Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2010

Matti Laakso

PK-YRITYKSEN TIETOTURVASUUNNITELMAN LAATIMINEN

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Syyskuu 2010 | 46 sivua

Ohjaaja Esko Vainikka

Matti Laakso

PK-YRITYKSEN TIETOTURVASUUNNITELMAN LAATIMINEN

Opinnäytetyössä selvitettiin, mitä asioita pk-yrityksen on huomioitava, kun laaditaan tietoturvasuunnitelmaa. Tarve tutkimukselle ilmaantui, kun Yritys X (nimi muutettu) käynnisti koko organisaation laajuisen projektin tietoturvan kehittämiseksi. Projektin tarkoituksena oli kehittää heidän yleistä toiminnan laatua, parantaa kilpailukykyä ja vastata asiakkaiden muuttuviin tietoturvatarpeisiin.

Tutkimus tehtiin toimeksiantona IT-alan yritykselle, mutta aihetta lähestyttiin silti yleisestä näkökulmasta. Tavoitteena oli toteuttaa dokumentaatio, jonka avulla mikä tahansa pk-yritys voi kehittää omaa tietoturvatyöskentelyään ja luoda oman tietoturvasuunnitelman.

Työn teoriaosuudessa painotettiin tietoturvasuunnitelmaan liittyvien asioiden esittelyä. Ensimmäiseksi tutustuttiin yleisiin aiheeseen liittyviin termeihin ja käsitteisiin. Perusasioiden selvittämisen jälkeen esitettiin tietoturvan osa-alueet ja tutkittiin samalla niiden osuutta tietoturvasuunnitelman laatimisessa. Teoriatietoa havainnollistettiin esimerkeillä siitä, miten lukija voi toteuttaa tietoturvaa omassa yrityksessään.

Opinnäytetyön empiirisessä osiossa toteutettiin toimeksiantajalle heidän käyttöönsä sopiva tietoturvasuunnitelma. Dokumentti laadittiin teoriaosuudesta saatavien tietojen perusteella, jotka ovat myös tiivistetysti taulukkomuodossa työn liiteosiossa. Taulukot perustuivat laadukkaisiin lähteisiin, kuten viralliseen tietoturvastandardiin. Empiirinen osuus julistettiin toimeksiantajan toiveesta salaiseksi, koska dokumentti sisältää luottamuksellista tietoa. Lopputuloksena valmistunut tietoturvasuunnitelma mahdollistaa toimeksiantajan tietoturvatyöskentelyn jatkuvuuden ja tehokkaamman kehityksen.

ASIASANAT: tietoturva, tietoturvasuunnitelma, tietoturvan osa-alueet

BACHELOR´S THESIS | ABSTRACT

UNIVERSITY OF APPLIED SCIENCES

Data processing | Data communication

September | 46 pages

Instructor Esko Vainikka

Matti Laakso

BUILDING AN INFORMATION SECURITY PLAN FOR SMALL-TO-MEDIUM SIZED COMPANY

The main purpose of this thesis was to find out what kind of things small and medium-sized business has to think about when building an information security plan. This information were needed when Company X (name changed) decided to launch organization wide project to develop their information security, improve competitiveness and answer the customers rising information security needs.

The study was made as an assignment for Information Technology company but the subject was approached from common view. The goal was to produce documentation that was usable by any small to medium-sized business who wants to improve their information security or build and information security plan.

Question related to information security plan were highlighted in the theory section of the thesis. First the reader was introduced to common terms and concepts. After that the information security plan was studied trough the eight sections of information security. Examples were given to understand the theory better and to show how the reader can enhance his own business information security.

The knowledge gained from the theory was used to build an information security plan for Company X. The document was declared as secret because of the business critical data included in it. Appendix part of the thesis contains public information for all about the most commons things to take care of when building an information security plan.

KEYWORDS: Information security, information security plan, information security sections

SISÄLTÖ

KUVIOT

1 JOHDANTO

Tietoturvasta huolehtiminen on nousemassa yhä tärkeämmäksi osaksi yritysten päivittäistä liiketoimintaa. Lainsäädännön vaatimukset ja asiakkaiden muuttuvat tietoturvatarpeet kannustavat yrityksiä parantamaan toimintatapojaan. Asiakasvaatimusten ja kilpailuedun saavuttamiseksi Yritys X, nimi muutettu, päätti käynnistää koko organisaation tietoturvaa parantavan kehityshankkeen helmikuussa 2010. Yritys X on IT-alalla toimiva yritys, jolla on kymmeniä työntekijöitä ja useita toimipisteitä ympäri Suomea.

Kehityshankkeen suurimmaksi ongelmaksi muodostui yrityksen tietoturvasuunnitelman laatiminen. Otin vastaan toimeksiannon, jonka tehtävänä on selvittää, mitä asioita pk-yrityksen tulee huomioida kyseistä suunnitelmaa laadittaessa. Tutkimus on osa laajempaa kokonaisuutta, jossa Yritys X:n tavoitteena on muodostaa kokonaisvaltainen tietoturvan hallintajärjestelmä. Toimeksiantajan pyynnöstä osa opinnäytteestä tullaan julkistamaan salaiseksi, koska työn empiirinen osuus tulee sisältämään liiketoiminnan kannalta luottamuksellista informaatiota.

Tutkimuksen aihe ei ole uusi, mutta se on silti ajankohtainen, laaja ja haastava. Tietoturvasta on yleisesti saatavilla paljon erilaisia materiaaleja, joita hyödynnetään tässä työssä. Suunnitelman laatimista käsitteleviä materiaaleja on puolestaan vähemmän, mikä tekee työstä haastavan. Tutkimuksen teoriaosuudessa käsitellään tietoturvan perusteita, osa-alueita sekä osittain myös tietoturvan hallintajärjestelmää tutkimusongelman näkökulmasta. Lähteinä käytetään alan lehtiä, laadukkaita suomalaisia ja ulkomaalaisia kirjoja, virallisia tietoturvastandardeja sekä sähköisiä materiaaleja.

Teoriaosuus tulee sisältämään kahdenlaista tietoa. Ensin pyritään selvittämään tietoturvaan liittyvät termit selkeällä ja ymmärrettävällä tavalla. Tämän jälkeen kerrotaan, miten lukija voi toteuttaa asioita omassa yrityksessään. Teoriaa selvennetään myös esimerkkien avulla. Niiden tarkoitus on havainnollistaa, miten tietoturvaa voidaan parantaa eri IT-alan organisaatioissa. Esimerkit ovat

helposti sovellettavissa myös muiden alojen yrityksiin. Empiirisessä osuudessa käytetään hyväksi luotuja materiaaleja ja niiden avulla Yritys X:lle toteutetaan kattava tietoturvasuunnitelma.

Erääksi tutkimusta hankaloittavaksi ongelmaksi todettiin aiheen laajuus. Kaikkia tietoturvasuunnitelman kohtia ei ole järkevää toteuttaa itse, vaan ryhmätyöskentely on suositeltavaa. Päätimme yhdessä toimeksiantajan kanssa rajata opinnäytetyön empiiristä osiota siten, että tietoturvasuunnitelman laajemmat alakohdat sisällytetään työhön vain osittain. Näihin kohtiin luetaan esimerkiksi riskianalyysit, jotka Yritys X toteuttaa laajamittaisesti myöhemmin itsenäisesti. Usean toimipisteen täydelliset riskianalyysit olisivat suurentaneet opinnäytetyötä liian laajaksi. Lukuisten ja laajojen analyysien tekeminen on myös hieman alkuperäisen tutkimusongelman ulkopuolella. Lopulliseen salattuun versioon lisätään myös Yritys X:n omaa materiaalia, kuten esimerkiksi verkkoinfrastruktuuriin liittyvää dokumentaatiota ja salasanakäytäntöjä.

Saatuani toimeksiannon asetin itselleni muutamia tavoitteita. Ensisijaisesti pyrin siihen, että opinnäytetyön lopputulokset ovat toimeksiantajan käyttöön sopivia materiaaleja. Samalla yritän tuottaa työlle sellaisen teoriaosuuden, että sitä voitaisiin käyttää myös toisten pk-yritysten tietoturvatyöskentelyn kehittämisessä. Muina tavoitteina pidän henkilökohtaisen tietoturvaosaamisen sekä aiheeseen liittyvän ammattitaidon kehittymistä.

2 TIETOTURVALLISUUDEN PERUSKÄSITTEITÄ

Jokaisella yrityksellä on hallussaan tietoja, jotka ovat heille tärkeitä turvattavia kohteita. Toimenpiteitä ja menettelyitä, joilla nämä asiat suojataan, kutsutaan yhteisellä nimellä tietoturvaksi. (Hakala ym. 2006, 4.) Syitä tietojen turvaamiseen on monia. Esimerkiksi taloudellisesta näkökulmasta tärkeäksi muodostuu liikesalaisuuksien suojaaminen. Juridiset vaatimukset saattavat puolestaan määrätä erilaisten aineistojen, kuten henkilötietojen käsittelemisestä.

Yrityksen toimialasta ja koosta riippuen, tietoturvaa voidaan toteuttaa eri tavoilla. Varsinais-Suomen Yrittäjä –lehden haastattelema yliopettaja Esko Vainikka kuitenkin huomauttaa, että tietoturvasta vain 20 prosenttia on teknistä suojaamista, kuten palomuurilaitteistojen ja virustorjuntaohjelmistojen käyttöä. Loput 80 prosenttia ovat puolestaan hallinnollisia toimenpiteitä, jotka sisältävät esimerkiksi kouluttamista ja päivittäisten toimintatapojen ohjeistamista. (Harju 2010, 23.)

Perinteisessä jaottelussa tietoturva koostuu kolmesta tavoitteesta: tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta. Nykyisin tätä kolmen kohdan määrittelyä ei kuitenkaan pidetä tarpeeksi kattavana. Esimerkiksi luottamuksellisuus ja eheys voivat kadota jo tiedon siirtovaiheessa, mikäli joku on päässyt valtuudetta muokkaamaan siirrettävää informaatiota. Vastaanottaja luulee käsittelevänsä asianmukaista tietoa, olematta kuitenkaan täysin varma siitä. Tästä johtuen kiistämättömyys ja todentaminen on lisätty mukaan tavoitteisiin. (Raggad 2010, 20–23.)

2.1 Luottamuksellisuus, eheys ja saatavuus

Turvaamalla suojattavan kohteen luottamuksellisuus pyritään estämään tiedon näkyminen ulkopuolisille tahoille. Eheyden tarkoituksena on puolestaan varmistaa, että informaatiota ei päästä muokkaamaan ilman asianmukaisia valtuutuksia. Teknisillä toimenpiteillä, kuten salauksilla, voidaan esimerkiksi edistää tiedon luottamuksellisuutta ja eheyttä. Ulkopuoliset tahot eivät pysty lukemaan tai muokkaamaan kyseistä tietoa. Mikäli suojattava kohde on salattu, tallennettu fyysiselle ulkoiselle medialle ja toimitettu turvattuun tilaan, voidaan puhua jo hyvästä luottamuksellisuudesta ja eheydestä. Tiedon saatavuus on kuitenkin huono, koska käyttäjä joutuu ensin hakemaan tallennusmedian ja avaamaan salatun tiedoston. Luottamuksellisuuden, eheyden ja saatavuuden varmistaminen on yksittäin helppoa, mutta kaikkien kolmen yhtäaikainen toteuttaminen vaatii suunnittelua. (Järvinen 2002, 22–24.)

2.2 Todentaminen ja kiistämättömyys

Käyttäjän todentaminen on olennainen osa tiedon luottamuksellisuutta. Todentamisella tarkoitetaan sitä toimenpidettä, jolla esimerkiksi työntekijä todistaa IT-järjestelmälle olevansa valtuutettu ylläpitohenkilö. Tyypillinen todennus tapahtuu esimerkiksi oikealla tunnuksen ja salasanan yhdistelmällä. Vahvemmissa järjestelmissä voidaan käyttää useaa yhtäaikaista menetelmää, kuten sormenjäljen tunnistusta, sähköistä avainkorttia ja vaihtuvaa koodia. Kun käyttäjä on tunnistettu, voidaan hänelle luovuttaa asianmukaiset käyttöoikeudet. (Raggad 2010, 22–23.)

Väärinkäytön vähentämiseksi ja estämiseksi on järjestelmän käyttöä ja siellä tapahtuvia muutoksia seurattava. Tiedot voidaan tallentaa esimerkiksi erilliselle lokipalvelimelle. Näin on mahdollista myöhemmin kiistämättömästi todistaa käyttäjien tapahtumat tiettyinä kellonaikoina. (Järvinen 2002, 27–28.) Tietoja tallennettaessa on kuitenkin huomioitava myös luottamuksellisuus ja eheys. Mikäli lokipalvelimella tapahtuu tietomurto, eivät tiedot ole enää luotettavia. Tietojen kiistämättömyys on hävinnyt, koska luottamuksellisuutta ja eheyttä ei voida varmistaa.

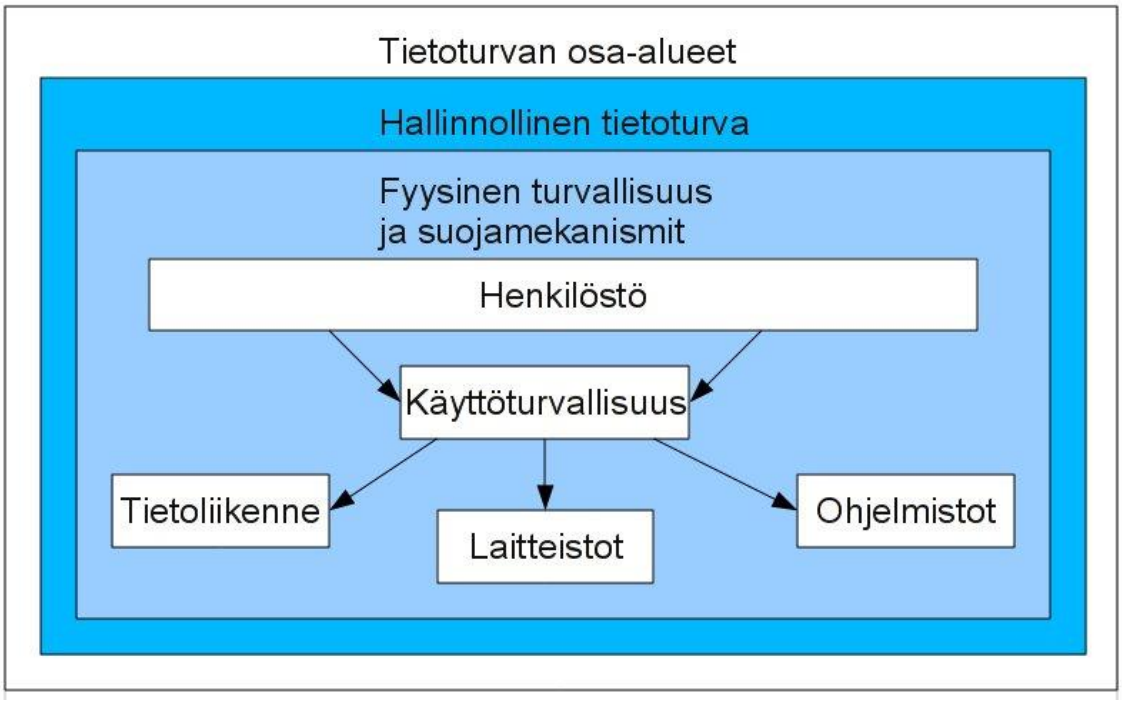
2.3 Tietosuoja

Yleisen tietoturvan lisäksi yritysten on pystyttävä tarjoamaan työntekijöilleen ja muille sidosryhmille lain velvoittama yksityisyyden suoja. Tämä tietosuojana tunnettu termi tarkoittaa ihmisestä kerättävien henkilökohtaisten tietojen tallennusta ja käsittelyä koskevia asioita. Termiä ei pidä sekoittaa tietoturvaan, jonka tarkoituksena on kokonaisvaltaisempi tietojen suojeleminen. (Järvinen 2002, 21.)

Nykyaikaiset Internetissä toimivat palvelut mahdollistavat esimerkiksi henkilön sijainnin näyttämisen kartalla matkapuhelimen avustuksella. Tällaisen palvelun tarjoaminen muille, ilman asianomaisen lupaa, olisi yksityisyyden loukkaamista. Yritysmaailmaan sopivampi esimerkki on työntekijöiden henkilötietojen paljastuminen ulkopuolisille henkilöille.

2.4 Tietoturvan osa-alueet

Yrityksen tietoturvallisuuden hallintaa voidaan havainnollistaa esimerkiksi kuviossa 1 esitetyllä perinteisellä tavalla, jossa tietoturva koostuu kahdeksasta erillisestä osiosta. Kuten kuvio osoittaa, hallinnolliset toimenpiteet ja fyysiset suojamekanismit luovat perustan muille osa-alueille. Työntekijät ovat puolestaan vastuussa laitteistojen, ohjelmistojen ja tietoliikenneverkkojen turvallisesta käytöstä, joten henkilöstön osaaminen ja turvallisuus ovat olennaisia osia suuressa kokonaisuudessa. (Ruohonen 2002, 4-5.) Yhdessä nämä kahdeksan osa-aluetta luovat kattavan näkökulman tietoturvalle. Perinteistä jaottelua käytetään myös paljon alan oppikirjoissa ja erityisesti suomenkielisissä teoksissa.



Kuvio 1. Tietoturva jaetaan perinteisesti kahdeksaan eri osa-alueeseen.

Toinen lähestymistapa on ajatella tietoturvaa yrityksen liiketoimintaprosessien kautta. Information Security Forumin (ISF) julkaisemassa teoksessa The Standard of Good Practice for Information Security 2007 (SOGP2007) käsitellään tietoturvan parhaita käytäntöjä kuudessa liiketoiminnan kannalta tärkeässä osiossa. ISF:n määrittelyssä yrityksen tietoverkot ja laitteistot luovat

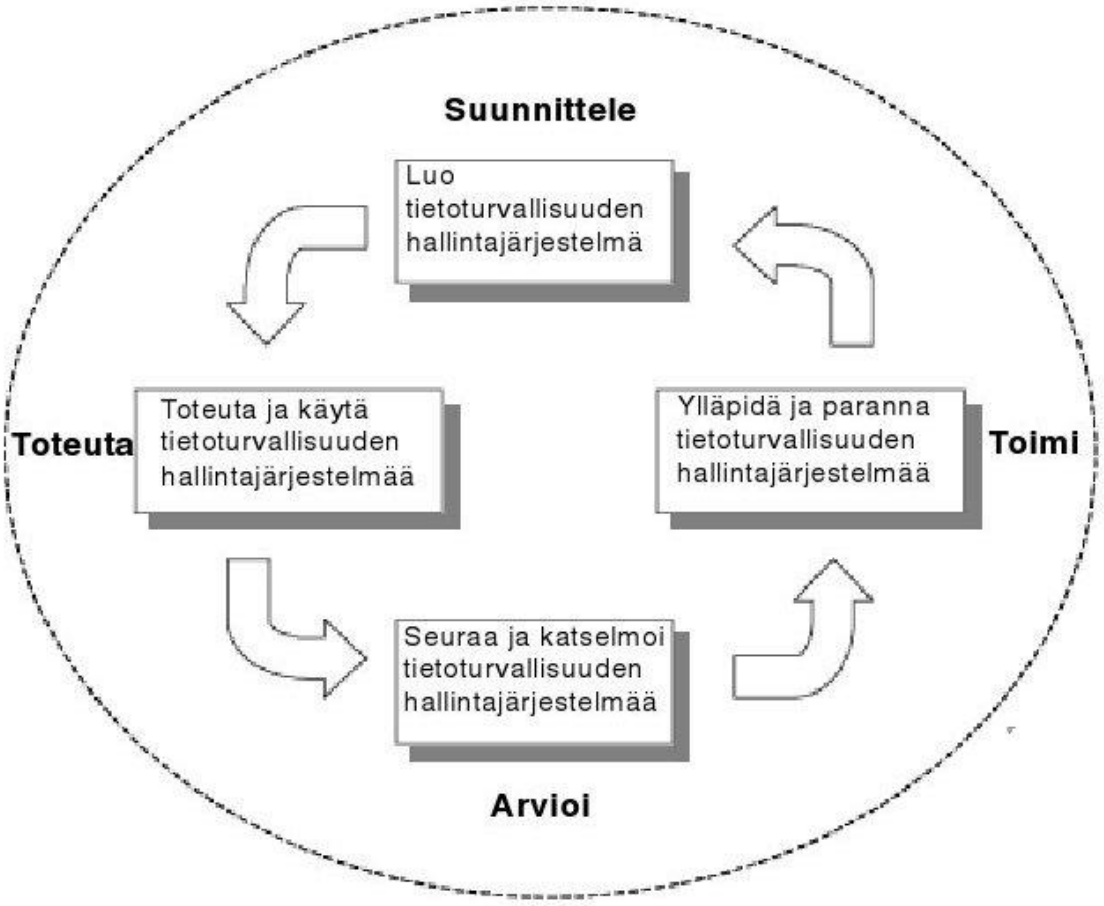
pohjan muille osa-alueille. Kun verkkojen ja laitteiden tietoturva on hallinnassa, voidaan keskittyä liiketoiminnan kannalta olennaisten järjestelmien turvaamiseen. Sen osa-alueen tärkeimpiä asioita ovat yleiset tietojärjestelmät sekä liiketoiminnassa tarvittavat ohjelmistot. Loput kolme osiota käsittelevät tietoturvan hallintaa sekä sovelluskehityksen ja työntekijöiden IT-käyttöympäristöjen turvallisuutta. (ISF 2007, 3.) Jotta yritysjohto saisi parhaan mahdollisen käsityksen tietoturvan laajuudesta, kannattaa heidän tutustua sekä perinteiseen että ISF:n tekemään jaotteluun.

3 TIETOTURVAN HALLINTAJÄRJESTELMÄ

Yritysjohdon tietoturvatyön organisoimiseksi ja helpottamiseksi kannattaa luoda erillinen tietoturvan johtamis- ja hallintajärjestelmä. Sen tulisi kattaa kaikki tietoturvan johtamisessa, hallinnoimisessa ja valvonnassa tarvittavat menettelyt ja toimenpiteet. Hallintajärjestelmä ei ole yksittäinen dokumentti, vaan moniosainen prosessi, jota on kehitettävä jatkuvasti. Yrityksen toimialasta ja koosta riippuen, tärkeimpiä hallintajärjestelmän osia ovat riskianalyysi, tietoturvapolitiikka, tietoturva-, jatkuvuus- ja toipumissuunnitelmat. Muita olennaisia asioita on löydettävissä esimerkiksi Valtiohallinnon tietoturvallisuuden VAHTI -työryhmän asiakirjasta Tietoturvallisuuden hallintajärjestelmän arviointisuositus. (VAHTI 2003.)

Tietoturvan johtamis- ja hallintajärjestelmän kehittämisessä suositellaan PDCA -mallia (Plan-Do-Check-Act). Suomenkielinen vastine on Suunnittele-Toteuta-Arvioi-Toimi. Kuviossa 2 on esiteltynä PDCA-mallin avainkohdat hallintajärjestelmän näkökulmasta. Suunnitteluvaiheessa määritellään suojattavat kohteet, mietitään millainen tietoturvan taso yritykselle halutaan ja lopuksi luodaan tietoturvan hallintajärjestelmä. Toteuttamisen jälkeen työtä arvioidaan ja kehitetään oikeaan suuntaan. Tilanteen muuttuessa suunnittelu ja muut toimenpiteet aloitetaan alusta. Näin prosessi saa jatkuvaa huomiota, joka

mahdollistaa sen kehittymisen. (Hakala ym. 2006, 106; ISO/IEC 27001:fi 2006, 8.)



Kuvio 2. Tietoturvan hallintajärjestelmän kehittäminen PDCA-mallia soveltaen (ISO/IEC 27001:fi 2006, 8).

3.1 Suojattavien kohteiden määrittely

Tietoturvallisuuden hallintajärjestelmän suunnittelu ja käyttöönotto kannattaa aloittaa tavoitteiden määrittelyllä. ”Ensimmäinen askel onnistuneeseen tietoturvaan on tietää, mitä pitää suojata”, toteaa yliopettaja Vainikka. Ne voivat olla esimerkiksi IT-järjestelmiä tai fyysisiä dokumentteja. Määrittelyn tavoitteena on tunnistaa yrityksen toiminnan kannalta tärkeimmät turvattavat asiat. Kun suojattavat kohteet on dokumentoitu, pitää ne vielä luokitella kriittisyyden mukaan. Liiketoiminnan kannalta oleellisimmat järjestelmät on turvattava ensin, joten ne on merkittävä tärkeysjärjestyksen kärkipäähän. Vastaavasti muut

laitteet, kuten testipalvelimet tai henkilöstön tietokoneet, sijoittuvat luokittelussa alempaan kategoriaan. (Harju 2010, 23.)

3.2 Riskienhallinta

Suojattavien kohteiden määrittelyn jälkeen on pohdittava tärkeitä tietoja uhkaavia ongelmatekijöitä. Riskienhallinnaksi kutsutaan kaikkia niitä toimenpiteitä, joilla näitä uhkia pyritään kontrolloimaan. Tässä tutkimuksessa käsitellään kuitenkin vain tietoturvan kannalta oleellisia riskejä, kuten esimerkiksi tietomurtoja tai varkauksia. Toisaalta myös vesiputken rikkoutuminen on ongelma, varsinkin IT-laitteita sisältävässä tilassa. Yrityksen kannattaakin luokitella kaikki erilaiset uhat ja niiden toteutumismahdollisuudet. Saatujen tietojen perusteella voidaan tehdä riskianalyysi, jonka tarkoituksena on kartoittaa liiketoimintaa uhkaavia tietoturvaongelmia. (Pk-yrityksen riskienhallinta 2010.)

3.3 Tietoturvapolitiikka

Riskianalyysistä paljastuvien epäkohtien korjaaminen aloitetaan tekemällä tietoturvapolitiikka. Se on yritysjohdon laatima ja allekirjoittama dokumentti, joka sisältää yleisellä tasolla tietoturvalinjaukset ja -tavoitteet. Asiakirja ei sisällä mitään teknisiä ohjeistuksia tai toimenpiteitä. Ne sijoitetaan erilliseen dokumenttiin, tietoturvasuunnitelmaan. Politiikan tarkoituksena on motivoida ja rohkaista henkilöstöä tietoturvallisempiin toimintatapoihin sekä osoittaa, että myös yritysjohto on mukana tässä prosessissa. (Laaksonen ym. 2006, 146.)

Tietoturvapolitiikan pitäisi olla juuri omalle yritykselle räätälöity dokumentti. Internetissä on luettavissa myös muiden tekemiä tuotoksia, mutta niiden suora kopioiminen ei ole järkevää. Laatimalla oman asiakirjan yritys varmistaa itselleen tärkeimpien asioiden huomioimisen ja kirjaamisen. Tietoturvapolitiikkaan dokumentoitavia asioita voivat olla esimerkiksi vastuut, koulutukset, yleiset linjaukset, tietojenkäsittelyn suojaaminen sekä laiminlyöntitapaukset (Laaksonen ym. 2006, 147).

3.4 Tietoturvasuunnitelma

Tietoturvapolitiikassa määriteltyihin tavoitteisiin pääseminen vaatii suunnitelmallisuutta ja loogista etenemistä. Yrityksen kannattaa luoda erillinen dokumentti, joka sisältää tarkasti käytössä olevat tietoturvaratkaisut. Kirjattavia asioita ovat esimerkiksi IT-järjestelmien suojamekanismit. Kyseisiä tietoja sisältävää asiakirjaa voidaan kutsua nimellä tietoturvasuunnitelma. Nimitys on kuitenkin harhaanjohtava, sillä dokumentti kuvaa nykyisiä tietoturvan ylläpitämiseksi tehtyjä teknisiä ja hallinnollisia toimenpiteitä. Parempi nimitys on esimerkiksi VAHTI -työryhmän käyttämä tietoturvakäytännöt ja -periaatteet. (VAHTI 2007.) Varsinainen suunnitelmaosa voidaan nimetä tietoturvan kehittämissuunnitelmaksi. Dokumenttien arkaluontoisen sisällön vuoksi kannattaa asiakirjat luokitella luottamuksellisiksi tai salaisiksi.

3.5 Jatkuvuus- ja toipumissuunnitelma

Mahdollisten poikkeustilanteiden varalle kannattaa laatia jatkuvuus- ja toipumissuunnitelmat. Näiden dokumenttien on tarkoitus sisältää kirjalliset ohjeet niistä toimenpiteistä, joilla yritys selviytyy erilaisista ongelmatilanteista (Laaksonen ym. 2006, 227.) Niitä ovat esimerkiksi palvelinhuoneiden tietomurrot. Mikäli tuotantolaitteiden eheydestä, luotettavuudesta tai saatavuudesta ei ole takuita, on yrityksellä oltava suunnitelma liiketoiminnan jatkuvuuden turvaamiseksi.

Jatkuvuussuunnitelmassa yritys määrittää keinot, joilla poikkeustilanteisiin varaudutaan ja miten ne hoidetaan. Riskien tiedostaminen ja hallinta sekä tärkeiden liiketoimintaprosessien palauttaminen normaalitasolle on myös tärkeä osa tätä suunnitelmaa. Vaikka useasti puhutaankin dokumentista, on jatkuvuussuunnittelu kokonainen prosessi, joka vaatii kehitystä ja ylläpitoa. Yritysjohdon lisäksi myös tietohallinnon ja muiden osastojen on syytä osallistua suunnitelman tekemiseen, jotta siitä saadaan mahdollisimman kattava. (Raggad 2010, 217.)

Jatkuvuussuunnitelmien lisäksi olisi hyvä tehdä myös toipumissuunnitelmia. Yleensä kyseisellä termillä viitataan niihin toimenpiteisiin, joilla palautetaan yksittäisiä osia liiketoimintaprosesseista. Esimerkkinä voidaan pitää palvelinympäristöjä. Jokaista asennettua järjestelmää varten pitäisi olla oma toipumissuunnitelma, joka sisältää keinot sen palauttamiseksi toimintaan. Mikäli tiedot ja kohteet on luokiteltu hyvin ja ohjeistus on ensiluokkaista, pystytään esimerkiksi tärkeimmät palvelimet palauttamaan nopeasti ja luotettavasti. Toipumissuunnitelmat tulee myös testata käytännössä ja varmistaa, että ne toimivat oikein. (Raggad 2010, 217–218.)

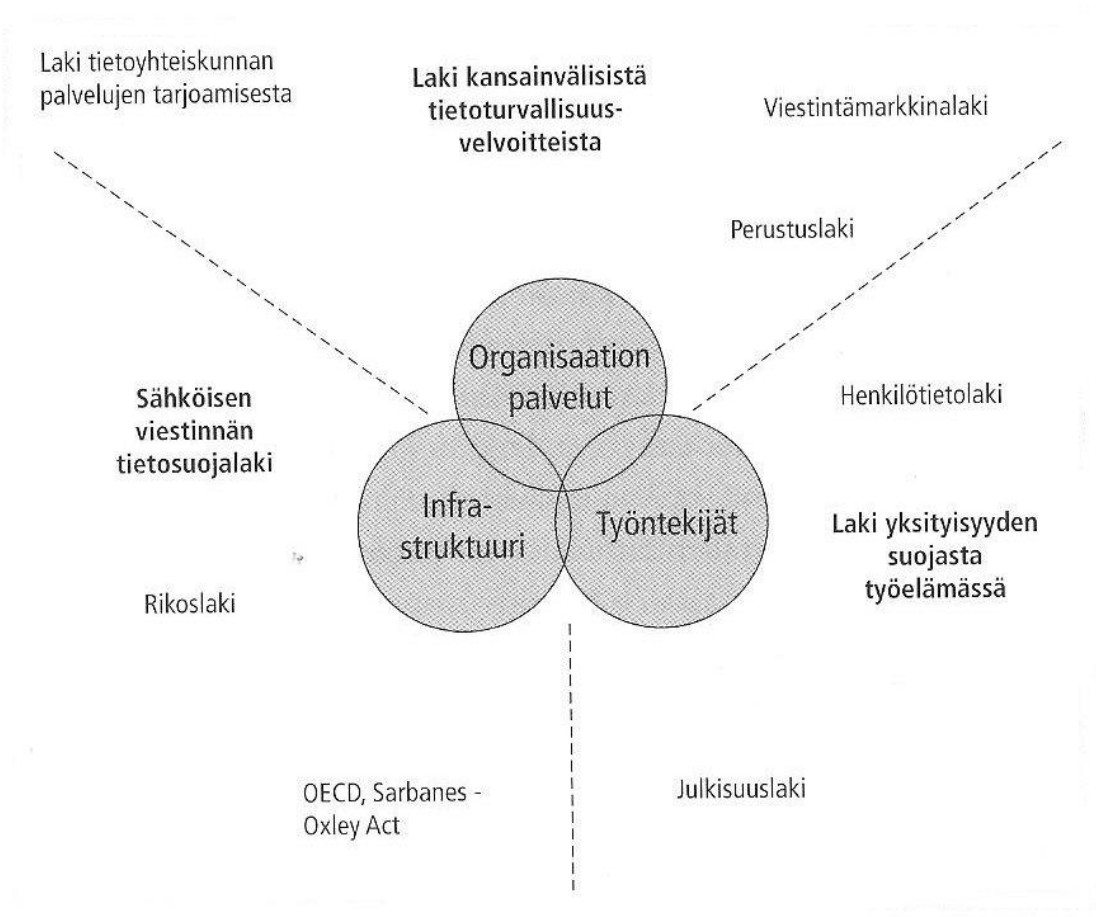
4 YRITYKSEN TIETOTURVAPERIAATTEET JA -KÄYTÄNNÖT

Ennen tietoturvaperiaatteiden ja -käytäntöjen kirjaamista yrityksen olisi hyvä tietää suojeltavat kohteet, niitä uhkaavat riskitekijät sekä yleiset linjaukset tietoturvapolitiikan muodossa. Lisäksi on tunnistettava lainsäädännön ja mahdollisten sopimusvelvoitteiden vaatimukset. Näiden kaikkien asiakirjojen laatiminen ei ole pakollista, mutta ne helpottavat olennaisesti yrityksen tietoturvatyöskentelyä. Laajamittainen dokumentointi auttaa myös tietoturvan hallintajärjestelmän organisoimisessa ja siitä on hyötyä esimerkiksi tietoturvasertifikaattia hakiessa. (Hakala ym. 2006, 108, 112.) Tämän tutkimuksen liiteosiossa on myös taulukoita, joiden tarkoituksena on auttaa yritysjohtoa suunnittelemaan ja toteuttamaan kattava tietoturvadokumentaatio.

Yrityksen toimialasta ja koosta riippuen tietoturvatarpeet vaihtelevat runsaasti erityisesti teknisten ja fyysisten vaatimusten osalta. Esimerkiksi muutaman henkilön työllistävä mainostoimisto ei tarvitse niin hyvin fyysisesti suojattua toimitilaa kuin keskisuuri tietoliikenneratkaisuja tarjoavat yritys. Tässä tutkimuksessa on pyritty selvittämään tietoturvan osa-alueita niin laajasti, että niistä olisi hyötyä mahdollisimman monelle yritykselle. Sen takia joidenkin osioiden kuvaukset saattavat olla huomattavasti laajempia kuin toiset.

4.1 Lainsäädännön vaatimukset

Yrityksen tietoturvaa suunniteltaessa, toteuttaessa ja kehittäessä on otettava huomioon laissa määriteltyjä asioita. Vaatimusten määrään vaikuttaa toimiala ja liiketoiminnan luonne, joten yrityksen on ensin selvitettävä omaa toimintaansa ohjaavat säädökset. (Laaksonen ym. 2006, 18.) Kuvio 3 havainnollistaa, miten eri lainsäädäntö käsittelee tietoturvaa. Organisaation toiminta on jaettu kolmeen eri kategoriaan, jotka liittyvät palveluihin, infrastruktuuriin ja henkilöstöön.



Kuvio 3. Tietoturvaa käsittelevät lait (Laaksonen ym. 2006, 23).

Lakien jako kategorioihin tuo käsittelyyn selkeyttä, mutta kuvio on silti vain viitteellinen. Selviä päällekkäisyyksiä on huomattavissa eri kategorioiden välillä. Kuten kuvio 3 osoittaa, oleellisia työntekijöiden omaan tietoturvaan vaikuttavia lakeja ovat henkilötietolaki sekä laki yksityisyyden suojasta työelämässä.

Vastaavasti infrastruktuuri-osioon sisällytetty sähköisen viestinnän tietosuojalaki määrittelee, miten yrityksellä on oikeus käsitellä henkilöstön luottamuksellisia tietoja esimerkiksi IT-järjestelmissä (Sähköisen viestinnän tietosuojalaki 16.6.2004/516).

Kuviosta 3 on havaittavissa myös tietoturvaan vaikuttavan lainsäädännön suuri määrä. Säädökset on jaettu useisiin lakeihin, mikä osaltaan hankaloittaa asian hallintaa yrityksen näkökulmasta. Siitä huolimatta Suomeen ei vielä ole säädetty erillistä tietoturvalakia. Uusien lakien sijasta yritykset haluavat viranomaisilta enemmän ohjeistusta tietoturvan suojamekanismien, valvonnan ja vaatimusten lainmukaiseen toteuttamiseen. (Laaksonen ym. 2006, 21.)

4.2 Standardit ja sertifiointi

Yritys voi halutessaan hakea todistusta tietoturvallisista toimintatavoistaan. Tätä toimenpidettä kutsutaan tietoturvallisuuden hallintajärjestelmän sertifioinniksi. International Organization for Standardization (ISO) on kansainvälinen organisaatio, joka on määritellyt sertifioinnissa vaadittavat kriteerit. Kyseiset vaatimukset ovat kuvattuna ISO/IEC 27001 -standardissa. Viimeistään sertifiointivaiheessa yritykseltä vaaditaan laajaa dokumentaatiota tietoturvan hallintajärjestelmästä. (Laaksonen ym. 2006, 106.)

Virallisten ISO -standardien hankkiminen on maksullista, mutta silti kannattavaa. Internetistä on saatavilla myös hyviä ilmaisia teoksia, kuten ISF:n laatima The Standard of Good Practise for Information Security 2007. Suomen kielellä laadukasta materiaalia tarjoaa esimerkiksi Valtiohallinnon VAHTI -työryhmä. He ovat julkaisseet vapaasti luettavaksi lukuisia tietoturvallisuuteen liittyviä ohjeistuksia ja suosituksia. (Valtiovarainministeriö 2010.)

Mikäli yritys haluaa kattavan tietoturvadokumentin, voidaan se luoda esimerkiksi kirjaamalla ISO:n ja ISF:n standardien pääkohdat yrityksen tietoturvaperiaatteisiin ja -käytäntöihin. Vaikka virallinen sertifikaatti ei olisikaan tavoitteena, kannattaa yrityksen silti tutustua mahdollisimman moneen aiheeseen liittyvään dokumenttiin ja ohjeistukseen. Esimerkiksi tähän

tutkimukseen on koottu tärkeimpiä asioita ISO:n ja ISF:n tietoturvastandardeista. Kokonaisuutta lähestytään kahdeksan eri osa-alueen näkökulmasta.

4.3 Hallinnollinen tietoturva

Yrityksen tietoturvalliset toimintatavat tarvitsevat johtamista ja kehittämistä, kuten muutkin yleiset liiketoiminnan prosessit. Hallinnollinen tietoturva sisältää menettelytavat muiden tietoturvan osa-alueiden ohjaamiseen. Tavoitteena on varmistaa, että kaikki eri osa-alueet ovat tarpeeksi hyvällä tasolla. Hallinnollisen tietoturvan näkyvimpiä tuotoksia ovat henkilöstön organisointi, yleiset linjaukset sekä erilaiset dokumentit, kuten tietoturvapolitiikka. (Ruohonen 2002, 5; Hakala ym. 2006, 10–11.) Liitteessä 1 olevassa taulukossa on listattuna muita oleellisia asioita, joita yrityksen pitäisi huomioida hallinnollisen tietoturvan näkökulmasta. Esimerkiksi yritysjohdon osallistuminen ja vastuualueiden jakaminen ovat tärkeitä tietoturvan hallinnan kannalta.

Tietoturvan johtamista pidetään erittäin laajana käsitteenä. Yrityksen ei silti välttämättä tarvitse tehdä muuta kuin varmistaa, että yleiset toimintatavat ovat lainsäädännöllisesti oikein. Esimerkkinä tästä voidaan pitää henkilötietojen käsittelyä. Laajempi johtaminen on kuitenkin suotavampaa, jotta yritys pystyy varautumaan mahdollisiin riskeihin ja ongelmatapauksiin. Erilaisten suunnitelmien laatiminen auttaa selviämään esimerkiksi poikkeustilanteista. Tärkeintä on kuitenkin sisällyttää tietoturvalliset toimintatavat päivittäisiin prosesseihin. Näin varmistetaan se, että tietoturva huomioidaan joka päivä sekä työntekijöiden että yritysjohdon tasolla. (Laaksonen ym. 2006, 115–116.)

4.4 Fyysinen tietoturva

Yrityksen toimitilojen sekä niissä sijaitsevien laitteiden suojaamista kutsutaan yleisesti nimellä fyysinen turvallisuus. Esimerkiksi tärkeitä tietoja sisältävän palvelimen eheyttä, luottamuksellisuutta ja saatavuutta ei voida varmistaa, mikäli se ei ole fyysisesti turvattu. Fyysinen uhka, kuten tulipalo, saattaa tuhota tietokoneita tai varmuuskopioita. Palo-, vesi- tai sähkövahingoilta suojautuminen

on tärkeässä osassa kokonaisvaltaisen tietoturvan hallintaa. Myös inhimilliset uhat, kuten varkaudet ja ilkivalta, tulee ottaa huomioon. Liitteessä 2 on kuvattuna muita tässä osa-alueessa huomioitavia asioita.(Hakala ym. 2006, 11.)

Kun työntekijöiden päivittäinen toimintaympäristö saadaan suojattua, voidaan keskittyä myös muiden tietoturvan osa-alueiden suunnitteluun ja kehittämiseen. Yrityksen koon, toimialan ja henkilöstön määrän perusteella voidaan karkeasti arvioida, millaisia fyysisiä suojakeinoja toimitilat vaativat. Mikäli liiketoiminta vaatii useiden palvelinten hallintaa, on myös fyysisen turvallisuuden oltava kunnossa. Vastaavasti vähemmän tietotekniikasta riippuvaiset yritykset keskittävät suojaukset muualle. Turvatoimet voidaan kohdentaa pelkästään tiettyyn toimitilan alueeseen, mutta kokonaisvaltainen suojaaminen on suositeltavampaa. Esimerkiksi palvelinhuoneen turvan tasoon vaikuttaa myös ympäröivien alueiden turvallisuus. Toimitiloja suunniteltaessa kannattaa tutustua ISO27000 -sarjan tietoturvastandardeihin sekä valtiovarainministeriön VAHTI -ohjeisiin. (Laaksonen ym. 2006, 125–127.)

4.4.1 Tärkeysluokittelu

Toimitilojen fyysisen tietoturvallisuuden suunnittelu kannattaa aloittaa tärkeysluokituksella. Tärkeimmät tilat ovat yleensä niitä, joissa käsitellään yrityksen ydinosaamisen kannalta olennaisia tietoja. Esimerkkejä tällaisista ovat tuotantolaitteita ja tuotekehitystoimintaa sisältävät alueet. Vähemmän tärkeitä kohteita ovat asiakaspalvelupisteet sekä piha- ja odotustilat. Näiden kahden tärkeysluokan väliin jäävät työhuoneet, joita ei välttämättä tarvitse suojata yhtä hyvin, mutta ulkopuolisten pääsy olisi silti hyvä estää. Kun yrityksessä tehdään riskikartoitusta ja -analyysiä, kannattaa myös toimitilojen eri alueet ottaa huomioon. Näin saadaan kerättyä myös parannusehdotuksia tilojen turvallisuuden lisäämiseksi. (Miettinen 1999, 177–178; Laaksonen ym. 2006, 125.)

4.4.2 Lämpötila ja tulipalot

Tärkeitä IT-tiloja suunniteltaessa pitää ottaa huomioon huoneen paloturvallisuus. Hyvä ilmastointi ja kunnolliset lämpötilan tarkkailulaitteet ovat olennaisia suojatoimia. Laitteet voidaan konfiguroida ilmoittamaan sallittujen raja-arvojen ylityksestä. Hälytys lähetetään esimerkiksi palvelinhuoneen fyysisestä tietoturvasta vastaavalle henkilölle tai tulipalon syttyessä suoraan paloviranomaisille. Asianmukaisilla seinämateriaaleilla voidaan puolestaan estää tulen leviäminen ulkopuolelle tai muualla syttyneen tulipalon pääseminen laitetilaan. (Laaksonen ym. 2006, 127.)

Automaattinen sammutuslaitteisto on myös hyvä vaihtoehto. Sen huonona ominaisuutena voidaan pitää hintaa, joka on ilmoituslaitteistoa kalliimpi. Halpa investointi puolestaan on alkusammuttimet. Erilaisilla sammutuspeitteillä tai käsisammuttimilla voidaan tukahduttaa pienet tulipalot. Yrityksen työntekijöiden kouluttaminen palotilanteisiin auttaa myös omalta osaltaan ehkäisemään suurten onnettomuuksien syntyä. (Miettinen 2002, 203-204.)

4.4.3 Vesi ja kosteus

Tärkeiden kohteiden suojelussa tulee käyttää varovaisuutta. Palvelinsalin suojaaminen tulipalolta automaattisen sammutuslaitteen avulla voi olla myös haitallista. Mikäli sammutuslaitteessa käytetään vettä, on huomioitava sähkölaitteiden vedensietokyky. Ylimääräisten aineiden pääsy palvelinhuoneeseen, esimerkiksi sammutuslaitteesta, voi tulla yhtä kalliiksi kuin tulipalo.

Viemäröinnin tai muun vesijohtoverkon tekemistä IT-tiloihin ei yleensä suositella. Jos tällaiseen on kuitenkin tarvetta tai vesiputket ovat jo paikallaan, tulee asia huomioida suunnittelussa. Esimerkiksi korotettu välilattia on eräs suoja tulvivaa lattiakaivoa vastaan. Vikatilanteissa automaattisesti sulkeutuvat venttiilit tai erilliset vuotoaltaat ovat hyviä keinoja rajoittaa veden leviämistä. Kannattaa myös muistaa, että jotkin ilmastointilaitteet toimivat veden avulla.

Kun tällainen laite hajoaa, voi vettä päästä valumaan väärään paikkaan. (Hakala ym. 2006, 305.)

4.4.4 Sähköhäiriöt

Salamaniskuista tai muista syistä johtuvat virtapiikit ovat odottamattomia mutta olemassa olevia riskitekijöitä. Liiallinen sähkönsaanti voi tuhota elektroniset laitteet ja niiden käsittelemän datan. Vastaavasti tilapäinen sähkökatkos voi aiheuttaa laitteiden sammumista ja tietojen katoamista. Pahimmassa tapauksessa sähköhäiriö voi aiheuttaa yritykselle pitkäaikaisia ongelmia, kuten tuotannon häiriintymistä. Halpa tapa suojata työntekijöiden tietokoneet virtapiikeiltä on käyttää ylijännitesuojan sisältäviä pistorasioita.

Olennainen osa IT-järjestelmien saatavuuden varmistamista on sähkönsyötön turvaaminen. Sen on oltava jatkuvaa, varsinkin tärkeiksi luokitelluissa tiloissa. Jatkuvuus voidaan toteuttaa varavirtageneraattoreilla tai järjestelmällä nimeltä UPS (Uninterruptible Power Supply). Näiden laitteiden tarkoituksena on tarkkailla virransyöttöä ja siinä tapahtuvia virheitä. Mikäli sähkönsyöttö katkeaa, käynnistyvät varavirtalaitteet automaattisesti. (Hakala ym. 2006, 310–311.)

4.4.5 Kulunhallinta

Yrityksen toimitiloissa liikkuvien työntekijöiden ja vieraiden liikkumista voidaan seurata ja rajoittaa teknisin keinoin. Tämä kulunvalvonnaksi kutsuttu aihealue on osa suurempaa kokonaisuutta, kulunhallintaa. Sen tehtävänä on johtaa, ohjeistaa, kehittää ja ylläpitää kulunvalvonnassa käytettyjä menetelmiä ja toimintatapoja. (Miettinen 1999, 179–180.) Esimerkkinä voi toimia yrityksen työntekijä, jonka kulkuoikeuksista päätetään kulunhallinnassa, mutta kulunvalvonta sisältää keinot, joilla työntekijän liikkumista toimitiloissa rajoitetaan.

Tyypillisin kulunvalvontatoimenpide on ovessa oleva mekaaninen tai sähköinen lukko. Erityyppisillä lukitsemiskeinoilla on omat hyvät ja huonot puolensa. Mekaaninen lukko on perinteinen, mutta jos yrityksessä on paljon tiloja, joihin tarvitaan eri avaimia, voi mekaaninen lukko hankaloittaa päivittäistä toimintaa.

Sähköiseen avaimeen voidaan ohjelmoida pääsyoikeuksia, joilla pääsee moniin eri tiloihin. Näin selvitään yhdellä avaimella, kun vastaavasti mekaanisia avaimia saattaisi tarvita useamman kappaleen. Sähköisen version etuja on myös pääsyoikeuksien poistaminen tarvittaessa, esimerkiksi jos avain varastetaan.

Kulunvalvontaa voi tehostaa myös videovalvonnalla ja murtosuojauksilla. Yrityksen toimitiloihin voidaan asentaa varashälyttimiä ja muita vastaavia valvontalaitteita, jotka tarvittaessa hälyttävät esimerkiksi vartiointiliikkeen paikalle. Mikäli videovalvontaa käytetään, on muistettava myös tutustua kyseistä asiaa ohjaavaan lainsäädäntöön. Vaikka yrityksen kulunvalvonta olisikin ensiluokkaista, on lisäksi huomioitava ulkoiset uhat. Esimerkiksi siivoojilla ja huoltohenkilökunnalla voi olla pääsy toimitiloihin myös työajan ulkopuolella.

4.4.6 Muut uhat

Tulipalosta, vedestä tai sähköstä johtuvat uhat ovat yleisimpiä riskitekijöitä. Muita mainitsemisen arvoisia ongelmatekijöitä ovat myrkylliset aineet, sodat, maanjäristykset, eläimet ja ajoneuvot. (Krutz & Vines 2003, 326–328.) Kaikkia mahdollisia ongelmia vastaan ei voi kukaan suojautua. PK -yrityksen kannattaakin miettiä, mitkä ovat todelliset uhat ja miten niiltä suojaudutaan.

4.5 Laitteistoturvallisuus

Kaikkien yrityksen teknisten laitteiden suojaamista kutsutaan yhteisellä nimellä laitteistoturvallisuudeksi. Erityisesti tietoturvan näkökulmasta tärkeitä kohteita ovat esimerkiksi kannettavat tietokoneet, palvelimet, tulostimet ja matkapuhelimet. Suojamekanismien käyttöönoton jälkeen kannattaa ne kirjata erilliseen asiakirjaan. Laitteistodokumentaation tekemisen lisäksi muita olennaisia asioita on mainittu liitteessä 3. Erityisesti henkilöstön tutustuttaminen laitteistopolitiikkaan ja muihin yleisiin ohjeisiin on erittäin tärkeää. (Miettinen 1999, 221.) Moni ei välttämättä tiedä, että esimerkiksi hajonneen tietokoneen

kovalevyjen sisältö saattaa olla luettavissa, vaikka kone itsessään ei olisi toimiva.

4.5.1 Laitteiston turvaaminen

Laitteistoturvallisuuden suunnittelu ja toteutus voidaan aloittaa esimerkiksi inventaariolla. Yrityksen kannattaa selvittää, mitä laitteita on käytössä ja millaisia suojauksia ne vaativat. Yritysjohto voi määritellä omien laitteiden käyttöpolitiikan. Mikäli työpaikka tarjoaa henkilöstölleen kannettavan tietokoneen, ei työntekijällä pitäisi olla tarvetta tuoda omaa tietokonetta yrityksen tiloihin. Ylimääräiset laitteet ovat aina riski tietoturvalle. Esimerkiksi työntekijän omasta kannettavasta tietokoneesta voi levitä haittaohjelma yrityksen tietoverkkoon.

Tietoturvaan vaikuttaa myös laitteiden sijainti. Yrityksen kannattaa suojata toimitiloissa olevat laitteet siten, että varkauksien ja muiden fyysisten uhkien riskitekijät ovat mahdollisimman pienet. Esimerkiksi tietokoneita ei kannata sijoittaa poistumisteiden läheisyyteen, josta ne ovat helposti kannettavissa ulos. Vaikka yrityksen työntekijöitä olisikin paikalla, he eivät välttämättä pysty huomaamaan tai estämään varkautta. Kiinteistöjen hälytysjärjestelmät saattavat olla päivällä pois päältä, mikä helpottaa varkaita toimimaan nopeammin. (Laaksonen ym. 2006, 126.)

Muita laitteistoturvallisuuteen vaikuttavia tekijöitä ovat erilaiset lukitukset ja pääsynvalvonta. Erityisesti kannettavissa tietokoneissa on useasti erillinen paikka kaapelilukolle. Sen avulla on mahdollista lukita laite johonkin kiinteään esineeseen, kuten pöytään. Pääsynvalvonnan tavoite on, että ulkopuoliset henkilöt eivät pysty käyttämään laitetta luvatta. Esimerkiksi palvelinhuoneen tietokoneiden luvaton käyttö tulee estää fyysisesti ja mahdollisten etäyhteyksien kautta. (Miettinen 1999, 222–223.)

4.5.2 Laitteiden huoltaminen

Pitämällä laitteet toimintakuntoisina, voidaan välttyä odottamattomilta ongelmilta. Esimerkiksi palvelimen hajoaminen tuottaa ylimääräisiä töitä ja

kustannuksia. Rikkoutumisia voidaan vähentää varmistamalla jatkuva sähkönsyöttö ja suojaamalla laitteet ulkoisilta uhkatekijöiltä. Näitä ovat esimerkiksi vedestä ja lämpötilan vaihteluista johtuvat ongelmat. Yritysjohdon kannattaa miettiä myös huolto- ja ylläpitosopimusten tekemistä laitteiden osalta. Tavoitteena on, että ongelmatilanteessa tietojen luottamuksellisuus, eheys ja saatavuus säilyvät. Mikäli ylläpito laiminlyödään, voi rikkoutuneen laitteen mukana kadota paljon yritykselle tärkeitä tietoja. Kun laitteet hajoavat, pitää ne muistaa poistaa käytöstä asianmukaisilla tavoilla. (Hakala ym. 2006, 308.)

4.5.3 Laitteiston dokumentointi

Tietokoneiden ja muiden laitteiden ylläpitoa helpottaa kunnollinen laitteistodokumentaatio. Asiakirjaan kannattaa sisällyttää koneiden ominaisuudet, komponentit, asennetut ohjelmistot, mahdolliset huoltosopimukset ja muut tarvittavat asiat. Laitteiden tunnistamista helpottaa niiden merkitseminen. Esimerkiksi kannettavan tietokoneen pohjaan voidaan laittaa tarralappu, joka vastaa tiettyä tietuetta laitteistodokumentaatiossa. (Miettinen 1999, 224.)

4.6 Ohjelmistoturvallisuus

Tietojärjestelmissä käytettävien lisenssien ja ohjelmistojen hallintaa kutsutaan ohjelmistoturvallisuudeksi. Mukaan lasketaan niin työpöytä kuin palvelinkäytössäkin olevat ohjelmistot. Lisenssien hallinta ei kuulosta tärkeältä tietoturvallisuuden kannalta, mutta hallinnan laiminlyönti voi silti johtaa vakaviin tietoturvaloukkauksiin. Esimerkiksi virustorjuntaohjelmiston lisenssin käyttöoikeuden loppuminen voi samalla lopettaa itse ohjelman toimimisen. Asianmukaisella hallinnalla ja seurannalla tällaisilta ongelmilta voidaan välttyä. (Miettinen, 1999, 225–226; Ruohonen, 2002, 4.)

Kaikki olennaiset yrityksen ohjelmistoihin liittyvät asiat kannattaa kirjata tietoturvaperiaatteisiin ja -käytäntöihin. Liitteen 4 taulukosta selviää yleisimmät dokumentoitavat aihealueet, kuten kouluttaminen ja ohjelmistopolitiikka. Erityisesti varmuuskopiointikäytäntöjen ja tietoturvallisten toimintatapojen

ohjeistamiseen kannattaa käyttää aikaa. Henkilöstön on myös tiedettävä, mitä ohjelmistoja heillä on lupa käyttää työkoneillaan.

4.6.1 Suojaaminen luvattomalta käytöltä

Olennaista ohjelmistoturvallisuuden kannalta on ohjelmien ja järjestelmien luvattoman käytön estäminen. Yleisin tapa toteuttaa tämä suojatoimenpide on käyttäjän todentaminen esimerkiksi henkilökohtaisten tunnusten ja salasanojen avulla (Raggad 2010, 22). Yrityksen tietoturvaohjeistuksiin kannattaa lisätä kohta, jossa kerrotaan turvallisten ja monimutkaisten tunnusten luomisesta. Tietyn tyyppiset salasanat on helposti murrettavissa normaalin tietokoneen avulla. Kaikki yrityksen työntekijät eivät välttämättä ole tietoisia tästä, joten ohjeistuksen tekeminen on suotavaa. Ohjelmistojen luvatonta käyttöä voidaan rajoittaa myös käyttäjän sijainnin perusteella. Esimerkiksi jotkin sovellukset voidaan rajoittaa toimimaan vain yrityksen oman lähiverkon alueella.

4.6.2 Ohjelmien laatu ja tietoturvaominaisuudet

Huonosti toteutetut ohjelmat ovat haitaksi yrityksen tietoturvalle. Luvattoman käytön estäminen salasanoilla ei ole avuksi, mikäli käyttäjä pystyy ohittamaan todennusmekanismit. Siksi onkin tärkeää, että yrityksessä käytettävät ohjelmat ovat laadukkaita ja tietoturvallisia. (Rosendahl 2003.) Hyvänä esimerkkinä voidaan pitää käyttöjärjestelmää, johon valmistaja ei tee korjauspaketteja. Kyseisen ohjelmiston käyttäminen on suuri riski ja heikentää tietoturvallisuutta. Vaikka käyttöjärjestelmä olisikin suojattu, voi haavoittuvuus olla myös esimerkiksi toimisto-ohjelmassa. Rikolliset pystyvät käyttämään näitä ongelmia hyväkseen ja murtautumaan tietojärjestelmään.

Hyvä ohjelmisto mahdollistaa loki- eli tapahtumatietojen kirjaamisen muistiin. Näistä tiedoista voidaan selvittää esimerkiksi, kuka käyttäjä on ollut kirjautuneena järjestelmään tiettynä ajankohtana tai miltä koneelta kirjautuminen on tehty. Lokitiedot ovat erityisen hyödyllisiä ongelmatilanteiden selvittämisessä. Palvelimet voidaan konfiguroida tallentamaan kaikki normaalista toiminnasta poikkeavat tapahtumat ja lähettämään tiedot

ylläpitäjille. Näin järjestelmistä vastaavat henkilöt saavat ongelmasta välittömästi tiedon. (Miettinen 2002, 169.)

4.6.3 Ylläpito ja huolto

Ohjelmistoihin saattaa ilmestyä vikoja samalla tavalla kuin laitteisiinkin. Syy voi olla esimerkiksi virheellisissä järjestelmäpäivityksissä. Nämä viat saattavat estää ohjelman päivittäisen käytön. Ylläpito- ja huoltosopimukset ovat hyvä tapa siirtää vastuuta myös muille osapuolille. Mikäli yrityksen tietotaito riittää ja ohjelmiston käyttöoikeudet sen sallivat, voi korjauksia koittaa tehdä myös itse. Avoimen lähdekoodin ohjelmistot ovat käyttäjän muokattavissa, mikä mahdollistaa korjausten omatoimisen tekemisen.

4.6.4 Varmuuskopiointi

Vikatilanteista ja haittaohjelmista johtuneet ongelmat saattavat lamauttaa koko tietojärjestelmän. Aina eivät parhaatkaan virustorjunnat pysty suojaamaan koneita uusimmilta uhilta. Mikäli tällaiseen tilanteeseen joudutaan, voi käyttöympäristön uudelleenasentaminen olla ajankohtaista. Tiedot ovat helposti palautettavissa, mikäli varmuuskopiointi ja järjestelmien dokumentointi on hoidettu asianmukaisesti. Koneilla olevista ohjelmistoista ja niiden asetuksista kannattaa tehdä lista, jolloin niiden palauttaminen täysin alusta alkaen on nopeampaa ja luotettavampaa. Varmuuskopioinnin yritys voi järjestää siten, että tiedot on palautettavissa esimerkiksi kahden viikon takaiseen tilaan. (Miettinen 1999, 227–228.)

4.7 Tietoaineiston turvallisuus

Tietojen suojaaminen on tämän osa-alueen tärkein päämäärä. Muita olennaisia tähän osa-alueeseen liittyviä toimenpiteitä on listattuna liitteessä 5. Niitä ovat esimerkiksi käyttöoikeuksien määrittäminen, tiedostojen varmuuskopiointi ja palautus sekä tiedon turvallinen säilyttäminen ja tuhoaminen. Vaikka nämä toimet liittyvät vahvasti sähköiseen materiaaliin, ovat ne myös täysin päteviä paperisten dokumenttien käsittelyssä. Tämän osa-alueen sekä tietoturvan

käsitteet muistuttavat hyvin paljon toisiaan ja joskus ne mielletäänkin virheellisesti samaksi asiaksi. (Ruohonen 2002, 4; Hakala ym. 2006, 11.)

4.7.1 Tietojen luokittelu

Tietoaineistojen turvaaminen kannattaa aloittaa informaation tunnistamisella ja luokittelulla. Kun kohteet on tunnistettu, voidaan toteuttaa tarvittavat suojatoimenpiteet.(Miettinen 2002, 132.) Esimerkiksi työntekijöiden henkilötiedot ja liiketoiminnan kannalta tärkeät suunnitelmat ovat olennaisia turvattavia kohteita. Niiden päätyminen vääriin käsiin olisi yritykselle haitallista. Henkilötietojen käsittelyssä ja tallentamisessa on myös muistettava lainsäädännön määräykset.

Yrityksen päätettäväksi jää, miten tiedot luokitellaan. Helpoin tapa on jakaa informaatio salaisiin ja julkisiin dokumentteihin. Tämä voi kuitenkin olla liian karkea jako ja tuottaa ongelmia tiedon levittämisessä. Kolmen tai neljän luokan käyttäminen on monille yrityksille kaikkein yksinkertaisinta. Jakamalla tiedot julkisiin, sisäisiin, luottamuksellisiin ja salaisiin, saadaan aikaan jo monipuolinen jaotteluperiaate. Mikäli halutaan käyttää vain kolmea luokittelua, voidaan sisäiset tai luottamukselliset kategoriat jättää kokonaan pois. (Raggad 2010, 6-8.)

4.7.2 Tietojen käsittely ja säilyttäminen

Turvaluokittelun tekemisen ja ohjeistamisen jälkeen on työntekijöiden helpompi ymmärtää eri tietojen käsittelyn ja säilyttämisen periaatteita. Julkista informaatiota, kuten uusia tuotteita, voidaan esitellä esimerkiksi yrityksen Internet-sivuilla. Sisäisten, luottamuksellisten tai salaisten tietojen levittämisen periaatteet ovat yrityksen itse päätettävissä, kunhan sopimusten ja lainsäädännön vaikutus huomioidaan. Tyypillisesti luottamukselliseksi tai salaiseksi materiaaliksi määritellään arkaluontoiset dokumentit, kuten tuotesuunnitelmat ja palvelindokumentaatiot. (Raggad 2010, 6-8.)

Tietoturvallisten toimintatapojen edesauttamiseksi työntekijöille kannattaa ohjeistaa erilaisten materiaalien säilyttäminen ja tärkeiden tietojen

varmuuskopioiminen. VAHTI – työryhmä on koonnut Valtiohallintoa varten kattavan dokumentin, joka sisältää parhaita käytäntöjä erityyppisten asiakirjojen luokitteluun, käsittelyyn ja säilyttämiseen. Vaikka ohje on suunnattu valtiolle, sisältää se silti tärkeää informaatiota jokaiselle yritykselle, joka haluaa hoitaa tietoaineiston turvaamisen asianmukaisesti. (VAHTI 2000.) Varmuuskopioinnissa on muistettava myös tiedon fyysinen turvallisuus. Mikäli dokumentteja on tallennettu esimerkiksi ulkoisille kiintolevyille, on ne myös suojattava asianmukaisin keinoin. Tallennusmedioita ei saa jättää sellaiselle paikalle, jossa niiden tietoturva on uhattuna.

4.7.3 Tietoaineiston hävittäminen

Erityyppisten aineistojen hävittämiseen on monia keinoja. Näkyvin esimerkki paperimateriaalin tuhoamiseen on polttaminen tai paperisilppureiden käyttö. Lopputulos on nähtävissä heti eikä tietoa voida palauttaa. (Laaksonen ym. 2006, 161.) Sähköisten materiaalien tuhoaminen on yhtä helppoa ja tehokasta kuin fyysistenkin, kunhan toimintaohjeita noudatetaan. Pelkkä dokumentin poistaminen muistitikulta, tietokoneen kovalevyltä tai muulta tallennusmedialta, ei ole riittävää. Tiedoston muistipaikka tällöin vapautetaan, mutta sitä ei ylikirjoiteta.

Sähköisten tiedostojen turvalliseen hävittämiseen on olemassa erilaisia vaihtoehtoja. Yksi keino on tuhota tallennusmedia fyysisesti siten, että sitä on mahdotonta käyttää uudelleen. Toinen vaihtoehto on käyttää ylikirjoittamiseen kehitettyä sovellusta. Internetistä on saatavilla monia tällaisia ohjelmia sekä niiden käyttöohjeita. Jos tiedostoista halutaan lopullisesti eroon, on muistettava tuhota myös varmuuskopiot. Mikäli sähköisten materiaalien asianmukainen poistaminen laiminlyödään, voi siitä seurata ongelmia. Asiaan perehtyneet henkilöt pystyvät ilmaisohjelmien avulla palauttamaan datan tai osan niistä.

4.8 Tietoliikenneturvallisuus

Ne keinot ja laitteet, joilla pyritään suojaamaan dataverkoissa liikkuvan tiedon eheys, luottamuksellisuus ja saatavuus, ovat yhteiseltä nimeltään

tietoliikenneturvallisuus. Dataverkoiksi lasketaan tässä tapauksessa kaikki ne tiedonsiirtokanavat, joita yritys käyttää sähköisen informaation liikuttamiseen paikasta toiseen. (Hakala ym. 2006, 12.)

Tietoliikenneturvallisuuden suojaamiseksi on olemassa useita fyysisiä ja teknisiä keinoja, joista löytyy paljon ohjeistusta myös kirjoista ja Internetistä. Näiden suojamekanismien dokumentointi tietoturvaperiaatteisiin ja -käytäntöihin on järkevää, varsinkin jos verkko on monimutkainen. Kokonaisvaltainen verkon ja sen laitteiden dokumentointi auttaa myös ylläpidossa ja mahdollisten vikatilanteiden selvittelyssä. Liitteessä 6 on mainittuna myös muita kirjattavia asioita, kuten roolit ja vastuut. Yritysjohdon kannattaa nimetä tietoliikenneturvallisuudesta vastaavat henkilöt ja osoittaa heille käytettävissä olevat resurssit.

Tietoliikenneturvallisuuden laajuudesta johtuen ei tässä tutkimuksessa voida esittää läheskään täydellisiä teknisiä neuvoja, vinkkejä ja parannuskeinoja asian toteuttamiseksi. Mikäli yrityksellä ei vielä ole kokemusta ja ohjeistusta tietoliikenteen suojaamisesta, kannattaa sellaista hankkia. Nykyaikaisissa yrityksissä käytetään erityyppisiä dataverkkoja, joten niiden turvallinen käyttö on hallittava. Vaikka omaa Internet-yhteyttä ei olisikaan, niin esimerkiksi älypuhelimet ja muut vastaavat laitteet mahdollistavat datan liikuttamisen. Näiden laitteiden tietoturva on yhtä tärkeää kuin esimerkiksi tietokoneiden.

4.9 Yrityksen tietoliikenneyhteydet

Yksi tyypillisimmistä yrityksen käytössä olevista tietoliikenneyhteyksistä on Internet. Menetelmät, joilla Internetiä käytetään, vaihtelevat runsaasti. Pienemmät yritykset saattavat turvautua vain matkapuhelimen kautta käytettävään yhteyteen, kun taas suuremmat voivat ostaa kokonaisia valokuituyhteyksiä toimipisteisiinsä. Tietoliikenneratkaisuja hankkiessaan yrityksen kannattaa tutustua tarjontaan ja valita itsellensä sopivin ja tietoturvallisin vaihtoehto.

4.9.1 Tietoliikenneverkkojen suojaaminen

Erilaisten tietoliikenneyhteyksien muodosta ja laadusta huolimatta tärkeintä on niiden suojaaminen. Ensimmäiseksi kannattaa tarkistaa, että verkkolaitteisiin ei voida liittää ylimääräisiä koneita ilman, että ylläpitäjät tietävät siitä (Miettinen 2002, 157). Jos yrityksen toimitilat ovat samassa rakennuksessa muiden yritysten kanssa, saattaa jollain muulla olla myös pääsy samoihin laitteisiin. Tietoliikenneverkkojen ja fyysisen tietoturvan suunnittelua kannattaakin pohtia ryhmässä, jolloin suurin osa asioista tulee huomioitua kerralla.

Laitetasolla verkkojen tietoturvaa on parannettavissa esimerkiksi reitittimillä, kytkimillä ja palomuureilla. Näiden laitteiden avulla voidaan rakentaa fyysisesti tai virtuaalisesti eri verkkoja ja rajoittaa niissä liikkuvaa dataa. Mikäli yrityksessä käytetään langattomia tekniikoita, on tietoliikenneturvallisuudesta vastaavan henkilön tiedettävä myös niistä aiheutuvat riskitekijät. Esimerkiksi vanhentuneiden salaustekniikoiden käyttö kasvattaa tietomurron todennäköisyyttä. (Krutz & Vines 2003, 110–111.)

4.9.2 Dokumentointi ja ohjeistaminen

Tietoliikenneturvallisuudessa, kuten muissakin osa-alueissa, dokumentointi ja ohjeistus ovat tärkeimpiä yksittäisiä toimenpiteitä. Yliopettaja Vainikka painottaa sitä, että henkilöstön on tunnettava riskit ja keinot niiltä suojautumiseen. Yritysjohdon on varmistettava, että työntekijät saavat tarvittavan koulutuksen tietoliikenneverkkojen käytöstä ja tietoturvasta yleisesti. (Harju 2010, 23.) Erityisesti etätyöskentelyn ohjeistaminen on tärkeää. Esimerkiksi väärin muodostetut yhteydet julkisista langattomista verkoista saattavat mahdollistaa tietoliikenteen salakuuntelemisen. Ylläpitäjiä varten kannattaa puolestaan laatia yrityksen tietoliikenneverkkojen rakennetta ja käytössä olevia suojatoimenpiteitä kuvaava asiakirja. Laadukkaasta dokumentaatiosta näkee nopeasti esimerkiksi IP-osoitteet sekä toisiinsa kytketyt verkkolaitteet.

4.10 Henkilöstöturvallisuus

Ihmisen käyttäytyminen ja toimiminen eri prosesseissa vaikuttaa paljon tietoturvallisuuden tasoon. Tämä johtaa siihen, että yrityksen työntekijöiden on tiedettävä, miten toimia eri tilanteissa, kuten esimerkiksi epäilyttävien tiedostojen avaamisessa. Henkilöstöturvallisuuteen kuuluvilla toimenpiteillä pyritään estämään työntekijöistä ja sidosryhmistä johtuvat tietoturvariskit. Liitteeseen 7 on kerättynä olennaisimpia tässä osa-alueessa huomioitavia asioita. Esimerkiksi uuden henkilön tai yhteistyökumppanin palkkaaminen ja vanhojen työntekijöiden eroaminen ovat hetkiä, jotka mittaavat yrityksen tietoturvakäyttäytymisen tasoa. (Raggad 2010, 16–17.)

Internetin uutispalstoilla on viikoittain luettavissa erilaisia tietoturvauutisia. Aiheet vaihtelevat haittaohjelmista tietomurtotapauksiin. Yrityksiin kohdistuvissa tietoturvahyökkäyksissä yhteistä on lähes aina ihmisen rooli. Nykyaikaiset tietokoneiden käyttöjärjestelmät ovat niin kehittyneitä, että rikollinen harvemmin pääsee koneille suoraan. Yrityksen henkilöstön tietoturvattomat työskentelytavat helpottavat rikollisten toimintaa. Parhaatkaan palomuurit tai suojaohjelmat eivät aina pysty pysäyttämään ihmisen tekemää tahallista tai tahatonta virhettä.

Inhimillisten virheiden avulla rikolliset pystyvät tuottamaan yritykselle liiketaloudellisia ongelmia. Mikäli yritysjohdon työntekijä aukaisee haittaohjelmalla varustetun sähköpostin liitetiedoston, voi rikollinen taho saada huomattavan suuret käyttöoikeudet tietojärjestelmään ja sitä kautta esimerkiksi liikesalaisuuksiin. Henkilöstöturvallisuuden tärkeyttä ei siis kannata unohtaa. ”Usein tietoturva vaarantuu pelkän huolimattomuuden seurauksena”, toteaa yliopettaja Vainikka. Siksi on tärkeää saada henkilöstö ymmärtämään tietoturvallisuuden merkitys omalle yritykselle. (Harju 2010, 23.)

4.10.1 Henkilöstön tai yhteistyökumppanin palkkaaminen

Tietoturvallisuudesta huolehtiminen voidaan aloittaa heti uuden työntekijän tai yhteistyökumppanin etsimisestä lähtien. Mikäli sopiva palkattava on jo löytynyt,

kannattaa hänelle tehdä jonkinlainen taustaselvitys. Suosittelijoilta tai vanhoilta työnantajilta kysyminen ovat tehokkaita keinoja. Näin voidaan varmistua ainakin siitä, että henkilön työhistoria on se, mitä hän väittää. Jos työntekijää haetaan kriittisiin tehtäviin, voi suojelupoliisin tekemä turvaselvityskin olla aiheellinen. Nämä ovat kuitenkin sellaisia asioita, joita työnantajan kannattaa miettiä tapauskohtaisesti ja maalaisjärkeä käyttäen. Taustaselvityksiä tehdessään yritys voi samalla myös tutustua työntekijään ja pohtia hänen sopivuuttaan yrityksen henkilöstöön. Jos prosessi etenee sopimusten tekovaiheeseen asti, kannattaa tietoturvallisuuteen keskittyä vielä enemmän. Salassapitosopimuksen kirjoittaminen ja yrityksen tietoturvapolitiikkaan sitouttaminen ovat oleellisia asioita rekrytoinnissa. (Laaksonen ym. 2006, 139–142.)

4.10.2 Henkilöstön organisointi

Työntekijältä vaadittava tietoturvaosaaminen vaihtelee työtehtävien perusteella. Yrityksen IT-osastolta vaaditaan teknistä tietämystä, kun taas yritysjohdon on tunnettava hallinnollinen tietoturva. Kaikkia kuitenkin yhdistävät yhtenäiset toimintatavat. Pitämällä erillisiä tietoturvakoulutuksia voidaan parhaita käytäntöjä levittää kaikille tasapuolisesti. Ohjeistamisen ja kouluttamisen tärkeyttä ei koskaan saa unohtaa. Näiden lisäksi työntekijöiden on vielä muistettava toimia, kuten ohjeissa kerrotaan.

Yrityksissä työskentelee usein sellaisia henkilöitä, joiden tietoturvattomat toimintatavat vaarantavat koko yrityksen menestymisen. Tällainen henkilö voi olla esimerkiksi tietojärjestelmien pääkäyttäjä tai ylimmän johdon työntekijä. Heitä yhdistää pääsy kriittisiin tietoihin, kuten henkilötietoihin tai palvelinhuoneisiin. Huomioitava asia on myös se, että tällainen avainhenkilö ei välttämättä ole edes yrityksen oma työntekijä. Hän voi olla myös yhteistyökumppanin henkilöstöä, esimerkiksi palvelimen pääkäyttäjä. Yritysjohdon on varmistettava, että myös alihankkijat toimivat tietoturvallisella tavalla. (Miettinen 1999, 171; Hakala ym. 2006, 11.)

4.10.3 Työsuhteen päättyminen

Yrityksen tietoturvajärjestelmää testataan erityisesti silloin, kun työsuhteet tai yhteistyösopimukset päättyvät. Esimerkiksi vuosia samassa paikassa työskennellyt henkilö on voinut saada haltuunsa yritystä koskevia tietoja, kuten käyttöoikeuksia, -tunnuksia ja materiaaleja. Vaikka avaimet ja muut fyysiset tavarat saataisiinkin takaisin, jää työntekijälle silti paljon arkaluontoista informaatiota. Yritysjohdon on varmistettava, että poislähtevää osapuolta pidetään täysin ulkopuolisena tietoturvallisuuden näkökulmasta. Hänen käyttö- ja pääsyoikeutensa IT-järjestelmiin on poistettava ja muulle henkilöstölle on ilmoitettava työsuhteen päättymisestä. (Miettinen 2002, 108.)

4.11 Käyttöturvallisuus

Yrityksen päivittäisten toimintojen ja rutiinien turvaamista kutsutaan yleisesti käyttöturvallisuudeksi. Tämä osa-alue sisältää kaikki manuaalisen ja automaattisen tietojenkäsittelyn suojatoimenpiteet, kuten salasanojen hallinnoinnin ja järjestelmien valvonnan. Käyttöturvallisuuden luonteen vuoksi sitä pidetään joskus ylimääräisenä kahdeksantena tietoturvan osa-alueena. Yrityksen päätettäväksi jää, halutaanko esimerkiksi salasanakäytännöt dokumentoida useampaan kertaan. Ne voidaan kirjata sekä ohjelmisto- että käyttöturvallisuuteen, tai vaihtoehtoisesti vain toiseen osa-alueeseen. (Miettinen 2002, 158–159; Hakala ym. 2006, 12.)

5 YRITYS X:N TIETOTURVASUUNNITELMA(SALATTU)

6 TIETOTURVAN MERKITYS YRITYKSILLE

Erilaisista tietoturva-asioista muistuttaminen on nykyään jo arkipäivää niin yrittäjien kuin yksityishenkilöidenkin elämässä. Aiheen merkitystä ja tärkeyttä

painotetaan jatkuvasti erilaisissa viestimissä. Verkkojulkaisuissa on kuukausittain luettavissa tietomurroista tai ohjelmistojen haavoittuvuuksista ja suurimmat tapaukset päätyvät jopa lehtiin sekä televisioon.

6.1 Kokonaisuuden hallinta

Tietotekniikasta aiheutuvien riskien määrät yrityksissä vaihtelevat huomattavasti liiketoiminnasta riippuen. Esimerkiksi mitä enemmän yrityksellä on käytettävissään erilaisia IT-järjestelmiä ja tietokoneita, sitä useampia riskitekijöitä ne saattavat aiheuttaa. Tietokirjailijan ja tietoturva-ammattilaisen Petteri Järvisen mielestä yritykset kyllä tietävät olemassa olevat ongelmat, mutta eivät osaa käytännössä ratkaista niitä (2010, 6).

Hoitamalla tietoturvan hallinnan asianmukaisesti, voidaan uhkien toteutumisen todennäköisyyttä pienentää. Samalla tavalla yritykset pyrkivät vähentämään myös muista aiheista, kuten liiketoiminnasta tai henkilöstöstä, aiheutuvia riskejä. Tietoturvasta huolehtiminen on siis riskienhallintaa, kuten muidenkin ongelmien hallitseminen. (Järvinen 2010, 6.)

Tietoturvan tärkeyden merkitystä yrityksille ei voida liikaa korostaa. Nykyaikainen liiketoiminta vaatii, että ongelmat hoidetaan asianmukaisilla tavoilla. Asiakkaiden, henkilöstön ja yrityksen omien arkaluontoisten tietojen paljastuminen ulkopuolisille saattaisi olla haitallista yrityksen toiminnalle. ”Tietoturvan kunnollinen hoitaminen on nykypäivänä yritykselle elinehto”, kuten yliopettaja Vainikka toteaa (Harju 2010, 23).

6.2 Tietoturvan toteuttaminen

Yritysjohdon laiminlyödessä tietoturvallisuuden ylläpidon, altistavat he yrityksen turhille riskitekijöille. Kyseinen riski on helposti poistettavissa, sillä tietoturvaa voidaan parantaa pienillä keinoilla, eikä se vaadi suuria summia rahaa. Jo pelkästään hallinnollisilla toimenpiteillä ja tehtäväkohtaisilla koulutuksilla voidaan valistaa henkilöstöä tarpeeksi. Koulutustenkaan ei tarvitse olla laajoja ja useita tunteja kestäviä. Esimerkiksi viikoittaisin lähetettävällä

tietoturvasähköpostilla tavoitetaan koko henkilöstö ja ohjeita saadaan levitettyä työntekijöiden tietouteen.

Tietoturvan toteuttamiseksi ei aina ole pakollista muodostaa suuria suunnitelmia ja muita asiaan liittyviä dokumentteja, mutta ne auttavat kokonaisuuden hallinnassa. Aihe on joka tapauksessa osa nykyaikaista liiketoimintaa ja tärkeitä tietoja on pystyttävä turvaamaan, jotta liiketoiminta jatkuisi normaalisti. Mikäli yritys haluaa kehittää tietoturvallisia toimintatapoja, kannattaa kokonaisuuteen ensin tutustua esimerkiksi tietoturvan osa-alueiden kautta (Yrityksen tietoturvaopas 2010a; 2010b).

7 PÄÄTELMÄT

Tutkimukseni tarkoituksena oli selvittää, mitä pk-yrityksen on otettava huomioon tietoturvasuunnitelmaa laatiessaan. Sain työn toimeksiantona Yritys X:ltä, joka tarvitsi informaatiota tietoturvan kehittämisprojektia varten. Mielestäni sain koottua erittäin kattavasti teoriatietoa alkuperäisen tutkimusongelman näkökulmasta. Hallittuani teorian tarpeeksi hyvin pystyin rakentamaan Yritys X:lle kattavan tietoturvadokumentaation.

Lähdeaineistoon tutustuessani havaitsin, että kotimaisissa kirjoissa mainitaan hyvin vähäsanaisesti tietoturvaperiaatteiden ja -käytäntöjen tai tietoturvasuunnitelman laatimisesta. Tarvittavaa tietoa piti etsiä ulkomaalaisista lähteistä. Kirjat olivat laadukkaita lähteitä, mutta käsittelivät asiaa omalta kannaltani väärästä näkökulmasta. Vasta tietoturvastandardia tutkiessani onnistuin löytämään tarvitsemiani asioita. Yllättävänä pidän sitä, että vanhemmista kirjalähteistä löytyi yksityiskohtaisemmin ja konkreettisemmin ohjeita tietoturvan toteuttamiseksi kuin uudemmista kirjoista.

Standardeissa oli myös eroja. Epävirallisen SOGP2007-standardin luulisi olevan heikkotasoisempi kuin virallisen ISO 27001:n. Havaitsin kuitenkin, että kyseiset dokumentit täydentävät toisiaan erittäin hyvin. Pelkästään yhteen tietoturvadokumenttiin tutustuminen ei ole mielestäni järkevää. Tarpeeksi

kattavan informaation saa vasta, kun tutustuu useampaan aiheeseen liittyvään tuotokseen.

Aiheen laajuus aiheutti ongelmia sen rajauksessa. Tarvittavan teoriatiedon hankkiminen oli kohtuullisen haastavaa, mutta samalla palkitsevaa ja opettavaista. Varsinaiset ongelmat olivat empiirisen osuuden toteuttamisessa. Yritys X:n liiketoiminnan luonteen vuoksi kaikkia materiaaleja ei voinut tuottaa itse, vaan henkilöstöä oli haastateltava useassa tapauksessa. Mikäli yrityksellä olisi esimerkiksi vain viisi työntekijää ja yksi toimipiste, tarvittavien dokumenttien laatiminen olisi huomattavasti helpompaa. Ongelmista huolimatta tietoturvaperiaatteet ja –käytännöt sekä kehittämisehdotukset saatiin kuitenkin kirjattua onnistuneesti yrityksen dokumentointijärjestelmään.

Tutkimuksen alussa asettamani tavoitteet saavutettiin onnistuneesti. Yritys X sai tarvitsemansa teoriatiedon sekä tietoturvaperiaatteet ja –käytännöt –dokumentin, jota he voivat tulevaisuudessa itse päivittää. Tämän lisäksi oma henkilökohtainen tietotaitoni sekä ammatillinen osaamiseni kehittyivät jatkuvasti työn edetessä.

Suunnittelin toteuttavani teoriaosuuden mahdollisimman yleishyödylliseksi dokumentiksi, ja uskon onnistuneeni tehtävässä. Tekstissä kerrotaan kattavasti eri tietoturvan osa-alueista ja niihin liittyvien suojamekanismien toteuttamisesta. Lukijalle selvitetään myös tietoturvan peruskäsitteitä ja yleisiä termejä. Teoriaosuus tarjoaa sellaisenaan paljon luotettavaa ja hyödyllistä informaatiota myös muiden pk-yritysten tarpeisiin.

Yrityksen tietoturvaan perehtymättömälle henkilölle voi tulla yllätyksenä aiheen monimuotoisuus ja laajuus. Kyseessä ei ole pelkkään virustorjuntaan ja tietoliikenteen suojaamiseen keskittyvä asia, kuten monesti uskotaan. Joissakin tapauksissa yrityksen tietoturvan rakentaminen saattaa alkaa jopa toimitilojen suunnittelusta lähtien. Tutkimustyötä tehdessäni yllätyin itsekin välillä tietoturvan laajuudesta.

Uskon, että saamieni tietojen perusteella pystyn tulevaisuudessa toimimaan työtehtävissä, jotka liittyvät yrityksen tietoturvan kehittämiseen ja ylläpitoon.

Aihe on ollut ja tulee varmasti jatkossakin olemaan tärkeässä osassa kaikkien yritysten liiketoimintaa. Nähtäväksi jää kehittyykö rikollisten tietomurroissa käyttämät menetelmät niin tehokkaiksi, että teknisen tietoturvan hallinta on tulevaisuudessa entistä tärkeämpää. Toisaalta huonommallakin tekniikalla selviytyy, kunhan henkilöstön osaamisesta on huolehdittu ja tietoturvaa hallitaan oikeaoppisesti.

LÄHTEET

Hakala, M.; Vainio, M & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

Harju, E. 2010. Tietoturvasta huolehtiminen on elinehto. Varsinais-Suomen Yrittäjä 3/2010, 23.

Information Security Forum 2007, ISF. The Standard of Good Practise for Information Security, SOGP2007. Viitattu 19.5.2010 https://www.isfsecuritystandard.com/SOGP07/index.htm > Download the Standard.

ISO/IEC 27001:fi. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto. Viitattu 19.5.2010 http://sfs.fi/it/aihealueet/tietoturva/standardit/.

Järvinen, P. 2002. Tietoturva & yksityisyys. 2. painos. Jyväskylä: Docendo Finland Oy.

Järvinen, P, 2010. Tietoturva on riskienhallintaa. Varsinais-Suomen Yrittäjä 5/2010, 6.

Krutz, R. L. & Vines R. D. 2003. Tietoturvasertifikaatti. CISSP. Suom. Suominen, E. Helsinki: Edita Publishing Oy.

Laaksonen, M.; Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita Publishing Oy.

Miettinen, J. E. 1999. Tietoturvallisuuden johtaminen. Näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari Oyj.

Miettinen, J. E. 2002. Yritysturvallisuuden käsikirja. Helsinki: Talentum Media Oy.

PK-RH 2010. Pk-yrityksen riskienhallinta. Viitattu 25.5.2010 http://www.pk-rh.fi/startti-riskienhallintaan/mita-riskienhallinta-on/.

Raggad, B. G. 2010. Information Security Management. Concepts and Practice. Boca Raton: CRC Press.

Rosendahl, M. 2003. Tietoturva palvelee kaikkia - on jokaisen vastuulla. Helsingin yliopiston atk-osaston tiedotuslehti 1/2003. Viitattu 14.4.2010 http://www.helsinki.fi/atk/lehdet/103/Tietoturva%20palvelee%20kaikkia.html.

Ruohonen, M. 2002. Tietoturva. Jyväskylä: Docendo Finland Oy.

Sähköisen viestinnän tietosuojalaki 16.6.2004/516.

VAHTI 2000. Valtiohallinnon tietoaineistojen käsittelyn tietoturvallisuusohje. VAHTI 2/2000. Viitattu 30.8.2010 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3386/name.jsp.

VAHTI 2003. Tietoturvallisuuden hallintajärjestelmän arviointisuoritus. VAHTI 3/2003. Viitattu 19.5.2010 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53808/name.jsp.

VAHTI 2007. Tietoturvallisuudella tuloksia. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. VAHTI 3/2007. Viitattu 19.5.2010 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071128Tietot/name.jsp

Valtiovarainministeriö 2010. Tietoturvallisuus. Viitattu 3.6.2010 http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/index.jsp.

Yrityksen tietoturvaopas 2010a. Viitattu 21.7.2010 http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/index.html.

Yrityksen tietoturvaopas 2010b. Viitattu 21.7.2010 http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/suunnittelu.html.

LIITTEET

Liite 1. Hallinnollinen tietoturva

Taulukko 1. Tärkeimmät hallinnollisessa tietoturvassa huomioitavat ja dokumentoitavat asiat (ISO/IEC 27001:fi 2006, 32–34; ISF 2007, 15–23).

Aihe	Tarkennus
Nykytilan kartoitus	Tunnistetaan tietoturvan nykyinen taso, kehityskohteet ja lainsäädännön vaikutukset toimintaan.
Riskienhallinta	Sisäisten ja ulkoisten riskien kartoitus ja analysointi.
Yritysjohdon osallistuminen	Sitoutuminen tietoturvatyöhön ja tarvittavien resurssien osoittaminen.
Tietoturvapolitiikka	Laaditaan yrityksen toimintaa ohjaava tietoturvapolitiikka.
Vastuualueet, organisointi ja viestintä	Nimetään erityisesti tietoturvasta vastaavat henkilöt. Sovitaan viestintä ja raportointikäytännöistä.
Tietoturvaohjelman laatiminen	Tarpeeksi kattavan ohjeistuksen ja koulutuksen tarjoaminen työntekijöille. Päämääränä tietoturvatietouden lisääminen ja ohjeiden kehittäminen.
Sopimukset	Tietoturva-asioista mainitseminen henkilöstöön, asiakkaisiin tai ulkoistukseen liittyvissä sopimuksissa.
Suunnitelmat	Jatkuvuus-, toipumis- ja tietoturvan kehittämissuunnitelmien laatiminen ja ylläpito.

Liite 2. Fyysinen tietoturva

Taulukko 1. Tärkeimmät fyysisessä tietoturvassa huomioitavat ja dokumentoitavat asiat (ISO/IEC 27001:fi 2006, 38; ISF 2007, 34).

Aihe	Tarkennus
Turva-alueiden määrittely	Jaetaan toimitilojen alueet tärkeyden mukaan erilaisiin turva-alueisiin.
Suojaaminen	Otetaan käyttöön ja kirjataan eri alueiden suojatoimenpiteet, kuten kulunvalvonta, murtohälyttimet tai paloturvallisuuteen vaikuttavat tekijät.
Kouluttaminen	Huolehditaan henkilöstön osaamisesta fyysisen tietoturvan suojaamisessa. Laaditaan ohjeita erilaisten laitteiden ja tapahtumien hallintaan.
Riskitekijät	Mikäli esimerkiksi IT-tiloissa on riskitekijöitä, kuten vesipisteitä, on ne otettava huomioon tietoturvallisuuden näkökulmasta.

Liite 3. Laitteistoturvallisuus

Taulukko 1. Tärkeimmät laitteistoturvallisuudessa huomioitavat ja dokumentoitavat asiat (ISO/IEC 27001:fi 2006, 38–40; ISF 2007, 32–40).

Aihe	Tarkennus
Inventaario	Tunnistetaan ja dokumentoidaan suojattavat kohteet, niiden tärkeys sekä omistaja. Laitteet olisi hyvä myös merkitä fyysisesti.
Laitteistopolitiikka	Dokumentoidaan mitä laitteita saa ja ei saa käyttää. Esimerkkinä omien tietokoneiden ja tallennusmedioiden käyttö.
Laitteistodokumentaatio	Laitteiden ominaisuuksien, resurssien, käyttöoikeuksien sekä -ohjeiden dokumentointi. Myös laitteisiin tehdyt muutokset tulee dokumentoida esimerkiksi päiväkirjamaisesti.
Yleinen suojaus	Kuvataan vesi-, tuli- ja sähkövahingoiden sekä varkauden estämiseksi tehdyt suojatoimenpiteet.
Käyttöoikeudet	Laitteiden käyttöoikeuksien tekninen ja hallinnollinen toteuttaminen, sekä tietojen dokumentointi.
Sopimukset	Mahdollisten huolto- ja ylläpitosopimusten laatiminen ja dokumentointi.
Ohjeistaminen	Laitteiden käytön kouluttaminen kirjallisesti ja suullisesti.
Käytöstä poistaminen	Kirjataan toimenpiteet, jotka laitteelle on suoritettava ennen sen poistamista käytöstä. Esimerkkinä kovalevyjen ylikirjoittaminen.

Liite 4. Ohjelmistoturvallisuus

Taulukko 1. Tärkeimmät ohjelmistoturvallisuudessa huomioitavat ja dokumentoitavat asiat (ISO/IEC 27001:fi 2006, 29–31, 48–62; ISF 2007, 40–50).

Aihe	Tarkennus
Inventaario	Kirjataan yrityksessä käytössä olevat ohjelmistot sekä niiden versiot ja lisenssit. Jokaiselle ohjelmistolle on merkittävä myös vastuuhenkilö.
Ohjelmistopolitiikka	Yrityksessä sallittujen ja kiellettyjen ohjelmistojen listaaminen. Kielletyt ohjelmat kannattaa perustella esimerkein.
Ohjelmistodokumentaatio	Ohjelmistojen ominaisuuksien, resurssien, käyttöoikeuksien sekä -ohjeiden dokumentointi. Myös ohjelmistoihin tehdyt muutokset tulee dokumentoida.
Haittaohjelmilta suojautuminen	Kuvataan toimenpiteet, joilla yritys suojautuu esimerkiksi viruksilta.
Kouluttaminen	Henkilöstöä on ohjeistettava kirjallisesti ja suullisesti ohjelmistojen turvallisesta käytöstä, päivitysten asentamisesta sekä esimerkiksi arkaluontoisten tietojen salaamisesta.
Järjestelmien kuvaukset	Esimerkiksi palvelinympäristön tietoturvan lisäämiseksi tehdyt asetusmuutokset on dokumentoitava ja ohjeistettava ylläpitäjille.
Varmuuskopiointi	Varmuuskopiointikäytännöt ja niiden ohjeistukset on dokumentoitava ja tarpeen mukaan julkaistava myös henkilöstölle.
Sopimukset	Dokumentoidaan mahdolliset ohjelmistoihin liittyvät tukisopimukset ja niihin liittyvät avunpyyntöperiaatteet.

Liite 5. Tietoaineiston turvallisuus

Taulukko 1. Tärkeimmät tietoaineiston turvallisuudessa huomioitavat ja dokumentoitavat asiat (ISO/IEC 27001:fi 2006, 34; ISF 2007, 17).

Aihe	Tarkennus
Inventaario	Tunnistetaan ja dokumentoidaan suojattavat kohteet.
Luokittelu	Luokitellaan ja merkitään suojattavat kohteet niiden tärkeyden mukaan.
Omistaja	Jokaisella kohteella on oltava omistaja, joka vastaa tiedon suojaamisesta ja käsittelystä.
Tiedon salaaminen	Kuvataan tiedon salaukseen liittyvät käytännöt ja periaatteet. Koskee niin tallennettavia, kuin käsiteltäviäkin tietoja.
Ohjeistaminen	Henkilöstölle on luotava ohjeita tiedon luokitteluun, käsittelyyn, tallentamiseen ja tuhoamiseen.

Liite 6. Tietoliikenneturvallisuus

Taulukko 1. Tärkeimmät tietoliikenneturvallisuudessa huomioitavat ja dokumentoitavat asiat (ISO/IEC 27001:fi 2006, 41–47; ISF 2007, 42).

Aihe	Tarkennus
Roolit ja vastuut	Tietoliikenteestä vastaavat henkilöt on nimettävä ja heille on asetettava selkeät vastuualueet.
Verkon rakenne	Yrityksen tietoliikenneverkot ja niissä käytetyt tietoturvaratkaisut on dokumentoitava tarkasti. Kunnollinen dokumentointi helpottaa esimerkiksi ylläpitoa.
Datan suojaaminen	Kuvataan ne keinot, joilla tietoverkoissa liikkuva data suojataan lähetyksen aikana. Tarvittaessa luodaan myös ohjeistus.
Ohjeistaminen	Ylläpitoa ja peruskäyttäjiä varten omat ohjeistuksensa. Kuvataan esimerkiksi WLAN-verkkojen käytön periaatteet henkilöstölle.
Sopimukset	Mahdolliset verkon huolto- ja ylläpito- ja ulkoistamissopimukset on kuvattava tarkasti ongelmatilanteita varten.

Liite 7. Henkilöstöturvallisuus

Taulukko 1. Tärkeimmät henkilöstöturvallisuudessa huomioitavat ja dokumentoitavat asiat (ISO/IEC 27001:fi 2006, 36; ISF 2007, 16–17).

Aihe	Tarkennus
Roolit ja vastuut	Henkilöstölle on selkeästi määriteltävät omat vastuualueensa ja varahenkilökäytännöt. Pyritään välttämään tietoturvan kannalta vaarallisia työyhdistelmiä.
Tietoturvapolitiikka	Tietoturvapolitiikan hyväksyminen ja sen mukaan toimiminen on olennainen osa henkilöstön tietoturvallista työskentelyä.
Työsuhteen alkaminen ja päättyminen	Kuvataan ne toimenpiteet, jotka on tehtävä aina, kun yrityksen tulee uusi työntekijä tai joku eroaa tehtävästään.
Tietoturvakoulutus	Ilman kunnollista kouluttamista ei voida olettaa, että henkilöstö osaa työskennellä tietoturvallisesti. Dokumentoidaan työntekijöiden tietoturvatietouden lisäämiseksi tehdyt asiat.
Ulkoistaminen	Tietoturva-asioista huolehtiminen on oleellista myös ulkoistamisessa. Kirjataan ne toimenpiteet, joilla varmistetaan muualta hankitun palvelun tietoturvan taso.