottaen. Lisäksi tuodaan ajankohtaisena aiheena esille covid-19 pandemian vaikutukset saatavuuteen. Luvussa 3 käsitellään yksitellen kaikki tietoturvallisuuden osa-alueet, luvussa 4 käydään läpi tietosuojaa ja siihen liittyviä lakeja ja säädöksiä, luvussa 5 tarkastellaan mitkä asiat ohjaavat tietoturvallisuutta, luvussa 6 määritellään tietoturvakartoituksen ja siihen oleellisesti kytköksissä olevan riskienhallinnan prosessit, ja lopulta luvussa 7 käydään läpi itse tietoturvakartoituksen prosessia valitun työkalun (Katakri) teoriaan pohjautuen. Luvussa 8 pohditaan työn aikana saavutettuja tuloksia ja tavoitteiden toteutumista.

2 TIETOTURVALLISUUS KÄSITTEENÄ

Tietoturvallisuus on hyvin laaja aihe, josta on saatavilla valtavasti tietoa kirjallisuuden, ohjeiden, artikkeleiden, standardien sekä lakien muodossa (Andreasson & Koivisto 2013, 17). Kyberturvallisuuden sanaston mukaan tietoturvallisuus ja -turva muodostuu järjestelyistä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Lisäksi myös oloilla, joissa tietoturvariskit ovat hallinnassa, voidaan viitata tietoturvallisuuteen ja tietoturvaan. Keinoja tietoturvariskien hallintaan saamiseksi on valtavasti. Tämä onnistuu esimerkiksi kulunvalvonnan, tilojen lukituksen, asiakirjojen turvallisen säilytyksen ja hävityksen, tietojen salauksen ja varmuuskopioinnin sekä palomuurin, virustorjuntaohjelman ja varmenteiden käytön avulla. (Turvallisuuskomitea 2018, 15.)

Tiedon ja tietojärjestelmien tulisi olla vain niiden käyttöön oikeutettujen tahojen saatavilla siten, että sivullisten ei ole mahdollista käsitellä, muuttaa tai poistaa tietoja. Lisäksi käyttöoikeuden omaavankin tahon on sallittua käyttää tietoja ja järjestelmiä vain työtehtävissään. Haittaohjelmat, laitteisto- tai ohjelmistoviat, asiaton toiminta tai muut vahingot, tapahtumat tai häiriötilanteet eivät saa paljastaa, muuttaa tai tuhota tietoa, järjestelmiä ja palveluita niiden luotettavuuden, eheyden ja ajantasaisuuden takaamiseksi. (VAHTI 4/2013, 17.)

Tietoturvallisuuden toteuttamisessa tulisi pysyä alati kehittyvän teknologian vauhdissa mukana, mikä edellyttää korostetusti menetelmien jatkuvaa seuraamista sekä toimenpiteiden kehittämistä tarpeiden mukaan. Täydellisen turvallisuuden saavuttaminen on lähes mahdotonta saavuttaa, minkä takia tietoturvallisuutta tulisikin toteuttaa toiminnan jatkuvuuden varmistamisen kannalta. (Elinkeinoelämän keskusliitto 2020.)

Tietoturvan kannalta organisaation tulee tunnistaa mitä tietoa se käyttää, miten kyseistä tietoa käytetään ja kuinka tärkeää tieto on organisaatiolle. Tietoturva ei ole projekti vaan se on prosessi, joka uudistuu jatkuvasti teknologian kehittymisen ja digitalisaation etenemisen mukana. Se mikä toimii tänään voi olla huomenna vanhaa. Tietoturvan ammattilaisten tulisikin ohjata muuta organisaatiota toimimaan oikein jatkuvan viestinnän sekä kouluttamisen keinoin. Vain näin organisaatiolle tärkeää tietoa osataan käsitellä sen vaatimalla huolellisuudella. (Andreasson & Koivisto 2013, 11–12.)

2.1 Tietoturvallisuuden tärkeys

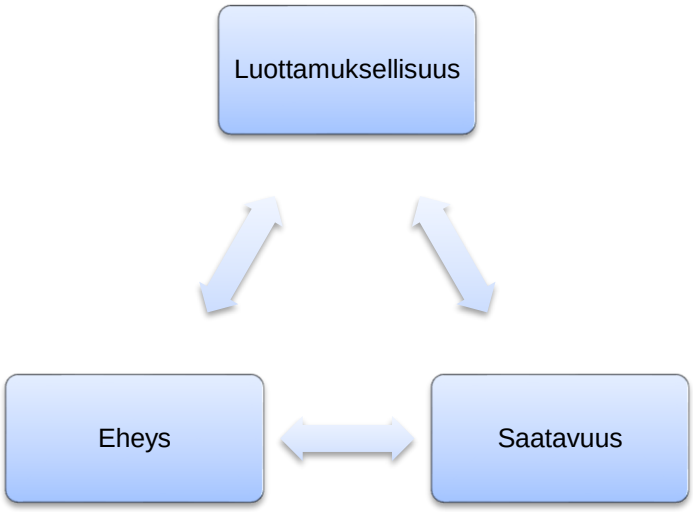
Tietoturvallisuuden tärkeyden käsittämiseksi täytyy ensin miettiä mahdollisia riskejä, joita tietoturvallisuuteen liittyy. Rouskun mukaan riskejä ovat esimerkiksi tietovuoto, yksityisyyden suojan menetys, taloudelliset menetykset ja tietojen menetys. Suomen lait sekä EU velvoittavat huolehtimaan tietoturvallisuudesta, jonka lisäksi myös yhteistyösopimukset muiden organisaatioiden kanssa pakottavat huolehtimaan omien luottamuksellisten tietojen ohella toisen organisaation, kuten toimittajan tai yhteistyötahon sekä asiakkaiden tiedoista. Tietoturvasta tinkiminen voi pahimmillaan aiheuttaa valtavia taloudellisia, aineellisia ja jopa henkilövahinkoja. (Rousku 2014, 73–74.) Tietoturvallisuus voidaan useinkin kokea ylimääräisenä muusta toiminnasta erillisenä toimintona, joka vaikeuttaa tai jopa estää käyttäjän toimintaa. Todellisuudessa sen tulisi kuitenkin vahvistaa yrityksen liiketoimintaa mahdollistamalla ja helpottamalla nykyisen sekä uuden teknologian ja palveluiden käyttämistä. (Järvinen & Rousku 2017, 31–32.)

Hyvin hoidettu organisaation tietoturva luo edellytykset sen kehitykselle mahdolliset riskit halliten. Kaikkien työntekijöiden tulisi olla tietoisia omasta roolistaan sekä käsittelemänsä tiedon merkityksestä organisaatiolle, sillä organisaation tietoturva on yhtä vahva kuin sen heikoin lenkki. Tietoyhteiskunnan kehitys on mahdollistanut runsaan tiedon keräämisen, mahdollisesti jopa tarpeettoman sellaisen. On muistettava, että tiedot voivat myös päätyä vääriin käsiin. Ajoittain tapahtuvat tietovuodot osoittavat tietoturvallisuuden toteutumisen tärkeyden. (Andreasson & Koivisto 2013, 12–13.)

Voidaan helposti ajatella että organisaation tietoturvaa toteuttaa vain jokin tietty määrätty taho, mutta tosiasiassa siitä huolehtiminen on jokaisen organisaatiossa työskentelevän velvollisuus. Suurimpia syitä tietoturvallisuuden ongelmille ovat muun muassa kiireet, huolimattomuus ja osaamattomuus. Pelkästään inhimillisen erehdyksen seurauksena väärää sähköpostiviestissä olevaa www-linkkiä painettaessa voi koneelle asentua haittaohjelma, joka asettaa koneella olevat tiedot vaaraan. Verkostoituneessa toimintaympäristössä harva taho on vastuussa vain omasta tietoturvallisuudestaan, jolloin edellämainitun kaltainen tietovuotoriski saattaa asettaa myös muiden organisaatioiden ja mahdollisten asiakkaiden luottamukselliset tiedot vaaraan. (VAHTI 4/2013, 18; Rousku 2014, 74.)

2.2 Tietoturvallisuuden kolme tavoitetta

Tietoturvallisuuden perustana toimivat kolme päätavoitetta. Nämä ovat luottamuksellisuus, eheys ja saatavuus, jotka muodostavat yhdessä tietoturvallisuuden triadin (kuvio 1). Andressin mukaan tietoturvallisuuden triadi (CIA triad) antaa mallin, jonka avulla voidaan miettiä turvallisuuskonsepteja. (Andress 2011, 23–24.) Tietoturvallisuuden päätavoitteet ja niihin liittyvät menetelmät ovat kaikki läheisesti toisiinsa kytköksissä.



Kuvio 1. Tietoturvallisuuden triadi (Andress 2011, 24).

2.2.1 Luottamuksellisuus

Turvallisuuskomitean ylläpitämässä kyberturvallisuuden sanastossa luottamuksellisuudella tarkoitetaan sitä, ettei kukaan sivullinen voi saada tietoa haltuunsa (2018, 15). Toisin sanoen tiedon tulisi olla vain niiden henkilöiden tai järjestelmien käytettävissä, joilla on sen käytölle tiedonsaanti- ja käyttöoikeus (Rousku 2014, 29).

Yritysten keskeisissä tietojärjestelmissä käsitellään monenlaista tietoa, usein myös salassa pidettävää sellaista (VAHTI 5/2004, 22). Tietojen oikeaoppinen käsittely vaatii sen luokittelua organisaation oman tietojen luokitteluprosessin mukaisesti. Tiedon luokittelun vaatimuksena on myös että organisaatio osaa tunnistaa, mikä sen hallussa olevasta tiedosta on tärkeää. (Järvinen & Rousku 2017, 46.) Salassa pidettävän tiedon luokittelua käsitellään tarkemmin luvussa 5.

Luottamuksellisuuden pettäminen voi aiheuttaa yritykselle suurtakin taloudellista haittaa. Tämä kuitenkin riippuu paljon käyttöoikeudettoman haltuun päätyneen tiedon sisällöstä ja määrästä. Tiedon vuotaminen saattaa vaikuttaa niin organisaation maineeseen, kuin myös suorina taloudellisina menetyksinä vahingonkorvausten tai sanktioiden muodossa. (Järvinen & Rousku 2017, 40). Useimmiten kolhu organisaation maineessa vaikuttaa lopulta myös yrityksen taloudelliseen tilanteeseen esimerkiksi vähentyneen asiakasliikenteen takia.

2.2.2 Eheys

Tiedon eheys tarkoittaa sitä, että se on yhtäpitävää alkuperäisen tiedon kanssa ja että se ei saa muuttua hallitsemattomasti (Turvallisuuskomitea 2018, 22). Tietoa voi muuttaa vain ennakkoon määriteltyjen käsittelysääntöjen mukaisesti, jonka lisäksi tietoa muokkaavalta taholta vaaditaan tarvittava käyttöoikeus. Lisäksi eheyden saavuttamiseksi kriittiseksi tunnistetun tiedon tulee olla palautettavissa kaikissa olosuhteissa. (Rousku 2014, 29–30.)

Yritykselle saattaa seurata merkittäviä kustannuksia, mikäli yrityksen toiminnan kannalta kriittistä tietoa päästään muuttamaan hallitsemattomasti siten, että sen oikeellisuuteen ei voida enää luottaa. Jos tiedon hallitsematon muutos havaitaan, kustannukset aiheutuvat tietojen palauttamiseen tai uudelleen keräämiseen kuluneesta menetetystä ajasta sekä muista aiheutuneista kustannuksista. Vastaavasti jos muokattua tietoa päätyy huomaamattomasti yrityksen käyttöön, voi siitä aiheutua vahinkoa niin yksityishenkilöille kuin yritykselle itselleen. (Järvinen & Rousku 2017, 40.)

2.2.3 Saatavuus

Saatavuudella tarkoitetaan sitä, että haluttua tietoa päästään hyödyntämään ja käyttämään silloin kun sitä tarvitaan (Turvallisuuskomitea 2018, 22). Kriittisten tietojärjestelmien on siis kyettävä toimimaan keskeytyksettä olosuhteista riippumatta. Saatavuuden toteutuminen vaatii muun muassa huolellista suunnittelua, testausta, varajärjestelmiä sekä tietojärjestelmän tilan jatkuvaa seurantaa, jotta saavutetaan riittävä käytettävyys mahdollisissa häiriö- ja poikkeustilanteissa. (VAHTI 05/2004, 22). Myös Rousku (2014, 30) on saatavuuden suhteen samoilla linjoilla. Palvelussa tai ICT-järjestelmässä olevien tietojen on oltava sitä tarvitseville käyttäjille ennakkoon määritellyn vasteajan puitteissa.

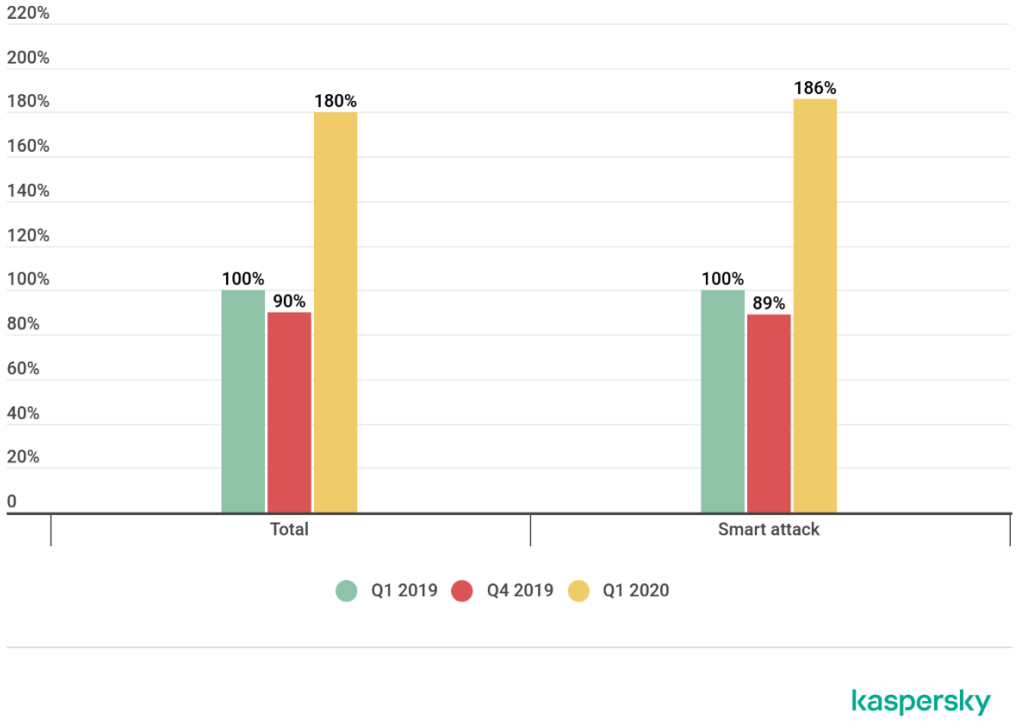
Palvelulle asetettavat tavoitteet on mahdollista sopia palvelutasosopimusten avulla (SLA). Yhteiskunnan digitalisoitumisen myötä yhä useammat palvelut ovat tarjolla vuorokauden ympäri ja vuoden jokaisena päivänä, minkä takia saatavuus on entistäkin tärkeämpi tavoite.

Monet asiat kuten esimerkiksi järjestelmissä esiintyvät virheet voivat vaikuttaa palvelun ja tiedon saatavuuteen. Yksi suurimpia uhkia saatavuuden kannalta on DOS-hyökkäys, joka on verkkohyökkäyksen muoto, jonka tarkoituksena on eri keinoin ylikuormittaa kohteena oleva palvelin sen käyttämisen estämiseksi.

Johonkin palveluun kohdistuva palvelunestohyökkäys saattaa aiheuttaa sen, että yrityksen tarvitsema tieto ei ole saatavilla. Palvelunestohyökkäyksestä aiheutuvat vahingot ovat täysin riippuvaisia hyökkäyksen kohteena olevan palvelun kriittisyydestä yrityksen toiminnalle. (Järvinen & Rousku 2017, 41.)

2.2.4 Covid-19 pandemian vaikutukset saatavuuteen

Covid-19 pandemian vuoksi vuoden 2020 alku on ollut poikkeuksellinen myös tietoturvallisuuden kannalta. Valtaosan elämät ovat siirtyneet lähes täysin verkkoon – ihmiset ympäri maailman työskentelevät, opiskelevat, tekevät ostoksia sekä viettävät vapaa-aikansa verkossa. Tämä heijastuu suoraan vuoden 2020 ensimmäisen neljänneksen palvelunestohyökkäysten määrän kasvuna. Eniten hyökkäyksiä on kohdistunut lääketieteellisten organisaatioiden, kuljetuspalveluita tarjoavien tahojen, pelipalveluiden sekä opiskelualustojen verkkosivustoille ja palveluihin. Kuviossa 2 on havainnollistettu 2020 ensimmäisen neljänneksen (Q1) DDoS hyökkäysten määrää verrattuna 2019 vuoden ensimmäiseen neljännekseen ja 2019 viimeisen neljänneksen (Q4) DDoS lukuihin. Kuviosta voidaan päätellä, että palvelunestohyökkäysten määrä on kasvanut räjähdysmäisesti normaalitilanteeseen nähden. (Kupreev ym. 2020.)



Kuvio 2. Palvelunestohyökkäysten määrä on kasvanut räjähdysmäisesti (Kupreev ym. 2020).

DDoS-hyökkäyksistä opiskelualustoja kohtaan on havaittu myös Suomessa, ja tästä on uutisoitu paikallisessa mediassa näkyvästi. Liikenne- ja viestintäviraston Traficomin Kyberturvallisuuskeskuksen tiedotteen mukaan palvelunestohyökkäyksiä on tehty lähes päivittäin. Kyberhyökkäykset rasittavat verkko-opiskeluympäristöä ja häiritsevät etäopiskelua. Hyökkäysten on kuitenkin kerrottu olevan varsin kotikutoisen oloisia, mistä voidaan päätellä niiden olevan todennäköisesti lasten ja nuorten tekemiä. (Kirsi 2020.)

3 TIETOTURVALLISUUDEN OSA-ALUEET

Tietoturvallisuus voidaan jakaa useaan eri osa-alueeseen. Valtiovarainministeriö on jaotellut tietoturvallisuuden kahdeksaan erilliseen osioon, jotka ovat hallinnollinen tietoturvallisuus, ohjelmistoturvallisuus, laitteistoturvallisuus, tietoliikenneturvallisuus, tietoaineistoturvallisuus, käyttöturvallisuus, henkilöstöturvallisuus sekä fyysinen turvallisuus (VAHTI 03/2007). Edellä mainittujen ohella myös tietosuoja ja yksityisyydensuoja, joita käsitellään tarkemmin luvussa 4, ovat tärkeässä roolissa osana tietoturvallisuutta.

3.1 Hallinnollinen tietoturvallisuus

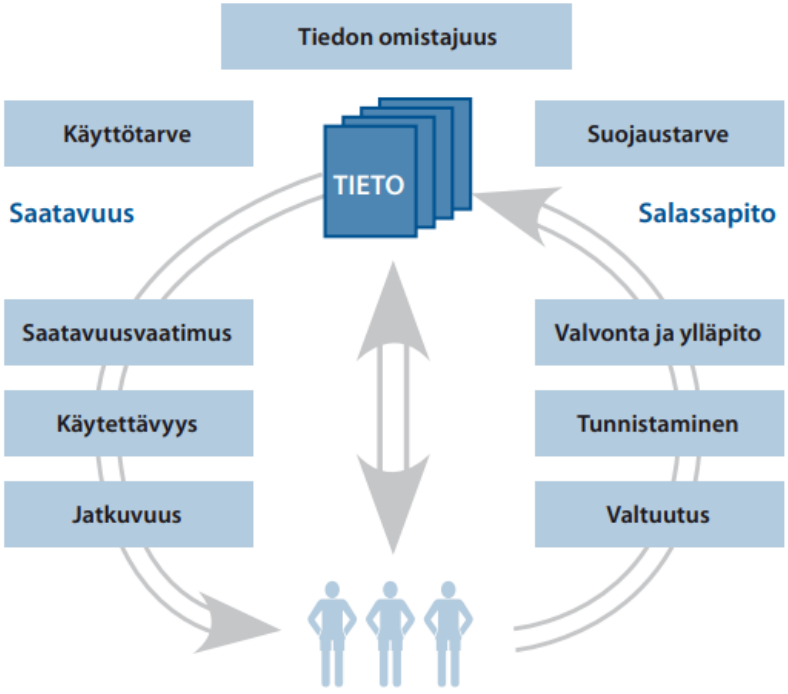
Hallinnollinen tietoturvallisuus sivuaa monia muita tietoturvallisuuden osa-alueita, sillä se on tietyllä tapaa ajateltuna sekä nimensä mukaisesti tietoturvallisuuden johtamista. Hallinnollisessa tietoturvallisuudessa määritellään hallinnollisin keinoin, miten tietoturvallisuutta käsitellään. Hallinnollisia tietoturvallisuuteen tähtääviä keinoja ovat muun muassa tehtävien ja vastuiden määrittely, henkilöstön ohjeistus sekä organisaatiojärjestelyt. Esimerkiksi toimintaprosessien dokumentoiminen sekä riskianalyysi ovat hallinnollisen turvallisuuden vaatimuksia. (VAHTI 04/2004, 27–28.)

Hallintatoimilla seurataan ja arvioidaan tietoturvatoimien tehokkuutta ja tarkoituksenmukaisuutta. Lisäksi hallintajärjestelmää tulisi kehittää jatkuvasti erilaisia kypsyysmalleja sekä standardeja hyväksikäyttäen tietoturva-asioiden systemaattisen hallinnan valmiuksien parantamiseksi. Tilastotieteilijä ja professori William Edwards Deming on kehittänyt niin sanotun PDCA-mallin, jonka nimi tulee sen vaiheista plan, do, check ja act. Tätä samaa mallia hyödynnetään ISO/IEC 27001 -standardin suomennoksessa, jossa vaiheet ovat vastaavasti suunnittele, toteuta, arvio ja toimi. Hallintajärjestelmän PDCA-mallille ominaista on myös jatkuva parempien tuloksien tavoitteleminen tietoturvapolitiikkaa, tietoturvatavoitteita, saatuja tuloksia, tapahtumien valvonnan analysointia, korjaavia ja ehkäiseviä toimenpiteitä sekä johdon katselmuksia avuksi käyttäen. (Andreasson & Koivisto 2013, 42–43.)

3.2 Henkilöstöturvallisuus

Valtionhallinnon tietoturvasansaston mukaan henkilöstöturvallisuutta toteutetaan hoitamalla henkilöstön oikeuksien hallintaan, luotettavuuteen, sijaisjärjestelyihin, henkilöstön suojaamiseen ja työsuhteeseen sekä työyhdistelmiin liittyviä turvallisuustekijöiden järjestelyitä, joiden lisäksi myös henkilön soveltuvuutta tulisi mitata (Valtionhallinto 2008, 33). Esimerkiksi henkilöstön luotettavuutta ja soveltuvuutta varten uuden työnhakijan taustat voidaan selvittää tarvittavilta osin. Toinen hyvin yleinen henkilöstöturvallisuuden toimenpide on salassapitosopimuksen allekirjoittaminen.

Monet edellä luetelluista järjestelyistä sisältyvät henkilöstöstä aiheutuvien riskien hallintaan. Henkilöstöturvallisuuden keskiössä on ihminen, minkä takia sen merkitys tietojen turvaamisen suhteen on keskeinen. Organisaation henkilöstö ylläpitää tietovarastoja ja -järjestelmiä ja käsittelee tietoa kaikissa sen elinkaaren vaiheissa. Koska organisaatioissa käsitellään usein myös salassa pidettävää tietoa, salassapitoon ja käytettävyyteen liittyvien riskien hallinta on iso osa henkilöstöturvallisuutta. Tätä kuvataan kuvassa 1. (VAHTI 02/2008, 12.)



Kuva 1. Henkilöstöturvallisuuden haasteet tiedon ja sen saannin turvaamisessa (VAHTI 02/2008, 12).

3.3 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan ohjelmistojen turvallisuuden takaamista. Ymmärtääksemme mitä ohjelmistoturvallisuus on ja mitä menetelmiä sen toteuttamiseksi käytetään, tulisi ensin tietää mitä ohjelmistot oikeastaan ovat. Ohjelmistoja ovat esimerkiksi laiteohjelmistot, varusohjelmistot sekä sovellusohjelmistot. Laiteohjelmistot toteuttavat koneen perustoimintoja, varusohjelmistot ovat tietokoneen käytön mahdollistavia perusohjelmistoja kuten käyttöjärjestelmät, ja sovellusohjelmistot ovat käytännössä kaikkia niitä ohjelmistoja, joita loppukäyttäjä käyttää esimerkiksi tietyn tehtävän suorittamiseen. (TEPA-termipankki.)

Ohjelmistoturvallisuuden turvatoimet kohdistuvat kaikkiin edellä mainittuihin ohjelmistotyyppeihin sisältäen esimerkiksi valvonta- ja lokimenettelyjä, ohjelmistojen ylläpito- ja päivitystoimenpiteitä sekä ohjelmistojen turvallisuudelle asetettavia vaatimuksia ja prosesseja. Näitä kaikkia tarkastellaan ohjelmiston käyttöä, kehittämistä ja hankintaa ajatellen. Lisäksi tärkeää on ohjelmistoja käyttävän osapuolen saama riittävä koulutus ja ohjeistus turvallisen käytön varmistamiseksi. (VAHTI 03/2007, 69.)

Ohjelmistojen päivittäminen on hyvinkin arkinen asia, johon jokainen törmää lähes päivittäin. Tämä ei enää koske vain organisaation omia teknisiä laitteita, vaan esimerkiksi myös henkilöstön omia mobiililaitteita sekä tietysti käytettäviä ohjelmistoja. Pilvipalveluiden yleistyessä organisaation tiedot ovat muutaman hipaisun päässä myös mobiililaitteilla. Päivittämisen päätavoitteena on korjata ohjelmissa olevia virheitä sekä mahdollisia tietoturvahaavoittuvuuksia, mutta toisinaan ne tuovat myös uusia hyödyllisiä toimintoja. Uudet päivitykset voivat kuitenkin myös aiheuttaa uusia tietoturvariskejä, tai jokin virhe saattaa myös estää ohjelman toimintaa. Tämän takia tietohallinto saattaakin testata päivityksiä rajatussa ympäristössä ennen koko organisaation laajuista asentamista. Samasta syystä päivitysten tekemisestä tulisi olla yhtenäinen ja tiedotettu ohjeistus. (Järvinen & Rousku 2017, 103.)

3.4 Laitteistoturvallisuus

Valtionhallinnon tietoturvasanaston mukaan laitteistoturvallisuudella pyritään turvaamaan laitteiston kaikkia elinkaaren vaiheita sen käyttöönottoasennuksesta laitteiston

turvalliseen poistoon. Näiden välillä laitteistoa tulee ylläpitää toiminnan varmistamiseksi. (VAHTI 08/2008, 57.)

Andreasson ja Koivisto (2013, 65) esittävät kirjassaan useita eri näkökulmia laitteistoturvallisuudesta. Useimmiten organisaation laitteiden elinkaareen liittyvistä asioista sovitaan palvelusopimuksissa. Ennakkoon sovituilla vasteajoilla sekä määrittelyillä voi olla iso rooli tietoturvatason ylläpitoa sekä tietoturvapoikkeamiin reagointia ajatellen. Toiminnalle kriittistä laitteistoa voi esimerkiksi pitää varalla myös omassa varastossaan, jotta vahingon sattuessa ei olla riippuvaisia toimittajan toimintanopeudesta. Laitteiston ylläpidossa tulisi pitää huolta siitä, että poikkeamasta toipumisen jälkeen kaikki laitteen tiedostot ovat palautettavissa ajan tasaisista varmuuskopioista. Lisäksi tietoturvapäivityksistä tulisi huolehtia siten, että ne tehdään säännöllisesti.

Tietoturvaa toteuttamassa -kirjassa tuodaan esille eri näkökulmia omien laitteiden käytöstä töissä. Trendi omien laitteiden käyttämisen suhteen on lisääntynyt, mille löytyy argumentteja sekä puolesta että vastaan. Työntekijä haluaa vähentää käytettävien laitteiden määrää, jonka lisäksi osa kokee, että oma laite on sekä parempi että joustavampi. Organisaatio voi tällöin säästää laitehankintakuluissa. Vikatilanteen sattuessa tilanne saattaa kuitenkin olla toinen, koska iso määrä eri laitteita vaikeuttaa lähituen työtä vain sen takia, että jokaisella on erilainen laite, joka toimii eri tavalla kuin vakioidut laitteet. Tämä aiheuttaa sen, että vian ratkaisuun kuluu turhaan työaikaa. Lisäksi yleinen haaste on koneen käyttöoikeudet ja hallinta sekä tietojen omistajuus eli se, miten työ- ja henkilökohtaiset tiedot pidetään erillään. Mikäli työnantajalla ei ole oikeuksia asentaa käyttäjän omaan laitteeseen haittaohjelmien torjuntaa, palomuuria, salausta tai mahdollisuutta etätyhjentää laite, se ei voi varmistaa laitteen ja sen sisältämän tiedon turvallisuutta. Tästä aiheutuu tietoturvariskejä työnantajan verkolle ja tietojärjestelmille. (Andreasson & Koivisto 2013, 66–67.)

3.5 Tietoliikenneturvallisuus

Säädetyt lait, normit ja toimet ohjaavat tietoliikenneturvallisuutta. Tietoliikenneturvallisuuden tarkoituksena on toteuttaa tietoturvallisuutta tiedonsiirtoyhteyksien käytettävyyteen, tiedonsiirron turvaamiseen, suojaamiseen ja salaamiseen, käyttäjän tunnistamiseen ja verkon varmistamiseen liittyvien toimenpiteiden avulla. (VAHTI 08/2008, 103.)

Tietoliikenneturvallisuuden toteutuminen organisaatiossa vaatii sitä, että sen tietoliikennetoiminnot sekä niitä toteuttavat verkkojärjestelmät tulee suunnitella ja rakentaa hyvän tiedonhallintatavan mukaisesti tiedon eheyden, luottamuksellisuuden ja saatavuuden suojaamiseksi. Edellä mainittujen ohella myös dokumentaatio on erittäin tärkeä osa-alue tietoliikenneturvallisuuden toteutumiseksi. Dokumentaatio onkin usein tyypillinen kehityskohde organisaatioissa sen ollessa vain osittaista, vanhentunutta tai pahimmillaan se puuttuu kokonaan (Andreasson & Koivisto 2013, 76). Tietoliikenneturvallisuuteen kuuluu esimerkiksi tietoliikennelaitteiston kokoonpano ja sen luettelointi, ylläpito, muutosten ja käytön valvonta, ongelmatilanteiden kirjaus, viestinnän salaaminen sekä säännöllinen testaaminen. Tietoliikenneturvallisuuden keinoin pyritään estämään tiedon joutuminen vääriin käsiin. (Mts. 69.)

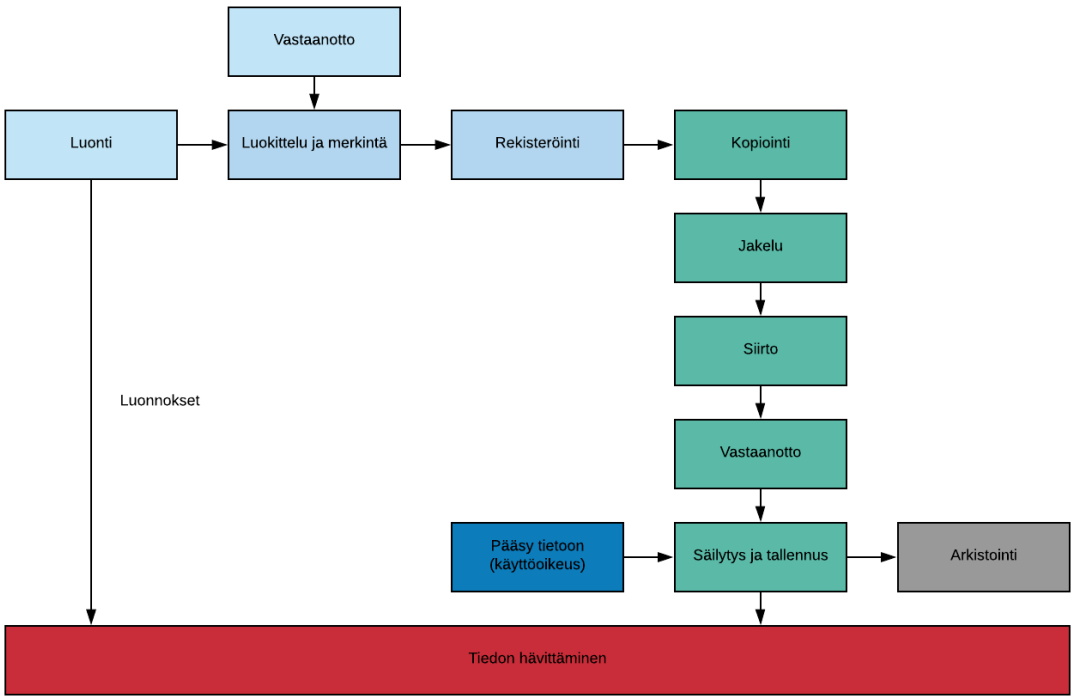
Tietoliikenneturvallisuutta säädetään useissa laeissa, joista on puolestaan taas johdettu hyödyllisiä ohjeita organisaatioiden hyödynnettäväksi. Tietoliikenneturvallisuuteen liittyy esimerkiksi laki sähköisen viestinnän palveluista (7.11.2014/917). Sisäverkko-ohje (VAHTI 03/2010) on johdettu sähköisen viestinnän tietosuojalaista (16.6.2004/516), joka on sittemmin kumottu lailla sähköisen viestinnän palveluista, joka on mainittu yllä. Ohje sisältää esimerkiksi verkon rakenteen, verkon aktiivilaitteiden, päätelaitteiden sekä hallinnan/valvonnan tarkistuslistat monien muiden ohella. Tarkistuslistojen avulla voidaan varmistaa, että tietoliikenteen menetelmiä läpikäydessä mitään oleellista ei jää tarkistamatta. (Andreasson & Koivisto 2013, 70.)

3.6 Tietoaineistoturvallisuus

Organisaatioissa käsitellään valtavia määriä sähköisessä muodossa olevaa tietoa, mutta myös paperille tallennettua tietoa hyödynnetään edelleen päivittäin. Koska tietoa on niin valtavasti, tulee sitä hallinnan helpottamiseksi luetteloida sekä luokitella. Tietovälineiden hallinnan tulisi olla ohjeistettua niiden koko elinkaaren osalta, jotta tiedon käytettävyys, eheys ja luottamuksellisuus voidaan ylläpitää (VAHTI 08/2008, 101).

Tietoaineistoturvallisuudella tarkoitetaan tietojen suojausta riippumatta siitä, missä tallennusmuodossa se on, eli oli se sitten sähköisesti tallennettua tai esimerkiksi paperille tulostettua. Se koskee paperiasiakirjojen ohella kaikkia mahdollisia teknisiä laitteita, joilla tietoa voidaan tallentaa tai kerätä. Tietoaineistojen turvallisuuden varmistaminen koskee sen koko elinkaarta ja siitä on vastuussa koko henkilöstö. (VAHTI 03/2007, 55.)

Kuviossa 3 on kuvattu tietoaineiston elinkaari Valtiovarainministeriön määrittelyn mukaan. Kun tietoa luodaan tai vastaanotetaan, se tulee ensin luokitella ja merkitä luokittelun mukaisesti. Tietoaineistoa käytetään monin eri tavoin, sitä esimerkiksi kopioidaan ja jaetaan. Tietoaineiston käyttäjällä tulee olla siihen käyttöoikeus. Lopulta kun tietoaineistoa ei enää tarvita, se hävitetään asianmukaisin keinoin.



Kuvio 3. Tietoaineiston elinkaari (VAHTI 03/2007, 55).

Tietoaineistojen saatavuutta ja käytettävyyttä, sekä eheyttä ja luottamuksellisuutta voidaan hallita luokittelemalla aineisto eri luokkiin tiedolle asetettujen vaatimusten pohjalta. Tiedon luokittelu onnistuu suojaustasojen sekä turvallisuusluokitusten avulla. Näillä voidaan määritellä, kuinka arvokasta käsiteltävä tieto on. Suojaustasoja ja vastaavasti turvaluokituksia on yhteensä neljä. Näitä käsitellään tarkemmin luvussa 5. (VAHTI 02/2010, 51.)

3.7 Käyttöturvallisuus

Käyttöturvallisuuden menetelmin pyritään luomaan ja ylläpitämään tietoteknisesti turvalliset toimintaolosuhteet tietotekniikan käyttämiseksi. Menetelmät itsessään liittyvät moneen muuhun tietoturvan osa-alueeseen. Tämän toteutumiseksi tulee varmistaa, että käyttöoikeuksia hallitaan sovitusti, ohjelmistot ja laitteistot toimivat ja ovat ajantasaisia, ylläpito-, kehittämis- ja huoltotoimintojen turvallisuustoimenpiteistä on huolehdittu, varmuuskopiointia vaativat tiedot on varmuuskopioitu, häiriötilanteet raportoidaan ohjeistuksen mukaisesti ja kaikki tietojärjestelmät on suojattu haittaohjelmilta. Etätyöskentely on tänä päivänä entistäkin suositumpaa, mikä tuo omat haasteensa myös käyttöturvallisuutta ajatellen. Etätyön tekemisestä tulisi olla varta vasten laaditut työn erityispiirteitä vastaavat tietoturvaohjeet, joiden mukaan työntekijät ovat velvoitettuja toimimaan. Työvälineenä mukana kulkeva kannettava tietokone sekä älypuhelin sisältää ja kykenee välittämään valtavan määrän dataa, jota tulisi turvata siten, että vääriin käsiin joutuessaan siitä ei aiheudu haittaa organisaation toiminnalle. Luottamuksellisen tiedon tulee olla salattua, jonka lisäksi tulee käyttää tietoliikenteen suojaamiseen sekä rajoittamiseen tarkoitettuja menetelmiä, etenkin mikäli laitteet ovat kytkettynä turvattomaan verkkoon. (VAHTI 03/2007, 65–67.)

Myös Järvinen ja Rousku (2017, 59) ovat sitä mieltä, että laitteiden mukana kuljettaminen sekä julkisissa tiloissa käyttäminen asettaa laitteen sekä samalla sen sisältämän tiedon alttiiksi varkaudelle. Tällaisia tilanteita ajatellen tulisi siis olla valmiiksi olemassa organisaation sisäiset ohjeet oikean toiminnan varmistamiseksi. Sen lisäksi että laitteet ovat alttiina varkaudelle, tulisi osata ottaa huomioon, millaisissa tiloissa mitäkin tietoa on mahdollista käsitellä. Salassa pidettävistä työasioista ei tulisi keskustella eikä myöskään salaiseksi luokiteltua tietoa käsitellä julkisissa tiloissa tai kulkuvälineissä, koska tietoa voi tällöin joutua ihan huomaamatta sellaisen tahon tietoon kenelle se ei kuulu. Tietoturvallisuus on helposti ajateltuna vain teknisiä menetelmiä sekä säännöksiä, mutta todella monessa asiassa selviää maalaisjärkeä käyttämällä. Mikäli kuitenkin joudut käsittelemään salassa pidettävää tietoa julkisella paikalla, tulisi käyttää tietoturvallisuutta edesauttavia apuvälineitä kuten esimerkiksi tietosuojakalvoa, joka estää tai vähintäänkin vaikeuttaa muita kuin itse koneen käyttäjää näkemästä ruudun sisältöä. (Järvinen & Rousku 2017, 154.)

3.8 Fyysinen turvallisuus

Elinkeinoelämän keskusliiton (2020) mukaan organisaation tulee suojata sen toimipaikkoja ja -tiloja kustannustehokkaasti sekä riskiarvioihin perustuen. Perimmäinen tavoite fyysisen turvallisuuden tavoittelussa on, että organisaation tiloissa on mahdollista työskennellä sekä asioida turvallisesti että vailla häiriöitä. Lisäksi arvokkaaksi luokitellun tiedon tai materiaalin oikeudeton käyttö sekä varkaudet tulisi estää.

Organisaation tulisikin siis itse huolehtia omasta fyysisestä turvallisuudesta ja sen suojauksista suhteutettuna omaan toimintaan ja siihen liittyviin riskeihin. Näin saadaan taattua hyvä toimintavarmuus kaikissa olosuhteissa. Fyysisellä turvallisuudella tarkoitetaan henkilöiden, aineistojen, laitteistojen, postitoimitusten, toimitilojen sekä varastojen suojaamista erilaisilta tuhoilta ja vahingoilta. Keinoja tämän toteuttamiseksi ovat esimerkiksi kulunvalvonta, kameravalvonta, muu tekninen valvonta ja tilojen vartiointi. Organisaation tulisi olla valmis suojautumaan esimerkiksi palo-, vesi-, sähkö-, ilmastointi- ja murtovahingoilta ilman, että sen toiminta keskeytyy. Lisäksi myös kuriirien ja tietoainestoja sisältävien lähetysten turvallisuuden ohjaamiseksi on olemassa omat toimenpiteensä. Tilaturvallisuuutta lisäävien toimien ja järjestelmien kehittämistarpeet tulisi ottaa huomioon vuosittain esimerkiksi vuosisuunnitelmien laatimisen yhteydessä. (VAHTI 03/2007, 59; VAHTI 08/2008, 30.) Fyysisen turvallisuuden toteutuminen vaatii organisaatiolta myös oman henkilöstön kouluttamista, jotta se osaa toimia oikein erilaisissa poikkeustilanteissa.

4 TIETOSUOJA

Tietosuoja tarkoittaa ihmisen yksityisyydensuojaa ja muita sitä turvaavia oikeuksia henkilötietoja käsiteltäessä. Oikeuksia ovat muun muassa tietojen luottamuksellisuuden säilyttäminen ja tietojen oikeudettoman saannin estäminen sekä henkilötietojen suojaaminen oikeudettomalta tai henkilöä vahingoittavalta käytöltä. (VAHTI 08/2008, 105.) Yksityisyydensuojalla huolehditaan henkilötietojen voimassa olevan lainsäädännön ja velvoitteiden mukaisesta käsittelystä (Rousku 2014, 76).

Tietosuojavaltuutetun toimiston mukaan tietosuoja on jokaisen perusoikeus, jolla turvataan rekisteröidyn oikeuksien ja vapauksien toteutuminen henkilötietoja käsiteltäessä. Sen avulla osoitetaan, milloin ja millä edellytyksillä henkilötietojen käsittely tapahtuu. Henkilötietojen käsittelyn tulee perustua aina lakiin, jonka lisäksi henkilötietojen suojaa koskevien säännösten noudattamista valvotaan riippumattoman viranomaisen toimesta. Tietosuojaa, sen periaatteita ja sitä käsitteleviä lakeja ja säädöksiä tarkasteltaessa tulee ensin ymmärtää siihen liittyvien termien merkitys. Kaikki sellaiset tiedot, joita voidaan käyttää luonnollisen henkilön tunnistamiseen, ovat henkilötietoja. Henkilötietoja ovat esimerkiksi henkilökortin numero, nimi, katuosoite tai puhelinnumero (Tietosuojavaltuutetun toimisto b). Ne voivat olla tallennettuna sähköisesti tiedostoihin ja tietokantoihin, perinteisesti paperille tai jopa kuva- tai äänitallenteelle. Henkilörekisterillä tarkoitetaan kaikkia samaan käyttötarkoitukseen käsiteltäviä henkilötietoja. Tällaisia ovat esimerkiksi asiakasrekisteri tai työntekijärekisteri (Tietosuojavaltuutetun toimisto c). Rekisteröidyllä tarkoitetaan sitä henkilöä, jota henkilötieto koskee. Sellaista tahoa, oli se sitten henkilö, yhteisö, yritys tai viranomainen, joka määrittelee miten ja miksi henkilötietoa käsitellään kutsutaan rekisterinpitäjäksi. (Tietosuojavaltuutetun toimisto a.)

Tietosuojaperiaatteita tulee noudattaa aina henkilötietoja käsiteltäessä niiden koko elinkaaren ajan, jonka lisäksi rekisterinpitäjällä tulee olla valmiudet osoittaa tietosuojaperiaatteiden tehokas toteutuminen. Henkilötietojen kaikki elinkaaren vaiheet suunnittelusta keräämiseen, käsittelyyn ja niiden poistamiseen ovat henkilötietojen käsittelyä. (Tietosuojavaltuutetun toimisto d.)

Tietosuojavaltuutetun toimiston mukaan tietosuojaperiaatteet asettavat henkilötietojen käsittelylle seuraavanlaisia ehtoja:

- Käsittelyn on oltava lainmukaista, asianmukaista ja rekisteröidyn kannalta läpinäkyvää.
- Keräyksen ja käsittelyn tulee vastata tiettyä lainmukaista ja tarkkaan määriteltyä tarkoitusta.
- Tietoa tulee kerätä vain tarkoituksenmukainen määrä käsittelyä varten.
- Tietojen oikeellisuutta on pidettävä ajan tasalla, virheelliset ja epätarkat tiedot tulee oikaista tai poistaa viipymättä.
- Tietoa tulee säilyttää sellaisessa muodossa, että rekisteröity voidaan tunnistaa vain tarpeen mukaisen ajan tarkoitusten toteuttamiseksi.
- Sitä on käsiteltävä turvallisesti ja luottamuksellisesti. (Tietosuojavaltuutetun toimisto d.)

Tietosuojaa käsitteleviä lakeja ja säädöksiä ovat EU:n yleinen tietosuoja-asetus (27.4.2016/679), sitä täsmentävä ja täydentävä tietosuojalaki (5.12.2018/1050), laki sähköisen viestinnän palveluista (7.11.2014/917) sekä työelämän tietosuojalaki eli laki yksityisyyden suojasta työelämässä (13.8.2004/759). (Tietosuojavaltuutetun toimisto e .) Työelämän tietosuojalakiin tehdyt muutokset tulivat voimaan 1.4.2019 alkaen (Laki yksityisyyden suojasta työelämässä annetun lain muuttamisesta 15.3.2019/347) sisältäen lähinnä EU:n yleisestä tietosuoja-asetuksesta, henkilötietolain kumoamisesta ja rikoslain muutoksesta johtuvia täsmennyksiä (Tietosuojavaltuutetun toimisto f).

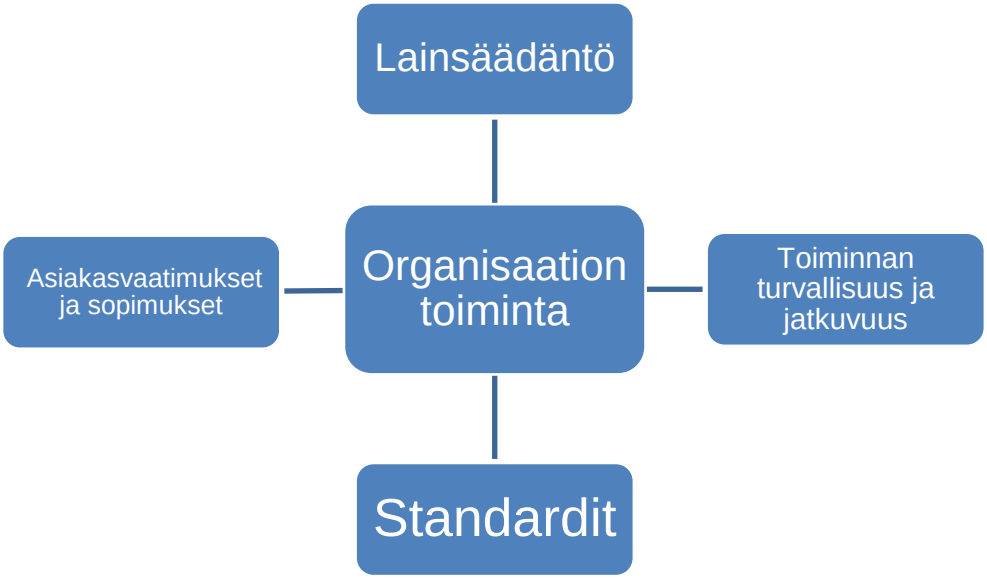
EU:n tietosuoja-asetuksessa kerrotaan, mitä oikeuksia rekisteröidyllä on kun henkilötietoja käsitellään jonkin yrityksen tai organisaation toimesta. Asetuksen mukaan rekisteröidyllä on oikeus saada tietoa henkilötietojen käsittelystä, päästä tietoihin käsiksi, oikaista tietoa, tulla unohdetuksi tai poistaa tiedot, siirtää tiedot toiseen järjestelmään, rajoittaa tiedon käsittelyä, vastustaa tiedon käsittelyä sekä olla joutumatta automaattisen päätöksenteon kohteeksi. On myös huomioitava, että kaikkia lueteltuja oikeuksia ei ole mahdollista käyttää kaikissa tilanteissa vaan tapauskohtaisesti tilanteeseen vaikuttaa se, millä perusteella henkilötietoja käytetään. (Tietosuojavaltuutetun toimisto g.)

Digitalisaation myötä kaikenlaisen tiedon kerääminen on valtavassa kasvussa. Kaiken muun tiedon ohella kerätään myös henkilötietoja, joita lähes kaikki verkossa toimivat palvelut edellyttävät ainakin nimen ja sähköpostiosoitteen osalta, jotta palvelun kaikkia ominaisuuksia pääsee hyödyntämään. Kaikki kerätty henkilötieto kerätään palvelun tarjoajan ylläpitämään henkilörekisteriin. On todella tärkeää, että henkilötietoja käsitellään oikein, koska vääriin käsiin joutuessaan rekisteröityyn saattaa kohdistua erilaisia uhkia

tiedon hallitsemattomasta käytöstä tai esimerkiksi väärentämisestä johtuen. Rikollisten käsissä henkilötiedot mahdollistavat esimerkiksi ostamisen tai myymisen toisen henkilön nimissä, henkilön kiristämisen arkaluonteisen tiedon avulla tai pahimmassa tapauksessa ne mahdollistavat koko identiteetin kaappaamisen. EU:n yleinen tietosuoja-asetus säädettiin henkilötietojen turvallisen ja tarkoituksenmukaisen käytön yhdenmukaistamiseksi ja mahdollistamiseksi. (Järvinen & Rousku 2017, 18–19.)

5 TIETOTURVALLISUUTTA OHJAAVIA TEKIJÖITÄ

Organisaatioiden tietoturvallisuus perustuu pitkälti riskien arviointiin. Tämä tarkoittaa sitä, että organisaation tulee tunnistaa omalle toiminnalle ominaiset uhkat, arvioida niiden aiheuttamat riskit, sekä antaa henkilöstölle ohjeet turvalliseen laitteiden ja palveluiden käyttöön. Riskienhallintaan tutustutaan tarkemmin luvussa 6. Tämän lisäksi tietoturvallisuutta säätelevät erilaiset kansainväliset lait ja standardit sekä asiakasvaatimukset ja sovitut sopimukset (kuvio 4). Voidaan siis sanoa että vaatimustenmukaisuus ohjaa tietoturvallisuutta. Yhtenäisillä kansainvälisillä laeilla sekä standardeilla pystytään velvoittamaan organisaatiot ja julkishallinnot toteuttamaan tietoturvallisuutta saman tavoitteen mukaisesti. (Järvinen & Rousku 2017, 31.)



Kuvio 4. Tietoturvallisuutta ohjaavia tekijöitä (Järvinen & Rousku 2017, 31).

Suomessa tietoturvallisuutta ja henkilöiden tietosuojaa säädellään lainsäädännöllä. Esimerkiksi 2016 voimaan tullut EU:n tietosuojauudistus on tuonut paljon uutta sääntelyä organisaatoiden toimintaan. Tämän lisäksi Suomessa tietoturvallisuuden toteuttamista helpottamaan on olemassa Valtiovarainministeriön todella laaja VAHTI-ohjeistus sekä Puolustusministeriön KATAKRI-auditointityökalu, joiden lisäksi hyödynnetään myös tiedon luokittelun keinoja määriteltyjen suojaustasojen ja turvaluokitusten mukaisesti.

5.1 VAHTI-ohjeistus

VAHTI on Valtiovarainministeriön Valtionhallinnon tietoturvallisuuden johtoryhmä, joka kehittää ja ylläpitää VAHTI-ohjeistusta, joka on yksi maailman kattavimpia yleisiä tietoturvaohjeistoja. Ohjeistus kattaa kaikki tietoturvallisuuden osa-alueet. VAHTI ohjaa, kehittää ja koordinoi hallinnon tietoturvallisuutta, ja sen toiminnalla onkin tarkoitus parantaa valtion tietoturvallisuutta. Vaikka VAHTI-ohjeistukset on pohjimmiltaan tarkoitettu valtionhallinnon käyttöön, ovat ne selkeytensä takia helposti hyödynnettävissä myös yritysten tietoturvatoiminnassa. (Valtiovarainministeriö; Andreasson & Koivisto 2013, 30.)

5.2 KATAKRI-auditointityökalu

Katakri eli kansallinen turvallisuusauditointikriteeristö on alun perin puolustusministeriön johdolla viranomaisten ja elinkeinoelämän yhteistyössä valmisteltu. Nykyään sen uudistamistyöstä ja hallinnoinnista on vastuussa ulkoministeriössä toimiva Kansallinen turvallisuusviranomainen eli NSA. (Katakri 2015, 2.)

Katakri 2015 on tietoturvallisuuden auditointityökalu viranomaisille, jolla voidaan mitata kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Sitä voidaan myös käyttää apuna yrityksen turvallisuusjärjestelyiden toteutumisen arvioinnissa yritysturvallisuusselvityksessä, sekä turvallisuustyössä ja sen kehittämisessä. Siihen on koottu voimassa olevaa lainsäädäntöä sekä Suomea sitovia kansainvälisiä tietoturvallisuusvelvoitteita mahdollisimman hyvin aikaa kestävään muotoon. Esitettyjen vaatimusten yhteydessä on viitattu lähdeviittauksin kuhunkin lakiin tai säädökseen kutakin vaatimusta koskien. Katakri on jaoteltu kolmeen erilliseen kokonaisuuteen, jotka ovat turvallisuusjohtaminen, fyysinen turvallisuus ja tekninen turvallisuus. (Katakri 2015, 3.) Näitä kokonaisuuksia käsitellään tarkemmin luvussa 7.

Katakri on kaikkien vapaasti ladattavissa sekä käytettävissä Puolustusministeriön www-sivuilta.

5.3 Suojaustasot ja turvaluokitukset

Tietoaineistojen saatavuutta ja käytettävyyttä sekä eheyttä ja luottamuksellisuutta voidaan hallita luokittelemalla aineisto eri luokkiin tiedolle asetettujen vaatimusten pohjalta.

Tiedon luokittelu on toteutettu suojaustasojen sekä turvallisuusluokitusten avulla, joilla voidaan määritellä kuinka arvokasta käsiteltävä tieto on. Suojaustasoja ja vastaavasti turvaluokituksia on yhteensä neljä. (VAHTI 02/2010, 51.)

Suojaustasot määritellään laissa Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 9 § (1.7.2010/681) seuraavasti:

1. *suojaustaso I, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle;*
2. *suojaustaso II, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle;*
3. *suojaustaso III, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle;*
4. *suojaustaso IV, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle.*

Edellä ensimmäisen momentin neljännessä kohdassa tarkoitettuun suojaustasoon kuuluvaksi voidaan luokitella muukin kuin salassa pidettäväksi säädetty asiakirja, jos asiakirjan luovuttaminen on lain mukaan viranomaisen harkinnassa tai asiakirjaan sisältyviä tietoja saa lain mukaan käyttää tai luovuttaa vain määrättyyn tarkoitukseen ja jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681.)

Turvallisuusluokitukset määritellään vastaavasti neljään osaan, ja ne on määritelty laissa Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 11 § (1.7.2010/681) seuraavasti:

Jos asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle viranomaisten toiminnan julkisuudesta annetun lain 24 §:n ensimmäisen momentin toinen ja seitsemännestä kymmenenteen kohdissa

tarkoitetulla tavalla, salassa pidettävän asiakirjan suojaustasoa koskevan merkinnän yhteyteen tai sen sijasta voidaan tehdä erityinen turvallisuusluokitusmerkintä.

Turvallisuusluokitusmerkintä tehdään :

1. *suojaustasoon I kuuluvaan asiakirjaan merkinnällä "ERITTÄIN SALAINEN";*
2. *suojaustasoon II kuuluvaan asiakirjaan merkinnällä "SALAINEN";*
3. *suojaustasoon III kuuluvaan asiakirjaan merkinnällä "LUOTTAMUKSELLINEN";*
4. *suojaustasoon IV kuuluvaan asiakirjaan merkinnällä "KÄYTTÖ RAJOITETTU".*

Turvallisuusluokitusmerkintää ei saa käyttää muissa kuin 1 momentissa tarkoitetuissa tapauksissa, ellei merkinnän tekeminen ole tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai asiakirja muutoin liity kansainväliseen yhteistyöhön. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681.)

Tietojen luokittelemiseksi edellä lueteltujen valtioneuvoston asetuksen ehtojen mukaisesti olisi ensin tärkeää tunnistaa mikä tieto on julkista ja mikä salassa pidettävää. Tietovuodoilta välttyminen on hyvin epätodennäköistä, mikäli organisaatio ei tunnista mikä tieto on arvokasta ja mikä ei (Rousku 2014, 89). Muun kuin julkisen tiedon käsittely vaatii tyypillisesti normaaleista toimenpiteistä poikkeavia käsittelymenetelmiä. Tämä korostuu etenkin henkilötietoja käsiteltäessä, koska osa niistä on salassa pidettävää. Lisäksi on oleellista tietää, minkä kaltaista tietoa itse työtehtävissään käsittelee. Tietojen luokitteleminen ja tiedon käsittelyyn liittyvä ohjeistus kuuluu kaikille, ja kaikkien tulisi niitä siis noudattaa. Ohjeita noudattamalla tietoturvallinen työskentely kulkee mukana myös julkisen tiedon eheyden ja saatavuuden toteuttamisessa. (Järvinen & Rousku 2017, 45–46.)

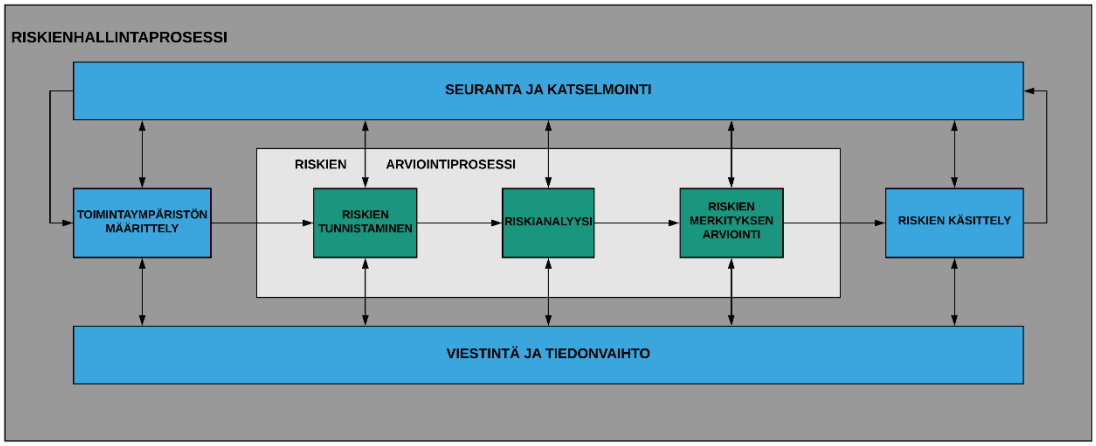
6 TIETOTURVAKARTOITUS- JA RISKIENHALLINTAPROSESSI

Tietoriskit nousevat yhä useammin esille organisaatioissa tehtävissä riskiarvioinneissa. Järvinen ja Rousku (2017, 147) kertovat tietoturvallisuuden olevan uhkien tunnistamista sekä niiden hallitsemista osana muuta riskienhallintaa. Organisaatiossa käytössä olevat tietoturvatoimenpiteet olisikin hyvä perustaa säännöllisesti tehtävään ja kattavaan tietoriskien arviointiin. Näin toimittuaan organisaatio pystyy hyödyntämään riskien arviointia osana riskienhallintaa ja toiminnan suunnittelua. Uusien uhkakuvien takia myös organisaation toiminnan taustalla toimivaa teknistä tietoturvallisuutta tulisi jatkuvasti kehittää (Mts. 149). Tietoriskejä tulisi arvioida organisaation omien toimintojen ja niiden saavuttamiseksi asetettujen tavoitteiden perusteella. Lisäksi riskit tulisi suhteuttaa vallitsevaan lainsäädäntöön sekä toimintaympäristön vaatimuksiin. Vuonna 2009 laadittu ISO 31000 -standardi kuvaa riskienhallinnan termit, prosessit ja periaatteet. Sitä voivat hyödyntää julkiset organisaatiot, yksityisyritykset, järjestöt, ryhmät ja jopa yksityishenkilöt. (Andreasson & Koivisto 2013, 38–39.)

VAHTI on laatinut kyseisen ISO 31000 -standardin pohjalta riskienhallintaohjeen tavoitteenaan tehostaa ja yhdenmukaistaa ministeriöiden, virastojen, laitosten sekä muun julkisen hallinnon riskienhallintaa. Ohjetta on mahdollista soveltaa laaja-alaisesti useimpiin organisaation toimintoihin. Jokainen organisaatio on kuitenkin itse vastuussa omista riskien käsittelyä koskevista päätöksistä ja niiden pohjalta tehdyistä toimenpiteistä. (Valtiovarainministeriö.)

Ohjeessa on selkeästi määritelty riskienhallintaprosessi, joka itsessään sisältää kaikki riskeille tehtävät toimenpiteet, joita tulisi toteuttaa johdon hyväksymiä riskienhallinnan toimintaohjeita ja -malleja sekä riskienhallintapolitiikkaa noudattaen. Onnistuneen riskienhallinnan tulisi olla sekä aktiivista että muutoksiin reagoivaa. Tämän toteutumiseksi riskienhallinnan kehittämisen tulisi olla määrätietoista ja tarkoituksenmukaista, ja sen tulisi olla osa jokaisen organisaation työntekijän arkipäiväistä työtä. Yksinkertaisesti tulkittuna riskienhallintaprosessi alkaa toimintaympäristön määrittelyllä, missä tehdään rajaukset riskien arvioinnin osalta. Tämän onnistuminen vaatii sen, että organisaatio tunnistaa merkittävimmät riippuvuudet. Seuraava vaihe on riskien arviointiprosessi, jossa tunnistetaan toiminnalle ominaiset riskit ja mahdollisuudet, luodaan niiden pohjalta riskianalyysi ja lopuksi arvioidaan riskien merkitystä organisaation toiminnalle. Arvioinnin

tavoite on auttaa päätösten teossa liittyen käsiteltäviin riskeihin ja niiden tärkeysjärjestykseen. Tämän jälkeen riskien käsittelyprosessissa päätetään riskikohtaisista toimenpiteistä. Koko prosessin kaikkia vaiheita seurataan ja katselmoidaan valvonnan ja tarkastuksen keinoin, jotta riskienhallintakeinojen vaikuttavuudesta ja tehokkuudesta voidaan varmistua. (Valtiovarainministeriö 2017, 18–28.) Tätä prosessia kuvataan kuviossa 5.



Kuvio 5. Riskienhallintaprosessi (Valtiovarainministeriö 2017, 18).

Tietoturvakartoitusta organisaatiolle miettiessä vaihtoehtoja on loputon määrä. Tietoturvakartoitus on mahdollista ostaa palveluna kolmannelta osapuolelta tietoturvakonsultointina, jonka lisäksi internet on pullollaan erilaisia ohjeita tietoturvakartoituksen koostamiseksi ja toteuttamiseksi. Esimerkiksi Santa Fe Groupin hallinnoima ja ylläpitämä Standard Information Gathering (SIG) Questionnaire on yksi tunnettu tietoturvakartoituksen työkalu, jota organisaation on myös mahdollista hyödyntää tietoturvallisuuden itsearvioinnissa sen lisäksi, että kartoitus toteutettaisiin kolmannen osapuolen toimesta (Santa Fe Group).

Tietoturvaan ja -kartoitukseen liittyvän tietoaineiston valtavan määrän takia on hyvä ensin tutustua kartoituksen rakenteeseen. UpGuard-sivustolla on esitelty selkeä kahdeksanvaiheinen opas, jossa käydään vaiheittain läpi miksi ja miten tietoturvakartoitus olisi hyvä toteuttaa. Prosessi tulisi aloittaa tunnistamalla kuinka arvokasta organisaation käsittelemä tieto on, jonka jälkeen tulisi tunnistaa ja priorisoida organisaation voimavarat tärkeysjärjestykseen sen ajatusmallin mukaisesti, että kartoitus rajataan vain tärkeimpiin voimavaroihin. Näin kartoituksesta saadaan mahdollisimman tarkoituksenmukainen.

Seuraavaksi tulisi tunnistaa ja arvioida yrityksen toiminnalle ominaisia riskejä sekä haavoittuvuuksia ja niiden vaikutuksia. Näiden pohjalta tulisi analysoida jo olemassa olevia toimintamenetelmiä ja ratkaisuja riskien ja haavoittuvuuksien varalle, sekä tarvittaessa ottaa käyttöön uusia tai muokata vanhoja paremmin soveltuviksi. Tämän jälkeen laskelmoidaan riskeistä ja haavoittuvuuksista johtuvien skenaarioiden tapahtumisen todennäköisyyksiä sekä seurauksia organisaation toiminnalle. Todennäköisyyksien perusteella voidaan jälleen priorisoida riskit suhteuttamalla tiedon arvoa ennaltaehkäisyn kustannuksiin. Lopulta viimeisessä vaiheessa prosessin kaikki vaiheet ja niiden tulokset dokumentoidaan yhtenäiseksi raportiksi. (Tyas Tunggal 2020.)

Myös kotimaisesta tietoturvallisuuteen liittyvästä kirjallisuudesta löytyi hyviä suuntaa antavia esimerkkejä ja malleja, joita voi hyödyntää tietoturvakartoituksen laatimisessa. Kimmo Rouskun Kyberturvaopas -kirjassa on esitelty yksinkertainen malli siitä, minkälainen tietoturvaan liittyvä testi voisi olla, ja kuinka sen tuloksia tulisi tulkita (2014, 38–47). Työpaikan tietoturvaoppaassa on puolestaan esitelty esimerkki tietoturvan kymmenen kohdan huoneentaulusta, johon on listattu kymmenen tietoturvallisuuden toteuttamisen kannalta tärkeää toimintatapaa. Listatut toimintatavat liittyvät muun muassa hyviin salasanakäytäntöihin, huolelliseen laitteiden, palveluiden ja tiedostojen käyttöön sekä oman organisaation tietoturvaohjeiden seuraamiseen ja noudattamiseen. (Järvinen & Rousku 2017, 152–156.) Andersson ja Koivisto (2013, 250-251) esittelevät vastaavanlaisen 10 kohdan tietoturva- ja tietosuojahuoneen taulun.

7 CASE JIMM'S PC-STORE OY

Opinnäytetyön tekemisestä sovittiin toimeksiantajaorganisaation kanssa ensin kartoittamalla sopivaa aihetta, josta kumpikin osapuoli hyötyisi tasapuolisesti. Toimeksiantajan kanssa sovittiin tietoturvakartoituksen sekä sen pohjalta laaditun raportin tekemisestä, koska edellisestä kokonaisvaltaisesta tietoturvallisuuden kartoituksesta on jo aikaa. Yritys on myös kokenut merkittävän organisaatiomuutoksen, jonka lisäksi yrityksen koko on kasvanut paljon vuosien mittaan toiminnan sekä liikevaihdon kasvun myötä. Kartoituksen avulla organisaatio saa päivitettyä tietoa sen tietoturvallisuuden tasosta sekä ehdotuksia mahdollisista tietoturvallisuutta parantavista toimenpiteistä.

Tietoturvakartoitusta varten laaditun kyselyn tulokset sekä niiden pohjalta laadittu raportti jätetään työstä pois salassa pidettävänä materiaalina, koska ne sisältävät yrityksen liiketoiminnan kannalta luottamuksellista tietoa.

7.1 Yrityksestä

Jimm's PC-Store Oy on vuonna 2001 perustettu tietotekniikan, komponenttien ja viihde-elektroniikan verkkokauppa, joka työllistää tällä hetkellä noin 50 työntekijää. Yritys panostaa vahvasti verkkokauppaan, mutta tarjoaa silti asiakkailleen mahdollisuuden asioida myös noutomyymälässä toimipisteellään Turussa. Verkkokauppaan panostamisesta kertoo se, että Jimm'sin asiakaspalvelu on tavoitettavissa puhelimitse, sähköpostitse sekä verkkosivuilla olevan chat-palvelun kautta vuorokauden ympäri ja vuoden jokaisena päivänä. Lisäksi yritys hyödyntää vahvasti sosiaalista mediaa yhtenä kontaktikanavista. Yritys on vahvasti vuorovaikutuksessa alan harrastajien foorumeilla, ja on lähtenyt mukaan tukemaan alati kasvavaa eUrheilua. Vuoden 2018 alussa organisaatio koki suuren muutoksen, kun Jimm's PC-Store myytiin saksalaiselle Caseking-verkkokaupalle, ollen nyt osa Caseking Group-konsernia. (Jimm's PC-Store -verkkosivut)

7.2 Tietoturvakartoituksen tekeminen Katakrin avulla

Aluksi tutustuin tietoturvallisuuden teoriaan ja aloin vertailemaan eri työkaluja sekä ohjeita tietoturvakartoituksen tekemiseksi. Toimeksiantajaorganisaatiolle on aikaisemmin tehty tietoturvakartoitus pohjautuen Santa Fen hallinnoimaan SIG-kyselyyn. Tutkin mahdollisuutta hyödyntää samaa kyselyä tulosten helpomman vertailtavuuden takia, mutta SIG-kyselyn uusin versio ei ole vapaasti käytettävissä, vaan se on maksullinen lisenssi. Vanhempaa SIG-kyselyn versiota ollaan käytetty aikaisemmin osana Turun AMK:n kurssimateriaaleja, mutta koulun materiaaleissa oleva versio todettiin liian vanhaksi, jotta sitä voisi hyödyntää tietoturvakartoituksen tekemisessä. Lisäksi SIG-kyselyn käyttöehdoissa on mainittu, että sen muokkaaminen ilman Santa Fe:n erillistä konsultointia on ehdottomasti kielletty. Kysely kokonaisuudessaan olisi myös ollut sisällöltään liian laaja käytettävissä oleviin resursseihin nähden. Tutustuttani tarkemmin kansallisen turvallisuusauditointikriteeristön (Katakri) sisältöön ja rakenteeseen, totesin sen soveltuvan mainiosti käyttötarkoituksiini. Katakrissa on selkeä ja perusteltu rakenne ja se on hyvin sovellettavissa Jimm’s PC-Storen tarpeisiin, jonka lisäksi siinä esiteltyjen kattavien esimerkkitapausten sekä vaatimusten ansiosta sitä on myös mahdollisuus käyttää hyödyksi kartoituksen tuloksia analysoidessa.

Tietoturvakartoituksen kysymyspatteristoa tehdessä hyödynsin Katakrin lisäksi muuta tässä opinnäytetyössä jo esiteltyä tietoaineistoa ja ohjeistuksia kuten esimerkiksi luvussa 6 esiteltyä UpGuard-sivustolta löytyvää opasta tietoturvakartoituksen rakenteesta. Kartoitusta varten laaditut kysymykset löytyy opinnäytetyön liitteenä.

Katakrissa tietoturvallisuus ollaan jaoteltu turvallisuusjohtamiseen, fyysiseen turvallisuuteen sekä tekniseen tietoturvallisuuteen. Tätä rakennetta käytettiin hyödyksi tietoturvakartoituksen kysymyksiä laadittaessa. Rakenteen hyödyntäminen helpottaa kartoituksen tulosten analysointia, jolloin tarvittavat kehitys- ja parannusehdotukset voidaan antaa kootusti ja kohdistetusti esimerkiksi hallinnollisissa keinoissa olevia puutteita koskien.

Katakri jakaa tietoturvallisuuden kolmeen osa-alueeseen: turvallisuusjohtamiseen, fyysiseen turvallisuuteen ja tekniseen tietoturvallisuuteen, jotka käsitellään seuraavissa kappaleissa.

7.2.1 Turvallisuusjohtaminen

Katakrissa turvallisuusjohtaminen osa-alueena muodostuu henkilöstöturvallisuudesta ja hallinnollisesta turvallisuudesta, joihin liittyvien menetelmien avulla yrityksen turvallisuus ja sen hallinta määritellään osaksi koko organisaation päivittäistä toimintaa. Lähtökohta hyvälle turvallisuusjohtamiselle on, että johto sitoutuu organisaation turvallisuustyöhön ja että tehty turvallisuustyö tukee koko organisaation toimintaa. Tämä tarkoittaa sitä, että laaditut turvallisuusperiaatteet viestitään henkilöstölle ja tarvittaville sidosryhmille. Turvallisuuden hoitamisen tehtävät ja vastuut tulee myös olla määritelty niin että keskeisimmille osa-alueille on nimetty tekijät, jotka tuntevat omat vastuualueensa sekä valtuutensa tietoturvallisuuden toteutumisen varmistamiseksi.

Jotta turvallisuusjohtamisen osa-aluetta voidaan käyttää tarkoituksenmukaisesti, tulee arviointia kohdentaa siihen osaan organisaatiota, jossa tietoa käsitellään. Tietoturvallisuuden toteutuminen vaatii myös organisaatiolta riittävää asiantuntemusta.

Hallinnollisen ja henkilöstöturvallisuuden lisäksi riskienarviointi sekä -hallinta suhteutettuna suojattavaan tietoon ja kohdeorganisaation toimintaan tulee ottaa huomioon. Riskienhallinta on koko organisaation johtamiseen ja toimintaan sisältyvä prosessi, jota tulee soveltaa kaikessa organisaation toiminnassa. Riskienhallinnalla tavoitellaan, että organisaation toimintaedellytyksiä vaarantavat tekijät tunnistetaan ja toimintaan kohdistuvat riskit saadaan hallitusti pidettyä sellaisissa rajoissa, ettei organisaation toiminta ja tavoitteet olisi uhattuina. Riskienhallinnan tulisi olla luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä. (Katakri 2015, 3, 6–8.)

7.2.2 Fyysinen turvallisuus

Katakrissa fyysistä turvallisuutta tarkastellaan viranomaisen salassa pidettävän tietoaineiston suojaamisen näkökulmasta siten, että se ei voi paljastua oikeudettomasti. Fyysisillä turvatoimilla on tarkoitus estää sekä ulkopuolisten että sisäisten tahojen asiaton pääsy salassa pidettäviin tietoihin esimerkiksi estämällä tunkeutuminen, havaitsemalla luvattomat toimet sekä mahdollistamalla henkilöstön luokitus tiedonsaantitarpeen mukaisesti. Katakri määrittää tilat ja tilaryhmät erilaisiin alueisiin: hallinnolliseen alueeseen, turva-alueeseen ja tekniseen turva-alueeseen. Tämä aluejako perustuu EU:n neuvoston turvallisuussääntöihin.

Fyysisen turvallisuuden perusta on suunnittelussa, ja valitut toimet tulisi valita sekä mitoittaa uhkakartoitukseen ja riskienarviointiin pohjautuen. On esimerkiksi tärkeää tunnistaa, missä tiloissa suojattavaa tietoa käsitellään ja minkä suojaustason tietoja tilassa käsitellään. Nimensä mukaisesti fyysiset turvatoimet muodostuvat rakennusten ja tilojen suunnittelusta rakenteellisiin suojaratkaisuihin, käytettäviin turvajärjestelmiin ja -laitteisiin sekä turvallisuutta ylläpitäviin menettelytapoihin. Näiden toteutuksessa hyödynnetään monitasoisen suojaamisen periaatetta, jolloin toteutetaan joukko toisiaan täydentäviä turvatoimia. Tällaisia toimia ovat esimerkiksi kulunvalvonta ja kameravalvonta. Mahdollisuuksien mukaan organisaation tilat muodostaisivat keskenään sisäkkäisiä vyöhykkeitä, joista kaikkein sisimmät tilat olisivat korkeimman suojaustason tiloja. (Katakri 2015, 16–17.)

7.2.3 Tekninen tietoturvallisuus

Teknisen tietoturvallisuuden osa-alueessa kuvataan vaatimukset, joilla voidaan varmistaa riittävät turvallisuusjärjestelyt salassa pidettävän tiedon sähköisissä käyttöympäristöissä. Kuten fyysisessä turvallisuudessa ja turvallisuusjohtamisessa, myös teknisen tietoturvallisuuden tarkoituksenmukainen käyttö edellyttää riskienarvioinnin pohjalta tapahtuvaa vaatimusten tulkintaa kyseessä olevaan ympäristöön kohdistettuna. Teknistä tietoturvallisuutta tarkastellaan tietoliikenteen, tietojärjestelmien, tietoaineistojen ja käyttöturvallisuuden vaatimusten osalta, jonka lisäksi se käsittelee myös tiettyjä asiakokonaisuuksia vaatimuksineen. Näitä asiakokonaisuuksia ovat esimerkiksi verkon rakenne, langattomat verkot, etäkäyttö, järjestelmien kovennus ja haittaohjelmasuojaus. (Katakri 2015, 29–44.)

8 POHDINTA

Opinnäytetyön tavoitteena oli tehdä työn toimeksiantajalle tietoturvakartoitus sekä raportoida sen tuloksista kootusti. Toimeksiantajana työssä toimineella Jimm's PC-Storella oli omana tavoitteenaan tarkastella kokonaisvaltaisesti tietoturvallisuuden nykyistä tasoa, sekä kehittää omaa toimintaansa entisestään. Tietoturvakartoitus on tähän tarkoitukseen hyvä keino, koska vaatimustenmukaisuus, jota kartoituksen avulla voidaan mitata, ohjaa tietoturvallisuutta. Tietoturvallisuuden tulisi taas olla integroitu osaksi organisaation päivittäistä toimintaa. Työn tuloksena saatiin aikaan yrityksen käyttöön soveltuva tietoturvakartoitus, jonka avulla saatiin päivitettyä tietoa yrityksen tietoturvallisuudesta, sekä mahdollisista kehityksen kohteista.

Tietoturvakartoituksen laatimiseksi sekä toteuttamiseksi tuli ensin perehtyä tietoturvakartoituksen tekemiseen teorian tasolla. Tämän onnistumiseksi tuli kuitenkin myös ymmärtää mitä tietoturvallisuus ylipäätään on, miksi se on tärkeää ja mistä se tarkalleen koostuu. Oleellista oli myös tutustua tietoturvallisuutta ohjaaviin tekijöihin kuten lakeihin, asetuksiin ja ohjeistuksiin. Tämän jälkeen yksittäisenä isompana työn vaiheena oli itse tietoturvakartoituksen laatiminen, toteuttaminen ja tulosten analysointi raportin muotoon. Kartoituksen avulla saavutetut tulokset on jätetty julkaisusta pois salassa pidettävänä materiaalina, koska ne sisältävät yrityksen liiketoiminnan kannalta luottamuksellista tietoa. Laaditut ja käytetyt kysymykset löytyvät kuitenkin työn liitteenä.

Heti työn alkuvaiheilla kävi selväksi, että tietoturvallisuus on aiheena todella laaja, ja siitä on saatavilla valtavasti tietoa kirjoissa, sähköisissä lähteissä sekä laadituissa tutkimuksissa. Haasteeksi tässä vaiheessa muodostui ensinnäkin luotettavien ja ajantasaisten materiaalien sekä lähteiden löytäminen vanhentuneiden ja epäluotettavien joukosta. Lisähaasteita esimerkiksi kirjallisuuden tavoittelussa aiheutti kirjastojen kiinniolo Covid-19 -pandemian seurauksena määrätyn poikkeustilan takia. Työn toteuttamiseksi saatiin lopulta rajattua luotettavat ja eheät lähteet, joista saatua tietoa ammentamalla toimeksianto sekä tämä opinnäytetyö on laadittu. Lähteiden hakuun ja tutustumiseen liittyen huomattiin että esimerkiksi useat VAHTI-ohjeet olivat edelleen ajantasaisia ja luotettavia tiedonlähteitä niiden vanhemmasta julkaisuajankohdasta huolimatta.

Toimeksiannon toissijaisena tavoitteena olin pitänyt alusta alkaen oman tietämyksen sekä osaamisen kehittymistä, joka sekin toteutui hienosti opinnäytetyöprojektin edetessä. Oma toiminta esimerkiksi suunnittelemisen ja sen mukaisen toteuttamisen

suhteen koki valtavan kehityksen aikaisempaan nähden. Lisäksi kehitin omaa tietämystä ja osaamista tietoturvallisuudessa, mistä on varmasti hyötyä tulevaisuuden työtehtävissä. Kehittämisen varaa voisi suunnitelmallisuuden kehittymisestä huolimatta olla ajankäytössä sekä vielä tarkemmassa työn rajaamisessa. Etenkin projektin alkuvaiheilla tiedon valtava määrä aiheutti sen, että yksittäiseenkin lähteeseen oli mahdollista saada kulumaan päiviä aikaa sen sisältämien tärkeimpien asioiden sisäistämiseksi. Myös mielenkiintoisiin aiheisiin törmätessä tulisi pidättäytyä aikaisemmin määriteltyjen rajauksien sisäpuolella.

Kokonaisuudessaan työn loppuun saattamisen jälkeen voidaan todeta, että tietoturvallisuus on sellainen asia, jota kukaan ei voi jättää täysin huomiotta. Tietoturvallisuuden keinoin pyritään varmistamaan organisaation liiketoimintaa. Kun tietoturvallisuuden menetelmät ja prosessit ovat toimivia ja organisaation päivittäiseen toimintaan integroituja, se kehittää ja vahvistaa organisaation valmiuksia tulevaisuuden teknologioita ja niiden mukanaan tuomia haasteita ajatellen. Lisäksi on huomioitava, että tietoturvallisuudesta ei vastaa ainoastaan yrityksen johto tai turvallisuuteen koulutettu ja kouluttautunut henkilöstö, vaan se on jokaisen organisaation työntekijän velvollisuus. Tämä kuitenkin vaatii sitä, että oikeat toimintamallit ovat kaikille ohjeistettu tai koulutettu.

LÄHTEET

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma Oy.

Andress, J. 2011. The Basics of information security – Understanding the Fundamentals of InfoSec in theory and Practice. United States of America: Elsevier Inc.

Elinkeinoelämän keskusliitto 2020. Tietoturvallisuus. Viitattu 8.5.2020 https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/tietoturvallisuus/.

EU:n yleinen tietosuoja-asetus 27.4.2016/679. Saatavilla https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504.

Jimm's PC-Store verkkosivut. Viitattu 6.6.2020 https://www.jimms.fi/fi/Info/Contact.

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas – tunnista uhat, hallitse riskit. Helsinki: Alma Talent.

Kirsi K. 2020. Kyberhyökkäykset häiritsevät etäkoulua – tekijöinä lapset ja nuoret. YLE. Viitattu 8.5.2020. Saatavilla https://yle.fi/uutiset/3-11286403.

Kupreev, O.; Badovskaya, E. & Gutnikov, A. 2020. Securelist - DDoS attacks in Q1 2020. Kaspersky. Viitattu 8.5.2020 https://securelist.com/ddos-attacks-in-q1-2020/96837/.

Laki sähköisen viestinnän palveluista 7.11.2014/917. Saatavilla https://finlex.fi/fi/laki/ajantasa/2014/20140917.

Laki yksityisyyden suojasta työelämässä 13.8.2004/759. Saatavilla https://www.finlex.fi/fi/laki/ajantasa/2004/20040759.

Laki yksityisyyden suojasta työelämässä annetun lain muuttamisesta 15.3.347/2019. Saatavilla https://www.finlex.fi/fi/laki/alkup/2019/20190347.

Puolustusministeriö. Katakri 2015 – Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 25.5.2020 https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf.

Rousku, K. 2014. Kyberturvaopas – Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum Media Oy.

Santa Fe Group. Standardized Information Gathering (SIG) Questionnaire. Viitattu 31.5.2020 https://sharedassessments.org/sig/.

TEPA-termipankki. Viitattu 19.5.2020 https://termipankki.fi/tepa/fi/.

Tietosuojalaki 5.12.2018/1050. Saatavilla https://www.finlex.fi/fi/laki/ajantasa/2018/20181050.

Tietosuojavaltuutetun toimisto a. Tietosuoja. Viitattu 31.5.2020 https://tietosuoja.fi/tietosuoja.

Tietosuojavaltuutetun toimisto b. Tietosuoja - Mikä on henkilötieto? Viitattu 31.5.2020 https://tietosuoja.fi/mika-on-henkilotieto.

Tietosuojavaltuutetun toimisto c. Organisaatiot - Kerro käsittelystä rekisteröidylle. Viitattu 31.5.2020 https://tietosuoja.fi/rekisteroidyn-informointi.

Tietosuojavaltuutetun toimisto d. Organisaatiot – Tietosuojaperiaatteet. Viitattu 31.5.2020 https://tietosuoja.fi/tietosuojaperiaatteet.

Tietosuojavaltuutetun toimisto e. Tietosuoja - Tietosuojalainsäädäntöä. Viitattu 31.5.2020 https://tietosuoja.fi/lainsaadanto.

Tietosuojavaltuutetun toimisto f. Tietosuoja - Tietosuojalaki. Viitattu 31.5.2020 https://tietosuoja.fi/tietosuojalaki.

Tietosuojavaltuutetun toimisto g. Yksityishenkilöt – Tunne oikeutesi. Viitattu 31.5.2020 https://tietosuoja.fi/tunne-oikeutesi.

Turvallisuuskomitea 2018. Kyberturvallisuuden sanasto. Viitattu 8.5.2020 https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/.

Tyas Tunggal, A. 2020 How to perform a cyber risk assessment: Step-by-Step Guide. Viitattu 31.5.2020. https://www.upguard.com/blog/cyber-security-risk-assessment.

VAHTI 04/2004. Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. Viitattu 9.5.2020 https://www.vahtiohje.fi/web/guest/5/2004-valtionhallinnon-keskeisten-tietojarjestelmien-turvaaminen.

VAHTI 03/2007. Tietoturvallisuudella tuloksia – Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Viitattu 9.5.2020 https://www.vahtiohje.fi/web/guest/tietoturvallisuudella-tuloksia.

VAHTI 02/2008. Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta. Viitattu 9.5.2020 https://www.vahtiohje.fi/web/guest/2/2008-tarkein-tekija-on-ihminen-henkilostoturvallisuus-osana-tietoturvallisuutta.

VAHTI 08/2008. Tietoturvasanasto. Viitattu 24.5.2020 https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto.

VAHTI 02/2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Viitattu 12.5.2020 https://www.vahtiohje.fi/web/guest/2/2010-ohje-tietoturvallisuudesta-valtionhallinnossa-annetun-asetuksen-taytantoonpanosta.

VAHTI 04/2013. Henkilöstön tietoturvaohje, Tietoturvallisuus – mitä se on? Viitattu 8.5.2020 https://www.vahtiohje.fi/web/guest/4/2013-henkiloston-tietoturvaohje.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681. Saatavilla Saatavilla https://www.finlex.fi/fi/laki/ajantasa/2010/20100681.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681. Annettu Helsingissä 1.7.2010. Saatavilla https://www.finlex.fi/fi/laki/ajantasa/2010/20100681.

Valtiovarainministeriö 2017. Ohje riskienhallintaan. Viitattu 31.5.2020 http://julkaisut.valtioneuvosto.fi/handle/10024/80013.

Valtiovarainministeriö. Riskienhallinnan ohjeita. Viitattu 31.5.2020 https://vm.fi/riskienhallinnan-ohjeita.

Valtiovarainministeriö. VAHTI-toiminta. Viitattu 30.5.2020 https://vm.fi/vahti.

Tietoturvakartoituksen kysymykset

TURVALLISUUSJOHTAMINEN

1. Onko yrityksellä johdon hyväksymä ja voimassa oleva tietoturvasuunnitelma?
2. Onko kyseinen tietoturvasuunnitelma vastuutettu tietylle taholle, joka ylläpitää sitä?
3. Järjestääkö yritys henkilökunnalle sekä tarvittaville sidosryhmille säännöllisesti tietoturvakoulutusta?
4. Onko tietoturvakoulutuksen sisältö dokumentoitu?
5. Onko turvallisuusohjeistus henkilöstön helposti saatavissa?
6. Koska tietoturvasuunnitelmaa on tarkasteltu ja tarpeen mukaan muokattu viimeksi?
7. Onko turvallisuuden hallintaan liittyvät tehtävät vastuutettu tietylle taholle?
8. Onko henkilöstöturvallisuus ja siihen liittyvät tehtävät vastuutettu tietylle taholle?
9. Onko fyysinen turvallisuus ja siihen liittyvät tehtävät vastuutettu tietylle taholle?
10. Onko tietotekninen turvallisuus ja siihen liittyvät tehtävät vastuutettu tietylle taholle?
11. Onko vastuu turvallisuusdokumentaation kattavuuden ja ajantasaisuuden säännöllisestä seuraamisesta vastuutettu tietylle taholle?
12. Onko yrityksellä riittävästi asiantuntemusta sekä tietotaitoa tietoturvallisuuden toteutumisen varmistamiseksi?
13. Arvioidaanko resurssien riittävyyttä tietoturvallisuuden toteutumiselle säännöllisin väliajoin?
14. Onko yrityksellänne käytössä riskienhallintaprosessi?

15. Valitse kohdat, jotka pitävät paikkaansa riskienhallintaprosessin osalta.

16. Onko riskienhallintaprosessin ylläpito vastuutettu tietylle taholle?

17. Onko riskienhallintaprosessin avulla saadut johtopäätökset kuvattu yrityksen tietoturvasuunnitelmassa?

18. Onko yrityksellä dokumentoitu toiminnan jatkuvuussuunnitelma toipumisen ja jatkuvuuden varmistamiseksi?

19. Sisältääkö toiminnan jatkuvuussuunnitelma korjaavia sekä ehkäiseviä toimenpiteitä?

20. Tunnistaako yritys riippuvuudet ulkoisista tekijöistä sekä niiden vaikutuksista omaan toimintaan?

21. Tunnistaako yritys oman toiminnan vaikutuksen muihin?

22. Järjestetäänkö yrityksessä testejä toiminnan jatkuvuuden osalta?

23. Onko yrityksellä päivitetyt ajantasaiset ohjeet hätä- ja poikkeustilojen kuten esimerkiksi tulipalon tai pandemian varalle?

24. Ovatko hätä- ja poikkeustilojen ohjeet henkilökunnan helposti saatavilla?

25. Onko yrityksellä dokumentoitu suunnitelma turvallisuuspoikkeamien hallintaan?

26. Onko suunnitelmassa määritelty taho(t), joille turvallisuuspoikkeamista tai niiden epäilyistä tulee ilmoittaa?

27. Onko tämä tieto viestitetty koko henkilökunnalle oikeaoppisen toiminnan varmistamiseksi?

28. Kirjataanko ilmoitetut poikkeamat ylös, jotta niitä voidaan hyödyntää jatkuvuus- sekä turvallisuuspoikkeamien suunnitelmien kehitystyössä?

29. Onko yrityksessä käytössä menetelmiä tiedon luokittelemiseksi?

30. Onko tietosisällöltään salassa pidettävät aineistot ja asiakirjat varustettu suojaustasoa kuvaavalla merkinnällä?

31. Onko henkilökuntaa koulutettu salassa pidettävän tietoaineiston oikeaoppisesta käsittelystä?

32. Valitse työsuhteen elinkaaren vaiheista ne, joista on olemassa selkeät dokumentoidut ohjeet

a. Rekrytointi / perehdytys / työsuhteen aikaiset muutokset / työsuhteen päättyminen

33. Onko yrityksellä erityisohjeistusta, miten kiire- tai varahenkilöstön kanssa tulee toimia?

34. Valitse vaihtoehdot, joiden osalta yritys selvittää työntekijöiden taustoja.

a. Rikokset / huumeet / koulutus / suosittelijat / työhakemus,cv

35. Onko yrityksellä käytössä salassapito- tai vaitiolositoumusmenettely?

36. Koskeeko salassapito- tai vaitiolositoumusmenettely koko henkilökuntaa?

37. Ylläpidetäänkö yrityksessä salassa pidettävän tiedon käsittelyä edellyttävien työtehtävien listaa?

38. Onko kyseisen listan ylläpito ja seuranta vastuutettu jollekin taholle?

39. Onko yrityksellä dokumentoitu menettelytapa tiedonsaantitarpeen määrittämiseksi?

FYYSINEN TURVALLISUUS

40. Onko yrityksellä voimassa oleva fyysisen turvallisuuden suunnitelma?

41. Onko yrityksen tiloissa mahdollista hyödyntää kehäsuojausta?

42. Muodostavatko tilat sisäkkäisiä vyöhykkeitä, joista sisimmässä on kaikkein korkein suojaus?

43. Onko yrityksellä käytössä pääsyoikeuksien hallinnan menetelmiä?

44. Onko yrityksellä omaa koulutettua ja valvottua turvallisuushenkilökuntaa?

45. Onko yrityksellä sopimus ulkoisen toimijan kanssa kiinteistön sekä organisaation tietojen koskemattomuuden takaamiseksi?

46. Onko kameravalvonnan kuvaa mahdollista seurata reaaliajassa valvomosta?

47. Onko kulunvalvonnan hallintajärjestelmän menettelytavat dokumentoitu?

48. Miten yrityksen oma henkilökunta tunnistetaan?

a. Kuvallinen henkilökortti (aina esillä) / Kuvallinen henkilökortti (esitettävä pyydettäessä) / Henkilökohtainen tunnistaminen

49. Onko kulkuoikeuksien myöntäminen vastuutettu jollekin taholle?

50. Onko myönnetyistä kulkuoikeuksista laadittu dokumentti?

51. Ylläpitääkö myönnettyjen kulkuoikeuksien dokumenttia nimetty vastuuhenkilö?

52. Kuinka usein myönnettyjen kulkuoikeuksien ajantasaisuutta tarkastellaan?

53. Voiko yrityksen tiloihin tulla vierailijoita?

54. Onko vieraiden olintilaa rajattu?

55. Onko vieraille sallittu tila selkeästi/näkyvästi rajattu?

56. Käyttävätkö yrityksen tiloissa vierailevat henkilöt näkyvää tunnistetta, kuten vierailijakorttia? (silloin kun vierailijat liikkuvat vierailijoille sallitun tilan ulkopuolella)

57. Onko henkilökuntaa koulutettu vierailijoita koskevista menettelytavoista?

58. Onko yrityksen tiloissa luvallista kuvata? Onko sitä rajattu jotenkin?

59. Onko yrityksellä voimassa olevia toimintaohjeita tiloissa tehtävien muutosten osalta?

60. Valitse seuraavista järjestelmistä sekä laitteista ne, joita yrityksellä on käytössä.

a. kassa- tai turvakaapit ja elementtiholvit / ovet, aukot ja lukot heloineen / hälytysjärjestelmät / kulunvalvontajärjestelmät / kameravalvontajärjestelmät / liiketunnistimet / paperisilppurit

61. Valitse seuraavista järjestelmistä sekä laitteista ne, jotka ovat hyväksyttyjen teknisten standardien tai vähimmäisvaatimusten mukaisia.

a. kassa- tai turvakaapit ja elementtiholvit / ovet, aukot ja lukot heloineen / hälytysjärjestelmät / kulunvalvontajärjestelmät / kameravalvontajärjestelmät / liiketunnistimet / paperisilppurit

62. Valitse seuraavista järjestelmistä sekä laitteista ne, joiden testaus ja huolto on säännöllistä.

a. kassa- tai turvakaapit ja elementtiholvit / ovet, aukot ja lukot heloineen / hälytysjärjestelmät / kulunvalvontajärjestelmät / kameravalvontajärjestelmät / liiketunnistimet / paperisilppurit

63. Onko yrityksellä käytössä avainten hallintajärjestelmä?

64. Onko toimitilojen, toimistojen, huoneiden, kassaholvien ja turvasäilytysyksiköiden avainten ja avaustunnisteiden hallintamenettelyt dokumentoitu?

65. Onko avainten ja avaustunnisteiden hallintajärjestelmä sekä siihen liittyvä dokumentointi vastuutettu tietylle taholle?

66. Onko jaetuista sekä vastuuhenkilön hallussa olevista avaimista olemassa ajantasainen luettelo?

67. Tarkistetaanko avainten hallintaoikeutta säännöllisesti?

68. Turvasäilytysyksiköiden ja kassaholvien avaustunnisteet vaihdetaan

a. Uuden säilytyspaikan vastaanoton yhteydessä / Mikäli avaustunnisteen tunteva henkilö poistuu yrityksen palveluksesta / Mikäli tiedot ovat vaarantuneet tai sitä epäillään / Kun jokin lukoista on huollettu tai korjattu / Vähintään 12kk välein

69. Onko yrityksellä keinoja salakatselun estämiseksi?

70. Onko yrityksellä keinoja salakuuntelun estämiseksi?

71. Yrityksen toiminnan kannalta kriittiset palvelimet ja laitteet on tunnistettu ja varmennettu

a. murtoa vastaan / ilkivaltaa vastaan / tulipaloa vastaan / lämpöä vastaan (ylikuumeneminen) / pölyä vastaan / sähkönkäytön katkoksia vastaan

72. Suojataanko ja valvotaanko yrityksen toiminnan kannalta kriittisten palvelin- ja laitetilojen olosuhdesensoreita?

TEKNINEN TIETOTURVALLISUUS

73. Onko yrityksellä omia palvelimia?

74. Käyttääkö yritys pilvipalveluita?

75. Onko tietojenkäsittely-ympäristö erotettu muista ympäristöistä?

76. Onko tietoliikenneverkko jaettu erillisiin verkkoalueisiin?

77. Valvotaanko ja rajataanko verkkoalueiden välistä liikennettä siten, että vain toiminnalle välttämätön liikennöinti on sallittu?

78. Onko tietojenkäsittely-ympäristössä varauduttu yleisiin verkkohyökkäyksiin? (esimerkiksi DDoS)

79. Valitse seuraavista protokollista ne, jotka on otettu huomioon yrityksen verkon suodatuksissa.

a. IPv4 / IPv6 / VPN

80. Valitse yrityksen järjestelmät, joista tarpeettomat protokollat on poistettu käytöstä.

a. Työasemat / Palvelimet / Verkkolaitteet

81. Onko verkosta ja siihen liittyvistä suodatus- ja valvontajärjestelmistä olemassa yhtenäinen dokumentaatio, jota ylläpidetään sen koko elinkaaren ajan?

82. Onko liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen ja poistaminen vastuutettu ja organisoitu?

83. Onko dokumentaatiossa kuvattu verkkorakenne verkkoalueineen?

84. Onko tietojenkäsittely-ympäristön palomuurisäännöt sekä palomuurien konfiguraatiot varmuuskopioitu?

85. Kuinka usein palomuurisäännöstöä tarkistetaan?

a. 3kk välein / 6kk välein / 12kk välein / harvemmin / aina merkittävien muutosten yhteydessä

86. Onko laitteiden ja liittymien hallinta vastuutettu tietylle taholle? (palomuurit, reitittimet, kytkimet yms.)

87. Onko laitteiden ja liittymien hallintayhteydenotot sallittu vain hyväksytyistä lähteistä vähimpien oikeuksien periaatteen mukaisesti? (palomuurit, reitittimet, kytkimet yms.)

88. Onko yrityksen tiloissa käytössä suojattuja langattomia verkkoja?

89. Onko langattomaan verkkoon kytkettyjen laitteiden määrää rajoitettu?

90. Onko yrityksen tiloissa henkilökunnan verkosta eriytetty vieraiden käyttöön tarkoitettu langaton verkko?

91. Onko järjestelmien käyttöoikeuksien käsittely ja myöntäminen dokumentoitu ja ohjeistettu?

92. Tarkistetaanko käyttöoikeuksien myöntämisen yhteydessä, että oikeuden saaja kuuluu henkilöstöön, tai on muutoin oikeutettu?

93. Onko järjestelmien käyttöoikeuksien hallinta vastuutettu tietylle taholle?

94. Onko järjestelmän käyttäjistä olemassa voimassa oleva ajantasainen lista?

95. Kuinka usein käyttäjälistaa tarkistetaan?

a. 3kk välein / 6kk välein / vuoden välein / harvemmin / en osaa sanoa

96. Jääkö jokaisesta myönnetystä käyttöoikeudesta dokumentti?

a. Sähköinen / paperi / ei jää / en osaa sanoa

97. Onko henkilöstömuutoksista ilmoittamisesta käyttöoikeuksia hallinnoivalle taholle olemassa selkeä ja toimiva käytäntö?

98. Onko korkeamman suojaustason materiaalit erillään julkisesta sekä muiden suojaustasojen tiedoista / käsitelläänkö kaikkea tietoa korkeimman suojaustason mukaisesti?

99. Onko tarkistusoikeuden varaavien tiedon omistajien tiedot säilytetty tietojärjestelmissä muista erillään?

100. Miten tarkistusoikeuden varaavien tiedon omistajien tiedot on eriytetty?

a. Loogisella tasolla (palvelinten virtualisointi tai käyttöoikeuksin rajoitetut verkkolevyasemat) / Fyysisellä tasolla (dedikoidut fyysiset laitteet) / Ei ole / en osaa sanoa

101. Onko kaikilla yrityksen henkilökunnan jäsenillä yksilölliset henkilökohtaiset käyttäjätunnisteet?

102. Käytetäänkö kaikkien käyttäjien kohdalla tunnistusta ja todennusta?

103. Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin johtaa tunnuksen:

a. Lukittumiseen / Väliaikaisen lukittumiseen / Ei seuraamusta / en osaa sanoa

104. Ovatko kaikkien käytettävien järjestelmien ja sovellusten ylläpitotunnukset henkilökohtaisia?

105. Mikäli yllä oleva ei ole kaikkialla toteutettavissa, onko yhteiskäyttöisille tunnuksille olemassa sovitut ja dokumentoidut salasanojen hallintakäytännöt?

106. Onko yrityksellä käytössä voimassa oleva selkeästi määritelty salasanapolitiikka?

107. Käytetäänkö kaksivaiheista tunnistusta niissä järjestelmissä missä se on mahdollista?

108. Käytetäänkö yrityksessä laitetunnistusta?

109. Onko verkon aktiivilaitteiden oletussalasanat vaihdettu yrityksen oman politiikan mukaisiksi?

110. Onko vain laitteille tarpeelliset verkkopalvelut päällä, jonka lisäksi ne on rajattu vain tarpeellisiin verkkoliittymiin?

111. Onko verkkolaitteiden ohjelmistot turvapäivitysten osalta ajan tasalla?

112. Onnistuuko verkkolaitteiden hallinta vain käyttäjä tunnistamalla ja todentamalla?

113. Onko hallintayhteyksissä käytössä istuntojen aikakatkaisu?

114. Onko palvelimien ja työasemien verkkopalvelut minimoitu, ja rajattu vain toiminnan kannalta välttämättömiin?

115. Onko yrityksellä käytössä verkkoliikenteen vain välttämättömään rajaava palomuuriratkaisu?

116. Sisältääkö alusta vain järjestelmän tarvitsemat ohjelmistokomponentit?

117. Onko alustan komponenttien, prosessien, hakemistojen ja lisäohjelmien käyttöoikeudet asetettu vähimpien oikeuksien periaatteen mukaisesti?

118. Onko käyttöjärjestelmään ja sovellusohjelmistoihin asennettu tarpeelliset turvallisuuspäivitykset?

119. Onko järjestelmiin automaattisesti generoitujen tilien oikeudet rajattu minimiin tai onko ne poistettu kokonaan käytöstä?

120. Onko laitteiden oletussalasanat vaihdettu yrityksen oman politiikan mukaisiksi?

121. Lukittuuko järjestelmä automaattisesti, jos sitä ei käytetä vähään aikaan?

122. Onko käyttöjärjestelmän automaattisen ohjelmakoodin suorituksen mahdollistavat ominaisuudet kytketty pois?

123. Onko työasemille asennetut ohjelmistot turvallisesti konfiguroituja?

124. Onko BIOS-asetuksiin pääsy suojattu salasanalla?

125. Onko järjestelmän tukemia lisäturvallisuusominaisuuksia käytössä?

126. Onko yrityksessä yhtenäinen suunnitelma sekä ohjeistus haittaohjelmien suojauksen käytöstä sitä vaativissa kohteissa?

127. Onko suunnitelman ylläpito sekä toteutuksen seuraaminen ja valvonta vastuutettu jollekin taholle?

128. Tuottavatko torjuntaohjelmistot havainnoista lokitietoja sekä hälytyksiä?

129. Päivittyvätkö haittaohjelmatunnisteet säännöllisesti?

130. Onko henkilökuntaa ohjeistettu haittaohjelmien uhkista sekä yrityksen tietoturvasuunnitelman mukaisesta toiminnasta?

131. Seurataanko haittaohjelmahavaintoja sekä hälytyksiä säännöllisesti?

132. Yrityksessä suodatetaan haittaliikennettä:

a. Sähköpostin yhdyskäytävissä / WWW-liikenteen yhdyskäytävissä / Ei suodateta / En osaa sanoa

133. Onko yrityksellä dokumentaatio lokien keräys-, luovutus-, hälytys- ja seurantapolitiikasta toiminnan vaatimukset huomioon ottaen?

134. Ovatko tallenteet riittävän kattavia, jotta tietomurrot tai niiden yritykset voidaan todentaa jälkikäteen?

135. Kuinka pitkään keskeisiä lokeja säilötään?

a. 3kk / 6kk /12kk / Pidempään / En osaa sanoa

136. Onko lokitiedot ja niiden kirjauspalvelut suojattu luvattomalta pääsyltä?

137. Lokitus on käytössä seuraavissa laitteissa:

a. Työasemat / palvelimet / verkkolaitteet / Ei missään edellä mainituista / En osaa sanoa

138. Lokitiedoista selviää:

a. verkkolaitteille tehdyt hallintatoimenpiteet, koska ja kenen toimesta / toiminta / käyttäjäaktiviteetit / turvaan liittyvät tapahtumat / poikkeukset / Ei mikään edellä mainituista / En osaa sanoa

139. Tehdäänkö yrityksessä verkon valvontaa?

140. Tunnistaako yritys oman verkkoliikenteensä normaalin tilan?

141. Onko olemassa menettely, jonka avulla poikkeamat havaitaan?

142. Onko olemassa menettely normaalitilanteesta poikkeavien tapahtumien havaitsemiseksi?

143. Onko olemassa menettely poikkeamista toipumiseen?

144. Tapahtuuko edellä mainittujen toimien havainnointi:

a. Automatisoitujen havainnointi- ja hälytystyökalujen avulla? / Manuaalisesti esimerkiksi lokeja tarkastelemalla? / En osaa sanoa

145. Onko tietojenkäsittely-ympäristön toipumiseksi olemassa olevat prosessit, sekä tekniset menetelmät dokumentoitu?

146. Käytetäänkö yrityksessä salausratkaisuja salassa pidettävien tietojen luvattoman paljastumisen ja muuntelun estämiseksi?

147. Ovatko salaiset avaimet vain valtuutettujen käyttäjien ja prosessien käytössä?

148. Ovatko salausavaintenhallinnan prosessit ja käytännöt dokumentoituja?

149. Mitkä seuraavista salausavaintenhallinnan vaatimuksista toteutuvat?

a. Avaimet ovat kryptografisesti vahvoja / Avainten jakelu toteutuu turvallisesti / Avainten säilytys toteutuu turvallisesti / Avaimet vaihdetaan säännöllisesti / Vanhentuneet/paljastuneet avaimet vaihdetaan pikimmiten / Avainten valtuuttamaton vaihto on estetty / En osaa sanoa

150. Tehdäänkö yrityksessä ohjelmistokehitystä?

151. Edellytetäänkö palvelun/sovelluksen/järjestelmän toteutukselta turvallisen ohjelmoinnin periaatteiden täyttämistä?

152. Sitoutuuko palvelun/sovelluksen/järjestelmän toimittaja turvallisuuspuutteiden korjaamiseen koko sen elinkaaren ajan, tai onko turvallisuuspuutteiden korjaamiselle jokin muu menettely?

153. Edellytetäänkö palvelun/sovelluksen/järjestelmän rajapinnoilta kestävyyttä yleisiä hyökkäysmenetelmiä vastaan?

154. Ohjelmiston toimittajalta edellytetään:

a. ohjelmistokehittäjän riittävää tietoturvatietoutta / ohjelmistokehityksen aikaista tietoturva-analyysia, riskien havaitsemista ja kontrollointia / ainakin ulkoisten rajapintojen testausta (vialliset syötteet, suuri määrä syötettä) / politiikkaa helposti ongelmia aiheuttavien funktioiden ja rajapintojen käytöstä / arkkitehtuurin ja lähdekoodin katselmointia / ohjelmakoodin testaamista automatisoidulla staattisella analyysillä / ohjelmakoodin versionhallintaa ja kehitystyökalujen eheyttä / En osaa sanoa

155. Onko hankituista ohjelmistoista olemassa dokumentaatio?

156. Ohjelmistolta edellytetään

a. että se käyttää vain pientä määrää määriteltyjä portteja / että dynaamisia portteja käyttävät rajataan pieneen porttiavaruuteen / ohjelmistot toimivat "peruskäyttäjän" oikeuksin / Ei mitään vaihtoehdoista / En osaa sanoa

157. Onko yrityksellä toimintaohjetta salassa pidettävän materiaalin välittämisestä sähköisesti?

158. Seuraavien tiedonsiirtomenetelmien liikenne on salattu:

a. Puhelinliikenne / Sähköposti / Pikaviestimet / Telekopio (faksi) / Ei mikään vaihtoehdoista / En osaa sanoa

159. Kun salassa pidettävää tietoa siirretään tietoverkon yli, onko se asianmukaisesti salattua?

160. Onko yrityksellä toimintaohjetta salassa pidettävän materiaalin välittämisestä postitse tai kuriirilla?

161. Onko yrityksellä toimintaohjetta salassa pidettävän tiedon jäljentämisestä?

162. Sovelletaanko jäljennöksiin ja käännöksiin alkuperäistä asiakirjaa koskevia turvatoimia?

163. Onko yrityksellä toimintaohjetta salassa pidettävän tiedon turvaamiseksi sen koko elinkaaren ajan?

164. Onko yrityksellä toimintaohjetta tietoaineistojen luotettavasta hävittämisestä?

165. Hävitetäänkö tietojärjestelmien käytön yhteydessä syntyvää väliaikaistietoa säännöllisesti?

166. Väliaikaistietoa hävitetään:

a. Työasemista / palvelimista sekä vastaavista järjestelmistä / Ei kummastakaan tai väliaikaistietoa ei hävitetä / En osaa sanoa

167. Onko yrityksellä toimintaohjetta laitteiden ja laitteiston tietoa tallentavien osien hävittämisestä?

168. Onko yrityksessä käytössä tietojenkäsittely-ympäristönn muutoksenhallintamenettely?

169. Onko verkot, järjestelmät ja niihin kuuluvat laitteet, ohjelmistot ja asetukset dokumentoitu siten, että mahdolliset muutokset on mahdollista havaita vertaamalla toteutusta ja dokumentaatiota?

170. Dokumentaatio sisältää:

a. Verkkokuvat / laiterekisterit / ohjelmistorekisterit / tiedot laitteistojen konfiguraatioista / tiedot ohjelmistojen konfiguraatioista / Ei mitään vaihtoehdoista tai dokumentaatiota ei ole / En osaa sanoa

171. Tarkkaillaanko tietojenkäsittely-ympäristöjä luvattomien muutosten ja laitteistojen havaitsemiseksi?

172. Onko yrityksen työntekijöiden mahdollista tehdä etätöitä?

173. Onko yrityksellä voimassa olevaa toimintaohjetta turvallisen etätyön toteuttamiseksi, ja onko se helposti henkilökunnan saatavilla?

174. Onko työntekijän sallittua viedä salattua materiaalia sisältäviä tietovälineitä yrityksen tilojen ulkopuolelle?

175. Onko henkilökuntaa tiedotettu/opastettu kyseisten tietovälineiden turvallisesta käyttö- ja säilytysmenetelmistä?

176. Onko etäkäyttö mahdollista vain käyttöympäristöön hyväksytyillä laitteilla?

177. Onko etäkäyttö mahdollista vain hyväksyttyjä etäyhteyksiä käyttämällä?

178. Onko etäyhteyksien käytön edellytyksenä vähintään kahteen tekijään perustuva käyttäjäntunnistus?

179. Onko yrityksellä toimintaohjetta tietojenkäsittely-ympäristön koko elinkaaren ajalle ohjelmistohaavoittuvuuksien hallitsemiseksi? Onko sen ylläpito vastuutettu jollekin taholle?

180. Seurataanko viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden tahojen tietoturvatiedotteita?

181. Onko yrityksellä toimintaohjetta turvapäivitysten hallitusta asentamisesta?

182. Suoritetaanko verkolle, sen palveluille, palvelimille sekä verkkoon kytketyille työasemille haavoittuvuusskannauksia?

183. Onko yrityksellä toimintaohjetta salassa pidettävää informaatiota sisältävien varmuuskopioiden suojaamisesta niiden koko elinkaaren ajan?

184. Onko varmuuskopiointi mitoitettu yrityksen toimintavaatimuksiin nähden riittoisaksi?

185. Testataanko varmuuskopioinnin ja palautusprosessin toimivuutta säännöllisesti?

186. Onko palautusprosessista olemassa riittävän tarkka/yksityiskohtainen dokumentaatio?

187. Onko varmuuskopion ja alkuperäisen järjestelmän fyysinen sijoituspaikka riittävän eriytetty, jotta vältetään molempien samanaikainen menettäminen?