OULUN AMMATTIKORKEAKOULU

Maria Ollila

TIETOTURVASUUNNITELMA PK-YRITYKSELLE

TIETOTURVASUUNNITELMA PK-YRITYKSELLE

Maria Ollila
Opinnäytetyö
Kevät 2019
Tietojenkäsittelyn tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma

Tekijä(t): Maria Ollila
Opinnäytetyön nimi: Tietoturvasuunnitelma PK-yritykselle
Työn ohjaaja: Teppo Räisänen
Työn valmistumislukukausi ja -vuosi: Kevät 2019 Sivumäärä: 28

Tietoturvasuunnitelma PK-yritykselle tehtiin yritykselle, jolla ei ollut aikaisempaa kirjoitettua tietoturvasuunnitelmaa. Työn tavoitteena oli suunnitella ja kirjoittaa tietoturvasuunnitelma kyseiselle yritykselle. Suunnitelman tekemisessä käytettiin aiheeseen liittyvää alan kirjallisuutta. Päätuloksena oli toimiva tietoturvasuunnitelma.

Tietoturvasuunnitelma on yksi yrityksen keinoista ennaltaehkäistä teknologian ja digitaalisuuden kehittämiä uhkakuvia, kuten huijausviestit, erilaiset tietokonevirukset, sekä salasanojen urkinnat, joilla pyritään saamaan haltuun yritykselle tärkeää tietoa. Sen kolme keskeisintä pääasiaa ovat luottamuksellisuus, eheys ja saatavuus, eli tiedon saa ainoastaan ihminen, jolla on siihen oikeus, oikeaan aikaan ja että tieto ei ole muuttunut missään vaiheessa.

Yrityksen tietoturvaan kuuluu kolme eri tasoa, joista tietoturvasuunnitelma on keskimmäinen, korkeimmalla on tietoturvapolitiikka ja alimmaisena tietoturvaohjeistukset. Tietoturvapolitiikka on yrityksen yleinen kanta tietoturvaan. Tietoturvasuunnitelma toteuttaa tietoturvapolitiikan tavoitteita ja tietoturvaohjeistukset ovat tarkempia ohjeita yksittäisiä tietoturvakohteita varten.

Opinnäytetyön lopputuloksena oli tietoturvasuunnitelma, mikä oli myös tavoitteena. Se otetaan käyttöön yrityksessä kevään 2019 aikana. Tulevaisuudessa tietoturvasuunnitelmaa on tarkoitus kehittää vastaamaan entistä paremmin uusiin uhkakuviin, sekä yrityksen tarpeisiin.

Asiasanat: tietoturva, yrityksen tietoturva, tietoturvasuunnitelma

ABSTRACT

Oulu University of Applied Sciences
Degree programme in Business Information

Author(s): Maria Ollila
Title of thesis: ICT Security Plan for SM-Business
Supervisor(s): Teppo Räisänen
Term and year when the thesis was submitted: Spring 2019 Number of pages: 28

ICT Security Plan for SM-Business was made for business that had no previously written plan. The goal was to plan and write ICT security plan for this company. The plan was made by using literature about information security. The result was an ICT security plan for the business.

ICT security plan is one tool for the company to prevent threats that have come up with technology and digitalization, for example computer viruses, scam messages and password security attacks. Meaning behind them is to steal valuable information from the company. The three main things in ICT security plan are confidentiality, integrity and availability. Meaning that only person who is allowed gets the information, that hasn't been change, at the right time.

The business side of information security has three levels. The ICT security plan is the middle one. The uppermost level is information security politics and the lowest are the detailed instructions for information security. The politics is how the information security is viewed in the company. The plan is for how to meet the goals in the politics and the detailed instructions is for specific information security tasks.

The thesis' result was the ICT Security Plan for the business as was the goal. It will be put in the action during the Spring 2019. In the future, the plan is meant to be develop even further to respond to different threats and company's needs.

Keywords: information security, business information security, information security plan

SISÄLLYS

1 JOHDANTO

EU:n tietosuoja-asetus astui voimaan 25.5.2018. Tämä tietosuoja-asetus asettaa tarkat raamit yrityksille, kuinka asiakkaiden, sekä työntekijöiden henkilötietoja tulisi käsitellä. Lista on pitkä ja yhtenä listan vaatimuksena on, että yrityksellä on tietoturvasuunnitelma. Tietoturvasuunnitelman avulla yritys pysyy kartalla missä heidän heikot kohtansa ovat, että myös mitä he voivat tehdä tietoturvamurron jälkeen.

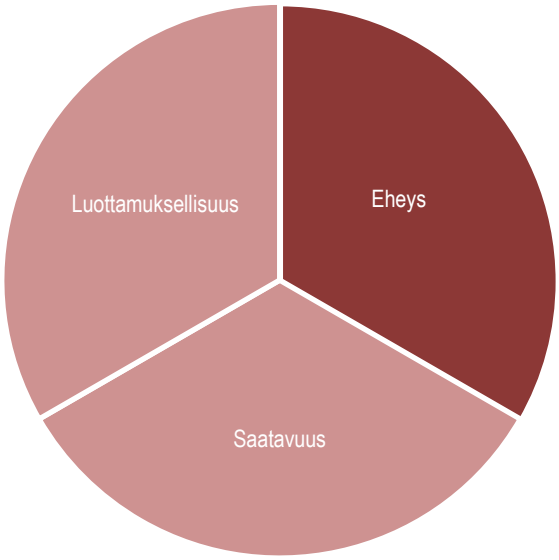
Olen työskennellyt eräässä Pk-yrityksessä maaliskuusta 2018 alkaen. EU:n tietosuoja-asetus on ollut siellä esillä, kun sen mukaisia toimia on tehty. Yhtenä projektina oli yritykselle tietoturvasuunnitelman tekeminen, jonka otin opinnäytetyöni aiheeksi. Tietoturvasuunnitelma tehdään vuosille 2018-2020.

Tietoturvasuunnitelman tarkoituksena on havaita yrityksen vahvuudet ja heikkoudet, sekä varautua pahimpiin mahdollisiin skenaarioihin ja vastata näihin. Yrityksen X:n erikoisuutena on tiheästi vaihtuva henkilöstö, joka luo omalta osaltaan haasteita tietoturvasuunnitelman tekemiseen. Suunnitelman pitää olla mahdollisimman kattava, sekä helposti luettava, että seuraava henkilöstö pystyy jatkamaan sen toteutusta.

2 TIETOTURVAN PERUSTEET

”Tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja saatavuuden takaamista” (Rousku 2014, 47).

Tietoturvallisuus on laaja käsite, joka sisältää paljon asiaa. Nykyaikaisessa digitaalisessa yhteiskunnassa tietoturva on erittäin tärkeää pitää kunnossa niin yrityksissä kuin yksittäisillä henkilöillä. Yleisesti se kuitenkin jaetaan kolmeen osaan (kuvio 1), jotka ovat mainittu ylempänä.



Kuvio 1: Tietoturvallisuuden kolme osa-aluetta

Luottamuksellisuus tarkoittaa tietoturvassa sitä, että tiedot ovat vain niiden henkilöiden ja organisaatioiden saatavilla, joille on tietoihin oikeus, eikä niitä saa paljastaa toisille. Tietojärjestelmissä tämä tarkoittaa erilaisia käyttöoikeuksia eri käyttäjillä. Käyttäjätunnukset, salasanat ja fyysinen turvallisuus ovat kaikki osia luottamuksellisuutta. On tärkeää pitää salasanat piilossa, ettei kukaan ulkopuolinen saa niitä käsiinsä ja sitä kautta pääsyä tietoihin, joita hänellä ei ole oikeus nähdä. (Rousku 2014, 48; Rautiainen 2003, viitattu 3.11.2018.)

Eheyden tarkoituksena on pitää tieto mahdollisimman aitona, ettei se muutu tai tuhoudu hallitsemattomasti. Eheyttä on hankala korjata, kun se rikkoutuu. Tietoa saa toki muuttaa, mutta vain sellainen henkilö, johon on sillä oikeus, sekä laillisin keinoin. Varmuuskopiointi on yksi tapa varmistaa eheys, sekä eheyden palauttaminen. (Rautiainen 2003, viitattu 3.11.2018.)

Saatavuus tarkoittaa sitä, että tiedot ja tietopalvelut ovat saatavilla oikeaan aikaan sellaisille ihmisille, jotka niitä tarvitsevat. Palveluiden digitalisoidutta tämä tarkoittaa valmiutta 24/7, esimerkkinä voidaan antaa verkkopankit, sekä Kelan sähköinen asiointipalvelu, jotka ovat ihmisten tavoitettavissa vuoden jokaisena päivänä, mihin tahansa vuorokauden aikaan, pois lukien mahdolliset huoltokatkot. Uhkana saatavuudelle on palvelunestohyökkäykset, jotka kuormittavat palveluiden palvelimia ja estävät käyttäjien pääsyn palveluihin. (Rousku 2014, 50.)

Muita keinoja hahmottaa tietoturva ja sen riskit ovat muun muassa tietojen turvaaminen eli englanniksi information assurance sekä Parkerin kuusikko. Molemmissa malleissa on pohjana alkuperäinen kolmikko: luottamuksellisuus, eheys ja saatavuus, tuoden näiden rinnalle uusia ulottuvuuksia. Tietojen turvaamisessa on kaksi uutta osa-aluetta lisättynä alkuperäiseen kolmikkoon. Nämä kaksi osa-aluetta ovat todentaminen ja kiistämättömyys. Todentaminen tarkoittaa tässä tapauksessa, että käyttäjä pystytään tunnistamaan ja kiistämättömyys taas sitä, että käyttäjä ei voi sanoa tehneensä jotain, koska pystytään todistamaan, että hän teki niin. (Lord 2018, viitattu 5.2.2019.)

Parkerin kuusikossa mukaan tulee kolme uutta osa-aluetta, jotka muodostavat pareja aikaisemman kolmikon kanssa. Nämä kolme uutta aluetta ovat hallinta tai kontrolli, todentaminen ja käyttökelpoisuus. Hallinta ja kontrolli kertovat kuka määrää tiedosta, todentaminen on käyttäjän tunnistamista, ja käyttökelpoisuus tarkoittaa sitä, että tieto on käyttökelpoista kaikkien salausten jälkeenkin. (Marks 2018, viitattu 5.2.2019.)

Tietoturva on monen asian summa, mutta tärkein ja heikoin kohta tietoturvassa on aina ihminen. Ohjelmistot, toimitilat, sekä päätelaitteet voivat olla erittäin vahvasti suojattuja, mutta yksi salasanan vuoto vääriin käsiin aiheuttaa, vakavan turvallisuusriskin. Maailmassa liikkuu monia tietoturvauhkia, kuten erilaiset tietokonevirukset, troijalaiset, kiristysohjelmat, muutamia mainitakseni, mutta niillä ei yleensä ole pääsyä järjestelmään, ellei käyttäjä tee jotain ensin.

Tietoturva on tärkeä ottaa osaksi omia tapoja, niin yrityksissä kuin yksityiselämässäkin. Sen kanssa ei voi olla koskaan liian varovainen, ja varsinkin nykyisessä tietoyhteiskunnassa, jossa työt voi

viedä kotiinsa, on tärkeää pitää työ ja yksityiselämä erillään myös tietoturvan näkökulmasta. Käytäntöjä on monia, kuten työpuhelin, oma selain työasioille, jos niitä pitää hoitaa omalla koneella.

3 YRITYKSEN TIETOTURVA

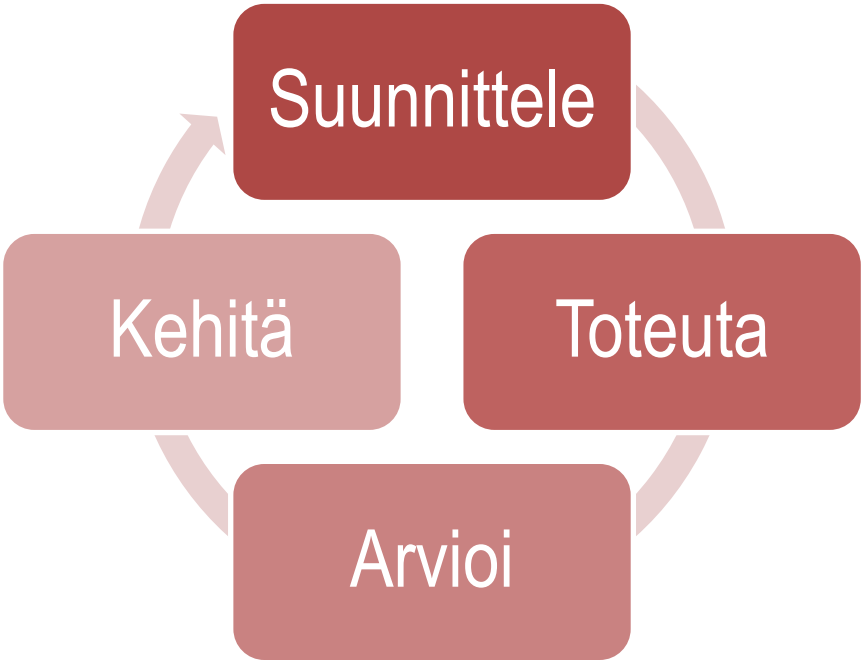
Tietoturva on tärkeä osa yritystä. Sen pitäisi olla myös luonnollinen osa yritys, mutta tämä ei välttämättä aina toteudu. Tietoturvan pitäisi kattaa myös yrityksen kaikki osa-alueet, joilla käsitellään tietoa jollain tavalla. Valitettavasti heikkoudet huomataan vasta silloin, kun joku on jo käyttänyt niitä hyväkseen, kuten murtautunut yrityksen tiloihin ja vienyt mennessään palan yritystä.

Yrityksen tietoturvan tilan voi tarkistaa erilaisilla kartoitustyökaluilta, kuten TIKKA Tietoturvallisuustilanteen kartoitustyökalu pienille yrityksille tai Keskustakauppakamarin tekemässä Tietoturvaopas yrityksille Turvallisuuden itsearviointi. (Keskuskauppakamari 2016, 20-36; Kurittu 2015, viitattu 3.11.2018.)

Yrityksen koolla ei ole tietoturvan tärkeyden kanssa mitään tekemistä. Jokaisella yrityksellä, oli se yhden hengen toiminimi valtaviin osakeyhtiöihin, on tietoja, joita on suojeltava. Tiedot, sekä niiden laajuus vaihtelevat yrityksen toimialan, sekä toimintaperiaatteen mukaan, mutta yhtä lailla tietoturva koskee kaikkea.

Yrityksen tietoturvallisuuden kannalta on tärkeää määrittää mahdolliset riskit, jotka uhkaavat yrityksen tietoturvaa, sekä luokitella yrityksen tiedot eri suojausluokkiin. Riskien lisäksi on arvioita, mitä arvokasta tietoa yritys haluaa suojella. Kaikki tiedot eivät ole samanarvoisia, eivätkä alemman suojaustason omaavat tiedot tarvitse yhtä vaativia turvatoimia kuin tärkeimmät tiedot.

Yksi tapa millä yrityksen tietoturvan parantamisen voi aloittaa on suunnittele – toteuta – arvioi - kehitä -malli. Nimensä mukaisesti siinä tehdään ensin suunnitelma, laitetaan se käytäntöön, arvioidaan suunnitelman toimivuutta ja kehitetään tarpeen vaatiessa. Tästä muodostuu kehä, joka takaa, että tietoturvaa kehitetään koko ajan eteenpäin, eikä jäädä vanhoihin käytäntöihin kiinni. (Valtiovarainministeriö 2009c, viitattu 18.11.2018.)



Kuvio 2: Tietoturvan kehittäminen

3.1 Lait ja standardit

Yrityksen tulee ottaa omassa tietoturvassaan huomioon monia lakeja, jotka osittain määräytyvät yrityksen toimialan mukaan. Aikaisemmin kaikkiin yrityksiin vaikuttavat tietoturvaan ja tietosuojaan liittyvät lait olivat henkilötietolaki ja laki tietosuojalautakunnasta ja tietosuojavaltuutetusta. Nämä lait korvattiin 1.1.2019 uudella tietosuojalailla, joka täydentää myös EU:n tietosuoja-asetusta. (Tietosuojavaltuutettu 2019, viitattu 5.2.2019)

Standardien avulla yritys voi sertifioida toimintansa tietoturvalliseksi. Tietoturvallisuuteen liittyviä standardeja on useita. Isoin näistä on International Organization of Standardization (ISO):n tietoturvan hallintajärjestelmän standardiperhe ISO/IEC 27000, johon kuuluu useita eri standardeja. Nämä standardit kuitenkin maksavat, että niitä pääsee edes lukemaan. Toinen kansainvälinen, mutta epävirallinen standardi, joka tulee ISO/IEC 27000, on Information Security Forumin (ISF) the Standard of Good Practice for Information Security 2018. (ISO 2018, viitattu 7.11.2018; ISF 2018, viitattu 7.11.2018.)

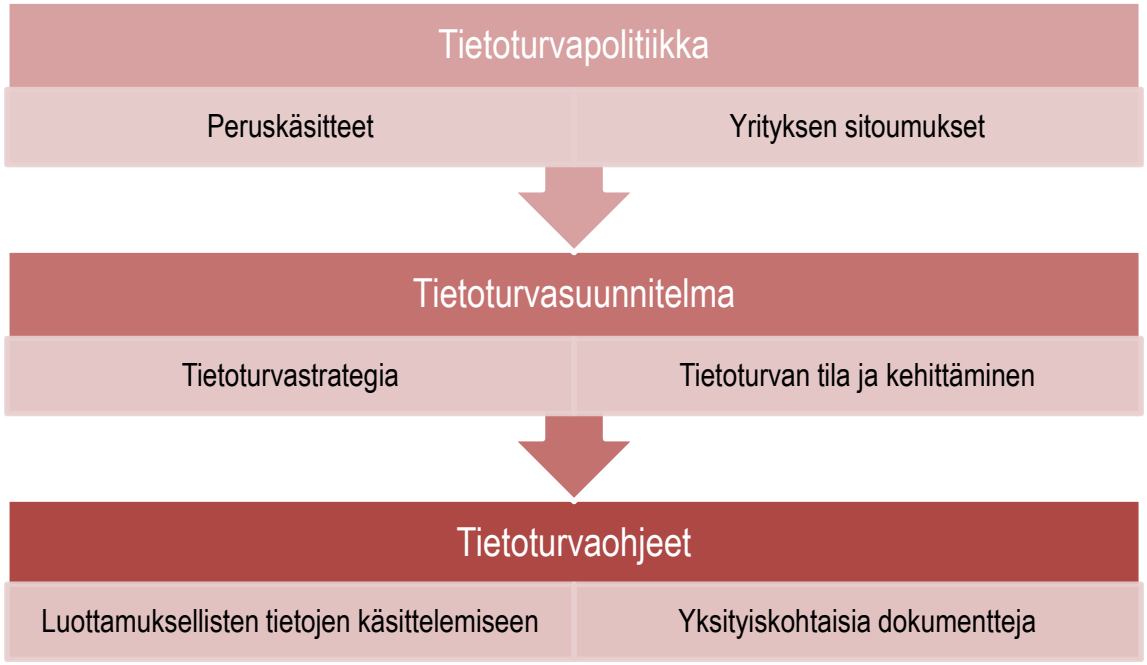
3.2 Tietoturvallisuuden johtamisen tasot

Yrityksen tietoturva koskee kaikkea yrityksessä toimivia, sekä myös ulkopuolisia, kuten asiakkaita tai alihankkijoita. Yrityksen tietoturvalla on kuitenkin olemassa useampia tasoja, joista vain osa on näkyvillä. Eri tasot myös mahdollistavat sen, että kaikki yrityksessä osallistuvat tietoturvaan. Tavallaan tietoturva lähtee kahdesta suunnasta, ylhäältä, sekä alhaalta. Yrityksen johdolla on tärkeä osa siinä, miten yrityksen tietoturvaan suhtaudutaan. Heidän tehtävänään on suunnitella yrityksen strategiat niin, että tietoturva on yksi osa. Alhaalta käsin taas jokaisella yrityksen työntekijällä on velvollisuus pitää tietoturva osana jokaista työtehtävää. Pienistä puroista syntyy suuri virta.

Yrityksen ylin tietoturvallisuuden johtaminen muodostuu tietoturvapolitiikasta. Sillä yrityksen johto määrittää yrityksen suhtautumisen tietoturvaan. Se on lyhyt ja ytimekäs dokumentti, jota ei ole tarkoitus muuttaa koko ajan. Se sisältää peruskäsitteet, yrityksen sitoutumiset, sekä tietoturvallisuuden ylläpidon, kehittämisen, sekä vastuun. Tietoturvapolitiikka ei sisällä mitään yksityiskohtaista yrityksen tietoturvasta ja näin ollen se voidaan näyttää tarpeen vaatiessa ulkopuolisille. (Miettinen 1999, 145-147.)

Tietoturvasuunnitelma on seuraava taso tietoturvapolitiikasta. Se käsittelee tarkemmin yrityksen tietoturvastrategian, sen heikkoudet ja kuinka niihin valmistaudutaan. Se antaa yleiskuvan yrityksen tietoturvan tilasta, sekä kuinka tietoturvallisuutta kehitetään eteenpäin. Tietoturvasuunnitelma ei ole muuttumaton ja se tehdäänkin määräaikaiseksi. Yrityksen tulisi vähintään vuosittain käydä tietoturvasuunnitelmansa läpi ja miettiä onko jokin muuttunut. Tietoturvasuunnitelma tulisi perusteellisesti uusia, kun yrityksen tilanne muuttuu ratkaisevasti, esimerkiksi muutto uusiin toimitiloihin. Tietoturvasuunnitelma tulisi olla vain yrityksen työntekijöiden ja johdon saatavilla.

Tietoturvaohjeet ovat viimeinen ja tarkin taso tietoturvallisuuden johtamisesta. Ne ovat erittäin tarkkoja ohjeita siitä, miten tietoturvan tulee toteutua tietyissä tehtävissä. Ne ovat tarkoitettu henkilöille, jotka työskentelevät noissa tehtävissä. Tietoturvaohjeistukset ovat erittäin tärkeitä, kun käsitellään luottamuksellisia tietoja, jotka liittyvät yritykseen tai sen asiakkaisiin. Ne ovat yksityiskohtaisia dokumentteja, jotka eivät saa ulkopuolisten käsiin.



Kuvio 3: Tietoturvan tasot

3.3 Tietoturvan osa-alueet

Tietoturvassa on monta osa-aluetta, joissa pitää ottaa omat yksityiskohdat huomioon suunnitelmaa tehtäessä. Jaottelussa voidaan käyttää apuna eri standardeja, jos yritys haluaisi hankkia sertifioinnin ja osoittaa tietoturvaosaamisensa sitä kautta. Suomessa tietoturvajaottelun voi löytää Valtionhallinon VAHTI-sivustolla, jossa tietoturva on jaettu kahdeksaan eri alueeseen: fyysinen turvallisuus, hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, käyttöturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja tietoliikenneturvallisuus. Tätä jaottelua on käytetty myös tässä opinnäytetyössä, kun tarkastellaan mitä kaikkea kukin osa-alue pitää sisällään tarkemmin.

Eri osa-alueet helpottavat yrityksen riskien analysoimista, sekä niiden hallitsemisesta. Tietoturva on loppupeleissä abstrakti käsite, joka näyttäytyy jokaiselle yritykselle hieman eri tavalla. Perusajatus on kaikille sama, mutta osa-alueiden avulla yritykset voivat keskittyä sellaiseen tietoturvaan, joka on heidän kannaltansa parhain.

3.3.1 Fyysinen turvallisuus

Fyysinen turvallisuus on olennainen osa tietoturvallisuutta, koska se käsittää kaiken liittyen tietojen, sekä koneiden fyysiseen turvallisuuteen. Yhtenä käsitteenä voidaan pitää toimitilaturvallisuutta, jossa pidetään huolta, että yrityksen toimitilat on asianmukaisesti suojattu eri uhilta. Toimitilojen uhkina voidaan pitää eri luonnonelementtejä, kuten tuli, vesi ja jää. Toisena riskiryhmänä ovat ihmiset, joilla ei ole pääsyoikeutta tiloihin, ja niihin päästessään aiheuttaa vahinkoa. Esimerkkeinä voidaan mainita murtoyritykset, varkaudet tai muu ilkivalta. (Laakso 2018a, viitattu 14.11.2018.)

Fyysisen turvallisuuden kannalta on tärkeää arvioida, mitä kaikkea yrityksen osia se koskee, sekä mikä näiden osien tärkeysjärjestys on. Paperit arkistot on turvattava vedeltä ja tulipalolta, kun taas tietotekniikan kanssa vaatimukset ovat tiukempia. Esimerkiksi palvelinhuoneissa on tärkeä mm. ylläpitää koko ajan samaa lämpötilaa, estää asiattomien pääsy tiloihin, sekä mahdollistaa sähkönsaanti hätätapauksissa. (Laakso 2010, 17-18.)

Fyysinen turvallisuus on otettava huomioon, kun yritys rakentaa uusia toimitiloja tai kunnostaa vanhoja. Jos yrityksen toimitilat on vuokrattu, niin turvallisuusjärjestelyt ja hallinta voi olla vuokraajan tai rakennuksen omistajan tehtävä. (Valtiovarainministeriö 2009, viitattu 14.11.2018.)

3.3.1.1 Pääsynhallinta

Pääsynhallinta eli englanniksi access control on yksi osa yrityksen hallinnollista, sekä fyysistä turvallisuutta. Sen tarkoituksena on taata, että kukaan, jolla ei ole oikeutta päästä käsiksi yrityksen tietoihin, ei niihin pääse. Fyysisellä puolella pääsynhallinta on kulunvalvontaa, joka yksinkertaisimmillaan on toimitilojen ovien pitäminen lukossa ja avaimien antaminen vain tietyille henkilöille. Isommissa yrityksissä kulunvalvonnasta voivat huolehtia vahtimestarit tai järjestyksenvalvojat, jotka tarkastavat jokaisen tulijan identiteetin esimerkiksi henkilökorteilla tai vierailijapasseilla.

Tietojärjestelmien ja tiedon kanssa pääsynhallinta on sähköistä ja tapahtuu pääosin tietokoneilla ja muilla laitteilla. Yksinkertaisimmillaan se on käyttäjätunnus ja salasana. Monimutkaisemmissa järjestelmissä voi olla käytössä henkilökortit, jotka asetetaan koneisiin, sekä naputellaan salasana tai pinkoodi, kun halutaan päästä sisälle järjestelmään. Erilaiset lukitus- ja pääsynhallintajärjestelmät ovat kehittyneet valtavasti teknologian myötä, eikä enää tarvitse vaihtaa koko yrityksen salasanoja

tai avaimia, jos työntekijä kadottaisi avaimen tai salasana joutuisi vääriin käsiin. Esimerkiksi suomalainen iLOQ on kehittänyt lukitusjärjestelmän, jossa on edelleen avain, mutta avaimiin pystyy ohjelmoimaan, mihin kaikkialle avaimella on pääsy. Avaimen kadotessa sen pääsyoikeudet voidaan vain evätä. (iLOQ, 2019, viitattu 1.4.2019.)

Pääsynhallintamenetelmiä on useita, joista kolme käytetyintä ovat harkinnanvarainen, pakollinen ja rooliperusteinen pääsynhallinta. Pääsynhallintamenetelmät voivat pätevät sekä fyysisiin tiloihin, että tietojärjestelmiin. Se mikä pääsynhallintamenetelmä tulisi valita riippuu täysin yrityksen tarpeista, sekä tavasta toimia. Muitakin menetelmiä on olemassa, kuten attribuuttipohjainen, sijaintiperusteinen tai riskiperusteinen pääsynhallinta.

Harkinnanvarainen pääsynhallinta, englanniksi discretionary access control, on järjestelmä, jossa järjestelmän kohteelle voidaan antaa oikeus antaa muille oikeuksia. Alkuperäisten oikeuksien antajaa kutsutaan omistajaksi, jolla yleensä on kirjoitus-, luku- ja suoritusoikeus ohjelmaan tai tiedostoon. Näitä kirjoitus-, luku- ja suoritusoikeuksia voidaan sitten myöntää eteenpäin muille käyttäjille. Harkinnanvarainen pääsynhallinta on joustava menetelmä, mutta se muodostaa myös tietoturvariskin. Käyttäjät voivat harkinnanvaraisen pääsynhallinnan avulla kopioida toisten tietoja tai tuhota tietoja viruksilla ja troijalaisilla. (Hu, Kuhn & Yaga, 2017, 3-4.)

Pakollinen pääsynhallinta, eli englanniksi mandatory access control, on harkinnanvaraista pääsynhallintaa jäykempi menetelmä. Siinä tiedostojen ja ohjelmien pääsynhallinnan oikeudet ovat etukäteen määriteltyjä, ja tiedoilla on omat tasonsa. Ihminen, jolla on tietyn tason oikeudet, pystyy pääsemään omalle tasolleen, sekä kaikille tasoille sen alapuolella. Esimerkkinä pakollisen pääsynhallinnan järjestelmästä ovat tietoaineistojen luokittelu, jolla määritellään mikä tieto on salassa pidettävää ja mikä ei. Ihminen, jolla on pääsy suojaustaso II:n materiaaleihin pääsee siis myös tasoille III ja IV, mutta ei tasolle I. Tietoturva on pakollisessa pääsynhallinnassa parempi, koska koko ajan tiedetään jokaisen oikeuden taso ja mihin kaikkialle hän pääsee. (NIST, 2014, F-11.)

Roolipohjainen pääsynhallinta, eli role-based access control, on pakollisen ja harkinnanvaraisen pääsynhallinnan välimaastossa joustavuutensa suhteen. Siinä oikeudet määritellään rooleille, jotka sitten määrätään käyttäjille. Roolin oikeuksien muuttuessa, ne päivittyvät kaikille käyttäjille, joilla kyseinen rooli on. Yksittäisen käyttäjän oikeuksia ei voi muuttaa kuin vaihtamalla tämän roolia. (Signhal, Winograd, Scarfone, 2007, 3-14.) Wordpress-julkaisujärjestelmä perustuu roolipohjai-

seen pääsynhallintaan. Siinä rooleja ovat muun muassa pääkäyttäjä, kirjoittaja ja tilaaja. Pääkäyttäjällä on kaikki oikeudet järjestelmään, hän voi kirjoittaa artikkeleja, muokata sivustoa ja päättää muiden käyttäjien oikeuksista. Kirjoittaja pystyy kirjoittamaan artikkeleita ja tilaaja vain lukemaan niitä.

3.3.2 Hallinnollinen tietoturvallisuus

Hallinnollinen tietoturvallisuus käsittää yrityksen tietoturvapolitiikan, sekä muut hallinnolliset keinot, joilla yritys pitää huolen tietoturvastaan. Sen alaisuuteen kuuluvat erilaiset ohjeistukset, tehtävien ja vastuiden määrittelyt, sekä suunnitelmat ja sopimukset. Dokumentaatiot ovat erittäin tärkeä osa hallinnollista tietoturvaa, sillä niillä varmistetaan yrityksen lähtötaso tietoturvan suhteen, sekä se mihin yritys on menossa. (Laakso 2018b, viitattu 14.11.2018; Valtiovaranministeriö 2009, viitattu 14.11.2018.)

Hallinnollinen tietoturva on yrityksen johdon tapa sitouttaa koko yritys, jokaista työntekijää myöten noudattamaan tietoturvaa. Kaikki lähtee tietoturvapolitiikasta, jolla määritellään siis organisaation tietoturva. Tämän jälkeen tulevat erilaiset suunnitelmat, joiden avulla voidaan varautua ja valmistautua, sekä erilaiset ohjeistukset ja koulutukset työntekijöille. Tietoturvapolitiikan yläpuolelle voidaan vielä nostaa tietoturvallisuuden hallintapolitiikka, jossa määritellään tietoturvallisuuden suunta ja tavoitteet. (Andreasson & Koivisto 2013, 33, 36-37.)

3.3.3 Henkilöstöturvallisuus

Henkilöstöturvallisuudella varmistetaan, ettei yrityksen tietoturva kärsi, kun uutta henkilöstöä palkataan tai kun henkilöstö siirtyy uusiin tehtäviin yrityksen ulkopuolelle. Toinen henkilöstöturvallisuuden näkökulma on estää henkilöiden tekemät virheet, jotka voivat aiheuttaa rikollisen pääsyn yrityksen tietojärjestelmiin. Henkilöstöturvallisuus kulkee mukana työntekijän palkkaamisesta hänen eroamiseensa asti.

Henkilöstöä palkatessa on tärkeää tutkia henkilön taustat hyvin hänen tehtävän kuvansa edellyttämällä tarkkuudella. Henkilötaustan tutkiminen tapahtuu muun muassa suositusten varmistamisella

tai jopa suojelupoliisin tekemällä henkilöturvallisuusselvityksellä. Yrityksen todetessa henkilön sopivan tehtävään, ja palkatessaan hänet, on suositeltavaa tehdä salassapitosopimus. Salassapitosopimus voi kestää henkilön työuran päättymisen jälkeenkin useamman vuoden.

Henkilön työsuhteen päättyessä henkilöstöturvallisuuden tehtävänä on varmistaa, ettei yritys menetä tietoja henkilön mukana, sekä estää henkilön pääsy tulevaisuudessa yrityksen tiloihin. Tämä tarkoittaa kaikkien yrityksen tavaroiden, avaimien, henkilökorttien ja muiden vastaavien palauttamista. Lisäksi henkilön lähtiessä on hänen työtehtävänsä joko kokonaan tai osissa jaettava jatkettavaksi. Tapauksesta on myös tiedotettava asianmukaisille henkilöille, kuten työtovereille ja asiakkaille, että he osaavat olla jatkossa yhteydessä oikeisiin ihmisiin. (Miettinen 1999, 169-170.)

3.3.4 Käyttöturvallisuus

Käyttöturvallisuus liittyy olennaisesti yrityksen arkisiin prosesseihin. Siihen kuuluvat muun muassa järjestelmien valvonta, ylläpitäminen ja päivittäminen. Sen päätavoitteena on tietotekniikan toimintavarmuus, sekä kuinka varautua mahdollisesti, jos jotain tapahtuu. (Valtiovarainministeriö 2009d, viitattu 18.11.2018.)

Esimerkkinä käyttöturvallisuudesta on varmuuskopioiden ottaminen. Tietojen olisi hyvä olla useammassa paikassa, mahdollisten tietoteknisten ongelmien takia. Tietokoneiden kovalevyt eivät ole maailman varmin paikka tietojen säilyttämiseen, vaan tiedot voivat yhtäkkiä pyyhkiytyä niiltä väärien toimenpiteiden vuoksi. Kopiointi toiseen paikkaan varmistaa, ettei mitään tärkeää kuitenkaan menetetä, jos näin ikävästi pääsee käymään.

3.3.5 Laitteistoturvallisuus

Laitteistoturvallisuus koskettaa kaikkia yrityksen teknisiä laitteita, kuten tietokoneet, palvelimet, tulostimet ja matkapuhelimet. Sen avulla määritetään, kuka pystyy käyttämään mitäkin laitetta ja millä oikeuksilla. Laitteiston pitäminen kunnossa, sekä työntekijöiden ohjeistaminen laitteistojen käyttämisestä on tärkeää. (Laakso 2010, 21-22.)

Osana laitteistoturvallisuuteen kuuluu laitteistojen dokumentointi. Yrityksen tulee tietää, mitä laitteita sillä on käytössä, sekä koska laitteet on ostettu tai otettu käyttöön. Vanhemmat laitteet ovat

alttiimpia tietoturvamurroille, koska niillä ei välttämättä ole enää valmistajan tukea eli päivityksiä uusimpia tietoturvauhkia vastaan. Täytyy myös ottaa huomioon, että laitteillakin, kuten tiedoillakin on omat suojaustasonsa. Yksi tietokone pitää sisällään paljon yritykselle tärkeitä tietoja toisin kuin esimerkiksi tulostin. Nykyään tosin tulostimetkin ovat monitoimilaitteita, joiden avulla voidaan päästä käsiksi yrityksen verkkoihin ja sitä kautta verkoissa oleviin tietokoneisiin.

Laitteistojen sijoittaminen, sekä fyysinen turvaaminen on myös osa laitteistoturvallisuutta. Varsinkin, kun tietokoneet ja puhelimet ovat pienentyneet huomattavasti vuosien aikana. Tietokoneen sijoittaminen huoneen takaosaan pienentää varkauden riskiä, kun varkaan pitäisi kävellä koko huoneen poikki verrattuna siihen, että tietokone olisi sijoitettuna oven viereen, josta sen voisi vain napata mukaansa. (Laakso 2010, 22.)

3.3.6 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus koskee kaikkia niitä ohjelmia, joita yrityksen tietokoneet ja puhelimet sisältävät. Sen suojausmenetelmiin kuuluu sovellusten ja niiden lisenssien pitäminen ajan tasalla. Aika ajoin esimerkiksi Windowsissa ilmaantuu haavoittuvuuksia, joita Microsoft paikkaa uusilla käyttöjärjestelmän ja ohjelmistojen päivityksellä (Linnake 2018, viitattu 18.11.2018).

Ohjelmistoissa, kuten laitteistoissakin, dokumentointi, sekä työntekijöiden kouluttaminen on tärkeää. Työntekijä, joka ei osaa käyttää ohjelmistoa oikein, voi tehdä sen kanssa paljon tuhoa yrityksen tärkeiden tietojen kannalta. Dokumentaatio taas auttaa vastuuhenkilöitä pysymään kärryillä siitä, minkälaisia ohjelmistoja yrityksellä on käytössä, ja mitä niiden kaikkien päivittäminen vaatii. Varmuuskopiointi on myöskin ohjelmistoturvallisuudessa hyväksytty keino turvata toiminta. (Miettinen 1999, 226-228.)

Yhtenä asiana ohjelmistoissa täytyy ottaa huomioon erilaiset pilvipalvelut, jotka ovat kasvattaneet suosiotaan helppokäyttöisyyden ja etätyöskentelyn takia. Tietojen ja sovellusten ollessa pilvipalveluiden alla voi kuka tahansa pitää etäpäivän kotona, kun kaikki tiedot ovat helposti saatavilla. Pilvipalveluiden kanssa tietoturva-asiat eivät ole niin paljon yrityksen harteilla, vaan osa tietoturvavastuusta siirtyy palveluntarjoajalle. Esimerkiksi jos palveluntarjoajan palvelimille hyökätään, vika ei ole yrityksessä, mutta jos yrityksen työntekijä antaa pilvipalvelutunnuksensa verkkorikollisille, vika on työntekijän. Pilvipalveluiden tuottajiin kannattaa tutustua huolellisesti, sekä selvittää missä

maassa palveluiden palvelinkeskukset sijaitsevat, koska sijainti määrittää miten palveluntarjoajan tulee käsitellä yrityksen tietoja. (Wallenius, 2019, viitattu 1.4.2019.)

Ohjelmistoturvallisuuteen voidaan vaikuttaa jo siinä vaiheessa, kun mietitään uusien ohjelmien hankkimista. Yrityksen kannattaa panostaa laatuun ja tietoturvallisuuteen, vaikka halpa hinta houkuttelisikin. Pilvipalveluiden suhteen pitää ottaa selville, minkälaista palvelua tarjotaan, mitä tietoa sinne laitetaan, ja miten palvelun tarjoaja toteuttaa koko palvelun. Taustatöiden tekemiseen kannattaa panostaa, sekä arvioida onko mahdollinen ohjelmisto juuri omalle yritykselle.

3.3.7 Tietoaineistoturvallisuus

Tietoaineistoturvallisuuden tarkoituksena on pitää tieto turvassa. Yrityksen tietoturvan kohdalla on jo mainittu tietojen luokittelu, sekä mitä niistä kannattaa suojata. Tietoaineistoturvallisuus on tälle yksi nimitys. Yrityksellä on yleensä paljon tietoja ja tiedostoja, jotka eivät ole kaikki yhtä tärkeitä. Karkeasti voidaan käyttää kahta luokitusta, julkista ja salattua, tarvittaessa voidaan näiden kahden väliin lisätä luokitukset sisäinen, että luottamuksellinen (Laakso 2010, 26).

Tietojen luokittelun jälkeen on helpompi määritellä kuinka tietoja tulisi käsitellä ja siirtää. Julkisia tietoja on kevyempi käsitellä kuin täysin salattuja. Yrityksen tulee itse määritellä käytännöt, miten salattuja tietoja käsitellään, miten niitä saa siirtää, unohtamatta tietojen tuhoamista. Tähän kaikkeen pitää antaa selkeät ohjeet työntekijöille, että ongelmilta vältyttäisiin. Säilytyksessä on otettava huomioon myös fyysinen turvallisuus, varsinkin jos tiedot ovat paperilla tai ulkoisella kovalevyllä.

Tietojen paperikopiot ovat yleensä helpompi tuhota kuin digitaaliset kopiot. Digitaalisten kopioiden kanssa pelkkä tietokoneen roskakoriin siirtäminen ei riitä, vaan tiedot pystytään palauttamaan takaisin tämänkin jälkeen. Digitaalisten kopioiden tuhoamiseen kannattaa käyttää siihen suunniteltua ohjelmistoa, eikä varmuuskopioiden tuhoamista saa unohtaa.

3.3.8 Tietoliikenneturvallisuus

Tietoliikenneturvallisuuden päätavoitteena on suojata tiedon eheys, luottamuksellisuus ja saatavuus, sen liikkuessa dataverkossa. Nykyaikana tämä tarkoittaa Internettiä, sekä yrityksen sisäisiä

verkkoja. Se koskee myös kaikkia yrityksen koneita ja laitteita, joilla on pääsy yrityksen verkkoihin, kuten tietokoneet, älypuhelimet, sekä monitoimilaitteet. (Laakso 2010, 27.)

Tapoja turvata tietoliikenneturvallisuus on monia ja ne riippuvat täysin myös yrityksen verkkoratkaisuista. Tietokoneiden kanssa palomuuri on tehokas tapa pitää tietoliikenneyhteydet kunnossa ja estää tarvittaessa mahdolliset tunkeutujat yrityksen verkkoon. Dokumentaatio on tässäkin tapauksessa tärkeää, koska se auttaa hahmottamaan kokonaisuuden.

4 EU:N TIETOSUOJA-ASETUS

EU:n tietosuoja-asetus astui voimaan 25.5.2018. Sen tarkoituksena on turvata EU:n kansalaisten henkilötietoturva asettamalla yritykselle tarkemmat kriteerit, kuinka tietoa saa käsitellä. Tietosuoja-asetuksen rikkomisesta voi koitua yritykselle massiivinen sakko, joka voi olla enimmillään 4% yrityksen liikevaihdosta tai 20 miljoonaa euroa suuremman summan mukaan. Saksassa ensimmäiset tietosuojarikesakot annettiin somepalvelulle Knuddels.de:lle syksyllä. Sakkojen määräksi tuli lopulta 20 000 €. (Laitila 2018, viitattu 5.2.2019.)

Asetuksena EU:n tietosuoja-asetus on suoraan sovellettavaa oikeutta, tarkoittaen että se on sellaisenaan yhtä kuin yksi Suomen laeista. Jäsenmailla on kuitenkin kansallinen liikkumavara, minkä avulla voidaan säädellä poikkeuksia, sekä täsmennyksiä. Suomessa tuli vuoden 2019 alussa voimaan tietosuojalaki, joka täydentää EU:n tietosuoja-asetusta. (Korhonen 2018, viitattu 5.2.2019.)

Asetuksen päätarkoituksena oli päivittää henkilötietodirektiivin periaatteet nykyaikaan, jonka lisäksi sen tavoitteena oli yhtenäistää jäsenmaiden tietosuoja käytänteitä. Näiden lisäksi haluttiin myös vahvistaa rekisteröityjen itsemääräämisoikeutta, sekä yksilön oikeuksia. Muita tavoitteita olivat sisämarkkinaulottuvuuden, tietosuojan huomioiminen globaalin ulottuvuuden kannalta, sekä tehostaa tietosuojasääntöjen täytäntöönpanon valvontaa. (Andreasson, Riikkonen & Ylipartanen 2017, 28.)

Yritykselle EU:n tietosuoja-asetus on tuonut uusia vaatimuksia, miten käsitellä asiakkaiden, sekä työntekijöiden henkilötietoja, että muita rekistereitä. Yrityksen suositellaan tietosuoja alkukartoitusta, jotta selviää millä tolalla yrityksen tietosuoja on kaikissa prosesseissa ja alihankkijoiden kanssa. Alkukartoituksessa otetaan huomioon muun muassa mitä henkilötietoja yrityksellä on hallussaan, sekä mitkä lait näihin tietoihin vaikuttavat, sekä millä tolalla tietoturva, että miten tietosuojaperiaatteet on huomioitu. Yksi tapa tehdä tämä kaikki on tietotilinpäätös, joka on raportti tietojen käsittelyn keskeisistä asioista. (Andreasson ym. 2017, 39.)

Alkuarvioinnin jälkeen on tärkeää päättää tavoitetila, sekä miten siihen päästään. EU:n tietosuoja-asetus nimittäin vaatii yrityksiltä osoitusvelvollisuutta. Tämä tarkoittaa käytännössä, että yrityksen on pystyttävä osoittamaan konkreettisesti, kuinka tietosuojatyötä suunnitellaan ja tehdään. Tämä voidaan hoitaa kattavalla dokumentoimisella, johon kuuluu prosessien ja ohjeiden tallentaminen

kirjalliseen muotoon. Dokumenteihin kuuluvat muun muassa eri tietosuoja- ja tietoturvaprosessit, henkilöstölle suunnatut ohjeistukset, sekä koulutukset, että myös riskiarvioinnit. (Andreasson 2017, 41.)

Tietosuoja asetus tuo paljon vaatimuksia yrityksille, mutta samalla se on myös yksi avain yrityksen menestymiseen. Nykymaailmassa digitalisaatio on nousevassa asemassa, ja se pitää ottaa huomioon myös yrityksissä. Digitalisaation myötä kumpuaa uusia riskejä, jotka vaikuttavat tietosuojaan ja tietoturvaan. On tärkeää pysyä kartalla, mitä tietoturva- ja tietosuojariskejä on esillä mediassa, ja reagoida niihin tarvittavalla nopeudella ja voimalla, jos ne koskettavat omaa yritystä. Yritykset, jotka pitävät huolta tietoturvastaan ja tietosuojastaan, ovat asiakkaiden ensimmäinen valinta digitalisoituvassa maailmassa.

5 YRITYS X:N TIETOTURVASUUNNITELMA

Yritys X:n tietoturvasuunnitelman kanssa lähtökohtana oli, ettei mitään aikaisempia tietoturvakäytäntöjä oltu dokumentoitu. Tietoturvan dokumentoiminen tuli ajankohtaiseksi vasta EU:n tietosuoja-asetuksen takia. Tietoturvasuunnitelman kirjoittamiseen ei ole kuitenkaan olemassa yksityiskohtaisia ohjeita, koska jokainen yritys on yksilöllinen. Jokaisessa yrityksessä tietoturvan osa-alueet painottuvat eri tavalla, mikä tekee yksityiskohtaisen ohjeistuksen kirjoittamisesta hankalaa.

Yritys X:n tapauksessa korostui erityisesti henkilöstöturvallisuus. Yrityksen henkilöstössä on vuosittain suurta vaihtuvuutta, joka tuo omat haasteensa henkilöstön rekrytointiprosesseihin, sopimuksiin, sekä perehdyttämiseen. Toinen korostuva asia oli pääsynhallinta yrityksen toimistoon, sekä tietokoneille, mihin tarvittiin selkeämmät ohjeistukset.

Näiden lisäksi tietoturvasuunnitelma ei yksinään riittänyt yritykselle, vaan sitä kirjottaessa ilmeni vaatimukset dokumentoida myös jatkuvuus- ja toipumissuunnitelmat. Riskien kannalta tehtiin kaikki yrityksen osa-alueita koskeva riskianalyysi, josta pystyttiin näkemään yrityksen tilanne ja varautumiskohteet. Tietoturvasuunnitelmaa tarvittiin myös inventaariot yrityksen laitteistosta ja ohjelmistoista.

Itse tietoturvasuunnitelma rakentui tietoturvan osa-alueiden mukaisesti. Osa-alueiden nimet toimivat tietoturvasuunnitelman otsikoina, sekä jaotteluna. Suunnitelma pidettiin yksinkertaisena ja tiiviinä, jotta se olisi helposti ymmärrettävissä, sekä kehittävissä eteenpäin. Tietoturvaa on kehitettävä eteenpäin koko ajan ja liian monimutkaisen suunnitelman kirjoittaminen aluksi olisi hankaloittanut tätä. Lisäksi käytäntöjen pitäminen yksinkertaisena helpottaa niiden integroimista yrityksen jokapäiväisiin toimenpiteisiin. Alle olevasta taulukosta löytyy, mitä kaikkiin osa-alueisiin kuului.

Osa-alue	**Sisältö**
Hallinnollinen turvallisuus	Nykytilan seloste, yrityksen riskianalyysi, tietoturvapolitiikka, tietoturvaohjelma, sopimukset ja suunnitelmat
Fyysinen turvallisuus	Alueiden määrittely, kulunvalvonta, paloturvallisuusohjeet

Henkilöstöturvallisuus	Rekrytointi, tietoturva työsuhteen alusta loppuun, tietoturvakoulutus
Käyttöturvallisuus	Salasanaohjeet, käyttöohjeet ohjelmistoihin
Laitteistoturvallisuus	Laitteistoinventaario, laitteiden käyttöohjeet, omien laitteiden käyttöohjeet
Ohjelmistoturvallisuus	Ohjelmistoinventaario, ohjelmistojen käyttöohjeet, kouluttaminen ja varmuuskopiointi
Tietoaineistoturvallisuus	Tietoaineistoinventaario, ohjeistaminen ja salaaminen
Tietoliikenneturvallisuus	Roolit ja vastuut, ohjeistus

Taulukko 1: Tietoturvan osa-alueet tietoturvasuunnitelmassa

6 POHDINTA

Tietoturva ja tietosuoja ovat nykyisessä yritysmaailmassa erittäin tärkeitä asioita. Hyvin hoidettuina ne ovat kilpailuetu, kun taas huonosti hoidettuna yrityksen tulevaisuus voi olla vaakalaudalla. Tietoturva ja -suoja kietoutuvat yhteen. Tietosuoja antaa vaatimukset tietoturvalle, ja tietoturva puolestaan mahdollistaa tietosuojan toteuttamisen.

Tietoturvasuunnitelma on tärkeä osa yrityksen tietoturvatyötä. Yrityksen alkaessa panostaa tietoturvaansa kannattaa tietoturvasuunnitelma pitää yksinkertaisena ja perusasiat läpikäyvänä. Ajan kanssa yritys löytää parhaimmat käytännöt oman tietoturvansa toteuttamiseen ja näin pystytään itse suunnitelmaa päivittämään. Tietoturva ei ole koskaan valmis. Maailmassa kehittyy aina uusia digitaalisia ja fyysisiä uhkia, joista ei vielä edes tiedetä. On tärkeää pysyä kehityksen mukana. Suunnittele-toteuta-arvioi-kehitä-malli on tässä erittäin hyvä apuväline.

Huomasin tausta-aineistoa kerätessäni, että parhaimmat kirjat, jotka kertovat konkreettisesti tietoturvasta ja tietoturvasuunnitelmista eivät ole kaikista uusimpia. Tietotekniikka on kehittynyt todella paljon viimeisten vuosien aikana, ja kehittyy koko ajan lisää, mikä vaatii ajan tasalla pysymistä. Perusasiat ovat kuitenkin edelleen samat, kuten myös suojattavat asiatkin. Mukaan vain on tullut uusia uhkia ja tapoja suojautua niiltä.

Tämän opinnäytetyön tavoitteena oli tehdä tietoturvasuunnitelma pk-yritykselle, ja tavoite toteutui. Lähdin tutkimaan asiaa pohjilta ilman sen suurempaa aikaisempaa kokemusta tai taustatietoa. Tietoa tietoturvasta ja tietosuojasta löytyy todella paljon, jopa liikaakin alkuun. Tiedon määrä voi aluksi vaikuttaa siltä, että itse tietoturvasuunnitelmassa tarvitsee ottaa kaikki huomioon, mutta välillä yksinkertainen on kaunista. Tietoturvasuunnitelmasta ei tullut sellaista kuin aluksi ajattelin, mutta siitä tuli selkeä ja yksinkertainen ensi alkuun. Sitä on hyvä lähteä kehittämään eteenpäin ja muokkaamaan yrityksen muuttuviin tarpeisiin.

EU:n tietosuoja-asetuksesta kirjoitin oman lukunsa, koska se oli yhtenä syynä tietoturvasuunnitelman tekemiseen, ja lisäksi erittäin ajankohtainen. Uudesta tietosuoja-asetuksesta voisi kirjoittaa kokonaisen opinnäytetyön, varsinkin kun uusi tietosuojalaki astui voimaan tammikuussa 2019. Samalla tavalla kuin tietoturvankin kanssa tietosuojakin elää ajan kanssa, ja sitä on valmis oltava

päivittämään ja pysymään ajan tasalla, varsinkin sen vaatimusten suhteen, jotka tarkentuvat ennen pitkää.

Kokonaisuutena tietoturvasuunnitelman kirjoittaminen on haaste, jota varten pitää lukea paljon, tutkia asioita yrityksen näkökulmasta ja tehdä päätöksiä. Tietoa löytyy paljon, josta täytyy vain poimia yrityksen kannalta oleellisimmat asiat ja niiden perusteella lähteä rakentamaan toimivaa suunnitelmaa.

LÄHTEET

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

Andreasson, A. Riikonen, J. & Ylipartanen, A. 2017. Osaava tietosuojavastaava. Helsinki: Tietosanoma Oy

Hu, V. Kuhn, R & Yaga, D. 2017. Verification and Test Methods for Access Control Policies /Models. NIST Special Publication 800-192. National Institute of Standards and Technology. Viitattu 1.4.2019 https://doi.org/10.6028/NIST.SP.800-192.

iLOQ. 2019. Digitaalinen lukitusjärjestelmä. Viitattu 1.4.2019 https://www.iloq.com/fi/teknologiat/digitaalinen-lukitusjarjestelma-iloq-s10/

ISF. 2018. The ISF Standard of Good Practice for Information Security 2018. Viitattu 7.11.2018 https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/.

ISO. 2018. ISO/IEC 27000 family - Information security management systems. Viitattu 7.11.2018 https://www.iso.org/isoiec-27001-information-security.html.

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

Keskuskauppakamari. 2016. Tietoturvaopas yrityksille. Viitattu 3.11.2018 https://kauppakamari.fi/wp-content/uploads/2016/11/tietoturvaopas-yrityksille.pdf.

Korhonen, S. 2018. Tällainen kollegio mätkäisee gdpr-sakot Suomessa. Tivi. 15.11.2018. Viitattu 5.2.2019 https://www.tivi.fi/Kaikki_uutiset/tallainen-kollegio-matkaisee-gdpr-sakot-suomessa-6749387.

Kurittu, A. 2015. TIKKA Tietoturvallisuustilanteen kartoitustyökalu pienille yrityksille. Helsinki: Elinkeinoelämän keskusliitto EK, Helsinki: Viestintävirasto. Viitattu 3.11.2018 https://ek.fi/wp-content/uploads/TIKKA_Tietoturvallisuus_opas.pdf.

Laakso, M. 2010 PK-yrityksen tietoturvasuunnitelman laatiminen. Tietojenkäsittely. Opinnäytetyö. Viitattu 14.11.2018, http://www.theseus.fi/handle/10024/20793.

Laakso, M. 2018. Hallinnollinen tietoturva. Tietojesiturvaksi.fi. Viitattu 14.11.2018 https://tietojesiturvaksi.fi/tietoturvasuunnitelma/hallinnollinen-tietoturva.

Laitila, T. 2018. Gdpr puri saksalaista chattisivustoa – 20 000 euron sakot tietovuodon jälkeen. Tivi. 23.11.2018. Viitattu 5.2.2019, https://www.tivi.fi/Kaikki_uutiset/gdpr-puri-saksalaista-chattisivustoa-20-000-euron-sakot-tietovuodon-jalkeen-6750663

Linnake, T. 2018. Tarkista, että sait tämän päivityksen – Windows on vaarassa, hyökkäyksiä tehdään jo. Iltalehti. Viitattu 18.11.2018 https://www.is.fi/digitoday/tietoturva/art-2000005824494.html.

Lord, N. 2018. Information Protection vs. Information Assurance: Differentiating Between Two Critical IT Functions. Digital Guardian. Viitattu 5.2.2018 https://digitalguardian.com/blog/information-protection-vs-information-assurance-differentiating-between-two-critical-it.

Marks, P. 2018. Cybersecurity and the Parkerian Hexad. Staffhost Europe. Viitattu 5.2.2019 https://www.staffhosteurope.com/blog/2018/10/cybersecurity-and-the-parkerian-hexad.

Miettinen J. E. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari Oyj.

NIST. 2014. Security and Privacy Control for Federal Information Systems and Organizations. NIST Special Publication 80-53. Viitattu 1.4.2019 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Rautiainen. J. 2013. Tietoturvan kolme kovaa: Luottamuksellisuus, eheys ja saatavuus. Juhan IT-blogi. Viitattu 3.11.2018 https://juhanit.wordpress.com/2013/08/25/tietoturvallisuuden-kolme-kovaa-luottamuksellisuus-eheys-ja-saatavuus/.

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

Scarfone, K. SInghal, A. Winograd, T. 2007. Guide to Secure WebServices. Special Publication 800-95. National Institute of Standard and Technology. Viitattu 1.4.2019 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf.

Tietosuojavaltuutettu. 2019. Henkilötietolaki. Viitattu 5.2.2019 https://tietosuoja.fi/henkilotietolaki.

Valtiovarainministeriö. 2009a. Fyysinen turvallisuus. Viitattu 14.11.2018 https://www.vahtiohje.fi/web/guest/fyysinen-turvallisuus.

Valtiovarainministeriö. 2009b. Hallinnollinen turvallisuus. Viitattu 14.11.2018 https://www.vahtiohje.fi/web/guest/hallinnollinen-turvallisuus.

Valtiovarainministeriö. 2009c. Tietoturvallisuuden organisointi. Viitattu 18.11.2018 https://www.vahtiohje.fi/web/guest/13.

Valtiovarainministeriö. 2009d. Käyttöturvallisuus. Viitattu 18.11.2018 https://www.vahtiohje.fi/web/guest/kayttoturvallisuus.

Wallenius, N. 2019. Johdatus pilvipalveluiden tietoturvaan. Wallenius Consulting. Viitattu 1.4.2019 https://niklaswallenius.fi/teknologiat/johdatus-pilvipalveluiden-tietoturvaan/.