Aleksi Kinnunen

Opas FINCSC-sertifikaatin kriteeristön vaatimusmäärittelyjen täyttämiseksi

Opinnäytetyö
Kevät 2020
SeAMK Tekniikka
Tietotekniikka

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: SeAMK Tekniikka

Tutkinto-ohjelma: Tietotekniikan insinööri

Suuntautumisvaihtoehto: Tietoliikenneverkot

Tekijä: Aleksi Kinnunen

Työn nimi: Opas FINCSC-sertifikaatin kriteeristön vaatimusmäärittelyjen täyttämiseksi

Ohjaaja: Alpo Anttonen

Vuosi: 2020 Sivumäärä: 32 Liitteiden lukumäärä:1

Digitaalisuuden kasvu lisää organisaatioille aiheutuvia uhkia sekä riskejä tietoturvallisuuden näkökulmasta. Organisaatioilla tulisi olla tarpeeksi tietoturvalliset toimintamenetelmät sekä ympäristö, jotta se ei ole haavoittuvainen tietoturvauhkille.

Työn tarkoitus on toteuttaa helposti käytettävä ja selkeä opas FINCSC-rekisteröidyn tuotemerkin sertifikaatin kriteerien täyttämiseksi. Tämä manuaali toimii selkeänä ohjeistuksena sertifikaattia tavoitteleville organisaatioille siitä, mitä kriteerit tarkoittavat sekä, kuinka kriteerien asettamiin vaatimusmäritteisiin päästään.

Työssä esitellään lisäksi tietoturvallisuuden perusperiaatteet sekä osa-alueet, joiden avulla avulla organisaatiot voisivat kehittää jatkuvuudenhallinnan menetelmiä toimivammiksi.

Avainsanat: tiedon eheys, tiedon luottamuksellisuus, tiedon saatavuus, tietoturva, FINCSC

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Information Networks

Author: Aleksi Kinnunen

Title of thesis: Guide for FINCSC -certification criteria

Supervisor: Alpo Anttonen

Year: 2020 Number of pages:32 Number of appendices:1

As digitalization increases it brings along a growing number of cyberthreats against organizations. Organizations and companies must have functioning cybersecurity procedures and functions to protect themselves from these threats.

The goal of this thesis was to produce a readable, and easy to use manual to meet the requirements set for the FINCSC certification criteria. The manual explains the meaning of every criteria and the procedures that need to be taken to meet the specific requirements. The thesis also considered the basic principles and parts of cybersecurity that give organizations a better understanding of the importance of continuity management.

Keywords: confidentiality, integrity, availability, cybersecurity, information security FINCSC

SISÄLTÖ

Kuva ja taulukkoluettelo

Käytetyt termit ja lyhenteet

EMP	Elektorninen pulssi, joka voi vauriottaa elektronisia laitteita. Se voi syntyä luonnollisesti tai ihmisen aiheuttamana (Electro Magnetic Pulse)
HMP	Korkeavoimainen mikroaalto, jolla voidaan lamauttaa elektronisia laitteita. (High-power microwave)
Tietoturvahäiriö	Tilanne tai tapahtuma, jonka seurauksena tietoturvallisuus on vaarantunut.
Tietoturvatapahtuma	Tilanne tai tapahtuma, jonka seurauksena tietoturvallisuus on voinut olla vaarantuneena.
UPS	Laite, jonka tehtävänä on taata kiinnitetyille laitteille katkeamaton virransyöttö pienten katkoksien varalta. (Uninterrubtable Power Supply)
VPN	Virtuaalinen näennäisverkko, jolla voidaan yhdistää eri sijainneissa toimivia verkkoja turvallisesti toisiinsa julkisen internetin yli. (Virtual Private Network)

1 JOHDANTO

1.1 Työn tausta

Tietotekniikan kehittyessä sekä tullessa tärkeämmäksi osaksi yritystoimintaa, kasvaa myös tietototurvan merkitys tietoliikenneympäristöissä. Tietoturva on erittäin laaja käsite, joka pitää sisällään laajan kirjon eri osa alueita hallinnon päätöksistä yksittäisen työntekijän toimintaan saakka. Tätä kokonaisuutta ja sen toimivuutta pyritään osoittamaan ja arvioimaan sertifikaateilla sekä standardeilla.´

Suurin ja kattavin standardi on ISO27000 ja sen sisältämät sarjat. ISO27000-standardin mukainen ympäristö voidaan sertifioida, jolloin kyseinen yritys voi osoittaa tietoturvallisuuden täydellisen tason. ISO27000-sertifikaatti on kuitenkin liian laaja sekä kattava pienemmille organisaatioille kuten pk-yrityksille. Tästä syystä on luotu sertifikaatteja, jotka soveltavat esimerkiksi ISO27000-standardia sekä muita standardeja luoden suppeamman kokonaisuuden, jolloin se on pienemmille organisaatioille resurssien sekä kannattavuuden kannalta relevantimpi.

JYVSECTEC on toteuttanut FINCSC-sertifikaatin, joka on rekisteröity tuotemerkki. Tämän tuotemerkin tavoitteena on kohottaa Suomalaisten yritysten tietoturvallisuutta. Tämä kyseinen sertifikaatti on kriteerisarja, jonka yritykset voivat sertifioifa itseauditoinnilla. Ongelmana kuitenkin tämän sertifikaatin toteuttamiselle pk-yrityksissä on sen luettavuus sekä ymmärrettävyys. Sertifikaatin tulisi olla kaikille toteutettavissa, mutta sen tekninen ulkoasu vaikeuttaa sen toteuttamista sellaisissa yrityksissä, joilla tietoteknistä osaamista ei juurikaan ole. Sertifiointiprosessi olisi huomattavasti helpompi toteuttaa, mikäli sillä olisi helppolukuinen ja ymmärrettävä toimintaohjesarja.

1.2 Työn tavoite

Työn tavoitteena on luoda FINCSC-standardille helposti käytettävä, ymmärrettävä ja luettava manuaali. Tämä manuaali toimii ohjeistuksena, kuinka FINCSC-standardin kriteerit täytetään sekä samalla ohjeistaa, kuinka tietyt osa-alueet olisi järkevintä toteuttaa.

1.3 Työn rakenne

Luvussa kaksi esitellään FINCS. Lisäksi kerrotaan, miksi organisaatiolle on hyötyä toteuttaa sertifiointi, ja kuinka sertifiointiprosessi toimii.

Luvussa kolme käsitellään tietoturvaa sekä sen perusperiaatteita ensisijaisesti ISO27000-standardisarjan mukaisesti.

Luvussa neljä käsitellään standardeja sekä sertifikaatteja, kerrotaan niiden välinen yhteys sekä esitellään niiden merkitys yrityksen tietoturvallisuuden kannalta.

Liitteenä tuotettu opas toimii FINCSC-sertifikaatin itseauditointiprosessin apuvälineenä. Kyseisessä oppaassa on kuvattu vaatimusmäärittelyt niiden merkityksineen sekä toteutusohjeet. Immateriaalioikeuksien vuoksi tämä liite on salattu.

2 FINCSC

2.1 Mikä on FINCSC

FINCSC on Jyväskylän ammattikorkeakoulussa toimiva kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskuksen JYVSECTECin tuottama ja hallinoima rekisteröity tuotemerkki. Sen tavoitteena on tukea Suomen kansallisen kyberturvallisuustrategian toimeenpanoa. FINCSC-sertifioinnilla organisaatio voi arvioida omia tietoturvakontrolliensa sekä tietosuojakäytänteiden asianmukaisuutta. Saavuttamalla FINCSC-sertifikaatti organisaatio osoittaa riittävän tasoisen tietoturvallisuuden. FINCSC-sertifikaatti on saatavissa kaksitasoisena, itseauditoituna tai ulkopuolisen arviontilaitoksen auditoimana, mikä on vaatimus FINCSC-plus-sertifikaatin saavuttamiseen. (JYVSECTEC, [viitattu 20.4.2020].)

2.2 Mitä lisäarvoa organisaatiolle FINCSC-sertifikaatin käytöstä

Tieto- ja viestintäteknologian ollessa korkeaa tasoa myös riskit sen käytössä kasvavat. Tämä tuo erityisesti ongelmia organisaatioiden yhteistyöhön liittyvissä kysymyksissä. Luottamuksen rakentaminen yhteistyötä varten täten on eritoten tärkeää. Osoittamalla oman organisaation kykyä ylläpitää omaa tietoliikennejärjestelmää ja asianmukaisia käytänteitä voidaan tältä osin osoittaa luottamuksen aiheellisuus. Mikäli organisaatio ei pysty osoittamaan riittävää osaamista tietoturvallisuutensa saralla, voi se jossain tapauksissa johtaa siihen, että jokin taho ei omien vaatimusmääritteiden vuoksi voi tehdä yhteistyötä sellaisen organisaation kanssa joka ei vaatimuksia täytä. (JYVSECTEC, [viitattu 20.4.2020].)

Organisaation oman tietoturvan kannalta on myös ehdottoman tärkeää olla ajan tasalla nykyisessä digitaalisessa maailmassa. Saavuttamalla FINCSC-sertifikaatin asettamat vaatimusmääritteet, voidaan osoittaa, että organisaation tietoturva on riittävä. Tämä tarjoaa turvaa ulkopuolisilta uhilta, jotka voivat vaikuttaa negatiivisesti organisaation toimintaan tai pahimmassa tapauksessa jopa täysin lamauttaa ne. (JYVSECTEC, [viitattu 20.4.2020].)

2.3 FINCSC-tuotemerkin saavuttaminen

FINCSC-sertifikaatin saavuttaminen alkaa hakemuksella osoitteessa www.fincsc.fi. Hakemuksen hyväksymisen jälkeen organisaatio saa tunnukset portaaliin, jossa vastataan sähköisesti kysymyspatteristoon. Täytetty itsearviointi katselmoidaan, jonka jälkeen hyväksytyn itsearvioinnin tehnyt organisaatio saa käyttöönsä FINCSC-sertifikaatin vuodeksi. (JYVSECTEC, [viitattu 20.4.2020].)

FINCSC-plus-sertifiointi toteutetaan ulkoisen arviointilaitoksen suorittamana. FINCSC-portaalissa jätetään tarjouspyyntö auditoinnista. Hyväksytyn tarjouksen jälkeen portaalisssa täytetään sähköinen auditointinäyttö, jota käytetään apuna organisaation vaatimustenmukaisuuden todentamiseen. Arviointilaitos suorittaa organisaatiossa auditoinnin, jonka jälkeen tehdään päätös lopputuloksesta. Hyväksytyn sertifioinnin johdosta organisaatio saa käyttönsä FINCSC-sertifikaatin kolmeksi vuodeksi. (JYVSECTEC, [viitattu 20.4.2020].)

3 TIETOTURVALLISUUS

3.1 Tietoturvallisuuden perusteita

Kaikentyyppiset ja -kokoiset organisaatiot pitävät hallussaan ja käsittelevät informaatiota. Tämä informaatio katsotaan omaisuudeksi, jolla on organisaatiolle arvoa, jolloin sitä tulisi suojata. Tämä saavutetaan toteuttamalla joukko turvamekanismeja, jotka on luotu luotu riskienhallintaprosessin kautta, ja joita hallitaan tietoruvallisuuden hallintajärjestelmällä. Tämä järjestelmä pitää sisällään politiikan, prosessit, menettelyt, organisaatiorakenteet, ohjelmistot ja laitteistot, joilla pyritään suojaamaan organisaation tieto-omaisuutta. Näiden turvamekanismien määrittämisen ja käyttöönoton jälkeen niitä tulee valvoa ja katselmoida mahdollisten parannusten varalta, jotta saavutetaan organisaation määrittämät turvallisuus- ja liiketoimintatavoitteet. Näiden turvamekanismien täytyy olla täydellisesti integroituna organisaation liiketoimintaprosesseihin. (ISO 27000 2017, 18-20.)

3.2 Tietoturvallisuuden päänäkökohdat

Tietoturvallisuus koostuu kolmesta päänäkökohdasta sekä siihen voidaaan sisällyttää muita tukevia ominaisuuksia. Päänäkökulmat ovat: informaation luottamuksellisuuden, eheyden ja saatavuuden säilyttäminen. Muut ominaisudet ovat: informaation tunnistus, kiistämättömyys ja todennus. Näiden tavoiteena on varmistaa liiketoiminnan kestävä menestys ja jatkuvuus sekä pitää haittavaikutukset mahdollisimman vähäisenä. (Traficom, [Viitattu 20.4.2020].)

3.2.1 Luottamuksellisuus

Käsiteltävään ja tietoturvaluokiteltuun tietoon on pääsy ainoastaan niillä henkilöillä, joille kyseisen tietosuojaluokituksen mukainen taso on myönnetty. Tähän liittyy myös pääsy tiedon käsittelytiloihin, tiedon käsittely- sekä tiedonsiirtolaitteistoihin. (ISO 27000 2017, 8.)

3.2.2 Eheys

Organisaaation hallussapitämä informaation tulee olla oikeaa sekä ajantasaista. Tieto ei saa vahingoittua, muuttua ulkopuolisen tai sisäisen virheellisen toiminnan seurauksena. Eheyden takaamisen vuoksi organisaatiolla täytyy olla tiedon elinkaaren kattava käsittelysäännöstö. Näiden käsittelysääntöjen kautta voidaan dokumentoida tiedon luominen, muuttaminen sekä tuhoaminen hallitulla toimintaketjulla. (VAHTI 5/2006, 31-32.)

3.2.3 Saatavuus

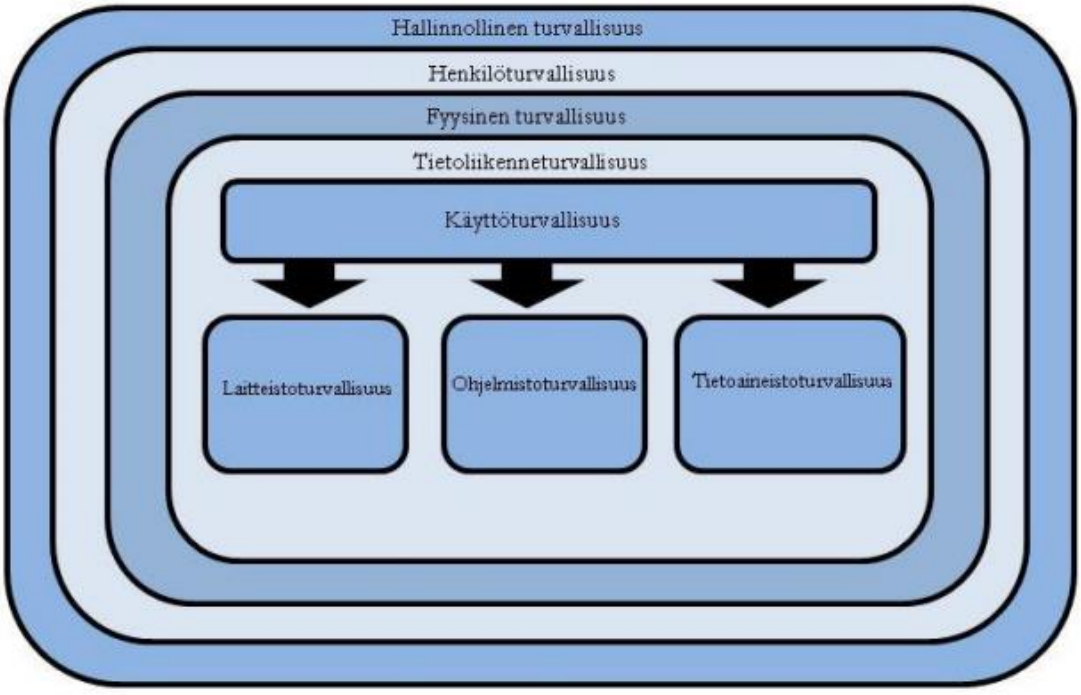
Tiedon tulee olla käytettävissä helposti sekä viiveettä niille, joilla on oikeus käsitellä haluttua tietoa. Tähän kuuluu lisäksi tietojen tekninen esittäminen sekä tietojen käytettävyydelle ja käsiteltävyydelle asetetut määritteet. Saatavuuden hallintaan käytettävän prosessi tulisi olla yhdenmukainen pääsynhallintapolitiikan kanssa. (ISO 27002, 2017, 23,48.)

Järjestelmän palvelutason tulee olla toteutettu häiriösietoiseksi siten, että se on käytettävissä myös poikkeustilanteissa. Tarkkailemalla ja säätelemällä järjestelmää voidaan havaita ongelmat sekä tulevat kapasiteettivaatimukset ennen häiriöiden tai muita toimintaa haittaavien tilanteiden ilmenemistä. (ISO 27002, 2017, 23,48.)

3.3 Tietoturvallisuuden osa-alueet

Tietoturvan kokonaisuuden käsittelemisen helpottamiseksi se voidaan jakaa osa-alueisiin. Yleisin sekä eniten käytetty tapa on jakaa se kahdeksaan alueeseen:

- Hallinnollinen tietoturvallisuus
- Henkilöstöturvallisuus
- Laitteistoturvallisuus
- Ohjelmistoturvallisuus
- Tietoliikenneturvallisuus
- Käyttöturvallisuus
- Tietoaineistoturvallisuus
- Fyysinen Turvallisuus. (ISO 27002, 2017.)



Kuva 1. Tietoturvan osa-alueet (Paavilainen 1998, 108.)

3.3.1 Hallinnollinen tietoturvallisuus

Tietoturvallisuus on jatkuva prosessi, jota kehitetään ja ylläpidetään organisaation hallinnon tasolla erinäisillä strategioilla sekä politiikoilla. Hallinnon tulee kehittää tietoturvapolitiikka, jossa määritellään sitoutumiset, tietoturvatavoitteet, prosessit ja toimintamallit, vastuut, resurssit sekä jatkuvan kehityksen toimintamalli. Tietoturvallisuuden kehittämisessä olennaisena osana on riskien ja uhkien arviointi sekä kartoittaminen. Optimaalisessa tilanteessa riskiin tai uhkaan on reagoitu jo ennen kuin se on toteutunut. (ISO 27001 2017, 7.)

Tietoturvapolitiikan mukaisiin tietoturvallisuusprosesseita koskevat roolit ja vastuut tulee jakaa ja yksilöidä selkeästi. Tiettyyn suojattavaan omaisuuteen tai tietoturvaprosessiin määritetyn henkilön vastuun tulisi olla dokumentoituna sekä henkilön pätevyyden tulisi olla vastuutason mukainen. Monessa organisaatiossa päävastuu tietoturvan kehityksessä ja toteutuksessa on määritetty tietoturvapäälikolle. (ISO 27002 2017, 11-12.)

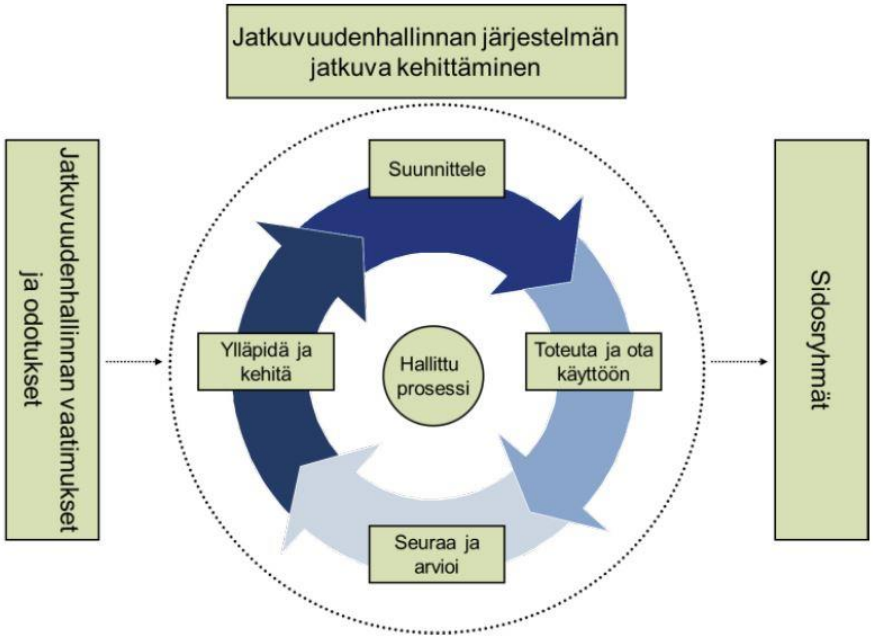
Tietoturvallisuuden jatkuvan kehityksen avuksi ja helpottamiseksi on kehitetty valmiita malleja. Yksi malleista on PDCA-vuosikello, jossa vuosi jaetaan neljään osaan, ja jonka jokaissa kvartaalissa on määritetty sen aikana tehtävät toimet. PDCA(Suunitele-Toteuta-Arvioi-Toimi)-mallin mukaiset toimet ovat:

Plan/suunittele: Suunitteluvaihe, jonka aikana laaditaan ja määritellään tietoturvallisuusvaatimusten mukaiset toimet ja prosessit tietoturvallisuuden parantamiseksi. (VAHTI 2/2016, 65.)

Do/toteuta: Toteutusvaihe, jonka aikana pannaan täytäntöön suunitellut toimet ja prosessit. Suunitelmat testataan ja raportoidaan. (VAHTI 2/2016, 65.)

Check/arvioi: Tarkistusvaiheen aikana tarkastellaan raportteja toteutusvaiheesta ja verrataan tuloksia määritettyihin tavoitteisiin. Tarpeen vaatiessa voidaan suorittaa ulkoinen auditointi. (VAHTI 2/2016, 65.)

Act/toimi: Toimintavaiheen aikana toteutetaan tarpeelliset muutokset prosesseihin ja toimintamalleihin, jotta lopputulos olisi vaatimuusmäärittelyiden mukainen. (VAHTI 2/2016.)



Kuva 2. PDCA-vuosikellon rakenne (VAHTI 2/2016, 65.)

3.3.2 Henkilöstöturvallisuus

”Henkilöstöturvallisuus on keskeinen osa organisaation turvallisuutta. Henkilöstöturvallisuudella pyritään takaamaan ihmisten turvallisuus ja toimintakyky suojaamalla heitä rikoksilta ja onnettomuuksilta. Lisäksi turvataan organisaation toiminnalle kriittiset henkilöresurssit. (Elinkeinoelämän keskusliitto, [viitattu 11.2.2020].)

Henkilöstöturvallisuuden tarkoituksena on turvata yrityksen työntekijöiden turvallinen työskenteleminen organisaatiossa sekä samalla suojata yrityksen

tietojen vuotamista henkilöstön kautta. Henkilöstöturvallisuutta voidaan yleisesti kuvata kolmessa vaiheessa: ennen, aikana ja jälkeen työsuhdetta. (VAHTI 3/2007, 57,58.)

Rekrytoinnissa tulisi tarkistaa tehtävään hakevan henkilön luotettavuus tarkistamalla hakijan taustat sekä hänen työhakemuksessa ilmoittamansa tiedot lakien, määräysten ja eettisten normien mukaisesti. Tarkistuksessa tulisi ottaa huomioon hakijan ansioluettelon oikeellisuus ja täydellisyys, koulutuksen tai ammatillisen pätevyyden paikkaansapitävyys sekä henkilöllisyys. Mikäli kyseinen rooli organisaatiossa on merkittävä tietoturvallisuuden kannalta, täytyy hakijalle tehdä myös yksityiskohtaisempi tarkistus, kuten rikosrekisterin tarkistus tai turvallisuusselvityksen teettäminen. Mikäli hakijasta teetetään turvallisuusselvitys, on tästä ilmoitettava hänelle hakuvaiheessa tai ennen selvityksen tekemistä (L726/2014, 2 luku). Ennen työsuhteen alkamista työntekijän kanssa on laadittava selkeä ja tarkka työsopimus. Työsopimuksessa määritellään työtehtävän vastuut sekä velvoitteet. Mikäli työntekijän työtehtävään kuuluu käsitellä organisaatiolle salaista tietoa, täytyy työntekijän kanssa kirjoittaa salassapitosopimus. (ISO 27002 2017, 16.)

Työntekijän työsuhteen alkaessa hänelle tulee perehdyttää hänen työtehtävä ja siihen kuuluvat vastuut. Tähän kuuluu organisaation tietojärjestelmien käytön, tiedon käsittely ja -luokittelu periaatteet sekä hänen roolinsa mukaiset tietoturvaodotukset. Työntekijälle täytyy myös tarjota tukiaineistoa sekä raportointiratkaisuja organisaation sisäisen laiminlyönnin esilletuomiseksi. Työntekijän täytyy myös olla tietoinen kurinpitomenetelmistä, mikäli hän rikkoo työsopimuksessa tai salassapitosopimuksessa määritettyjä ehtoja. Työntekijöiden tietoturvatason takaamiseksi tulisi organisaation järjestää tietoturvaopastusta ja -koulutusta säännöllisesti. Koulutus sekä perehdytys koskee myös niitä henkilöitä, joiden työtehtävä ja sen mukana muuttuneet tietoturvavastuut sekä tietoturvavaatimukset vaihtuvat. (ISO 27002 2017, 16.)

Työsuhteen päätyttyä työntekijällä on oltava tiedossa, millaiset tietoturvavastuut ja -velvollisuudet hänellä on voimassa sekä kuinka niitä noudatetaan. Nämä vastuut ja velvollisuudet tulisi sisällyttää työntekijän työsopimuksen ehtoihin. Työsopimuksen päätyttyä työntekijän tulee palauttaa organisaation omistama ja

suojattava omaisuus. Työntekijän omistamaa tietoa organisaatiosta hänen tulee rikoslain mukaan pitää salassa kahden vuoden ajan työsuhteen loputtua (L 10.8.2018/605, luku 30 §5). Organisaatiolla täytyy olla prosessi, jolla hallitaan lähtevät työntekijän tietojen ja pääsynhallinnan käsittelyjä. Tähän lukeutuu esimerkiksi sähköpostin ja muiden tietopankkien oikeuksien luovutus organisatiolle sekä pääsytunnisteiden muuttaminen, jotta työntekijä ei enää pääse käsiksi organisaation järjestelmiin. (ISO 27002 2017, 20.)

Organisaation henkilöstöturvallisuuteen sekä tietoturvallisuuteen kuuluu olennaisena osana myös henkilöstön suojeleminen ulkoisia vaikuttajia vastaan. Tähän lukeutuu työntekijöiden ja avainhenkilöiden työturvallisuuden varmistaminen. Yleisillä turvallisuus- ja evakuointiohjeilla pystytään ehostamaan työntekijöiden yleistä toimintaa organisaatiossa. Työntekijöiden tulisi pystyä työskentelemään ja matkustamaan turvallisesti työtehtävän vaatimissa tehtävissä. Tähän kuuluu ajantasaisten matkustusasiakirjojen sekä vakuutusten ylläpito. Avainhenkilöiden tai julkisesti esillä toimivien henkilöiden turvallisuutta voidaan kohentaa rajoittamalla heidän yhteystietojensa saatavuutta julkisista rekistereistä. Kiristys tai uhkatilanteiden varalle henkilöstöllä olisi hyvä olla tiedossa toimintamenettelyt. (Elinkeinoelämän keskusliitto, Henkilöstöturvallisuus, [viitattu 11.2.2020].)

3.3.3 Laitteistoturvallisuus

Laitteistoturvallisuuteen kuuluu käytettävän laitteen toiminnan, käytettävyyden ja tietoturvan varmistaminen, laitteen valmistus- ja hankintavaiheesta laitteen poistoon saakka. Laitteiston koko elinkaaren aikainen toiminta on turvattava, mihin kuuluu laitteiston asennus, ylläpitotoimet, tuki- ja takuu palvelut sekä laitteiston poistoon kuuluva asianmukainen hävitys. (Andreasson, 2013, 65.)

Laitteen ylläpito tulisi olla ennaltamääritetty toimenpideketju. Laitteen kulumista ja sen toimintaa tulee pystyä seuraamaan ja valvomaan jatkuvasti esimerkiksi valvontaohjelmistoilla. Laitteessa käytettävän järjestelmän ajantasaisuus sekä tietoturvapäivitykset tulee huolehtia säännöllisesti. Päivitysten yhteydessä on

kuitenkin varmistuttava siitä, että uusi versio on yhteensopivaa tuotannon kanssa, joten ne on testattava etukäteen. Laitteistossa toimivasta ohjelmistosta sekä laitteen sisältämästä datasta on oltava jatkuvasti ajantasaiset varmuuskopiot. Varmuuskopioon tulisi sisällyttää vähintään ohjelmistot ja sen asetukset sekä operatiiviset tiedot. Poikkeaman jälkeen voidaan täten varmistaa datan säilyvyys. (Andreasson, 2013, 65.)

Käytettävillä laitteilla tulisi olla ajanmukaiset sekä koko elinkaaren kattava palvelusopimus laitteen toimittajalta. Tietoturvaa tulee pystyä ylläpitämään vaaditulla tasolla, sekä tietoturvapoikkeamiin täytyy kyetä ragoimaan nopeasti. Tarvittaessa kriittisiä laitteistoja olisi hyvä olla varastossa valmiina, mikäli laitetoimittajan vasteaika ei ole vaadittujen määritysten mukainen. Mikäli käytetään palveluntarjoajia, joilla on hallussaa palvelu tai sen osia, tulisi varmistua laitteiden fyysisestä turvallisuudesta ja niiden sijoittamisesta laitetilaan asianmukaisesti. (Andreasson, 2013, 65.)

Laitteen elinkaari päättyy sen käytöstä poistamiseen tai tuhoamiseen. Tulisi varmistua, että laite ei sisällä organisaatiolle arkaluontoista materiaalia. Riippuen datan suojausluokituksesta, voidaan se poistaa ja käyttää ylikirjoitustyökaluja datan palauttamiskelvottomuuden varmistumiseksi. Mikäli kuitenkin koetaan, että tämä ei riitä, on tallennusmedian täydellinen tuhoaminen välttämätöntä. (ISO 27002, 2017. 25-26.)

Organisaation ulkopuolella käytettävillä laitteilla tulisi olla selvä linjaus niiden käytöstä, kuljetuksesta sekä turvallisuuden ylläpidosta. Laitteen tulisi olla turvattu mekaanisesti sen rikkoutumiselta. Laitteessa tulisi olla varkaudenesto- ja lukitusohjelmistot katoamisen tai varkauden varalle. Ongelmaksi voi muodostua omien laitteiden käyttö, sillä se aiheuttaa useita lisätoimenpiteitä sekä mahdollisia tietoturvariskejä. Tällaisten laitteiden käytölle tulisi olla selkeä linjaus organisaatiossa, koska kaikissa laitteissa tulisi olla virustorjunta sekä muut organisaation käytössä olevat tietoturvaa edistävät järjestelmät. Laitetta tulisi myös tarvittaessa pystyä hallitsemaan etänä, kopioida ja tuhota tiedot sekä lukitsemaan pois käytöstä. (ISO 27002, 2017, 13-15.)

3.3.4 Ohjelmistoturvallisuus

Organisaation järjestelmät ja laitteet sisältävät useita eri ohjelmistoja. Näiden ohjelmistojen ajantasaisuus ja tietoturvallisuus on varmistettava päivittämällä sekä seuraamalla niiden tarpeellisuutta organisaation järjestelmien kannalta. Organisaatiolla tulisi olla tarkasti tiedossa käytettävät ohjelmistot sekä niiden sisältämät lisenssit ja niiden voimassaolo. Ohjelmistojen laatu täytyy varmistaa ennen niiden käyttöönottoa, sekä ohjelmistojen elinkaaren aikana niitä on katselmoitava, jotta ne täyttävät tietoturvamäärittelyjen vaatimukset. (ISO 27002, 2017, 62-63.)

Ohjelmistot ja järjestelmät usein sisältävät ominaisuuden määrittää käyttäjätasot. Käyttäjätasot olisi määritettävä niin, että normaali käyttäjä ei voi vahingossa tai tahallisesti muokata ohjelmiston toiminnallisuutta. Käyttäjä- ja ylläpitotunnukset tulisi yksilöidä tarkoin, jotta ohjelmistojen ja järjestelmien lokitiedoista voidaan määritellä käyttäjän tekemät toimet tai muutokset. Tämä vaatii sen, että ohjelmisto kykenee tallentamaan lokitiedostoja. Tämä toiminta on tärkeä etenkin asiakirjajärjestemissä. Ylläpito-oikeudet olisi määritettävä tarkoin ja tällaiset oikeudet tulisi antaa vain niille, joilla on oikeus muokata ohjelmistojen toiminnallisuutta. Mikäli ohjelmistojen tai järjestelmän ylläpito on kolmannen osapuolen vastuulla, on määritettävä tarkoin sopimuksessa, miten heidän ylläpito-oikeuksia käytetään ja mihin tarkoituksiin. Näistä kaikista oikeuksista järjestelmiin ja ohjelmistoihin tulisi olla dokumentointi ja se tulisi pitää ajantasaisena. (ISO 27002, 2017. 27-34, 51-53.)

Ohjelmistoista tärkeä osa on virus- ja haittaohjelmatorjunta. Näiden ohjelmistojen ajantasaisuutta tulisi seurata erityisen tarkoin, sillä jatkuvasti kehittyvät haittaohjelmat tarvitsevat ohjelmistoissa uusia ominaisuuksia tunnistaakseen ja torjuakseen haittaohjelmat. Organisaatiolla tulisi olla selvä ja tiukka linjaus siitä, millaisia ohjelmia käyttäjät saavat asentaa. Hallinnoimattomat ja tuntemattomat sovellukset saattavat johtaa tietoturvavuotoihin, eheyden menettämiseen tai muihin tietoturvahäiriöihin. Ohjelmistot ja järjestelmät tulisi myös varmuuskopioda ennaltamäärättyn aikataulun mukaisesti, mikä voidaan myös automatisoida. (ISO 27002, 2017, 49,56.)

3.3.5 Tietoliikenneturvallisuus

Tietoliikenneturvallisuuden tarkoituksena on suunitella, toteuttaa ja ylläpitää organisaation käytössä oleva tietoliikenneverkko niin, että verkossa käsiteltävän ja siirrettävän tiedon eheys, saatavuus ja luottamuksellisuus olisi varmistettu. Turvallisen tietoliikenneverkon toteuttamiseen kuuluu tiedonsiirtoyhteyksien käytettävyyden, tiedonsiirron turvaamisen, suojaamisen, käyttäjän tunnistamisen ja verkon varmistaminen, näillä pyritään aikaansaamaan turvallinen tietoliikenne. Tämä käsittää muun muassa seuraavat asiat; tietoliikennelaitteistojen kokoonpanon, luetteloinnin, ylläpidon, muutosten valvonnan, ongelmatilanteiden kirjauksen, käytön valvonnan, verkon hallinnan, viestinnän salauksen ja varmistamisen, merkittävien tietoturvapoikkeamien tarkkailun, kirjaamisen ja selvittämisen sekä tietoliikenneympäristön testaamisen ja hyväksymisen. (Andreasson, 2013, 69, 70.)

Verkon suunnittelu ja rakennusvaiheessa tulee huomioida kokonaisvaltaisesti verkon käyttöön liittyvät seikat, kuten millaisia laitteita verkkoon liitetään ja millaista tietoa siinä liikkuu. Hallinta- ja valvontaliikenne sekä kiinteistöautomaation käyttämän tietoliikenteen tulisi käyttää eri yhteyttä kuin normaali toimistotietoliikenne. Verkon dokumentointi on tärkeää suunitteluvaiheesta asti. Verkosta tulee toteuttaa fyysinen verkkokuva. Tässä dokumentoinnissa näkyy kaapelointi, aktiivilaitteet ja niiden sijainti sekä pisteet, joista voi liittyä verkkoon sisältä sekä ulkoa. Fyysisen verkkokuvan lisäksi tulee toteuttaa looginen verkkokuva. Tähän on dokumentoitu verkossa toimivat verkkoalueet, virtuaaliverkot sekä langattomat lähiverkot. Lisädokumentointina tulisi olla laitedokumentointi, missä on lueteltuina kaikki laitteet, niiden käyttämät osoitteet sekä muuta tarvittavaa tietoa. Verkkoon suunitellut ja toteutetut suojaustoimenpiteet olisi myös hyvä dokumentoida. (Andreasson, 2013, 70,71.)

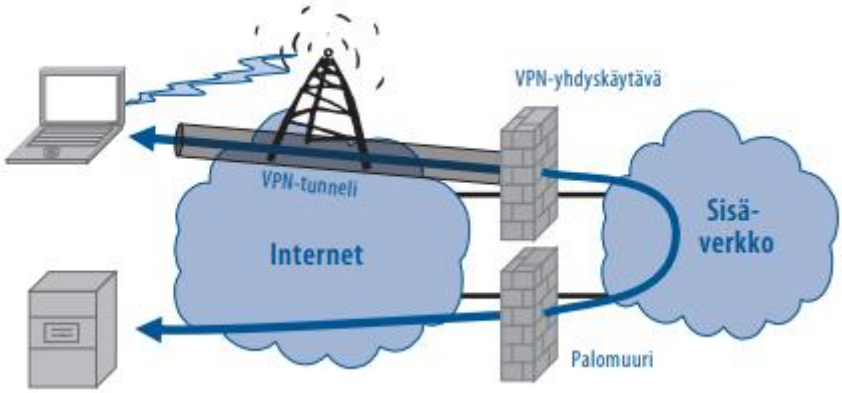
Tietoliikenneverkko tulee rakentaa siten, että ulkopuolinen fyysinen uhka olisi mahdollisimman pieni. Kaapelointi tulisi toteuttaa niin, että se on suojassa fyysisiltä uhilta, kuten katkaisemiselta, häirinnältä tai luvattomasti liittymiseltä. Verkkolaitteiden sekä ristikytkentäpaneelien tulisi olla sijoitettuna niin, että niiden toimintaan ei voi vaikuttaa muu kuin verkon valvoja. (VAHTI 3/2010, 33-35.)

Verkon tietoturvallisuus on taattava aktiivilaitteilla. Ulkopuolelta tulevat tunkeutumisyritykset ja hyökkäykset pitää pystyä sulkemaan verkon ulkopuolelle esimerkiksi palomuureilla. Palomuurit tulee konfiguroida ja säännöstö luoda niin, että vain sallitut ja tarpeelliset yhteydet sallitaan. Palomuurit eivät kuitenkaan suodata mitä dataa verkossa kulkee ja niiden avulla voidaan torjua uhat verkon ulkopuolelta, joten turvallisuusmäärittelyjen vaatiessa sisäverkossa kulkevaa dataa voidaan monitoroida havaitsemisjärjestelmillä (IDS) ja tarvittaessa estämisjärjestelmillä (IPS), jotka voivat katkaista yhteydet havaittuaan epäilyttävää toimintaa. (ISO 27002 2017, 54,58.)

Langattomissa verkoissa on suuremmat tietoturvariskit kuin kiinteissä verkoissa. Langattomiin yhteyksiin on helpompi aiheuttaa häiriötä tai liittyä luvattomasti. Salaamattomattomiin langattomiin lähiverkkoihin on erittäin helppoa liittyä sekä verkon kantavuusalue voi usein yltää myös organisaation tilojen ulkopuolelle. Langattoman verkon tietoturva-asetukset tulisi määritellä tarkkaan sekä siihen liittyminen tulisi aina todentaa. Langattomat verkot voidaan myös jakaa esimerkiksi vierailijaverkoksi, jonka kautta ei kulje organisaatiossa käsiteltävää dataa. Organisaation henkilöstölle on tarkoitettu oma verkko, jonka kautta pääsee kiinni organisaation sisäverkossa oleviin resursseihin suoraan tai organisaatiossa käytössä olevien VPN (virtual private network)-ratkaisujen avulla. Tässä verkossa tulee käyttää verkkoon liittyessä riittävää todennusmekanismia kuten WPA2 EAS. Suojamekanismien käytön lisäksi henkilöstölle tulisi olla luotuna linjaus kuinka langattomia verkkoja sekä VPN-yhteyksiä käytetään. (ISO 27002, 2017, 28,57-58.)

Palvelutason ja tiedon saatavuuden takaamiseksi tietoliikenneverkko tulee toteuttaa mahdollisimman vikasietoiseksi. Erityisesti organisaatiolle kriittiset komponentit tulisi varustaa kriittisyyden mukaan mitoitetulla varayhteydellä. Varayhteys olisi mitoitettava ja suhteutettava niin, että palvelutaso riittää ylläpitämään vaatimusmäärittelyjä poikkeustilanteissa, joissa varsinainen verkko ei toimi.

Saatavuuden edistämiseksi voidaan erottaa organisaation ulkoisia tai muita palveluja ylläpitävät palvelimet kriittisiä toimintoja ylläpitävistä järjestelmistä ja palvelimista. (ISO 27002, 2017, 58,81.)



Kuva 3. Havainnollistava kuva VPN-toiminnasta (VAHTI 5/2013, 26.)

3.3.6 Käyttöturvallisuus

Käyttöturvallisuuden tavoitteena on minimoida tietojenkäsittelyssä tapahtuvat virheet sekä ylläpitää ympäristön tietoturvallisuutta. Tähän kuuluu toimivuuden valvonta, käyttöoikeuksien hallinta, käytön ja lokien valvonta, ohjelmistotuki, ylläpito-, kehittämis- ja huoltotoimet, varmuuskopiointi sekä häiriödokumentointi. Käyttöturvallisuuden kulmakivenä ovat selkeät toimintaohjeet järjestelmän käyttäjälle sekä järjestelmän ylläpitäjälle. Ylläpitokäytäntöjen tulisi olla selkeästi jaoteltu sekä vastuutettu. Organisaation tietoturvaan vaikuttavien muutosten tulee olla hallittuja sekä niitä varten tulee luoda menettelyohjeet sekä kaikki muutokset olisi dokumentoitava sekä lokit tehdä tarkasti. Mikäli palvelua ylläpitää kolmas osapuoli, täytyy sopimuksen kautta olla selvillä osapuolien vastuu, ylläpitopalvelun taso sekä häiriötilanteiden vasteaika. (VAHTI 3/2007, 65-66.)

Organisaation tietoteknistä ympäristöä tulee valvoa palvelun kriittisyyden vaatimalla tasolla. Valvonta voi olla lokitietoihin perustuvaa passiivista valvontaa tai palvelun

aktiivista seuraamista sen yhteyden toimivuuden kannalta. Valvonta voi olla automatisoitu järjestelmä, joka raportoi sekä ilmoittaa katkoksista palvelussa. Kaikkien palvelujen toiminnasta tulisi kertyä lokitietoja, joiden tulisi olla järjestetty siten, että niitä ei pääse muuttamaan tietoturvapoikkeamien tai -murtojen yhteydessä. Näistä lokitiedoista saadaan selville mahdolliset tunkeutumisyritykset, väärinkäytökset sekä mahdolliset onnistuneet tunkeutumiset. Näiden lokitietojen avulla voidaan selvittää yksityiskohtaisesti palvelussa tapahtuneet tapahtumat. (VAHTI 3/2007, 66-68.)

Käyttöturvallisuus sisältää päätelaitteiden suojaamisen viruksilta ja haittaohjelmilta. Päätelaitteissa tulee olla ajantasaiset haittaohjelmien havaitsemis- ja esto-ohjelmistot. Näitä ohjelmistoja täytyy valvoa, katselmoida ja päivittää, jotta niiden toimintatehokkuus säilyy vaatimusmenettelyjen mukaisena. Käyttäjillä tulee olla riittävä tietoturvatietoisuus sekä ohjeistus siitä, mitä organisaation järjestelmiin saa asentaa tai millaisia toimia saa/ei saa tehdä. Tätä voidaan auttaa luomalla hallintakeinot, jotka estävät käyttäjien haitalliseksi katsotun toiminnan. Organisaation tulisi myös luoda jatkuvuussuunnitelma haittaohjelmahyökkäyksen toipumisen varalle, sen tulisi sisältää tiedostojen sekä ohjelmistojen varmuuskopioinnin ja palauttamiseen liittyvät toimet. (ISO 27002, 2017, 49-50.)

Käyttöturvallisuuteen liittyy myös salasanat ja niiden käyttö. Organisaatiolla tulisi olla selvä linjaus ja hallintajärjestelmä, joilla edistetään turvallisten salasanojen käyttöä. Tämä järjestelmä voi esimerkiksi pakottaa käyttäjät valitsemaan turvallisen salasanan ja pakottaa vaihtamaan se tietyn ajanjakson välein Henkilöstöä tulisi kouluttaa ja kertoa turvallisista sekä kuinka niitä käytetään ja suojellaan paljastumiselta. Yhteiskäyttöisten ylläpitotunnusten salasanoja on ylläpidettävä sekä vaihdettava määritettyjen tapahtumien jälkeen, esimerkiksi työntekjiän lähdettyä tehtävästään, tai tietyn ajanjakson välein. (ISO 27002 2017, 18,30,35.)

3.3.7 Tietoaineistoturvallisuus

Organisaatioissa käsitellään tietosisällöltään hyvinkin moninaisia asiakirjoja sekä tiedostoja. Tiedon luottamuksellisuuden ja eheyden säilyttämiseksi asiakirjat ja tiedostot on luokiteltava niiden sisältämän tietosisällön merkittävyyden mukaan

kategorioittain. Luokittelun tulee olla yhdenmukainen koko organisaatiossa ja sen tulisi olla sisällytettynä organisaation prosesseihin. Luokitteluperiaatteiden tulisi olla kytkeytyneenä pääsynhallintapolitiikkaan. Luokitteluun täytyy sisältyä koko organisaatiossa yhdenmukainen prosessi tiedon luomisesta, omistajuudesta, käsittelystä, säilytyksestä ja tuhoamisesta sekä arkistoinnista. Luokittelun ansiosta henkilöstö voi helposti tulkita miten tiettyä tietoa pitää käsitellä ja suojata. (ISO 27002 2017, 23-24.)

Salassapitoluokat määritellään yleisesti yritysmaailmassa neliportaisesti: julkinen, luottamuksellinen, salainen ja erittäin salainen. Nämä luokat voivat erota riippuen organisaatiosta, esimerkiksi valtionhallinto luokittelee luokat vain salattavalle tiedolle, joten julkista asiakirjaa ei erikseen luokitella. (VAHTI 2/2010, 57.)

Luokiteltu tieto on merkittävä sen luokitusta vastaavalla merkinnällä riippumatta siitä, onko tieto fyysisessä vai sähköisessä muodossa. Organisaatiossa tulee olla yleinen toimintamalli siihen, kuinka ja miten luokiteltu tieto merkitään. Mikäli tieto on julkista, sitä ei ole tarpeen merkitä, jotta resursseja ei tuhlaannu. Organisaation henkilöstön tulee olla tietoisia merkintämenettelyistä ja käytänteistä. Alla on esimerkki valtionhallinnon käyttämistä merkinnöistä. (ISO 27002 2017, 23-25.)

Kuva 4. Viralliset valtionhallinnan turvaluokittelumerkinnät (VAHTI 2/2010)

3.3.8 Fyysinen turvallisuus

Tiedon tai sen käsittelylaitteiston ollessa fyysisessä muodossa tulisi sitä myös suojata fyysisiltä uhilta, jotka voivat olla ulkoisia tai sisäisiä. Fyysisellä turvallisuudella tarkoitetaan siis laitteistojen, aineistojen, henkilöiden, toimi- ja varastotilojen suojaamista tuhoutumista ja vahingoittumista vastaan. Tähän sisältyy muun muassa kulunvalvonnan ja tilojen valvonnan, vartionnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan. Tietoturvaluokiteltua sisältävät tilat tai laitteistot, joilla käsitellään tietoturvaluokiteltua materiaalia tulee määritellä turva-alueisiin. Näillä turva-alueilla tulee noudattaa turvavaatimusten mukaisia määrityksiä. (VAHTI 1/2002, 5-9.)

Näihin määrityksiin tulisi kuulua kulunvalvonta, jolla estetään tietylle alueelle sellaisen henkilön pääsy, jolla ei ole oikeutta käsitellä kyseisellä alueella sijaitsevaa tietoa tai siellä olevaa laitteistoa. Tämä voidaan toteuttaa esimerkiksi kulkukorttijärjestelmällä, joka estää tiloihin pääsyn asiattomilta sekä, samalla ylläpitää rekisteriä, kuka on suojatulla alueella kulkenut. Tilaan johtavien kulunvalvottujen ovien tulisi olla samalla myös murtosuojattu, eikä tilaan tulisi päästä muuta reittiä. (ISO 27002 2017, 40)

Ympäristön luomia uhkia vastaan on myös suojauduttava asianmukaisesti. Laitetilat on suunniteltava ja toteutettava niin, että ympäristön aiheuttamat riskit olisivat mahdollisimmat vähäiset. Tällainen tila tarkoittaa rakenteellisesti sekä turvalaitteistollisesti huomioonotettujen seikkojen kokonaisuutta.

- Tilan paloturvallisuuteen vaikuttavat uhat pitää huomioida. Seinien ja ovien tulisi olla palovahvistettuja. Palon tunnistus- sekä sammutusjärjestelmät tulisi olla tilaan sopivat sekä ajantasaiset. Tilaan ei saa päästä savua muista huoneista esimerkiksi ilmanvaihtokanavia pitkin. Tilassa tulisi myös säilyttää mahdollisimman vähän palokuormaa kasvattavaa materiaalia

- Tilaan ei tulisi päästä vesivahingon sattuessa vettä. Viemärit ja vesiputket tulisi olla sijoitettuna tilan ulkopuolelle. Tilassa tulisi kuitenkin olla kosteusantureita.

- Tilan ilmankosteutta sekä lämpötilaa tulisi pystyä hallitsemaan. Tietotekniset laitteet tuottavat lämpöä ja voivat vioittua liiallisesta lämmöstä tai kosteudesta.

- Sähkön saatavuus tulisi olla turvattu poikkeustilanteissa. Varavoimakoneilla saadaan tuotettua sähköä laitteistoille isompien katkoksien aikana. UPS-varavirtalähteiden avulla voidaan taata sähkön saanti laitteille pienempien katkojen aikana. Lisäksi kyseiset UPS-varavirtalähteet suojaavat laitteistoja ylijännitepiikeiltä, jotka johtuvat esimerkiksi ukkosesta.

- Vandalismilta ja varkauksilta tila voidaan suojata rakenteellisilla ominaisuuksilla. Tilan tulisi olla ikkunaton ja rakenteellisesti toisen turva-alueen sisällä. Tilaan täytyy olla murtosuojattu sekä kulunvalvottu ovi.

- Mikäli turvavaatimukset niin määrittävät, täytyy tila suojata myös EMP- ja HMP- säteilyltä. Näitä säteitä voivat aiheuttaa esimerkiksi radiomastot tai lähistöllä toimivat tutkat. (VAHTI 1/2002, 14).

Fyysiseen turvallisuuteen lukeutuu myös tiedonsiirto- ja sähkökaapeloinnin suojaus luvattomasti liittymiseltä, häirinnältä tai tarkkailulta. Kaapeloinnin tulee siis olla suojattu niin, ettei siihen voi päästä käsiksi ja vaikuttamaan siinä kulkevaan dataan tai virtaan. (ISO 27002, 2017, 43.)

Kokonaisuuden toimivuuden kannalta on laadittava ohjesäännöt ja toimintaohjeet henkilöstölle sekä tiloista vastaaville henkilöille. Ohjeistuksen tulee kattaa turva-alueiden olemassaolo sekä niiden sisällä toimiminen. Mikäli jotkin toimet tarvitsevat erityisosaamista, esimerkiksi laitetiloissa toimivat erityispalosammuttimet, tulee niiden käytön vastuulla olevalla henkilöllä olla asianmukainen koulutus niiden käyttöä varten. (ISO 27002 2017, 39-42.)

Taulukko 1. Uhkatekijät ja suojaustasot (VAHTI 1/2002).

Toimitilaluokka	1	2	3	4
Uhkatekijä	Perustaso	Tehostettu-	Erityissuojaus	Täyssuojaus
Varkaus	X	X	X	X
Kulunvalvonta	X	X	X	X
Tunkeutuminen	X	X	X	X
Tulipalo	X	X	X	X
Ilkivalta	X	X	X	X
Lämpö	X	X	X	X
Savu	X	X	X	X
Vesivahinko	X	X	X	X
Pöly ja puhtaus	X	X	X	X
Laitevaurio, huolto	X	X	X	X
Koulutus	X	X	X	X
Henkilöstö	X	X	X	X
Ovet ja lukitus	X	X	X	X
Palo-osastointi	X	X	X	X
UPS	X	X	X	X
Olosuhdehälytys		X	X	X
Varavoima			X	X
Kameravalvonta			X	X
Tärinä ja värähtely			X	X
Kemikaalit			X	X
Rakenneratkaisu			X	X
Räjähteet			X	X
Polttotaisteluaineet			X	X
Valmiussuunitelma			X	X
Sammutuslaitteet			X	X
Vierailut ja tiedotus			X	X
Turvasopimukset			X	X
Varatilat (-keskus)			X	X
EMP ja säteily				X
HPM				X

4 TIETOTURVALLISUUDEN KÄSITTELY

4.1 Tietoturvan käsittelymallit

Tieoturvaa voidaan käsitellä useilla eri malleilla sekä lähestyä eri näkökulmista. Suomessa yleisimmin käytetyt mallit ovat: Puolustusministeriön turvallisuusauditointikriteeristö (KATAKRI), Valtiohallinnon tieto- ja kyberturvallisuuden johtoryhmän ohjeisto (VAHTI) sekä ISO/IEC 27000 -standardisarja.

Mainninan arvoisena, mutta hieman vanhentuneeksi muuttuneena mallina: Elinkeinoelämän Keskusliiton yritysturvallisuusmäärittely.

4.2 Standardit

Kattavin tietoturvaa käsittelevä standardi on ISO-organisaation tuottama julkinen ISO/IEC 27000-standardiperhe. Tämä standardi ohjeistaa ja määrittelee vaatimukset tietoturvallisuuden hallintajärjestelmän luomiselle, käyttämiselle, katselmoinnille, ylläpidolle sekä parantamiselle. Standardin vaatimuksia voidaan soveltaa riippumatta organisaation tyypistä tai koosta. Standardin useat eri osat käsittelevät eri aihealueita sekä toimivat ohjeistuksena, kuinka tietoturvallisuus ja hallintajärjestelmät toteutetaan.

4.3 Ohjeistukset ja auditointikriteeristöt

Valtionvarainministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) kehittämään ohjeistusta, jonka piiriin kuuluu kaikki tietoturvallisuuden osa-alueet. Näiden ohjeistuksen tarkoituksena on edistää digitaalisten toimintaympäristöjen valmiutta vastata haasteisiin. Kukin ohje kattaa tietyn tietoturvallisuuteen liittyvän näkökohdan. VAHTI-ohjeet ovat täysin julkisia, ja niitä saa käyttää yleisesti, vaatimuksena on ainoastaan alkuperälähteen mainitseminen. (Valtiovarainministeriö, [vittattu 27.4.2020].)

Katakri on viranomaisten auditointityökalu, jonka pohjana toimii voimassa oleva lainsaäädäntö sekä Suomea sitovat kansainväliset tietoturvavelvoitteet. Lähtökohtaisesti tämä on tarkoitettu käytettäväksi arvioimaan organisaatioiden kykyä suojata viranomaisen salassa pidettävää tietoa, mutta sitä voidaan käyttää myös organisaation sisäiseen ja organisaatioiden väliseen arvioimiseen. Katakri jakautuu kolmeen osa-alueeseen, joita voidaan käyttää omina kokonaisuuksina. Nämä osa alueet ovat: turvallisuusjohtaminen, fyysinen turvallisuus ja tekninen tietoturva. Koska Katakri on julkinen, läpinäkyvä, yhdenmukainen sekä laaja, voidaan sitä käyttää helposti vertailemaan organisaatioiden tai viranomaisten tietoturvallisuuden yhdenmukaisuutta sekä kehittämään organisaation turvallisuutta. Katakri soveltuu myös suoraan ISO-standardeihin sekä VAHTI-ohjeistuksiin. (Puolustusministeriö, [Viitattu 27.4.2020].)

4.4 Sertifikaatit ja sertifioituminen

Sertifikaatit ovat osoitus organisaatiolle siitä, että se on läpäissyt sertifikaatin asettamat vaatimusmääritteet tietyllä osa-alueella. Sertifiointia varten yrityksen on toteutettava sertifikaatin myöntäjän asettamat vaatimukset ja määritteet, jotka voidaan yleisesti osoittaa auditoinnilla. Sertifikaatit osoittavat organisaation kyvyn toimia sekä luottamuksen asiantuntemukseen myönnetyn sertifikaatin toimialueella. Sertifikaatit antavat organisaatiolle uskottavuutta organisaation toimintaan. (Dnvgl, [Viitattu 27.4.2020].)

FINCSC-sertifikaatti on JYVSECTECin rekisteröity tuotemerkki, joka osoittaa sertifioidun organisaation saavuttaneen riittävän tason tietoturvallisuudessa. FINCSC-sertifikaatti sisältää vaatimukset perustietoturvallisuudentason saavuttamiseksi, ja jolla osoitetaan organisaation tietoturvakontrollien ja tietosuojakäytänteiden asianmukaisuus. Mikäli organisaatio ei ole sertifioitunut FINCSC-jäsen, hän ei voi tietää, mitä se pitää sisällään, täten se ei tarjoa suurta hyötyä arvioimaan yhteistyökumppanin kyvykkyyttä vaikka hänellä olisikin FINCSC-sertifiointi.

Organisaatio voi sertifioitua ISO/IEC 27000 -standardisarjan valitsemallaan viitekehtyksellä. Tämä vaatii ulkopuolisen organisaation akkreditoitua ja auditoitua toimenpidettä, jossa katselmoidaan ja arvioidaan organisaation taso halutussa viitekehyksessä. Mikäli organisaation auditoitu tulos täyttää viitekehyksen asettamat vaatimusmääritteet, saa yritys sertifikaatin ISO/IEC 27000 -osa-alueesta. (ISO, [Viitattu 27.4.2020].)

5 YHTEENVETO

Tietoturvan ollessa laaja sekä monihaarainen käsite tämän oppaan luomisessa jouduttiin perehtyä suureen määrään lähteistöä. Standardit sekä valtionhallinnon oppaat tarjosivat kattavan materiaalin tietoturvan toteutuksesta sekä vaatimusmäärittelyistä tietoteknisissä ympäristöissä. Lähdemateriaalit tarjosivat paljon uutta tietoa ja ymmärrystä tietoturvaa koskien ja oppimista tapahtui runsaasti työtä tehdessä.

Haasteena oli määritellä teorian sekä oppaan laajuus. Asiasisältöä olisi saanut aikaan jokaisesta alakohdasta oman opinnäytetyön verran, mutta sitä täytyi rajata nykyiseen muotoon aiheen laajuuden vuoksi. Nykyinen muoto palvelee myös parhaiten sille määritettyä tarkoitusta.

Oppaan teossa olisi hieman voinut käyttää visuaalisesti miellyttävempiä ratkaisuja, mutta tarkoituksena oli kuitenkin tuottaa selkeä ja helposti käytettävä opas kriteeristölle, jolloin yksinkertaisella ulkoasulla voidaan vaikuttaa sen luettavuuteen ja ymmärrettävyyteen. Pohtiessani myös muita seikkoja, kuinka oppaastaa saadaan luotua selkeä ja toimiva kokonaisuus, tultiin lopputulokseen, että yksinkertaisella rakenteella, jossa avataan kriteeri kerrallaan, kerrotaan sen tarkoitus ja tekninen ratkaisu, oli kaikista relevantein vaihtoehto.

Opas luovutetaan toimeksiantajalle JYVSECTEC tietoturvakeskukselle ja he saavat käyttää sitä vapaasti FINCSC -tuotteeseen liittyen tarpeidensa mukaan.

LÄHTEET

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

Dnvgl. Ei päiväystä. Sertifiointi. [Verkkosivu]. [Viitattu 27.4.2020]. Saatavissa: https://www.dnvgl.fi/sertifiointi/Johtamisjarjestelmat/miksi-sertifioida.html

Elinkeinoelämän keskusliitto. Ei päiväystä. Henkilöstöturvallisuus. [Verkkosivu]. [Viitattu11.2.2020].Saatavana:https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/henkilostoturvallisuus/.

ISO 27000. 2017. Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto. Helsinki: Suomen Standardisoimisliitto SFS.

ISO 27001. 2017. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS.

ISO 27002. 2017. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Helsinki: Suomen Standardisoimisliitto SFS.

JYVSECTEC. Ei päiväystä. FINCSC. [Verkkosivu]. [Viitattu 20.4.2020]. Saatavissa: https://www.fincsc.fi/

ISO. Ei päiväystä. ISO/IEC information security management. [Verkkosivu]. [Viitattu 27.4.2020]. Saatavissa: https://www.iso.org/isoiec-27001-information-security.html

Laamanen, K. 2007. Johda liiketoimintaa prosessien verkkona. Ideasta käytäntöön. Espoo: Laatukeskus Excellence Finland.

Paavilainen, J. 1998. Tietoturva. Espoo: Suomen ATK-kustannus Oy.

Puolustusministeriö. Ei päiväystä. Katakri. [Verkkosivu]. [Viitattu 27.4.2020]. Saatavissa: https://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

VAHTI 5/2013. Päätelaitteiden tietoturvaohje. Helsinki: Valtionvarainministeriö.

VAHTI 3/2010. Sisäverkko ohje. Helsinki: Valtionvarainministeriö.

VAHTI 2/2016. Toiminnan jatkuvuuden hallinta. Helsinki: Valtionvarainministeriö.

VAHTI 3/2007. Tietoturvallisuudella tuloksia. Helsinki: Valtionvarainministeriö.

VAHTI 5/2006. Asianhallinnan tietoturvallisuutta koskeva ohje. Helsinki: Edita Prima Oy.

VAHTI 1/2002. Valtion viranomaisen tietoturvallisuustuön yleisohje. Helsinki: Valtionvarainministeriö.

Traficom. 2019. Tietoturva. [Verkkosivu]. Liikenne- ja viestintävirasto Kyberturvallisuuskeskus. [Viitattu 20.4.2020] Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva]

Valtiovarainministeriö. Ei päiväystä. VAHTI. [Verkkosivu]. Valtiovarainministeriö. [Viitattu 27.4.2020]. Saatavissa: https://vm.fi/julkaisut/vahti

L726/2014. Turvallisuusselvityslaki

L19.12.1889/38. Rikoslaki

LIITTEET

Liite 1. FINCSC kriteerist