TEKNILLINEN KORKEAKOULU
Sähkö- ja tietoliikennetekniikan osasto

Antti Nilsson

Tietoturvakartoitus yrityksen Internet-palveluja tuottavassa yksikössä

Diplomityö
7.1.2008

Valvoja: Professori Jukka Manner, FT

Ohjaaja: Otto Aalto, FM

Tekijä
Antti Nilsson

Päiväys
7.1.2008

Sivumäärä
V + 105

Työn nimi
Tietoturvakartoitus yrityksen Internet-palveluja tuottavassa yksikössä

Osasto
Sähkö- ja tietoliikennetekniikan osasto

Professuuri
S-38 Tietoverkkotekniikka

Työn valvoja
Professori Jukka Manner, FT

Työn ohjaaja
Otto Aalto, FM

Tässä tutkimuksessa keskityttiin tietoturvallisuuden aihepiiriin. Tutkimuksen teoreettisena tavoitteena oli selvittää, minkälaisista tekijöistä organisaation tietoturvallisuus muodostuu ja miten sitä voidaan hallita. Käytännön tavoitteena oli kartoittaa kohdeorganisaation tietoturvallisuuden nykytaso ja luoda kartoituksen perusteella suunnitelma organisaation tietoturvallisuuden kehittämiseksi.

Tutkimuksen teoriaosassa avattiin tietoturvallisuuden käsitteistöä ja pohdittiin tietoturvallisuuden merkitystä organisaatioille. Katsauksessa eriteltiin organisaation toimijoiden tehtäviä ja vastuita ja tutustuttiin ISO 17799 -standardiin, joka määrittelee yleisiä toimintaperiaatteita organisaation tietoturvallisuuden hallintaan. Tietoturvallisuuden hallintaa tarkasteltiin prosessina, jossa organisaation tietoturvastrategia ja riskienhallinta ohjaavat toiminnan kehittämistä. Lopuksi tutkittiin erilaisia tietoturvallisuuden kontrolleja tietoverkkojen, tietoaineiston ja saavutettavuuden suojaamiseksi.

Tutkimuksen käytännön osassa tehtiin kohdeorganisaatiolle tietoturvakartoitus, jonka pohjana käytettiin ISO 17799 -standardia. Kartoituksessa havaittiin runsaasti tietoturvallisuuden kannalta hyvin toteutettuja asioita: muun muassa tekniset suojaukset, jokapäiväinen toiminta ja erikoistilanteiden hallinta on hoidettu hyvin ja etenkin tiedon saavutettavuuteen on panostettu. Organisaation tietoturvallisuuteen liittyvät suurimmat ongelmakohdat kohdistuvat pääasiassa hallinnolliselle puolelle. Selkeitä puutteita havaittiin erityisesti tietoturvatyön organisoimisessa ja vastuunjaossa, strategisessa suunnittelussa ja dokumentoinnissa sekä tietoturvahäiriöiden ja parannuskohteiden hallinnan organisoimisessa. Kartoituksen tulosten pohjalta kohdeorganisaatiolle tehtiin kehityssuunnitelma, jonka avulla organisaatio voi lähteä kehittämään omaa tietoturvallisuuttaan ja korjata suurimmat havaitut puutteet. Kehitystyön myötä organisaatio pystyy tulevaisuudessa ylläpitämään riittävää tietoturvallisuuden tasoa ja siten vastaamaan liiketoiminnan edellyttämiin vaatimuksiin.

Avainsanat
tietoturvallisuus, ISO 17799, tietoturvakartoitus, tietoturvallisuuden kehittäminen, tietoturvallisuuden hallinta, riskienhallinta

Author
Antti Nilsson

Date
7.1.2008

Pages
V + 105

Title of Thesis
Evaluation of Information Security in a Corporate Division Producing Internet Services

Department
Department of Electrical and Communications Engineering

Professorship
S-38 Networking Technology

Supervisor
Professor Jukka Manner, Ph.D.

Instructor
Otto Aalto, MA

This study concentrates on information security. In the theoretical part of the study the goal was to find out in an organizational context what kinds of elements does information security consist of and how it can be managed. The goal of the hands-on part of the study was to conduct an information security assessment as a case study for a specific organization, and based on the evaluation to create a plan how to improve the state of the organization's information security.

The theoretical part of this study introduced the basic terms and concepts of information security and discussed the significance and need for information security in an organization. The study reviewed the tasks and responsibilities for different roles in an organization and presented the ISO 17799 standard, which defines common principles for managing information security in organizations. Information security management was studied as a process, in which the improvement actions are driven by the organization's strategy for information security and risk management. Finally, information security control mechanisms for securing computer networks and information assets where discussed, and mechanisms for assuring the availability of information were studied.

The case study involved in conducting an evaluation of information security for the target organization. The evaluation was based on the ISO 17799 standard. The results of the evaluation showed that a good part of the organization's information security is well implemented. For example, technical controls for information security, daily operations, and incident management are in good shape, and effort has been made on assuring the availability of information. On the other hand, the evaluation revealed that the largest problems in information security were focused in the administrative actions of the organization. Clear deficiencies were found especially in organization of and responsibilities in the actions on information security, strategic planning and documentation, and in the management of information security incidents and improvements. Based on the results of the evaluation an improvement plan was created for the case organization. Using the plan, the organization may start the process of improving information security and correct the most important problems found in the evaluation. With the actions of improvement the organization is able to maintain an adequate level of information security and to insure that business requirements are met.

Keywords
information security, ISO 17799, evaluation of information security, improving information security, information security management, risk management

ALKUSANAT

Tämä diplomityö on tehty organisaatiolle, joka on historiansa aikana ollut monellakin tapaa edelläkävijä omalla toimialueellaan. Koko elinkaarensa ajan se on elänyt jatkuvan muutoksen alla, kun työntekijät ovat kehittäneet innokkaasti organisaation toimintatapoja ja palveluita. Alun perin lähes harrastepohjalta käynnistynyt toiminta on muuttunut vuosien varrella ammattimaiseksi palveluntuotannoksi.

Tätä diplomityötä ei lähdetty tekemään sen vuoksi, että organisaatiossa olisi ollut ammottavia aukkoja tietoturvallisuudessa tai välittömiä toimenpiteitä vaativia konkreettisia tietoturvaongelmia. Sellaiset ongelmat olisi voitu ratkaista muillakin keinoilla. Tavoitteena oli ennemminkin luoda oppimiskykyiselle organisaatiolle valmiudet kehittyä entisestään tietoturvallisuuden osalta. Tähän tavoitteeseen tämä työ myös vastaa.

Näiden alkusanojen myötä haluan välittää kiitokset työni valvojalle Jukka Mannerille hänen hyvästä ohjauksestaan ja lukuisista rakentavista kommenteistaan työtäni kohtaan. Kiitokset kuuluvat myös työn ohjaajalle Otto Aallolle, jonka tuki diplomityölleni on ollut alusta alkaen yksi sen valmistumisen edellytyksistä. Hänen kiinnostuksensa työtä kohtaan ja luottamus minuun työn tekijänä ovat taanneet erinomaisen ympäristön työn tekemiselle.

Erityisen suuret kiitokset kuuluvat rakkaalle vaimolleni Annalle, joka on paitsi tukenut minua koko opintojeni ajan, myös opastanut minulle diplomityön tekemisen jaloa taitoa ja samalla vastannut työn oikolukemisesta. Kanssasi suuret haasteet muuttuvat yksinkertaisiksi ja mahdottomatkin vain vähän hankaliksi.

Helsingissä 7.1.2008,

Antti Nilsson

SISÄLLYSLUETTELO

LYHENTEET JA TERMINOLOGIA

BS	British Standard
DES	Data Encryption Standard
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPsec	Internet Protocol Security
IRC	Internet Relay Chat
ISO	International Organization for Standardization
MAC	Message Authentication Code
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
SHA	Secure Hash Algorithm
SQL	Structured Query Language
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wireless Fidelity Protected Access
WWW	World Wide Web
XSS	Cross-site scripting

riski	haitallisen asian mahdollisuus, muodostuu uhkasta ja vahingosta
tietoturva-kontrolli	tietoturvallisuuden toteuttamiseksi määritelty toimintaa tai tapahtumia säätelevä keino tai mekanismi
tietoturva-poikkeama	tila tai tapahtuma, jossa tietoturvallisuus on tai saattaa olla vaarantunut
uhka	jokin haitallinen tapahtuma, joka saattaa tapahtua
vahinko	menetyksen suuruus jos uhka toteutuu

1 JOHDANTO

Tieto on välttämätön resurssi kaikelle liiketoiminnalle. Jokaisella yrityksellä on hallussaan vähintään oman toiminnan kannalta tärkeätä tietoa ja useimmilla lisäksi myös asiakkaiden tietoja. Koska kaikki liiketoiminta perustuu tavalla tai toisella tiedon hyödyntämiseen, voidaan tiedon sanoa olevan yrityksen tärkein pääoma. Tästä syystä tiedon suojaaminen on kriittistä yritykselle. Tietotekniikan ja Internetin myötä tiedon määrä on kasvanut ja sen liikkuvuus on parantunut, minkä vuoksi tietoturvallisuustyö on hankaloitunut entisestään.

1.1 Tutkimuksen tausta

Tiedolla on arvo, joka riippuu sen ominaisuuksista, niille asetetuista vaatimuksista ja tiedon liiketoiminnallisesta hyödynnettävyydestä. Tiedon arvo voi siten olla rahallista, strategista tai molempia. Osa käsitellystä tiedosta on väistämättä julkista, kun taas osa, esimerkiksi tuotekehitykseen liittyvä tieto, on lähtökohtaisesti hyödyllisempää salaisena. Voidaan sanoa, että mitä harvemmalla on pääsy johonkin tietoon, sitä arvokkaampaa se on. Tiedon kopioituminen, tuhoutuminen, muuttuminen tai saavuttamattomiin joutuminen haittaavat tiedon hyödyntämistä ja vähentävät tiedon arvoa, ja sitä kautta myös hankaloittavat yrityksen toimintaa. (Virtanen, 2002, s. 40; Kyrölä, 2001, s. 37–39)

Tietoturvallisuuteen ja yksityisyyden suojaan liittyvät asiat ovat etenkin viime vuosina olleet suurta yleisöä kiinnostavia aiheita niin Suomessa kuin muualla maailmallakin. Vähäistä suuremmat julkisuuteen levinneet tietovuodot ja -paljastukset keräävät usein runsaasti medianäkyvyyttä, ensisijaisesti tiedon suojauksesta vastanneen tahon maineen kustannuksella. Virtasen esittämässä yritysturvallisuuden mallissa (Virtanen, 2002, s. 39–43) yrityksen suojeltavat kohteet on jaettu neljään osa-alueeseen: tietoon, henkilöstöön, muuhun omaisuuteen ja maineeseen. Tietoturvallisuudella on merkittävä rooli paitsi organisaation tiedon, niin myös maineen suojaamisessa.

Tietoturva sanana viittaa tiedon turvaamiseen joiltain sitä uhkaavilta tekijöiltä. Tässä tutkimuksessa selvitetään mitä tietoturva tarkalleen ottaen tarkoittaa sekä miltä, miksi ja miten tietoa oikeastaan turvataan. Kartoituksella tarkoitetaan johonkin tiettyyn aihepiiriin liittyvien asioiden merkityksen, arvon tai tilan perinpohjaista selvittämistä. Tutkimuksen puitteissa esitellään organisaatio, jonka tietoturvallisuuden tila kartoitetaan.

Työn taustalla on kohdeorganisaation halu pyrkiä kasvattamaan omaa kykyä puuttua mahdollisiin tietoturvaongelmiin ennaltaehkäisevästi, ja sitä kautta estämään mahdollisista tietoturvapoikkeamista aiheutuvat brändiin ja liiketoimintaan kohdistuvat haitalliset vaikutukset. Kohdeorganisaatio on yksityisellä sektorilla toimivan yrityksen sisäinen yksikkö, jonka tehtävänä on tuottaa Internet-palveluja sekä yrityksille että kuluttajille. Organisaation tietoturvallisuuteen kohdistuvat haasteet koostuvat siten ensisijaisesti Internet-toiminnasta ja asiakasrajapinnoista.

1.2 Tutkimuksen tavoitteet ja rajaukset

Tutkimusta suunniteltaessa on ensisijaisena lähtökohtana pidetty sitä, että tutkimuksen tavoitteet tukevat kohdeorganisaation tietoturvan kehittämiselle asettamiaan tavoitteita. Tämän tutkimuksen tavoitteet voidaan jakaa kahteen osaan: teoriaosaan ja käytännön osaan. Teoriaosan tarkoituksena oli tutustua tietoturvallisuuden aihepiiriin ja selvittää, minkälaisista tekijöistä organisaation tietoturvallisuus muodostuu ja miten sitä voidaan hallita. Teoriaosan kannalta tutkimuksen tavoitteena oli siten vastata seuraaviin tutkimuskysymyksiin:

- Mitä on tietoturvallisuus ja mikä on sen merkitys yrityksille?
- Miten yritysten tietoturvallisuutta voidaan hallita?

Käytännön osan tarkoituksena oli kartoittaa kohdeorganisaation tietoturvallisuuden nykytaso ja luoda kartoituksen perusteella suunnitelma organisaation tietoturvallisuuden kehittämiseksi. Tältä pohjalta tutkimuksen tavoitteena oli käytännön osassa vastata seuraaviin tutkimuskysymyksiin:

- Mikä on kohdeorganisaation tietoturvallisuuden nykytila?
- Miten kohdeorganisaation tietoturvallisuutta tulisi kehittää?

Koska tietoturvallisuuden tutkimuskenttä on hyvin laaja, on työssä rajoituttu erityisesti kohdeorganisaation kannalta oleellisiin asioihin. Käytännössä tämä tarkoittaa sitä, että teoriaosuudessa käsitellyt aiheet ovat yrityksen pohjatiedon kannalta oleellisia tietoturvatyön toteuttamiseksi ja tutkimuksen aihepiirin ymmärtämiseksi. Käytännön osassa tutkimus rajoittuu kohdeorganisaation piiriin ja siihen suoranaisesti vaikuttaviin seikkoihin.

1.3 Raportin rakenne

Tutkimusraportin rakenne jakautuu kahteen osaan: kirjallisuuskatsaukseen ja käytännön tutkimukseen. Luvuissa 2–4 käsitellään tutkimuksen aiheeseen liittyvää kirjallisuutta ja teoriaa ja lukujen 5–6 aihepiirinä on kohdeorganisaatiossa suoritettu tietoturvakartoitus. Viimeisessä eli seitsemännessä luvussa esitetään tutkimuksen yhteenveto.

Tutkimusraportin ensimmäisessä luvussa on käsitelty tutkimuksen taustoja ja tavoitteita. Lisäksi luvussa on esitelty tutkimuskysymykset. Raportin toisessa luvussa määritellään, mitä tietoturvallisuus on, ja käydään läpi tietoturvallisuuden merkitystä organisaatiolle ja sen toiminnalle. Luvussa jaotellaan organisaation tietoturvallisuuteen liittyvä toiminta loogisiin osa-alueisiin ja käsitellään lisäksi organisaation toiminnan merkitystä tietoturvalle.

Raportin kolmas luku käsittelee tutkimuksen kannalta oleellisia organisaation tietoturvallisuuden hallintaan liittyviä asioita, kuten tietoturvaan liittyvien asioiden organisoimista, riskienhallintaa tietoturvallisuuden kehittämisessä sekä ISO 17799 -tietoturvastandardin sisältöä ja hyödyntämistä. Neljännessä luvussa tutustutaan kohdeorganisaation toiminnan kannalta oleellisiin teknisiin kontrolleihin. Luvussa käsitellään tietoverkkojen ja -aineiston suojaamiseen sekä tiedon saavutettavuuteen ja toiminnan jatkuvuuden varmistamiseen liittyviä teknologioita.

Viidennessä luvussa esitellään kohdeorganisaatio, jonka tietoturvan tilaa ollaan kartoittamassa. Lisäksi käydään läpi kartoitustyön tavoitteet, kartoituksessa käytettävät tiedonkeruumenetelmät ja kartoitustyön käytännön toteutus. Luvun lopuksi esitellään kartoituksen tulokset.

Tutkimusraportin kuudennessa luvussa analysoidaan kohdeorganisaation tietoturvan nykytila kartoituksen tulosten perusteella. Tämän lisäksi organisaatiolle luodaan suunnitelma tietoturvan kehittämiseksi ja pohditaan kehityssuunnitelman toteuttamiseen liittyviä seikkoja. Seitsemännessä ja viimeisessä luvussa esitetään tutkimuksen yhteenveto ja johtopäätökset, analysoidaan tutkimuksen luotettavuutta ja sovellettavuutta sekä esitellään jatkotutkimukseen soveltuvia aiheita.

2 TIETOTURVALLISUUS YRITYKSISSÄ

Jotta voisi ymmärtää tarkemmin yritysten tietoturvallisuuteen liittyviä asioita, tulee ensin ymmärtää siihen liittyvät taustatekijät: mitä tietoturvallisuus on, miksi sitä tarvitaan, mitä kaikkia osa-alueita tietoturvallisuuden toimintojen on katettava ja mikä on työntekijöiden suhde tietoturvallisuuden onnistumiseen. Tässä luvussa tutustutaan tietoturvallisuuden määritelmään ja jaetaan organisaation tietoturvallisuuteen liittyvät asiat pienempiin, helpommin hallittaviin osa-alueisiin. Samalla tehdään katsaus organisaatioiden tietoturvallisuuden tarpeeseen, sekä käsitellään tietoturvakulttuurin ja tietoturvaan liittyvän tietoisuuden vaikutusta organisaation tietoturvallisuuden tasoon.

2.1 Tietoturvallisuuden määritelmä

Tietoturvallisuudella tarkoitetaan ensisijaisesti tiedon *luottamuksellisuuden*, *eheyden* ja *saavutettavuuden* säilyttämistä ennallaan. Näiden lisäksi tietoturvallisuuden käsittelemään piiriin voidaan liittää myös muita määreitä, kuten esimerkiksi *kiistämättömyys*, *aitous* ja *luotettavuus*. Toisin sanoen, tietoturvallisuudessa on pohjimmiltaan kyse tiedon arvoon vaikuttavien ominaisuuksien suojelemisesta. (Suomen Standardoimisliitto SFS [ISO 17799], 2006, 2.5)

Ylemmällä tasolla ajateltuna, ISO 17799 -standardin mukaan tietoturvallisuus tarkoittaa yrityksen kannalta ”tiedon suojaamista monenlaisilta uhkilta tarkoituksena varmistaa liiketoiminnan jatkuvuus, minimoida liiketoiminnalliset riskit sekä maksimoida investoinneista ja liiketoiminnan mahdollisuuksista saatu tuotto” (ISO 17799, 2006, 0.1). Valtionhallinnon määritelmä tietoturvallisuudelle luonnollisestikin eroaa tästä, koska valtiolla ei ole liiketaloudellisia tavoitteita. VAHTI-ohjeistuksen mukaan valtionhallinnossa tietoturvallisuudella pyritään suojaamaan yhteiskuntaa ja sen jäseniä merkittävältä vahingolta (Valtiovarainministeriö, 2003, s. 51).

Whitman ja Mattord (2005) määrittelevät tietoturvallisuuden organisaation toimijaksi, joka toteuttaa organisaatiolle neljä sen kannalta tärkeää toiminnetta:

1. Organisaation toimintakyvyn varmistaminen
2. Tietojärjestelmien sovellusten turvallinen käyttö
3. Organisaation keräämän ja käyttämän tiedon suojeleminen
4. Teknisten resurssien suojeleminen

Näillä neljällä konkreettisella toiminteella määritelmä pyrkii osoittamaan mihin tietoturvallisuudella käytännössä pyritään. Käytännössä Whitmanin ja Mattordin määritelmän voidaan katsoa sisältyvän edellä esitettyihin määritelmiin.

On hyvä huomata, että kaikki tieto ei tarvitse täydellistä suojaamista. Esimerkiksi julkisen tiedon osalta luottamuksellisuus ei ole tiedon haltijalle oleellinen seikka. Tällaisen tiedon eheydelle ja saavutettavuudelle voi kuitenkin olla suuriakin vaatimuksia. Toisaalta jokin tiedon ominaisuus voi olla toista tärkeämpi, esimerkiksi kellariholviin arkistoidun dokumentin saavutettavuudesta on tingitty luottamuksellisuuden ja eheyden hyväksi.

On myös tyypillistä, että tietoon liittyy jonkinlaista metatietoa. Tällaisella tiedolla on niin ikään omat vaatimuksensa tietoturvallisuuden kannalta. Esimerkiksi verkossa välitetyn sanoman lähde ja vastaanottaja ovat sanoman metatietoa, joka voi sopivassa kontekstissa paljastaa esimerkiksi asianmukaisesti suojatun luottamuksellisen viestin sisällön. Tarkasteltaessa jonkin tiedon tietoturvallisuutta on siis hyvä kiinnittää huomiota myös mahdollisen metatiedon merkitykseen tiedon turvallisuuden kannalta. (Anderson, 2001, s. 10)

Seuraavaksi käsitellään tarkemmin tiedon suojeltavia ominaisuuksia. On hyvä pitää mielessä, että tiedon ominaisuudet ovat riippumattomia siitä missä olomuodossa tieto kulloinkin on.

2.1.1 Luottamuksellisuus

Luottamuksellisuudella tarkoitetaan sitä, että kyseessä oleva tieto on vain siihen oikeutettujen henkilöiden käytettävissä (Hakala, Vainio & Vuorinen, 2006, s. 4; Valtiovarainministeriö, 2003, s. 25). Ylläpidettäessä tiedon luottamuksellisuutta pyritään siis estämään tiedon joutumista oikeudettoman kolmannen osapuolen käsiin. Luottamuksellisuutta voidaan suojata esimerkiksi salaamalla tieto tai sijoittamalla se siten, että ulkopuoliset eivät pääse siihen käsiksi (Hakala et al., 2006, s. 4).

Luottamuksellisuudesta puhuttaessa tarkoitetaan nimenomaan tiedon sisällön eikä niinkään tiedon yksittäisten ilmentymien suojaamisesta. Mikäli tiedon ilmentymä, esimerkiksi sähköisessä muodossa oleva salattu tiedosto joutuu oikeudettomalle osapuolelle, ei tiedon luottamuksellisuutta ole vielä rikottu. Tällöin kyse on *hallussapidon* loukkaamisesta. (Miettinen, 1999, s. 25–26)

2.1.2 Eheys

Eheydellä tarkoitetaan sitä, että tieto ei ole hallitsemattomasti tai valtuudettomasti muuttunut siitä, mikä sen on tarkoitettu olevan (Valtiovarainministeriö, 2003, s. 7). Muutoksella tarkoitetaan olemassa olevan tiedon muuttamisen lisäksi tiedon täydellistä tuhoamista sekä täysin uuden tiedon lisäämistä. Laajasti tulkittuna eheyden voidaan katsoa sisältävän myös sen, että tieto on tosiasiallisesti oikeata eikä sisällä tarkoituksellisia tai tarkoituksettomia virheitä (Hakala et al., 2006, s. 4). Tätä tiedon lähtökohtaista oikeellisuutta käsitellään kuitenkin usein erillisenä ominaisuutena, jota kutsutaan *luotettavuudeksi*, eikä sitä sellaisenaan sisällytetä eheyteen. Näin on myös tässä tutkimuksessa.

Eheyttä voidaan suojata esimerkiksi liittämällä tiedon oheen luotettavalla yksisuuntaisella menetelmällä muodostettu tarkistussumma. Tällöin tiedon eheys voidaan tällöin tarkistaa laskemalla tarkistussumma uudelleen ja vertaamalla sitä viestin sisältämään tarkisteeseen. Tällöin tarkisteen eheydestä on huolehdittava esimerkiksi käyttämällä tarkistussumman muodostamiseen luottamuksellista avainta. (Stallings, 2006, s. 324–328)

2.1.3 Saavutettavuus

Saavutettavuudella tarkoitetaan sitä, että tieto on siihen oikeutettujen henkilöiden osalta saatavissa käyttöön ja hyödynnettävissä haluttuna ajankohtana, halutussa ajassa ja vaaditulla tavalla (Valtiovarainministeriö, 2003, s. 22). Käytännössä saavutettavuudella tarkoitetaan sitä, että tieto on sijoitettu sellaiseen paikkaan mistä se on sen käyttöä ajatellen saatavilla hyödynnettäväksi käyttötarkoitukseen nähden hyväksyttävässä ajassa. Tiedon on oltava myös sellaisessa muodossa, että sen hyödyntäminen on mahdollista.

Saavutettavuutta voidaan suojata esimerkiksi toteuttamalla tietojärjestelmät niiden käyttötarpeet huomioiden riittävän varmatoimisiksi, sijoittamalla tieto käyttötarpeen edellyttämän hakuviiveen kannalta sopivalle etäisyydelle ja lukitustasolle sekä varautumalla riittävissä määrin tietoliikenne- ja kulkuyhteyksien toimimattomuuteen.

Monissa suomenkielisissä lähteissä saavutettavuutta tarkoittava englannin kielen sana *availability* esitetään käyttäen moniselitteistä termiä *käytettävyys*. Koska sana käytettävyys kuitenkin viittaa ensisijaisesti siihen mitä englannin kielen sanalla *usability* tarkoitetaan, käytetään tässä tutkimuksessa sekaannusten välttämiseksi yksiselitteisempää termiä saavutettavuus. Saavutettavuus on siis käytettävyyden reunaehto. Joissain lähteissä saavutettavuudesta käytetään myös termiä *saatavuus*.

2.1.4 Muut tietoturvallisuuden osatekijät

Luottamuksellisuus, eheys ja saavutettavuus muodostavat yhteydessä klassisen tiedon arvoon perustuvan tietoturvallisuuden määritelmän (Hakala et al., 2006, s. 4). Näiden kolmen ominaisuuden muodostamaa kokonaisuutta kutsutaan myös CIA-kolmioksi (Whitman & Mattord, 2005, s. 8–9) niiden englanninkielisten termien *confidentiality*, *integrity* ja *availability* alkukirjainten mukaan. Tähän määritelmään on esitetty useita laajennuksia eri lähteissä. Vaikka klassinen malli sisältääkin oleellisimmat tietoturvallisuuden osatekijät, on toisinaan hyödyllistä laajentaa määritelmää tarpeen mukaan.

Yhtenä oivana esimerkkinä laajennetusta määritelmästä voidaan käyttää Donn B. Parkerin esittelemää kuuden ominaisuuden mallia. Siinä tiedon suojattaviin ominaisuuksiin kuuluu klassisen määritelmän lisäksi hallussapito, *aitous* ja *hyödyllisyys* (viitattu: Miettinen, 1999, s. 23–28). Näistä hallussapito on esitelty jo luottamuksellisuuden yhteydessä.

Aitous on tiedon ominaisuus, joka määrittelee sen onko tieto alkuperäistä ja väärentämätöntä (Miettinen, 1999, s. 27). Joissain yhteyksissä aitoudella tarkoitetaan myös sitä, että tiedon alkuperä on luotettavasti tunnistettavissa (Valtiovarainministeriö, 2003, s. 1). Aitous on usein tiedon kannalta hyvin tärkeä ominaisuus, koska väärennetty tieto johtaa käytännössä virheellisiin päätelmiin, joiden seurauksena voi aiheutua suurtakin vahinkoa.

Hyödyllisyys on tiedon ominaisuus, joka määrittää sen onko tieto sellaisessa muodossa että sitä voidaan hyödyntää sen normaalissa käyttötarkoituksessa. Käytännössä tämä tarkoittaa sitä, että tiedon hyödyntäminen ei edellytä tavallisesta poikkeavia toimenpiteitä (Miettinen, 1999, s. 28). Tyypillisenä esimerkkinä ei-hyödyllisestä tiedosta voidaan pitää poikkeuksellisesti salattua dokumenttia, jossa tieto on periaatteessa saatavilla, mutta ilman salausavainta se ei ole hyödyllisessä muodossa käytön kannalta. Hyödyllisyyden määritelmä on osittain päällekkäinen tässä tutkimuksessa esitellyn saavutettavuuden määritelmän kanssa, sillä molemmat edellyttävät tiedon olevan hyödynnettävässä muodossa. Tämä johtuu siitä, että Parkerin mallissa saavutettavuus määritellään ilman hyödynnettävyyteen liittyviä vaatimuksia (Miettinen, 1999, s. 28).

Yksi tietoturvallisuuden määritelmän yhteydessä usein esiintyvä termi on *kiistämättömyys*. Kiistämättömyys ei sellaisenaan ole tiedon ominaisuus, vaan ennemminkin tiedon käsittelyyn liittyvä edellytys, joka voidaan sisällyttää tietoturvallisuuden määritelmään. Kiistämättömyydellä tarkoitetaan tiedon käsittelytoimenpiteiden kirjaamista siten, että niistä käy yksiselitteisesti selväksi kuka on tehnyt tiedolle mitä ja milloin. Tiedon käsittelyllä tarkoitetaan kaikkea tiedon lähettämiseen, lukemiseen ja muuttamiseen liittyviä toimen-

piteitä. Kiistämättömyyden tavoitteena on mahdollistaa kiistaton ja yksilöity tiedon käsittelyn jälkikäteinen todentaminen (Hakala et al., 2006, s. 4; Valtiovarainministeriö, 2003, s. 20). Kiistämättömyydestä on usein hyötyä myös tiedon aitouden määrittämisessä.

2.2 Tietoturvallisuuden tarve

Tietoturvallisuuden tarkoituksena on siis suojella organisaation hallitseman tiedon ominaisuuksia. Riskit ovat oleellinen osa liiketoimintaa ja organisaatioiden toimintaa. Tietoturvallisuuden roolina on kontrolloida sitä osaa organisaation riskeistä, joka liittyy sen hallitsemaan ja käsittelemään tietoon. Mitä hyötyä organisaatiolle tietoriskeiltä suojautumisessa oikeastaan on ja minkälaisilta uhilta tietoa ylipäänsä suojellaan?

Eri lähteiden (ISO 17799, 2006, s. 14; Kyrölä, 2001, s. 37–65; Miettinen, 1999, s. 44–69; Parker, 1997; Virtanen, 2002) pohjalta voidaan hahmottaa viisi eri syykokonaisuutta, joiden pohjalta organisaatiot pyrkivät ylläpitämään tai kehittämään tietoturvallisuutensa tasoa:

- Organisaation toiminnan tehostaminen
- Organisaation toiminnan jatkuvuuden varmistaminen
- Ulkopuolisten vaatimusten täyttäminen
- Organisaation ja sen tuotteiden maineen ylläpitäminen
- Kilpailuedun hankkiminen tai liiketoimintamalli

Nämä viisi syykokonaisuutta eivät ole toisensa poissulkevia, vaan organisaation tavoitteisiin kuuluu monesti useampiakin näistä yrityksen motivaatiota kuvastavista kokonaisuuksista.

Organisaation toiminnan tehostamisella tarkoitetaan sitä, että tietoturvallisuuden toimenpiteillä pyritään ehkäisemään tietoturvapoikkeamista aiheutuvaa tuotannon hidastumista sekä välttämään poikkeamasta syntyvien erilaisten suorien ja epäsuorien kustannusten lankeamista maksettavaksi. Käytännössä tämä lähestymistapa tähtää siihen, että tietoturvallisuuden toimenpiteillä pyritään takaamaan mahdollisimman häiriötön tuotantoympäristö. Organisaation toiminnan jatkuvuuden varmistamisella pyritään ylläpitämään tietoturvallisuutta sellaiselta tavoitepohjalta, että mahdollisen tietoturvapoikkeaman tapauksessa organisaatio pystyisi jatkamaan toimintaansa mahdollisimman nopeasti.

Ulkopuolisten vaatimusten täyttäminen pohjautuu yleensä lakeihin ja erilaisiin organisaatiota sitouttaviin sopimuksiin. Osa organisaatioiden käsittelemästä tiedosta on suojattava

ja käsiteltävä lainsäätäjän edellyttämällä tavalla. Tällaisia ovat esimerkiksi erilaiset henkilörekisterit (Henkilötietolaki) ja tietoliikenteen teletunnistetiedot (Sähköisen viestinnän tietosuojalaki). Osa juridisista vaatimuksista koskee kaikkia organisaatioita, osa vain tietynlaista liiketoimintaa harjoittavia tai säännellyllä toimialalla toimivia yrityksiä. Myös organisaation sidosryhmien tietojen suojaaminen kuuluu yrityksen velvoitteisiin (Kyrölä, 2001, s. 75–76).

Maine on oleellinen osa organisaation toimintaa. Liiketoimintaa harjoittavan organisaation maine määrittelee käytännössä sen tuottaminen palveluiden tai tuotteiden arvon. Jos organisaatiolla on hyvä maine, on asiakas valmiimpi käyttämään kyseisen organisaation palveluita. Huono maine taas karsii potentiaalisia asiakkaita. Nämä seikat pätevät paitsi organisaatioon itseensä niin myös sen tuottamiin myyntiartikkeleihin ja palveluihin (Herbig & Milewicz, 1997). Organisaation omasta tietoturvallisuudesta huolehtiminen varmistaa toiminnan uskottavuuden ja vaikuttaa myönteisesti yrityskuvaan (Miettinen, 1999, s. 61–69). Useimmiten näillä keinoin ylläpidetään tai jopa parannetaan organisaation kykyä toteuttaa sille asetettuja toiminnallisia tavoitteita.

Kilpailuedun hankkimisella pyritään tietoturvan kautta lisäämään organisaation kiinnostusta asiakkaiden silmissä. Koska jokaisella organisaatiolla on tarve suojella tietoaan, valitsee jatkuvasti yhä suurempi osa asiakkaista yhteistyökumppanikseen vain sellaisia organisaatioita, jotka pystyvät vakuuttamaan yrityksen tietoturvallisuuden olevan riittävällä tasolla. Kilpailutilanteessa tietoturvallinen luotettavuus saattaa olla merkittävässä osassa urakoitsijan tai alihankkijan valintaa, mikäli työn toteuttaminen edellyttää työn tilaajan kannalta arkaluontoisten tietojen käsittelyä. Joissain tapauksissa tietoturvallisuus liittyy oleellisesti organisaation liiketoimintamalliin, kuten esimerkiksi turvallisuuspalveluja tarjoavilla yrityksillä. Tällöin tietoturvallisuus on jo lähtökohtaisesti liiketoiminnan edellytys.

Liiketoimintaa harjoittavien organisaatioiden tietoturvallisuudessa on aina pohjimmiltaan kyse rahasta (Miettinen, 1999, s. 44), oli kyse sitten liiketoiminnan jatkuvuudesta, maineesta, kilpailuedusta tai liiketoimintamallista. Muun muassa toiminnan jatkuvuuteen liittyvän suunnittelun taustalla on käytännössä yrityksen tarve hallita suuria rahallisia tappioita. Jopa juridiset velvoitteet ja seuraamukset on useimmissa tapauksissa muunnettavissa kustannuksiksi. Tällaisessa pelkästään rahaan pohjautuvassa laskutavassa on etuna se, että tietoturvallisuuteen liittyviä laskelmia ja päätöksiä voidaan tehdä helposti liiketoiminnan harjoittamisesta tutuilla menetelmillä.

Voittoa tavoittelemattomien organisaatioiden motivaationa on yleensä kyseiselle organisaatiolle määriteltyjen tavoitteiden täyttäminen tai siihen tähtäävän toiminnan tehostaminen. Tällaisissa organisaatioissa päätöksiä ja rahan käyttöä ohjaa joko laissa sille määrätyt velvoitteet tai jokin muu tavoiteltava yhteinen etu.

Taulukko 1 esittelee Whitmanin (2003) tutkimuksen mukaisen jaottelun tietoturvallisuuden uhista. Jaotellut uhkakategoriat on pisteytetty niiden merkityksellisyyden mukaan tutkimuksessa kerättyjen tietojen perusteella. Kategorioiden merkityksellisyyttä voidaan siten verrata keskenään pisteytyksen perusteella. Tuloksista voidaan havaita, että ohjelmistohyökkäykset ovat selkeästi suurin uhka lähes kaksinkertaisella painoarvolla toiseksi merkityksellisimpään kategoriaan eli ohjelmistovikoihin verrattuna.

Taulukko 1. Tietoturvallisuuden uhkia (Whitman, 2003; Whitman & Mattord, 2005, s. 39).

Uhkakategoria	Esimerkki tapahtumasta	Painoarvo
Ohjelmistohyökkäys	Virukset, palvelunestohyökkäykset, madot	2178
Ohjelmistoviat	Virheet ohjelmakoodissa, tuntemattomat takaportit	1130
Inhimillinen virhe	Onnettomuudet, työntekijöiden virheet	1101
Teollisuusvakoilu tai luvaton tunkeutuminen tiloihin	Tiedon luvaton kopiointi	1044
Sabotointi tai vandalismi	Järjestelmän komponenttien tai tiedon tuhoaminen	963
Laitteistoviat	Vikaantunut laite	912
Varkaus	Järjestelmän komponenttien tai tiedon varastaminen	695
Luonnonvoimat	Tulipalot, tulvat, salamaniskut	611
Immateriaalioikeuksien loukkaus	Tekijänoikeusloukkaukset	495
Palveluntarjoajien palvelunlaadun poikkeamat	Sähkö, tietoliikenneyhteydet	434
Teknologian vanhentuneisuus	Ikääntyneet laitteet ja ohjelmat	428
Tiedolla uhkailu	Kiristäminen, tiedon paljastaminen	225

Kuten Whitmanin tutkimuksesta voidaan päätellä, tarvitaan tiedon turvaamiseksi käytännössä sekä teknisiä että hallinnollisia suojauksia. Yrityksen hallitsemaa tietoa säilytetään kolmessa eri olomuodossa: sähköisenä, fyysisenä ja muistinvaraisena. Yhteistä kaikille tiedon säilytysmuodoille on se, että yksikään niistä ei sellaisenaan ole turvallinen ilman erityisiä toimenpiteitä. Jokainen säilytysmuoto tuo oman, yksilöllisen haasteensa eri uhkia vastaan. Tietoa onkin suojattava sen arvon ja olomuodon mukaan tapauskohtaisesti sopivilla menetelmillä (Kyrölä, 2001, s. 24–25). Tätä varten organisaation tulisi huolehtia tietoturvastaan jatkuvasti päivittäisen toiminnan osana.

2.3 Tietoturvallisuuden osa-alueet

Tietoa on hankala hallita, koska sen käsittely, liikuttaminen ja säilyttäminen voidaan toteuttaa huomattavan monella eri tavalla. Hallinnan yksinkertaistamiseksi tietoturvallisuuden toiminnot jaetaan poikkeuksetta eri osa-alueiden alle. Kun tietoturvallisuutta käsitellään pienemmissä osissa, dokumenteista tulee helpommin seurattavia ja tietoturvallisuustyön organisointi helpottuu.

Tietoturvallisuuden jaottelu eri osa-alueisiin poikkeaa tyypillisesti eri lähteiden välillä. Tämä on seurausta ensisijaisesti siitä, että eri lähteillä on tapana käsitellä aihepiirejä hieman eri näkökulmista. Tässä tutkimuksessa käytetään niin ikään eri lähteiden perusteella muodostettua omaa osa-aluejakoa, joka pohjautuu ensisijaisesti ISO 17799 -standardiin. Tavoitteena käytetyssä jaottelussa on ollut muodostaa kohdeorganisaation ja tutkimuksen kannalta selkeä osa-aluejako, joka käyttää alalla vakiintunutta terminologiaa.

Taulukko 2. Tietoturvallisuuden osa-alueiden jaottelua kirjallisuudessa.

Tutkimuksen jaottelu	ISO 17799 (2006)	Valtiovarain-ministeriö, VAHTI (2003)	Miettinen (1999)	Tipton & Krause (2004)	Hakala et al. (2006)
Hallinnollinen turvallisuus	Tietoturvalli-suuden orga-nisoiminen Tietoturvahäi-riöiden hallinta Tietoturvallisuus-politiikka	Hallinnollinen turvallisuus	Hallinnollinen turvallisuus	Information security management	Hallinnollinen turvallisuus
Tietoaineisto-turvallisuus ja pääsynhallinta	Suojattavien kohteiden hallinta Pääsyoikeuksien valvonta	Tietoaineisto-turvallisuus	Tietoaineisto-turvallisuus Tietojen-käsittelyn turvallisuus	Information security management Access control systems and methodology	Tietoaineisto-turvallisuus
Toimitila-turvallisuus	Fyysinen turvallisuus ja ympäristön turvallisuus	Fyysinen turvallisuus	Toimitila-turvallisuus	Physical security Operations security	Fyysinen turvallisuus
Henkilöstö-turvallisuus	Henkilöstö-turvallisuus	Henkilöstö-turvallisuus	Henkilö-turvallisuus	Information security management	Henkilö-turvallisuus
Tietoliikenne- ja käyttö-toiminto-turvallisuus	Tietoliikenteen ja käyttötoimintojen hallinta	Tietoliikenne-turvallisuus Käyttö-turvallisuus	Tietoliikenteen turvallisuus Käyttö-toimintojen turvallisuus	Telecom., network and Internet security Operations security Enterprise security architecture	Tietoliikenne-turvallisuus

Tutkimuksen jaottelu	ISO 17799 (2006)	Valtiovarain-ministeriö, VAHTI (2003)	Miettinen (1999)	Tipton & Krause (2004)	Hakala et al. (2006)
Laitteisto- ja ohjelmisto-turvallisuus	Tieto-järjestelmien hankinta, kehitys ja ylläpito	Laitteisto-turvallisuus Ohjelmisto-turvallisuus	Laitteisto-turvallisuus Ohjelmisto-turvallisuus	Application program security Cryptography	Laitteisto-turvallisuus Ohjelmisto-turvallisuus
Liiketoiminnan jatkuvuuden hallinta	Liiketoiminnan jatkuvuuden hallinta	–	–	Business continuity planning	–
Vaatimusten-mukaisuus	Vaatimusten-mukaisuus	–	Yksityisyyden suoja	Law, investigation and ethics	–

Taulukko 2 esittelee tietoturvallisuuden osa-alueiden jaottelua kirjallisuudessa tässä tutkimuksessa käytettävän jaottelun suhteen. On hyvä huomata, että samalla rivillä olevat aihepiirit eivät välttämättä vastaa sisällöltään toisiaan kuin ainoastaan osittain. Kuten taulukosta voidaan huomata, jaottelu on pääosin melko yhtenäinen lukuun ottamatta sitä seikkaa, että osa lähteistä jättää liiketoiminnan jatkuvuuden hallinnan ja vaatimusten-mukaisuuden tietoturvallisuuden aihepiirin ulkopuolelle. Tämä on osittain selitettävissä sillä, että kyseiset aihealueet ovat helposti miellettävissä yleisiksi liiketoiminnallisiksi tavoitteiksi. Ne ovat kuitenkin hyvin oleellisia asioita juuri tietoturvallisuuden kannalta, joten niiden käsittely tulisi sisällyttää myös tietoturvallisuuden hallintaan.

2.3.1 Hallinnollinen turvallisuus

Valtionhallinnon VAHTI-ohjeistus määrittelee hallinnollisen turvallisuuden tarkoittavan yleisesti tietoturvallisuuteen tähtääviä hallinnollisia keinoja. Käytännössä tämä tarkoittaa muun muassa organisaation tasolla tehtäviä hallinnollisia järjestelyitä, tietoturvallisuuteen liittyvien tehtävien ja vastuiden määrittelyä sekä henkilöstön tietoturvakoulutukseen, -ohjeistukseen ja -valvontaan liittyviä toimenpiteitä (Valtiovarainministeriö, 2003, s. 11). Tässä tutkimuksessa hallinnollinen turvallisuus on määritelty siten, että se sisältää ISO 17799 -standardin luvut ”Tietoturvallisuuden organisoiminen” ja ”Tietoturvahäiriöiden hallinta”. Nämä luvut muodostavat hallinnollisesta organisoitumisesta ja toimenpiteistä koostuvan joukon. Tältä osin määritelmä mukailee siten VAHTI-ohjeistuksen määritelmää, niputtaen samaan kategoriaan kaikki hallinnolliset tietoturvatoimet.

2.3.2 Tietoaineistoturvallisuus ja pääsynhallinta

Tietoaineistoturvallisuudella tarkoitetaan tietoaineiston tietoturvallisuuteen tähtääviä toimenpiteitä. Aineistoturvallisuuden toteuttamiseksi käytetään keinoina muun muassa

tietoaineiston luettelointia, luokittelua sekä tietovälineiden hallinnan, käsittelyn, säilytyksen ja hävittämisen ohjeistamista (Valtiovarainministeriö, 2003, s. 1; ISO 17799, 2006, s. 50–56). Luetteloinnissa on kyse suojattavan tietoaineiston kirjaamisesta siten, että kohteet ovat yksilöitävissä ja että jokaiselle kohteelle on määritelty katastrofista toipumisen kannalta oleelliset tiedot, mukaan lukien tiedot tallennusmuodosta, sijainnista, varmuuskopioinnista ja arvosta liiketoiminnan kannalta. Samalla tiedolle tulisi määritellä omistaja, joka huolehtii tiedon ja sen säilytyspaikan luokittelusta sekä pääsynhallinnan määrittelystä ja säännöllisestä katselmoinnista. Lisäksi tulisi määritellä tiedon sallittu käyttö (ISO 17799, 2006, s. 50–54).

Luokittelun tarkoituksena on erotella tietoa erilaisiin ryhmiin niiden ”arvon, lakisääteisten vaatimusten, arkaluonteisuuden ja kriittisyyden perusteella” (ISO 17799, 2006, s. 54). Luokittelua käytetään tiedon turvallisuussuojauksen tarpeen, priorisoinnin ja laajuuden ilmaisemiseen. Turvallisuusluokka määrittelee siten sen, miten kyseiseen ryhmään luokiteltua tietoa tulisi hallita, käsitellä, säilyttää ja tuhota. Luokittelu ja sen säännöllinen katselmointi kuuluu kohteen omistajan vastuulle (ISO 17799, 2006, s. 54–56).

Tämän tutkimuksen puitteissa tietoaineistoturvallisuuden kanssa samaan osa-alueeseen on liitetty myös pääsynhallinnan toimenpiteet, sillä pääsynhallinta liittyy oleellisesti tietoaineistoturvallisuuden hallintaan. Pääsynhallinnalla tarkoitetaan yksinkertaisesti toimintoja ja menettelyitä, joilla ohjataan tiedon saantia siten, että ainoastaan valtuutetuilla henkilöillä tai sovelluksilla on siihen pääsy (Valtiovarainministeriö, 2003, s. 34). Pääsynhallinnan piiriin kuuluu käytännössä pääsynvalvonnan toimintaperiaatteiden määrittäminen ja toteuttaminen, käyttöoikeuksien hallinta, käyttäjän velvollisuuksien määrittely, tietoverkkoihin ja käyttöjärjestelmiin pääsyn hallinta, sovellukseen ja tietoon pääsemisen valvonta sekä tietokoneen matka- ja etäkäytön hallinta (ISO 17799, s. 122–152).

2.3.3 Toimitilaturvallisuus

Valtiohallinnon VAHTI-ohjeistus määrittelee toimitilaturvallisuuden käsittävän ”henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaamisen tuhoja ja vahinkoja vastaan” (Valtiovarainministeriö, 2003, s. 10). Tietoturvallisuuden kontekstissa voidaan ajatella, että toimitilaturvallisuudella suojataan henkilöstön muistinvaraisen tiedon lisäksi konkreettisia tieto- ja tiedonkäsittelyvälineitä tuhoilta ja vahingoilta, kuten esimerkiksi palo-, vesi-, sähkö-, ilmastointi-, murto- ja ilkivaltavahingoilta. Tietovälineitä ovat muun muassa muistikortit ja paperidokumentit, ja tiedonkäsittelyvälineitä esimerkiksi henkilökohtaiset tietokoneet ja palvelimet.

ISO 17799 -standardi määrittelee toimitilaturvallisuuden alueiden suojaamiseen liittyvinä turvallisuustoimenpiteinä sekä tietolaitteiden suojausjärjestelyinä eli laiteturvallisuutena. Alueiden suojelulla pyritään estämään luvaton tunkeutuminen organisaation toimitiloihin ja tietoaineistoihin, ja sitä kautta estämään toiminnan häiriintyminen. Keinoina tähän käytetään muun muassa fyysisiä turvarajoja, kulunhallintaa sekä suojausjärjestelyitä ulkopuolisilta fyysisiltä tuloilta ja vahingoilta – kuten esimerkiksi tulipalolta – suojautumiseen. (ISO 17799, 2006, s. 68–72)

Laiteturvallisuudella pyritään estämään omaisuuden häviäminen, vahingoittuminen, varastaminen ja vaarantuminen. Tätä kautta pyritään vähentämään tiedon luvattoman käytön riskiä sekä takaamaan organisaation toiminnan keskeytymättömyys. Keinoina käytetään laitteiden käyttötarkoituksen mukaista sijoittelua ja fyysistä suojausta, sähkönsyötön ja muiden peruspalveluiden varmistamista, kaapeloinnin suojaamista, laitteiden huoltamista ja hallittua käytöstä poistamista sekä toimitilojen ulkopuolisen käytön hallitsemista. (ISO 17799, 2006, s. 72–80)

2.3.4 Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan Valtionhallinnon ohjeissa ”henkilöstöön liittyvien tietoriskien hallintaa henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta” (Valtiovarainministeriö, 2003, s. 13). Käytännössä tämä tarkoittaa sitä, että henkilöstöturvallisuuden tehtävänä tietoturvallisuuden kontekstissa on suojella tietoa organisaation omalta henkilöstöltä. Koska tiedon hyödyntäminen kuitenkin edellyttää, että sitä käyttävällä henkilöllä on pääsy kyseiseen tietoon, ei riitä että tietoa suojellaan ainoastaan pääsynhallinnan keinoilla. Henkilöstöturvallisuuden tehtävänä on siis suojata tietoa myös siihen oikeutettujen henkilöiden väärinkäytöltä.

ISO 17799 -standardissa henkilöstöturvallisuuden suojatoimet on jaettu työsuhteen kannalta kolmeen loogiseen vaiheeseen: vaihe ennen työsuhteen alkamista, vaihe työsuhteen aikana ja työsuhteen päättymisen vaihe. Työsuhteella tarkoitetaan tästä tapauksessa myös organisaation sisällä tapahtuvia nimityksiä ja muuttuvia työtehtäviä, sekä ulkopuoliseen työvoimaan liittyviä sopimussitoumuksia. Tämä osoittaa sen, että henkilöstöturvallisuudesta tulee huolehtia jokaisen työntekijän kohdalla koko sen ajan kun kukin henkilö työskentelee organisaatiossa. Standardi määrittelee jokaiselle kolmelle työsuhteen vaiheelle omat erityiset toimenpiteet. (ISO 17799, 2006, s. 56–66)

Ennen työsuhteen alkua tehtävillä toimenpiteillä on tarkoitus varmistua siitä, että organisaation palvelukseen haettava henkilöstö, urakoitsijat ja muut ulkopuoliset työntekijät ymmärtävät velvollisuutensa organisaatiota kohtaan ja että he soveltuvat heille tarkoitettuihin tehtäviin. Lisäksi toimenpiteiden tarkoituksena on vähentää varkauksien, petosten ja väärinkäytösten riskiä (ISO 17799, 2006, s. 56–60). Työsuhteen aikaisten toimenpiteiden tarkoituksena on huolehtia siitä, että organisaatiolle työskentelevät henkilöt ovat tietoisia tietoturvallisuuden uhista, niiden merkityksestä sekä omista velvollisuuksista ja vastuistaan tietoturvallisuuden osalta. Toimenpiteillä olisi myös huolehdittava siitä, että kyseisillä henkilöillä on keinot tukea yrityksen tietoturvapolitiikkaa omassa työssään, sekä pyrkiä vähentämään inhimillisten virheiden riskiä (ISO 17799, 2006, s. 62–64). Työsuhteen päättymisen toimenpiteillä huolehditaan, että organisaatiolle työskentelevät henkilöt jättävät organisaation tai muuttavat työsuhdettaan hallitusti. Tähän sisältyy muun muassa käyttöoikeuksien poistaminen ja suojattavien kohteiden sekä työvälineiden palauttaminen (ISO 17799, 2006, s. 64–66).

2.3.5 Tietoliikenne- ja käyttötoimintoturvallisuus

Tietoliikenne- ja käyttötoimintoturvallisuudella tarkoitetaan tietojenkäsittelypalveluiden asianmukaisen ja turvallisen käytön varmistamista (ISO 17799, 2006, s. 80). Tietoliikenteen turvaamisella tarkoitetaan tietoturvallisuuden toteuttamista tietoliikenteen laitteiden, järjestelmien ja niissä kulkevien tietojen osalta (Valtiovarainministeriö, 2003, s. 48). Tietoliikenne kattaa kategoriana kaiken data- ja puhelinliikenteen, (Miettinen, 1999, s. 20) myös silloin kun tiedon välittämiseen käytetään siirrettäviä tietovälineitä tietoliikenne-verkkojen sijaan. Käyttötoimintoturvallisuudella tarkoitetaan tietojenkäsittelypalveluiden hallintaan ja käyttöön liittyvien toimintojen suojaamista (ISO 17799, 2006, s. 80).

Tietoliikenneturvallisuuden tavoitteena on ISO 17799 -standardia (ISO 17799, 2006, s. 80–94 & 96–114) mukaillen

- varmistaa tietojenkäsittelypalveluiden turvallinen ja asianmukainen käyttö,
- toteuttaa ja ylläpitää asianmukaista tietoturvallisuuden tasoa ja palveluntarjontaa ulkopuolisten kanssa tehtyjen tietoliikennepalveluiden toimitussopimusten mukaisesti,
- minimoida järjestelmän häiriöt,
- suojata tietojen ja ohjelmien eheys haittaohjelmien vaikutuksilta,
- varmistaa verkossa kulkevan tiedon ja verkon infrastruktuurin suojaukset,

- estää suojattavan tiedon oikeudeton paljastuminen, muuttuminen, siirtyminen tai tuhoutuminen,
- huolehtia siirrettävien tietovälineiden oikeasta käsittelystä,
- ylläpitää viestinnässä vaihdettujen tietojen ja ohjelmien turvallisuutta,
- varmistaa verkkopalveluiden turvallinen käyttö ja
- havaita luvattomat tietojenkäsittelytoimenpiteet.

ISO 17799 -standardi sisällyttää tietoliikenne- ja käyttötoimintoturvallisuuden yhteyteen myös tietojen varmuuskopioinnin. Tässä tutkimuksessa tietojen varmistusta käsitellään kuitenkin liiketoiminnan jatkuvuuden hallinnan osa-alueen yhteydessä, jonka piiriin aihe sopii paremmin.

2.3.6 Laitteisto- ja ohjelmistoturvallisuus

Laitteisto- ja ohjelmistoturvallisuuden osa-alueen tarkoituksena on varmistaa, että organisaation käytössä olevat tietojärjestelmät suunnitellaan turvallisesti, että järjestelmissä tapahtuva tietojenkäsittely on virheetöntä, käytetyt salausmekanismit asianmukaisia ja järjestelmän teknisten haavoittuvuuksien hallinta tehokasta, sekä huolehtia siitä, että järjestelmätiedostot ja ohjelmistot on asianmukaisesti turvattu. Tuotantojärjestelmien lisäksi laitteisto- ja ohjelmistoturvallisuuden osa-alue kattaa myös kehitys- ja tukiympäristöjen turvallisuusasiat (ISO 17799, 2006, s. 152–176). Yksinkertaistettuna voidaan sanoa, että laitteisto- ja ohjelmistoturvallisuudella pyritään varmistamaan, että organisaation tietojärjestelmien laitteistot ja ohjelmistot toimivat siten, että ne täyttävät organisaation liiketoiminnan edellytykset tietoturvallisuuden osalta.

2.3.7 Liiketoiminnan jatkuvuuden hallinta

Liiketoiminnan jatkuvuuden hallinta on tietoturvallisuuden osa-alue, joka tavoitteena on ehkäistä tietoturvapoikkeamasta johtuva liiketoiminnan keskeytyminen, suojata liiketoiminnan kriittisiä osa-alueita tietojärjestelmien merkittävien häiriöiden tai onnettomuuksien vaikutuksilta sekä taata poikkeustilanteessa liiketoiminnan viipeetön jatkuminen (ISO 17799, 2006, s. 184–190). Jatkuvuussuunnittelun ulottaminen tietoturvallisuuden alle perustuu siihen, että tieto on välttämätöntä yrityksen toiminnalle. Koska tietoturvallisuuden toimialue huolehtii organisaation tiedon turvaamisesta, on luonnollista että jatkuvuussuunnittelu on osana tietoturvallisuustyötä.

Liiketoiminnan jatkuvuuden hallinnalla pyritään kontrolloimaan sekä ihmisen että luonnon aiheuttamia toiminnan lamaannuttavia tapahtumia. Tähän kuuluu käytännössä varsinaisen tiedon suojelemisen lisäksi suojattaviin kohteisiin kuuluvien tietojärjestelmien toiminnan takaaminen kaikkien palvelun keskeytymiseen johtavien tapahtumien yhteydessä. Tällaisia ovat esimerkiksi tietokohteiden katoaminen sekä erilaiset katastrofit ja onnettomuudet. (ISO 17799, 2006, s. 184; Tipton & Krause, 2004, s. 1642)

2.3.8 Vaatimustenmukaisuus

Vaatimustenmukaisuudella tarkoitetaan tietoturvallisuuden yhteydessä sitä, että organisaation tietojärjestelmät, tietojen käsittely sekä hallittava tieto itsessään täyttävät niille asetetut ulkopuoliset vaatimukset. Tällaisia vaatimuksia ovat lait, asetukset, säännökset, sopimuksissa asetetut velvoitteet sekä erilaiset turvallisuusvaatimukset kuten esimerkiksi järjestelmän tietoturvallisuuden standardinmukaisuuden osoittavan sertifiointi-laitoksen myöntämän sertifikaatin edellytykset. Vaatimustenmukaisuuden piiriin kuuluu lisäksi huolehtiminen siitä, että organisaatio toimii käytössä olevan turvallisuuspolitiikan mukaisesti (ISO 17799, 2006, s. 192–202). Koska organisaatioiden tiedonkäsittelyyn liittyy hyvin monesti erilaisia vaatimuksia, on loogista että nimenomaan tietoturvallisuuden toimialue huolehtii näiden vaatimusten täyttymisestä. Vaatimukset voidaan ajatella uhkina, ja niiden täyttämättömyydestä voi seurata ennalta määritelty – usein rahallinen – vahinko.

2.4 Tietoisuus tietoturvasta ja tietoturvakulttuuri

Suojeltavaa tietoa joudutaan useimmiten käsittelemään jatkuvasti päivittäisen työnteon eri vaiheissa. Esimerkiksi tuotekehityksestä voidaan jopa sanoa, että työnteko käytännössä pohjautuu suojeltavalle tiedolle. Laajalti hyväksytty näkökanta asiaan on, että organisaation työntekijät ovat merkittävässä asemassa tietoturvallisuuden ylläpitämisessä (mm. Siponen, 2000b; Hansche, 2004; Vroom & R. von Solms, 2004). Joissain lähteissä (mm. Perry, 1985; Angel, 1993), ihmistä pidetään jopa tietoturvallisuuden heikoimpana lenkkinä (viitattu: Siponen, 2000b).

Järvinen (2002, s. 43) esittää teorian, jonka mukaan tietoturvallisuuden ja työntekijän mukavuuden tulo on vakio. Käytännössä tämä tarkoittaa sitä, että lisättäessä jonkin suojattavan kohteen tietoturvallisuuden tasoa heikkenee kyseisen kohteen käyttömukavuus samassa suhteessa. Kun käyttömukavuuden taso laskee alle yksilön henkilökohtaisen sietorajan, ryhtyy käyttäjä kehittämään keinoja, joilla mukavuutta saadaan lisättyä.

Usein käyttömukavuutta lisäävät keinot johtavat nimenomaan turvallisuusmekanismien kiertämiseen, eikä työn tehostamiseen muilla keinoin. Syynä on usein se, että työntekijät eivät ymmärrä kohteen turvallisuusvaatimuksia eivätkä suojaustoimenpiteiden merkitystä kohteen suojaamiselle. Dourish, Grinter, Delgado de la Flor ja Joseph (2004) havaitsivat omassa tutkimuksessaan, että suurin osa ihmisistä suhtautuu tietoturvasuojauksiin lähtökohtaisesti kielteisesti tai enintäänkin neutraalisti. Kielteisen suhtautumisen taustalla olivat usein henkilöiden omat kokemukset, jotka pohjautuivat virheellisiin odotuksiin suojauksien toiminnasta.

Edellä mainitut seikat ovat selvästikin seurausta siitä, että työntekijöille ei ole annettu riittävästi tietoa yrityksen tietoturvavaatimusten edellyttämistä toimintatavoista. Tätä näkemystä tukevat useat lähteet, muun muassa Hansche (2004), Siponen (2000a) ja Adams ja Sasse (1999), jotka kaikki esittävät, että selkeästi yleisin syy henkilöstöstä aiheutuneisiin tietoturvapoikkeamiin on nimenomaan tietämättömyys siitä miten toimitaan turvallisesti.

Adams ja Sasse (1999) toteavat, että kun henkilöllä ei ole riittävästi tietämystä jostain tietoturvaan liittyvästä seikasta, hän muodostaa omatoimisesti mielessään mallin, joka sisältää tilanteeseen liittyvät mahdolliset uhat ja arvion siitä kuinka tärkeitä suojaustoimenpiteet ovat. Nämä arviot ovat tyypillisesti erittäin epätarkkoja, kattavuu-deltaan puutteellisia, sisältävät virheellisiä käsityksiä ja pohjautuvat subjektiiviseen tietoon vaikuttavista tekijöistä ja niiden merkityksellisyydestä. Kun henkilön käytössä on riittävästi tietoa, hän pystyy myös tekemään oikeampia päätöksiä.

Työntekijät ovat monesti valmiita säätelemään omaa lähtökohtaista mukavuudentasoaan, mikäli organisaatio luo riittävät puitteet tietoturvakontrollien aiheuttaman lisävaivan ymmärtämiseksi. Jotta työntekijä tukisi johdon haluamalla tavalla yrityksen asettamia tavoitteita tietoturvallisuudelle, tulisi henkilöstön ymmärtää mitä varten kontrollit ovat olemassa ja mitä konkreettista hyötyä niistä on (Adams & Sasse, 1999). Työntekijöiden käyttäytymistä voidaan siten käytännössä säädellä muun muassa riittävästi yksilöivän ja opastavan työohjeistuksen avulla, muokkaamalla yrityksessä vallitsevaa tietoturvakulttuuria ja kollektiivista arvomaailmaa sekä lisäämällä työntekijöiden koulutusta (R. von Solms & B. von Solms, 2004).

Vroom ja R. von Solms (2004) esittävät, että organisaation tietoturvakulttuurilla on suuri vaikutus siihen, miten yksittäinen työntekijä toimii. Heidän mukaansa organisaation kulttuuri rakentuu kolmesta osatekijästä – yksilöistä, ryhmistä ja muodollisesta organisaatiosta – ja jokainen näistä tekijöistä on kaksisuuntaisessa vuorovaikutuksessa

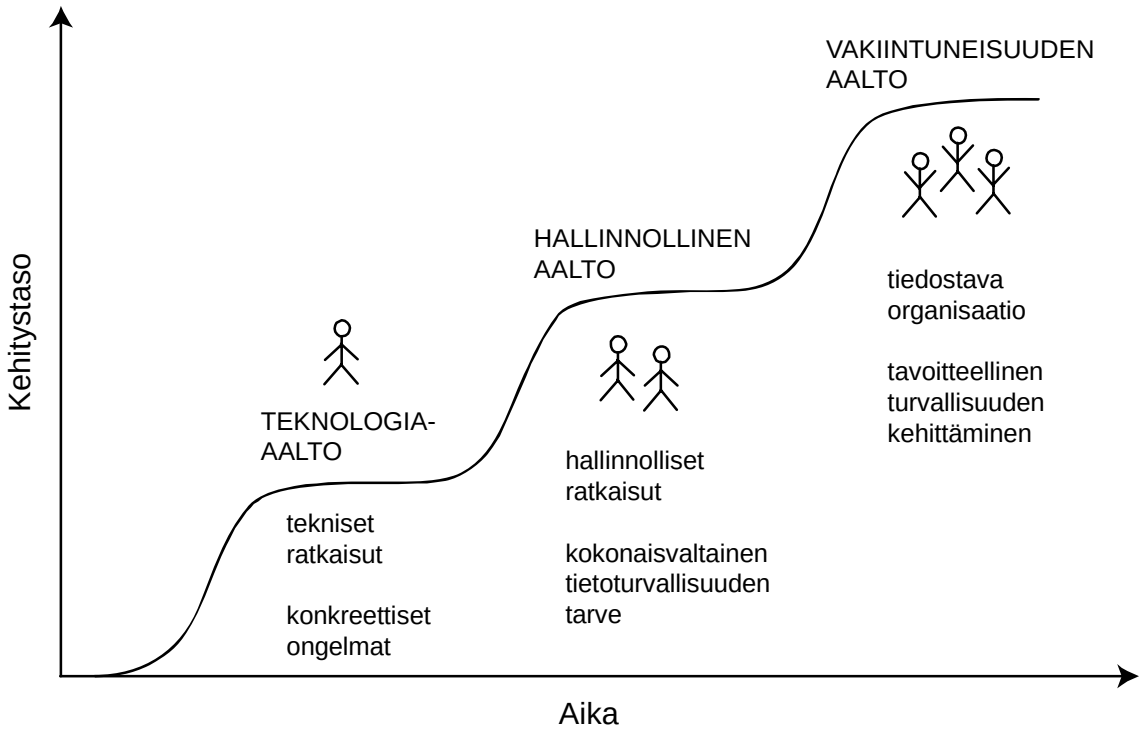
viereisen tekijän kanssa. Toisin sanoen, esimerkiksi yksilöt pystyvät vaikuttamaan ryhmien käyttäytymiseen, ryhmät organisaatioon, ja päinvastoin. Jokaisella osatekijällä on omanlaisensa vaikutus organisaation käytökseen, joten on oleellista, että tietoturvakulttuuria luotaessa sitä lähdetään kasvattamaan jokaiselta tasolta erikseen.

Henkilöstön suhtautumisella tietoturvallisuuteen on merkittävä rooli organisaation tietoturvallisuuden toteutumisessa. Kuten edellä on esitetty, työntekijöiden sitouttaminen tietoturvan toteuttaminen edellyttää suurta panosta nimenomaan organisaation johdolta. Käytännössä tämä tarkoittaa sitä, että johdon asenne ja tietoisuus tietoturvasta luo pohjan koko organisaation tietoturvallisuudelle.

B. von Solms (2000) esittelee tietoturvallisuuden kehityksen koostuvan kolmesta toiminnallisesta aallosta. Nämä aallot kuvaavat von Solmsin sanojen mukaan viimeisen puolen vuosisadan aikana tapahtunutta tietoturvallisuuden kehitystä, mutta ne voidaan nähdä myös kuvastavan yksittäisen organisaation vaiheita kokonaisvaltaisen tietoturvallisuuskulttuurin käyttöönottamisessa.

Näistä ensimmäinen eli teknologia-aalto kuvaa vaihetta organisaatiossa, jossa tietoturvallisuutta on pyritty tuomaan käyttöön teknisten ratkaisujen kautta. Teknisillä ratkaisuilla pyritään usein ratkaisemaan konkreettisia olemassa olevia ongelmia, ja ne ovat siten monesti myös ensimmäinen askel tietoturvallisuuteen. Toinen eli hallinnollinen aalto syntyy, kun organisaatio ryhtyy kehittämään hallinnollisia ratkaisuja tietoturvan parantamiseksi. Tässä vaiheessa kokonaisvaltaisen tietoturvallisuuden tarve on usein tiedostettu organisaation johdossa.

Kolmas vaihe eli vakiintuneisuuden aalto muodostuu, kun organisaatio muuttuu sellaiseksi, että tietoturvallisuuden tavoittelemisesta tulee osa jokapäiväistä toimintaa. Vaiheeseen kuuluu muun muassa tavoitteellinen tietoturvakulttuurin kehittäminen, tietoturvastandardien käytäntöjen omaksuminen ja toiminnan sertifioiminen, sekä tietoturvamittareiden kehittäminen ja seuranta. Vakiintuneisuuden vaiheessa voidaan puhua tiedostavasta organisaatiosta, sillä koko organisaatio on tietoinen yrityksen tietoturvan tavoitteista ja osallistuu sen toteuttamiseen johdon luoman strategian mukaisesti. Kuva 1 havainnollistaa tietoturvallisuuden aaltoja organisaatiossa.



Kuva 1. Tietoturvahallinnon kehitystasot organisaatiossa.

2.5 Yhteenveto

Tässä luvussa on käyty läpi tietoturvallisuuden perusteet organisaationäkökulmasta katsottuna. Aluksi esiteltiin tietoturvallisuuteen liittyvät peruskäsitteet ja selvitettiin mihin tietoturvallisuutta tarvitaan. Luvussa jaettiin lisäksi tietoturvallisuuden kokonaisuus helpommin hallittaviin osa-aluekokonaisuuksiin ja tutustuttiin siihen mitä kaikkea tietoturvallisuuden toimialueeseen kuuluu. Samalla käytiin läpi organisaation tietoturva-kulttuurin ja -tietoisuuden merkitys tietotuvallisuustyön kannalta. Näiden tietojen avulla on tarkoitus pystyä ymmärtämään tietoturvallisuuden peruskäsitteet ja niiden merkitys organisaation tietoturvatyön kannalta.

3 TIETOTURVALLISUUDEN HALLINTA

Tietoturvan toteuttaminen organisaatiossa perustuu tietoturvallisuuden hallinnan organisoimiseen ja sen johtamiseen. Pelkkä tietoturvakontrollien lisääminen ei takaa parempaa tietoturvallisuuden tasoa pitkällä tähtäimellä tarkasteltuna. Yksittäiset tietoturvakontrollit tarjoavat useimmiten ratkaisuja ainoastaan yksittäisiin olemassa oleviin ja tiedostettuihin ongelmiin. Hallinnollisen aallon mukanaan tuomien toimintamallien avulla organisaatio pystyy hallitsemaan teknologia-aaltoon nähden monimuotoisempia ongelmia, mutta varsinaisia kokonaisvaltaisia ratkaisuja sekään ei tuo. Käytännössä organisaation on pyrittävä vakiintuneisuuden aallon kuvaamaan tietoturvallisuuden hallinnan laajuuteen, jotta se pystyisi vastaamaan alati muuttuviin tietoturvariskeihin ja organisaation toiminnan asettamiin vaatimuksiin.

ISO 17799 -standardi (2006, s. 18) määrittelee organisaation tietoturvallisuustyön kriittisiksi menestystekijöiksi seuraavat asiat:

- organisaation toiminnan tavoitteiden mukainen tietoturvapolitiikka, tavoitteet ja toimenpiteet
- organisaation toimintakulttuurin mukainen yhtenäinen näkemys ja toiminnan puitteet tietoturvallisuuden toteuttamiseen ja hallintaan
- johdon näkyvä tuki ja kaikenkattava sitoutuminen
- hyvä yhteisymmärrys tietoturvallisuuden tavoitteista ja riskienhallinnasta
- tehokas turvallisuusasioista tiedottaminen ja koulutusten järjestäminen organisaation sisäisen tietoisuuden lisäämiseksi
- organisaation toimijoiden opastaminen tietoturvallisuuteen liittyvissä asioissa
- asianmukaiset resurssit tietoturvallisuuden hallinnan rahoittamiseksi
- tietoturvahäiriöiden tehokas prosessipohjainen hallinta
- tietoturvallisuuden hallinnan toteutumista valvovien mittareiden käyttöönottaminen

Näiden tekijöiden huomioiminen muodostaa terveen ja toimivan pohjan organisaation tietoturvallisuustyölle. Tässä luvussa tutustumme tarkemmin tietoturvallisuuden hallintaan liittyviin asioihin ja tietoturvallisuustyön toteuttamiseen liittyviin tekijöihin.

3.1 ISO 17799 -tietoturvastandardi

ISO 17799 on kansainvälinen standardi, joka määrittelee ohjeita ja yleisiä toiminta-periaatteita organisaation tietoturvallisuuden hallintatoimen käynnistämiseksi, ylläpitämiseksi ja parantamiseksi. Standardi tarjoaa yleistasoista opastusta yleisesti hyväksytyistä tietoturvallisuuden hallinnan tavoitteista. ISO 17799 esittelee myös useita käyttöön otettavaksi tarkoitettuja valvontatavoitteita ja kontrolleja. Standardi soveltuu käytettäväksi organisaation turvallisuusstandardien ja tehokkaiden turvallisuusjohtamisen käytäntöjen kehittämiseen, sekä luottamuksen lisäämiseksi organisaatioiden välisiin liiketoimiin. (ISO 17799, 2006, s. 20) [1]

ISO 17799 on teknisten toteutuksien osalta neutraali standardi, joka tarjoaa hyviä menettelytapoja paremman tietoturvallisuuden toteuttamiseen. Sen avulla voidaan luoda hyvä perusta organisaation tietoturvallisuuden kehittämistä varten ja se soveltuu myös organisaation tietoturvallisuuden nykytilan selvittämiseen tietoturvakartoituksen avulla (Kairab, 2005, s. 17–18). Kansainvälinen ISO 17799 -standardi pohjautuu Ison-Britannian kansallisen standardointilaitoksen alun perin luomaan BS 7799 -standardiin, ja tarkemmin nimenomaan sen ensimmäiseen osaan BS 7799-1. Standardin toinen osa BS 7799-2 määrittelee varsinaisen tietoturvallisuuden hallintajärjestelmän, ja sen uusin painos on julkaistu kansainvälisenä standardina ISO 27001 (Hakala et al., 2006, s. 46).

ISO 17799 jakautuu yhteensä 11 pääturvallisuuskategoriaan. Kukin kategoria sisältää valvontatavoitteen ja yhden tai useampia turvallisuusmekanismeja eli kontrolleja, joita voidaan käyttää valvontatavoitteen saavuttamiseen. Kontrollien yhteydessä esitettävät toteuttamisohjeet tarjoavat yksityiskohtaisempaa tietoa kontrollin toteuttamiseksi ja valvontatavoitteen saavuttamiseksi (ISO 17799, 2006, s. 24). Taulukko 2 (s. 11) esitteli standardin pääturvallisuuskategoriat.

Organisaatioiden tietoturvallisuuden osoittamiseksi sertifiointiorganisaatiot ovat myöntäneet sertifikaatteja sekä BS 7799-2 että ISO 27001 pohjalta järjestettyjen auditointien perusteella. Kummankin standardin vaatimusten täyttämisen edellytyksenä on käytännössä ISO 17799 -standardin toteuttaminen (Hakala et al., 2006, s. 49). Koska standardia käytetään oleellisena osana organisaatioiden tietoturvallisuuden sertifiointia, on se hyvä pohja myös tietoturvakartoitukselle.

---

[1] Tässä tutkimuksessa on käytetty ISO/IEC 17799:2005 -standardin suomennettua painosta ISO 17799:fi (ISO 17799, 2006), joka sisältää suomenkielisen käännöksen lisäksi englanninkielisen alkuperäistekstin. Ensisijaisena tietolähteenä on käytetty englanninkielistä tekstiä.

Organisaatio voi hyötyä standardinmukaisuudesta usein eri tavoin. Noudattamalla yleisesti hyväksyttyä ja käytettyä standardia voidaan vakuuttua siitä, että oma toiminta täyttää tietyt laatuvaatimukset ja että tietoturvallisuus ja sen hallinta on järjestetty johdon näkökulmasta riittävän hyvin ja johto voi siten nauttia omistajien luottamuksesta. Toisaalta, organisaatioiden välisessä kanssakäymisessä standardinmukaisuus tuo luotettavuutta toiminnan turvallisuudesta. Sertifioidun organisaation kanssa toimivalla toisella osapuolella on perusteltua syytä luottaa siihen, että asiat on hoidettu standardien mukaisesti. Joissain tapauksissa asiakas saattaa edellyttää standardinmukaisuutta, tai jopa sen todistamista sertifikaatilla.

ISO- ja IEC-organisaatioiden teknisen yhteistyökomitean tietoturvallisuudesta vastaava alakomitea valmistelee parhaillaan kansainvälistä tietoturvallisuuden standardisarjaa, jonka tarkoituksena on käsitellä tietoturvallisuuden hallintajärjestelmien vaatimuksia, riskienhallintaa, tietoturvallisuuden tason mittausta ja tietoturvallisuuden käyttöönoton opastusta. Standardisarjan numerointi alkaa standardista ISO/IEC 27000, ja ISO 17799 -standardin esipuheen mukaan seuraava painos ISO 17799 -standardista julkaistaan standardina ISO/IEC 27002. (ISO 17799, 2006, s. 12)

3.2 Tehtävät ja vastuut

Tietoturvallisuuden hallinnan ja kehittämisen kannalta tärkein toimija on organisaation ylin johto, jonka useimmiten muodostaa organisaation johtoryhmä, toimitusjohtaja mukaan lukien. Toimitusjohtaja vastaa tietoriskien hallinnan tarkoituksenmukaisuudesta ja sen oikeasta kohdistamisesta (Kyrölä, 2001, s. 234). Käytännössä tämä tarkoittaa sitä, että toimitusjohtaja vastaa myös organisaation tietoturvallisuuden kehittämispäätöksistä. Lisäksi toimitusjohtaja vahvistaa tietoriskien hallintaan liittyvän politiikan, organisaation ja vastuut (Kyrölä, 2001, s. 234).

Ylin johto luo organisaatiolle tietoturvapolitiikan ja päivittää sitä tarvittaessa. Johto vastaa myös tietoturvatyön organisoinnista. Johtoryhmästä valitaan tietoriskien hallinnan kehittämiselle vastuuhenkilö. Johtoryhmä tekee tietoriskien hallintaan liittyvät päätökset kehitystyön vastuuhenkilön ja mahdollisten toimintayksiköiden johtajien raportoinnin perusteella. Johtoryhmä hyväksyy tietoturvatyöhön liittyvät kulut (Kyrölä, 2001, s. 208–211). Johdon vastuulla on myös lisätä työntekijöiden tietoisuutta tietoturvasta sekä luoda organisaatiolle myönteinen tietoturvakulttuuri (R. von Solms & B. von Solms, 2004). Johto hyväksyy tietoriskien hallinnan toimintaperiaatteet ja valvoo tietoturvallisuuden tasoa (Kyrölä, 2001, s. 234).

Johtoryhmästä valittu vastuuhenkilö vetää tietoriskien hallinnan ja turvallisuuden johtoryhmää. Ryhmä vastaa organisaation tietoturvallisuuden kehittämisen koordinoinnista ja suunnittelusta. Vastuuhenkilö vastaa tietoturvallisuuden käytännön kehittämistyön johtamisesta ja työn tavoitteiden ja mittareiden määrittelystä. Ryhmässä toimiva tietoriskien hallinnan koordinoija puolestaan kerää yrityksessä tapahtuneet tietoturvapoikkeamat ja niistä aiheutuneet vahingot. Lisäksi koordinoija kokoaa yrityksen toimintayksiköiden kehittämistarpeet, -suunnitelmat ja -ohjelmat (Kyrölä, 2001, s. 142–145). Esimiehet kartoittavat koordinoijan avustamana kunkin toimintayksikön tietoriskit, asettavat kehitys-työlle tavoitteet ja laativat kehittämissuunnitelman (Kyrölä, 2001, s. 142 & 235).

Esimies raportoi toimintayksikössä kerätyt tiedot virhetilanteista ja niiden hallintaan kuluneista resursseista tietoturvallisuuden koordinoijalle. Kukin esimies vastaa yksikkönsä toiminnasta ja jatkuvuuden hallinnasta, tietoriskien ja -häiriöiden tunnistamisesta sekä varajärjestelyiden organisoimisesta. Esimiesten vastuulla on myös alaisten tietoisuus tietoturvallisuuteen liittyvistä ohjeista ja käytännöistä. Esimies selvittää alaisilleen ohjeiden ja velvoitteiden merkitykset sekä mahdolliset seuraamukset, valvoo että organisaation tietoturvapolitiikkaa ja -ohjeistusta noudatetaan ja tarvittaessa puuttuu laiminlyönteihin. Myös toimintamenetelmien riittävyyden säännöllinen arviointi suhteessa analysoituihin tietoriskeihin kuuluu esimiehelle. (Kyrölä, 2001, s. 211–217)

Työntekijöiden rooli tietoturvallisuuden kehittämisessä on usein hyvin pieni, sillä organisaation kehitystyö pysähtyy tyypillisesti esimiestasoon. Olisi kuitenkin hyvä huomioida, että työntekijät ovat päivittäin tekemisissä yrityksen käytännön asioiden kanssa ja huomaavat siten parhaiten varsinaiset puutteet turvallisuudessa. Työntekijöiden osuutta tietoturvallisuuden kehittämisessä kannattaisi siten kasvattaa. Tätä näkökantaa tukevat myös Adams ja Sasse (1999), jotka esittävät että yksi syy tietoturvallisuuden epäonnistumiseen on se, että työntekijöitä ei kuulla suojausmenetelmiä kehitettäessä. Seurauksena muodostetaan toisinaan työtehtävien kanssa ristiriidassa olevia kontrolleja, mikä puolestaan ohjaa työntekijöitä suojausten kiertämiseen.

Jokaisen työtekijän vastuulla on huolehtia suojeltavien kohteiden suojaamisesta organisaation antamien ohjeiden mukaisesti. Tämä edellyttää ensisijaisesti annettujen ohjeiden ymmärtämistä, yleistä huolellisuutta ja omien tiedon käsittelyyn liittyvien velvollisuuksien sisäistämistä. Velvoitteisiin sisältyy usein ainakin vaitiolovelvollisuus. Työntekijän vastuulle kuuluu myös työtehtäviin liittyvien virhetilanteiden asianmukainen hallitseminen ja toimintavirheiden ja -puutteiden asianmukainen raportointi esimiehelle. (Kyrölä, 2001, s. 217–221)

Kuva 2. Tietoturvallisuuden tehtävät ja vastuualueet organisaatiossa.

Kuva 2 havainnollistaa tietoturvallisuuden tehtävien ja vastuualueiden jakautumista organisaatiossa. Organisaation rakenne saattaa toisinaan erota edellä esitetystä. Sama vastuunjako on kuitenkin sovellettavissa myös muuntyyppisiin organisaatioihin. Tällöin osalla toimijoista on joko esitettyä laajempi vastuu, tai mahdollisesti jonkin tietyn tehtävän vastuu jakautuu useammalle toimijalle. Tärkeintä on kuitenkin, että vastuunjako on kaikille toimijoille selvä.

3.3 Tietoturvapolitiikka, -suunnitelma ja -ohjeet

Tietoturvapolitiikan tarkoituksena on tarjota johdon ohjaus ja tuki tietoturvallisuuden toteuttamiseen organisaation toiminnan tavoitteiden ja asiaankuuluvien lakien mukaisesti. Tietoturvapolitiikalla johto osoittaa organisaation tavoitteiden mukaisen suunnan tietoturvallisuuden toteuttamiseksi ja sitoutumisensa tietoturvan toteuttamiseen (ISO 17799, 2006, s. 28). Tietoturvapolitiikka laaditaan yleisellä tasolla ja siinä määritellään organisaation toiminnan edellyttämä tietojen turvaamisen aste, menetelmät, joilla haluttuun

turvallisuustasoon pyritään, sekä tietoturvallisuuden hallinnointiin ja kehittämiseen liittyvät käytännöt (Hakala et al., 2006, s. 7).

Tietoturvapolitiikka laaditaan kirjallisena ja sen tulisi mukailla organisaation seuraavan 5–10 vuoden strategista linjausta. Politiikan on tarkoituksena toimia ohjaavana lähtökohtana tietojärjestelmien suunnittelussa sekä tavoitteellisena toimintaohjeena eri toimintaprosessien vastuullisille esimiehille. Pitkän aikavälin linjausten vuoksi tietoturvapolitiikkaan ei ole tarkoituksenmukaista sisällyttää yksityiskohtaisia ohjeita muun muassa teknisten ratkaisujen osalta, vaan sisältö muodostuu pääasiassa erilaisista käytännöistä. Tietoturvapolitiikka tulisi tarkistaa vähintään vuosittain, jotta se vastaisi jatkossakin organisaation tarpeita. (Hakala et al., 2006, s. 7–8)

Hakala et al. (2006, s. 8–9) esittävät, että hyvä tietoturvapolitiikka koostuu seuraavista osa-alueista:

- tietoturvallisuuden määritelmä, turvallisuuden kannalta keskeiset kohteet, turvallisuustoimintojen laajuus ja tärkeys organisaation toiminnalle
- johdon tahdonilmaus ja tuki tietoturvan toteuttamiseksi
- rakenteet joiden avulla tietoturvallisuuteen pyritään
- yhteenveto tietoturvakäytännöistä
- yhteenveto ulkopuolisista vaatimuksista
- yhteenveto turvallisuuskulttuurin ja -tietoisuuden lisäämistoimista
- liiketoiminnan jatkuvuuden toimintojen kuvaus
- vastuualueiden ja tapahtumaraportoinnin määrittely
- sanktiot turvallisuuspolitiikan rikkomisesta
- luettelo organisaation tietoturvapolitiikkaa täydentävistä dokumenteista

Tietoturvapolitiikka kirjoitetaan luonteeltaan julkiseksi dokumentiksi ja sen tulisi olla selkokielinen ja ymmärrettävissä koko organisaation laajuudelta. Se voidaan tarvittaessa luovuttaa myös sidosryhmille osoituksena organisaation sitoutuneisuudesta tietoturva-työhön. Liitteenä olevat, tarkempia teknisiä yksityiskohtia sisältävät dokumentit ovat pääasiassa luonteeltaan salaisia ja tarkoitettu vain organisaation omaan käyttöön. (Hakala et al., 2006, s. 9)

Tietoturvasuunnitelmalla tarkoitetaan lyhyemmän aikavälin, noin 2–5 vuoden ajanjakson kattavaa kirjallista dokumenttia, joka sisältää konkreettisia suunnitelmia ja käytäntöjä, joilla pyritään toteuttamaan organisaation tietoturvapolitiikkaa. Sen avulla määritellään

kohdistetusti ja yksityiskohtaisesti työmenetelmät ja tekniset ratkaisut, joita organisaatiossa käytetään. Tietoturvasuunnitelman sisältö tulisi tietoturvapolitiikan tavoin tarkistaa vähintään vuosittain, mutta myös silloin kun esimerkiksi tietojärjestelmiin tai työmenetelmiin suunnitellaan oleellisia muutoksia. Suunnitelma on luonteeltaan salainen sen käytännön tietosisällön vuoksi. (Hakala et al., 2006, s. 9)

Tietoturvasuunnitelmasta muodostettavia yksityiskohtaisia työntekijöille tarkoitettuja toimintaohjeita kutsutaan *tietoturvaohjeistukseksi*. Joissain tapauksissa ohjeet voivat olla turvallisuussyistä tarkoitettu vain rajatulle joukolle henkilöstössä. Tietoturvaohjeet voivat sisältää hyvin paljon teknisiä yksityiskohtia eivätkä välttämättä aina sovellu sellaisenaan rutiinimaiseksi työohjeeksi. Hyvä ohjeistus selittää lukijalleen mikä ohjeen tarkoitus ja mitkä sen taustat ovat. Tietoturvaohje on myös luonteeltaan salainen sen sisällön yksityiskohtaisuuden vuoksi. (Hakala et al., 2006, s. 10)

3.4 Tietoturvallisuuden prosessi

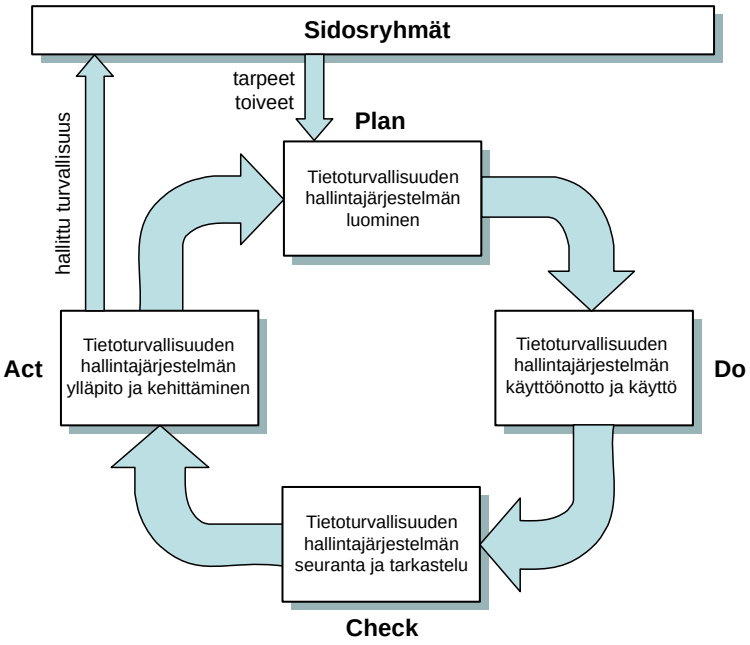
Tietoturvallisuuden parantaminen yksittäisillä projekteilla ei varsinaisesti johda ainakaan pitkäaikaiseen käytännön turvallisuuden parantumiseen. Tietoturvatyö tulisikin tästä syystä toteuttaa organisaatiossa aina prosessimuodossa. Tällöin tietoturvallisuus ja sen tarvitsema työ saadaan integroitua organisaation tavoitteelliseen työhön ja sitä kautta osaksi jokapäiväistä työtä. Tietoturvallisuuden ylläpitämisen ja kehittämisen tulisi olla organisaation tavoitteita toteuttava jatkuva tukiprosessi.

Prosessi on toimintakokonaisuus jolle on määritelty omistaja. Omistaja kantaa aina prosessin toiminnasta vastuun ja käytännössä useimmiten siirtää päätäntävaltaa alaisilleen delegoimalla prosessin tehtäviä. Vastuuta prosessista tai sen osista ei kuitenkaan voi siirtää (Hakala et al., 2006, s. 20–21). Prosessin omistajalla on oltava riittävästi valtuuksia prosessin pyörittämiseen ja hallintaan, joten käytännössä tietoturvallisuuteen liittyvien prosessien omistaja löytyy usein organisaation ylimmästä johdosta.

3.4.1 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmällä tarkoitetaan organisaation tietoturvan hallintaan tarkoitettua toiminnallista kokonaisuutta, joka kattaa koko tietoturvatyön aina organisaation tietoturvapolitiikasta yksittäisten kontrollien hallintaan (Kyrölä, 2005, s. 28). Tietoturvallisuuden prosessi on oleellinen osa hallintajärjestelmän käytännön toimintaa. Kansainvälinen ISO 27001 -standardi määrittelee yhden tunnustetuimmista ja sertifioi-

duimmista tietoturvallisuuden hallintajärjestelmän malleista. Standardissa hallinta-järjestelmän kehittäminen pohjautuu niin sanotun laatuympyrän eli PDCA-mallin (*Plan, Do, Check, Act*) mukaiseen prosessiin.



Kuva 3. PDCA-mallin mukainen prosessi (Hakala et al., 2006, s. 49).

Kuva 3 havainnollistaa tämän PDCA-prosessimallin kulkua. Malli perustuu prosessin aikana tapahtuvaan tarkkailuun ja oppimiseen, ja sitä kautta prosessin laadun jatkuvaan kehittämiseen (Crosby, 1991). PDCA-mallin mukaista prosessia voidaan hyvin soveltaa myös muihin tietoturvatyön työvaiheisiin.

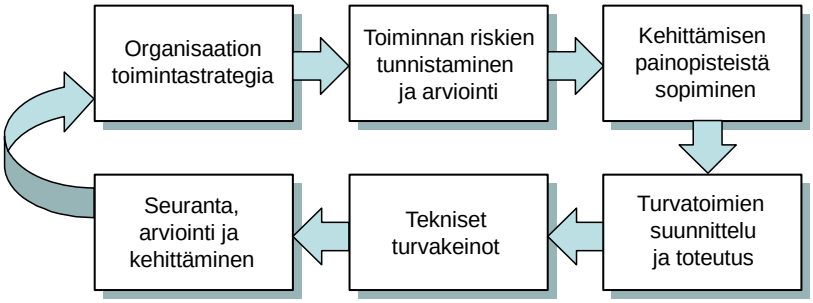
3.4.2 Prosessin vaiheet

Tietoturvallisuuden prosessin lähtökohtana on organisaation toimintastrategia, joka määrittelee organisaation tarpeet ja sen, miten turvallisuusprosessin sisällä toimitaan. Toiminnan riskien tunnistaminen ja arviointi on riskienhallinnan toimenpide, jossa toimintaan liittyvät riskit tunnistetaan ja niiden vaikutus toimintaan arvioidaan. Riskien-hallinta on prosessin kannalta erittäin tärkeä toimenpide ja sitä käsitellään yksityiskohtaisemmin myöhemmin tässä luvussa. Kehittämisen painopisteistä sopimisella tarkoitetaan sitä, että päätetään miten voimavaroja ja toimenpiteitä tullaan kohdentamaan.

Turvatoimien suunnittelu- ja toteutusvaiheessa kehitetään ja otetaan käyttöön suojattavien kohteiden tarvitsemat turvallisuusmekanismit ja muut hallinnolliset toimintamallit. Samalla suunnitellaan ja toteutetaan mittarit, joiden avulla toimenpiteiden toimivuutta voidaan

seurata. Suunnittelun jälkeen toteutetaan myös kontrollien tarvitsemat tekniset turvamekanismit.

Prosessiympyrän viimeinen vaihe ennen takaisinkytkentää koostuu käyttöönotettujen kontrollien seurannasta, arvioinnista ja kehittämisestä. Tämä on erittäin tärkeä vaihe, sillä sen avulla seurataan tehtyjen toimenpiteiden onnistumisen lisäksi myös niiden riittävyyttä. Seurannasta ja arvioinnista saatujen tietojen perusteella tehdään kehitysehdotukset, joiden perusteella toteutusta tulisi parantaa. Kuva 4 esittelee tietoturvallisuuden prosessin vaiheet. (Kyrölä, 2001, s. 35)



Kuva 4. Tietoturvallisuuden prosessi.

Kaikkiin prosessin vaiheisiin kuuluu osana toiminnan dokumentointi. Kartoitusten, suunnitelmien ja toimenpiteiden dokumentointi on oleellista, jotta organisaation toiminnasta on kirjallista näyttöä ja jotta tietoturvallisuuden prosessi on hallittavissa ja kehitettävissä.

3.4.3 Tietoturvakartoitus

Tietoturvakartoituksen suorittaminen on yleensä ensimmäinen työvaihe tietoturvallisuuden prosessin käynnistämisessä. Tällöin kartoituksen tarkoituksena on hankkia perustieto oman organisaation ja sen tietojärjestelmien tietoturvallisuuden nykytilasta. Kartoituksessa kerätyn tiedon pohjalta voidaan määritellä oleelliset riskikohteet ja tarvittavat toimenpiteet. Kun prosessi on saatu käynnistettyä, on kartoitus hyvä uusia säännöllisesti turvallisuuden tason mittaamiseksi ja aina kun tietoturvan toteuttamisessa tapahtuu oleellisia muutoksia (ISO 17799, 2006, s. 40).

Kuva 5 esittelee Kairabin (2005, s. 62–65) mallin mukaisen tietoturvakartoituksen eri vaiheet. Malli on jaettu viiteen eri päävaiheeseen, joihin kuhunkin sisältyy viisi eri alivaihetta.

Kuva 5. Tietoturvakartoituksen vaiheet (Kairab, 2005, s. 63).

Kairabin (2005, s. 64–65) mallin perustana on joustavuus. Koska tietoturvakartoitukset ovat yksilöllisiä ja niiden suorittaminen vaatii usein organisaatiokohtaisia ratkaisuja, on tärkeää että kartoitustyö pystyy mukautumaan niihin. Kairabin mallin eri välivaiheita voidaan mahdollisuuksien mukaan yhdistää ja työmäärää voidaan tarvittaessa painottaa aikataulullisista syistä eri vaiheisiin. Tärkein lähtökohta tietoturvakartoituksen suorittamisessa on organisaation liiketoiminnan tai muun tavoitteellisen toiminnan perusteellinen ymmärtäminen, koska se on välttämätön edellytys kartoitettavien riskien ymmärtämiselle. Liiketoiminnan tulisi ohjata turvallisuuskäytäntöjä eikä toisinpäin (Kairab, 2005, s. 64–65).

Tietoturvallisuuden prosessin käynnistävä organisaation ensimmäinen tietoturvakartoitus olisi hyvä antaa riippumattoman tahon suoritettavaksi eturistiriitojen, ulkopuolisen näkemyksen ja monesti myös ulkopuolisen organisaation paremman asiantuntevuuden vuoksi. Myöhemmät kartoitukset voidaan suorittaa edellisten kartoitusten pohjalta omatoimisesti, kunhan organisaatiolla vain on riittävä osaaminen kartoituksen tekemiseen. Toisinaan voi kuitenkin olla ulkopuolisia vaatimuksia esimerkiksi sidosryhmiltä, jotka edellyttävät että kartoituksen suorittaa aina riippumaton taho. Tämä edellytys sisältyy myös ISO 17799 -standardiin (2006, s. 40).

3.4.4 Poikkeamien ja havaittujen heikkouksien hallinta

Tietoturvapoikkeamiin varautuminen on yksi oleellinen osa tietoturvallisuuden hallintaa. Organisaatiossa tulisi olla oma prosessi tietoturvapoikkeamien käsittelemiseksi, jotta niiden käsittely olisi hallittua. Tämän prosessin hallinta on osa koko tietoturvallisuuden prosessia.

Samaa prosessia tulisi hyödyntää myös työssä havaittujen heikkouksien tai haavoittuvuuksien raportointiin ja käsittelemiseen.

ISO 17799 -standardi (2006, s. 176–184) käsittelee tietoturvapoikkeamien ja -heikkouksien hallintaa omassa luvussaan. Siinä asian käsittely on jaettu kahteen osaan: raportointiin ja hallintaan. Raportointia käsittelevän osion tarkoituksena on varmistaa, että tietoturvapoikkeamista ja havaituista heikkouksista raportoidaan mahdollisimman nopeasti ja tehokkaasti asiaankuuluvia hallinnollisia menettelyitä käyttäen. Raportointimenettelyt ja -perusteet tulisi olla yleisesti tiedossa ja vastuut selkeästi määritelty. Jälkimmäisen osion tarkoituksena on huolehtia siitä, että tietoturvapoikkeamien hallintaan käytetty toimintamalli on tehokas ja johdonmukainen. Poikkeamien ja havaittujen heikkouksien käsittelyyn tulisi olla selkeät ja ennalta sovitut vastuut ja menettelytavat. Toiminnassa tulisi huomioida myös mahdollinen todisteiden kerääminen ja todistusaineiston säilyttäminen. Myös poikkeamista oppiminen tulisi sisällyttää prosessiin (ISO 17799, 2006, s. 178–184).

Toiminnan jatkuvuuden kannalta on tärkeää, että organisaatio varautuu myös sellaisiin poikkeamiin, jotka ovat vaikutukseltaan suuria mutta mahdollisesti hyvin epätodennäköisiä. Tällä pyritään estämään toiminnan pysyvä keskeytyminen tai pitkäaikainen lamaantuminen. Jatkuvuussuunnittelussa tulisi käsitellä mahdollisimman kattavasti erilaiset toiminnan keskeytymiseen johtavat tilanteet ja suunnitella jokaisen tapauksen varalle korvaava toimintasuunnitelma. Suunnittelun tavoitteena on saada organisaation toiminta jatkumaan ainakin tärkeimpien toimintojen osalta mahdollisimman nopeasti, poikkeuksellisesta tilanteesta huolimatta (ISO 17799, 2006, s. 184–190).

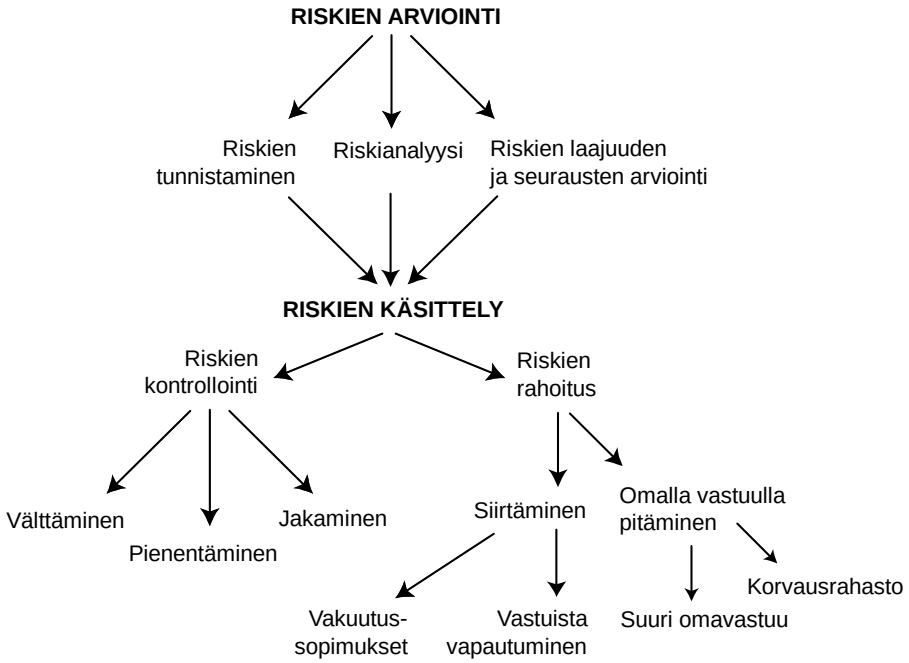
3.5 Riskienhallinta

Riskillä tarkoitetaan jonkin haitan mahdollisuutta. Matemaattisesti riski määritellään *uhan* ja *vahingon* tulona. Uhalla tarkoitetaan jotain haitallista tapahtumaa, joka saattaa tapahtua. Uhan numeerinen arvo on tuon haitallisen tapahtuman toteutumisen todennäköisyys. Vahinko taas kuvaa aiheutuvan menetyksen suuruutta, mikäli uhka toteutuu. Riskin numeerinen suuruus on siis vahingon odotusarvo. (Virtanen, 2004, s. 9–13)

Riskienhallinnalla tarkoitetaan uhkaavien vahinkojen hallitsemista organisaation omien turvallisuuteen liittyvien tavoitteiden mukaisesti (Suominen, 2003, s. 27). Tietoriskien hallinta on oleellinen osa tietoturvallisuuden toteuttamista organisaatiossa. Ilman riskien tunnistamista ja asianmukaista käsittelyä ei voida sanoa, että tietoturvallisuustyö olisi kattavaa ja tehokasta. Riskienhallinnalla pyritään kohdistamaan organisaation suojaus-

toimenpiteet ja tietoturvallisuuteen käytettävät varat toiminnan kannalta oleellisiin riskeihin. Kyrölän (2001, s. 37) mukaan tietoriskien hallinnan painopisteenä ”on kehittää sisäisiä toimintamenetelmiä ja tietojen käsittelytapoja, sähköisten tuotteiden ja verkkopalvelujen toimintaa sekä liikesuhteissa noudatettavia käytäntöjä”.

Tässä riskienhallintaa koskevassa osiossa esitellään riskienhallinnan toiminnalliset osa-alueet ja yleisimmät riskienhallintakeinot. Kuva 6 esittää näihin pohjautuvan riskienhallinnan prosessimallin vaiheineen (Suominen, 2003, s. 99) ja samalla havainnollistaa riskienhallintaan liittyviä työvaiheita.



Kuva 6. Riskienhallinnan prosessimalli.

Riskienhallinta koostuu kolmesta toiminnallisesta osa-alueesta: riskien arvioimisesta, riskienhallinnan toimenpiteistä ja riskienhallinnan organisoimisesta. Riskien arvioinnissa on kyse tutkimuksesta, jonka tarkoituksena on tunnistaa organisaation uhat ja arvioida niihin liittyvien vahinkojen suuruutta, sekä määritellä kullekin riskille sen haitallinen taso ja evaluoida sen kautta riskin merkitystä organisaatiolle. Riskienhallinnan toimenpiteillä tarkoitetaan arvioinnista saatujen tulosten perusteella tehtäviä toimenpiteitä, joilla pyritään poistamaan tai vähentämään riskejä, tai mahdollisesti kompensoimaan tai korjaamaan vahinkoja niiden jo tapahduttua. Riskienhallinnan organisointi käsittää riskien arvioinnin ja hallinnan toimien toteuttamiseksi käytetyt prosessit sekä turvallisuustyön tehtävänjaon. (Lonka et al., 2002)

3.5.1 Riskien arvioiminen

Riskien arvioiminen jakautuu tavallisesti kolmeen työvaiheeseen: riskien tunnistaminen, riskianalyysi ja riskien laajuuden ja seurausten arviointi. Riskien tunnistamisessa on kysymys organisaation toimintaan liittyvien vaaratilanteiden tunnistamisesta ja se on toimivan riskianalyysin lähtökohtainen edellytys. Erilaisten riskien tunnistaminen tulisi tehdä tapauskohtaisesti kunnollista logiikkaa hyödyntämällä, jotta työ ei olisi sattumanvaraista. (Suominen, 2003, s. 40–43)

Riskianalyysissä tunnistetut riskit käydään systemaattisesti läpi ja analyysin tuloksena saadaan selville riskien todennäköisyys eli uhka, riskien vakavuus ja riskeistä aiheutuvat seurannaisvaikutukset. Riskianalyysejä varten on olemassa lukuisia valmiita analyysimenetelmiä (Suominen, 2003, s. 35–40). Vorster ja Labuschagne (2005) ovat kehittäneet työkalun, jonka avulla voi valita tapauskohtaisesti sopivimman tietoriskien analyysimenetelmän viiden yleisesti käytetyn menetelmän joukosta.

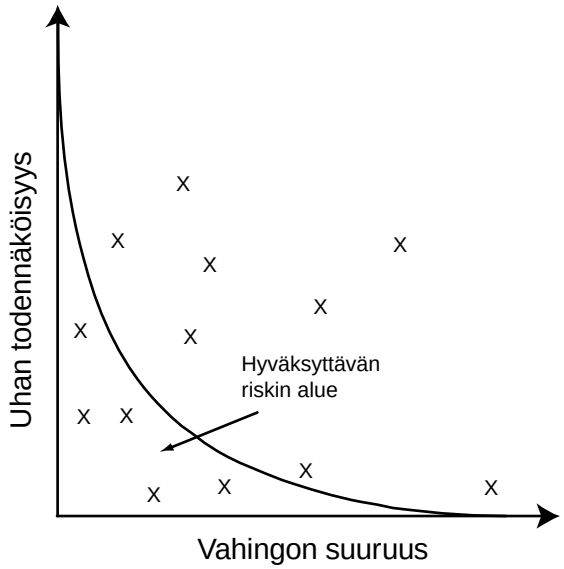
Riskejä voidaan määrittää kahdella tavalla: kvantitatiivisesti ja kvalitatiivisesti. Kummassakin menetelmässä on omat etunsa. Kvantitatiivisessa analyysissä kunkin riskin uhkaavalle vahingolle pyritään laskemaan numeerinen arvo. Kvalitatiivisessa analyysissä riski määritellään sen sijaan abstraktein termein, kuten esimerkiksi *suuri*, *keskisuuri* ja *pieni* (Covert & Nielsen, 2005). Kvantitatiivisen analyysin tekeminen voi muodostua hyvinkin työlääksi, sillä luotettavia tuloksia varten tulee usein kerätä hyvin kattava määrä aineistoa ja niiden perusteella toteuttaa huomattava määrä arvioita erilaisten tapahtumien mahdollisista kustannuksista. Käytännössä työmäärä lisääntyy oleellisesti tarkasteltavan kokonaisuuden koon kasvaessa. Kvalitatiivinen analyysi taas on monesti hyvä suuntaa-antava päätöksenteon apumalli tarkasteltaessa isompia kokonaisuuksia.

Riskien laajuuden ja seurausten arvioinnin tuloksena analysoidut riskit saatetaan keskinäiseen järjestykseen. Käytännössä riskejä tarkastellaan riskilajeittain ja jokaisen riskin uhkaa ja vahinkoja arvioidaan karkealla asteikolla. Organisaatiosta ja sen tarpeista riippuu, miten riskien tärkeysjärjestys määräytyy. Riskin numeerista arvoa voidaan käyttää kuvaamaan riskien suuruusluokkaeroja ja se parantaa riskien vertailtavuutta. (Suominen, 2003, s. 43–43)

Riskejä arvioitaessa määriteltävän vahingon tulisi kattaa kaikki ne suorat ja epäsuorat kustannukset, jotka kyseisen uhan toteutumisesta aiheutuu. Esimerkiksi organisaation maineelle on arvioitava jonkinlainen realistinen rahallinen arvo, jotta sen heikkenemisen seuraukset voitaisiin huomioida. Arvioiden ei aina tarvitse olla tarkkoja, vaan vahingot ja

uhat voidaan myös jakaa esimerkiksi muutamaan diskreettiin luokkaan. On myös muistettava, että vahinko lankeaa uhan toteutuessa aina kokonaisuudessaan maksettavaksi, eikä riskin numeerinen arvo kerro muuta kuin vahingon odotusarvon.

Eräs yksinkertainen ja pelkistetty tapa arvioida riskejä on asettaa riskit koordinaatistoon uhan ja vahingon mukaan (Suominen, 2003, s. 45). Riskien luokittelua varten valitaan yritykselle sopiva raja-arvo hyväksyttävälle riskille ja rajataan tämä alue koordinaatistosta. Tämän jälkeen koordinaatistosta on helppo tunnistaa toimenpiteitä vaativat riskit ja niiden pienentämiseen parhaiten sopiva menetelmä. Menetelmää havainnollistaa Kuva 7.



Kuva 7. Yksinkertainen riskien arviointimenetelmä.

Spears (2006) käsittelee käyttäjien osallistuttamista liiketoimintaprosesseissa olevien tietoriskien tunnistamiseen. Tässä yhteydessä käyttäjällä tarkoitetaan sellaista henkilöä, joka on käytännössä työnsä puolesta tekemisissä aiheena olevien asioiden kanssa. Ideana on, että ammattimainen henkilö, joka on jatkuvasti tekemisissä jonkin rutiininomaisen liiketoiminta-prosessin kanssa, tunnistaa prosessissa olevat tietoturvallisuuden ongelmat ulkopuolista toimijaa helpommin. Riskienhallinnan kannalta olisi ihanteellista toteuttaa riskianalyysit siten, että mukana analyysin tekemisessä olisi nimenomaisesti niitä henkilöitä, jotka ovat eniten tekemisissä tutkittavan aihepiirin kanssa.

3.5.2 Riskienhallinnan toimenpiteet

Riskienhallinnan toimenpiteet voidaan jakaa kahteen pääkategoriaan: riskien kontrolloi-miseen ja riskien rahoittamiseen. Riskien kontrolloiminen jakautuu osaltaan kolmeen ali-kategoriaan: välttämiseen, pienentämiseen ja jakamiseen. Riskien rahoittaminen jakautuu

vastaavasti kahteen alaluokkaan, jotka ovat siirtäminen ja omalla vastuulla pitäminen. Nämä aliluokat muodostavat tavallisimmat riskienhallintakeinot. (Suominen, 2003, s. 97–100)

Riskin välttämisellä tarkoitetaan sitä, että vahinkoa pyritään estämään pidättäytymällä riskialttiista toiminnasta, joka aiheuttaa kyseessä olevan uhan (Suominen, 2003, s. 101–102). Esimerkkinä tällaisesta toiminnasta voidaan pitää esimerkiksi etätyöskentelystä luopumista. Monien riskien välttäminen ei ole kuitenkaan organisaation toiminnan kannalta mahdollista tai järkevää ja välttäminen saattaa edellyttää jopa koko toiminnan lopettamista (Suominen, 2003, s. 102).

Riskin pienentämisellä pyritään vahingon tapahtumisen todennäköisyyden eli uhan tai varsinaisten vahinkojen pienentämiseen. Tällainen toimenpide voi olla esimerkiksi laitteen vaihtaminen luotettavampaan. Riskejä voidaan pienentää myös niitä jakamalla ja yhdistämällä. *Riskien jakamisella* tarkoitetaan riskin hajauttamista pilkkomalla riski useampiin itsenäisiin riskikohteisiin (Suominen, 2003, s. 102–105). Esimerkiksi jakamalla jokin tieto osissa eri kassakaappeihin pienentää koko tiedon luottamuksellisuuden vaarantumisen riskiä. *Riskien yhdistämisellä* tarkoitetaan riskikohteiden määrällistä lisäämistä kokonaisriskin vähentämiseksi (Suominen, 2003, s. 102–105). Esimerkiksi sijoittamalla sama tiedosto useammalle toisistaan riippumattomalle palvelimelle voidaan pienentää tiedon saavuttamattomuuden riskiä.

Riskien siirtämisellä tarkoitetaan riskin siirtämistä sopimuksen perusteella joko kokonaisuudessaan tai osittain jollekin toiselle osapuolelle (Miettinen, 2002, s. 30). Käytännössä tämä tarkoittaa riskin ulkoistamista joko vastuusta vapautumisen tai vakuutussopimusten kautta (Suominen, 2003, s. 97–100). Riskejä voidaan siirtää toiselle osapuolelle esimerkiksi alihankkimalla riskialttiit työvaiheet. Vastaavasti vuokra- ja leasing-sopimuksilla voidaan ulkoistaa esimerkiksi kiinteistöjen ja tietokoneiden huoltoon liittyviä riskejä (Suominen, 2003, s. 114–116).

Riskin rahoittamisella tarkoitetaan riskiin varautumista rahallisesti. Käytännössä organisaatiolla voi olla käytössään tällaisten riskien vahinkoja varten esimerkiksi sisäinen korvausrahasto tai sitten riski on katsottu sellaiseksi, että sen aiheuttama vahinko voidaan korvata tarvittaessa kokonaisuudessaan yrityksen kassasta. Rahoittamista käytetään yleisesti yrityksen toimintaan nähden pienten riskien hallintaan, hyvin pienen todennäköisyyden riskien kanssa, vaikeasti ennustettavien riskien tapauksissa (Miettinen, 2002, s. 30) sekä silloin kun omalla varautumisella saavutetaan riskin ulkoistamisen kustannuksiin ja

mahdollisen vahingon suuruuteen nähden taloudellista hyötyä, esimerkiksi yksittäisten riskikohteiden suuresta lukumäärästä johtuen.

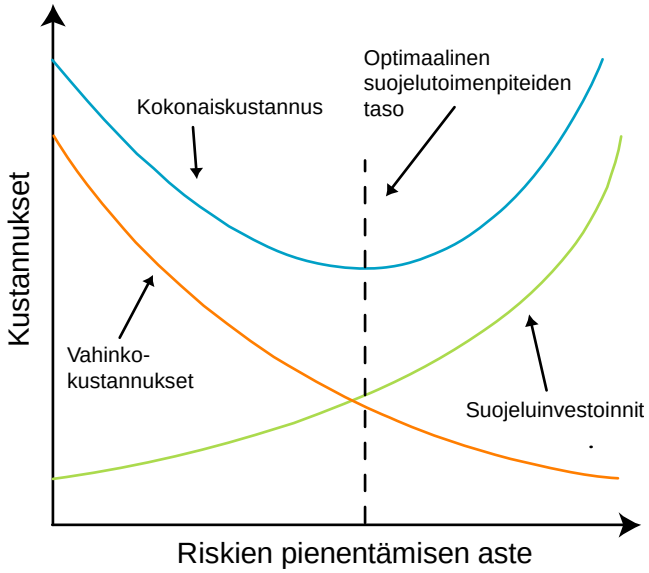
3.5.3 Riskienhallinnan organisointi

Riskienhallinta ei ole kertaluontoinen projektiin verrattavissa oleva toimenpide, vaan siinä on kyse jatkuvasta prosessista, joka edellyttää organisaatiolta pysyvää sitoutumista riskienhallinnan toiminnan ylläpitämiseksi. Riskienhallinta on oleellinen osa tietoturvallisuuden prosessia. Riskienhallinnan prosessi saadaan luontevasti käyntiin arvioimalla organisaation riskit ja tunnistamalla organisaation riskiprofiili. Tämän jälkeen voidaan tehdä hallintakeinoja koskevat päätökset. Riskienhallinnalla pyritään aina vahinkojen ennaltaehkäisyyn, joten organisaation täytyy tehdä ratkaisuja nykyhetken lisäksi myös tulevaisuuden varalta (Suominen, 2003, s. 99).

3.5.4 Riskienhallinta ja kustannukset

Vahinkojen torjuminen tulee tyypillisesti halvemmaksi kuin niiden korjaaminen (Järvinen, 2001, s. 45). Täydellisen tietoturvallisuuden tavoitteleminen ei ole käytännössä kuitenkaan realistista mm. tiukan turvallisuuden aiheuttaman organisaation toimintakyvyn heikkenemisen ja ylivarautumisen aiheuttamien suurten kustannusten vuoksi. Koska uhista aiheutuvat vahingot ja suojelutoimenpiteiden kustannukset mitataan tyypillisesti rahassa, voidaan organisaatiolle määrittää laskennallisesti sopiva suojeluinvestointien taso.

Mitä parempaa turvallisuuden tasoa tavoitellaan, sitä suuremmaksi suojelukustannukset nousevat. Toisaalta, paremmalla tietoturvallisuuden tasolla vähennetään toteutuneista uhista aiheutuneita vahinkoja. Kun nämä kustannukset ovat tiedossa, voidaan organisaatiolle laskea sen odotetut riskikustannukset. Optimaalinen suojeluinvestointien taso saavutetaan siinä pisteessä, jossa kokonaiskustannukset ovat pienimmillään. Kuva 8 havainnollistaa menetelmää (Suominen, 2003, s. 114–122).



Kuva 8. Tietoriskien kustannusten optimointi.

3.6 Yhteenveto

Tässä luvussa on käsitelty organisaation tietoturvallisuuden hallintaan ja sen järjestämiseen liittyviä asioita. Aluksi esiteltiin ISO 17799 -standardi, joka sisältää yleistasoista opastusta yleisesti hyväksytyistä tietoturvallisuuden hallinnan tavoitteista ja jonka pohjalta tämän tutkimuksen yhteydessä suoritettiin tietoturvakartoitus kohdeorganisaatiolle. Luvussa esiteltiin myös tietoturvallisuuteen liittyvät vastuut ja tehtävänjako organisaatiossa, tutustuttiin tietoturvapolitiikkaan, -suunnitelmaan ja -ohjeistukseen sekä avattiin tietoturvallisuuden prosessin tarkoitusta ja siihen liittyviä toimia. Lopuksi käsiteltiin tietoturvallisuuden hallinnan kannalta sen oleellisinta toimintoa, riskien hallintaa, joka nitoo yhteen liiketoiminnan ja tietoturvallisuustyön tavoitteet. Luvussa esitellyn tiedon avulla on tarkoitus pystyä ymmärtämään lähtökohtaiset vaatimukset tietoturvallisuuden hallinnan aloittamiselle, tarvittavat toimenpiteet tietoturvan hallintaan ja hallinnan merkitys organisaation tietoturvallisuuden kannalta.

4 TIETOTURVALLISUUDEN KONTROLLEJA

Kun organisaation toiminnan vaatimukset tietoturvallisuudelle on selvitetty, tietoriskit tunnistettu ja päätökset riskien käsittelystä on tehty, on vuorossa sopivien kontrollien valinta ja niiden käyttöönotto. Tietoturvakontrollilla tarkoitetaan tietoturvallisuuden toteuttamiseksi määriteltyä keinoa tai mekanismia, jolla säädellään esimerkiksi ihmisten tai teknisten välineiden toimintaa. Tässä luvussa tutustutaan kohdeorganisaation toiminnan kannalta oleellisiin teknisiin kontrolleihin.

4.1 Tietoverkkojen suojaaminen

Tietoliikenteen suojaaminen on merkittävä osa tiedon suojaamista nykyaikaisessa tiedonkäsittelyssä. Tietoa siirretään paikasta toiseen paitsi viestinnässä niin usein myös silloin kun tietoa käsitellään. Tieto voi liikkua organisaation yksityisen tietoverkon lisäksi myös julkisissa verkoissa, joista yleisin ja tunnetuin on Internet. Tällöin on erityisen tärkeää, että tieto on asianmukaisesti suojattu. Tietoliikenteen suojaamisella pyritään ensisijaisesti estämään tiedon luottamuksellisuuden tai eheyden vaarantuminen ja ehkäisemään tietojärjestelmien luvaton käyttö.

Lähes poikkeuksetta yksityinen verkko joudutaan käytännön syistä myös liittämään julkiseen verkkoon. Tällöin yksityisen verkon suojaaminen julkisesta verkosta tulevilta hyökkäyksiltä edellyttää ylimääräisiä toimenpiteitä. Sähköpostien liitetiedostoina ja ohjelmistojen mukana leviävät haittaohjelmat lisäävät organisaation sisältä tulevien hyökkäysten riskiä, kun työntekijät voivat epärehellisyyden lisäksi myös tahattomasti vaarantaa tietojärjestelmän turvallisuuden. Tietoverkkoihin kytkettyjen laitteiden suojaaminen niin ulkopuolisista kuin omastakin verkosta tulevilta hyökkäyksiltä on näin ollen erittäin tärkeä osa tietoverkkojen turvallisuutta.

4.1.1 Tietoverkkojen infrastruktuuri

Tietoverkkojen suojaamistoimenpiteiden tarkoituksena on vähintäänkin estää järjestelmään tunkeutuminen ja sen luvaton käyttö, ja sitä kautta estää muun muassa liikenteen salakuunteleminen tai väärentäminen. Tiedon saavutettavuuden kannalta on tärkeää, että infrastruktuuri on suunniteltu siten, että siihen ei muodostu liikenteellisiä pullonkauloja (ISO 17799, 2006, s. 88) ja että yhteydet on varmistettu liikenteen saavutettavuusvaatimusten edellyttämällä tavalla.

Tietoverkkoihin kytketyt palvelimet ja työkoneet ovat luontaisesti alttiimpia tietoteknisille hyökkäyksille kuin sellaiset koneet, joihin käsiksi pääseminen edellyttää fyysistä pääsyä koneelle. Nykyaikaisessa tietojenkäsittelyssä tietoverkkojen välttäminen ei käytännössä tule kyseeseen kuin ainoastaan poikkeuksellisissa tapauksissa ja Internet-palveluita tarjoavassa organisaatiossa sitä ei käytännössä voi edes ajatella. Tästä syystä palvelinten ja työkoneiden suojaaminen tietoverkkojen tuomilta uhilta kulkee käsi kädessä tietoturvallisuuden toteuttamisen kanssa. (Schneier, 2004, s. 176)

Kun verkkoja kytketään toisiinsa syntyy tilanne, jossa kuka tahansa toiseen verkkoon pääsevä voi liikennöidä myös siihen liitettyyn verkkoon. Liikennettä verkkojen välillä on voitava säädellä, jotta voidaan suojata yksityistä verkkosegmenttiä julkisesta verkosta tulevalta uhalta (Schneier, 2004, s. 189). Palomuuri on väline, jonka tarkoituksena on estää asiattomien henkilöiden pääsy johonkin verkkoon tai sen tarjoamaan palveluun (Hakala et al., 2006, s.187).

Palomuuri muodostaa verkkojen välille raja-alueen, jonka kautta kumpaankin suuntaan menevä liikenne joutuu kulkemaan. Palomuurille määritellyt säännöt ohjaavat sitä, minkälainen liikenne estetään ja mikä liikenne puolestaan saa jatkaa matkaansa. Palomuuri voidaan toteuttaa tarvittaessa millä tahansa verkkokerroksella, esimerkiksi suodattamaan liikennettä pelkkien IP-otsaketietojen tai vaikka sovellustason protokollan sisällön perusteella (Stallings, 2006, s. 622). Palomuuri tarjoaa useimmissa tapauksissa suojaa erilaisia verkkohyökkäyksiä – kuten esimerkiksi IP-osoitteiden väärennystä ja reititys-hyökkäyksiä – vastaan. Se tarjoaa myös sopivan pisteen verkon turvallisuusaiheisten tapahtumien valvontaan, ja palomuurin yhteyteen voidaan toteuttaa myös erilaisia verkonvalvontatoimintoja (Stallings, 2006, s. 624).

Palomuureja käsiteltäessä tulisi huomioida, että niillä ei voida suojautua sellaisia hyökkäyksiä vastaan, jotka pystyvät tavalla tai toisella ohittamaan palomuurin. Tällaisia tilanteita voi tulla vastaan silloin kun verkkoon pääsee jotain toista kautta, esimerkiksi soittosarjoja pitkin. Palomuurit eivät myöskään suojaa sisältä päin tapahtuvilta hyök-käyksiltä, sillä ne toimivat ainoastaan verkkojen rajoilla. Palomuurit eivät myöskään useimmissa tapauksissa pysty suojelemaan sovellustason hyökkäyksiltä, kuten esimerkiksi viruksilta tai muilta haittaohjelmilta. (Stallings, 2006, s. 624)

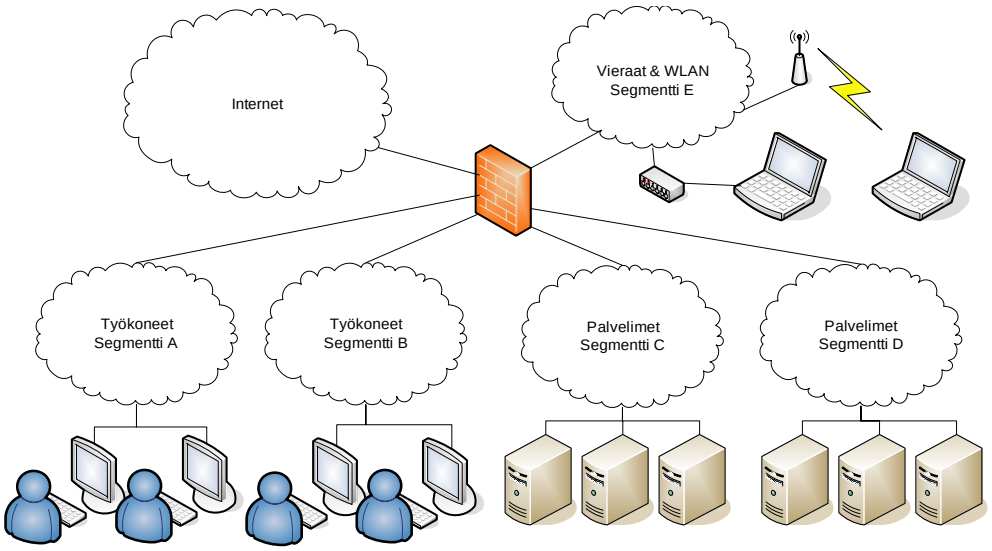
Palomuureja tulisi käyttää julkisen verkon liittymäkohtien lisäksi myös muiden hallitsemiin yksityisiin verkkoihin liityttäessä. Tämän lisäksi on suositeltavaa rajoittaa myös organisaation yksityisen verkon sisällä eri tietokoneita ja palvelimia omiin segmentteihinsä

niiden käyttöryhmien mukaan. Tällöin segmenttien välistä liikennettä voidaan rajoittaa halutulla tavalla ja väärinkäytösten riskiä voidaan vähentää, kun kaikkialta verkosta ei ole pääsyä joka puolelle. Verkkosegmenttejä voidaan muodostaa paitsi verkon fyysistä infrastruktuuria muuttamalla, myös muodostamalla virtuaalisia segmenttejä kytkinten ja reitittimien VLAN-määritysten avulla (Hakala et al., 2006, s. 185). Virtuaalisia lähiverkkoja (VLAN) voidaan muodostaa verkkolaitteiden välillä muun muassa IEEE 802.1Q -standardin mukaisella protokollalla (Cisco Systems, 2006a).

Verkkojen yhdistämiseen tarvitaan aina myös reitittimiä, jotta verkkojen välillä voidaan liikennöidä. Reitittimillä voidaan monesti suodattaa liikennettä kuten palomuureillakin, käytännössä kuitenkin useimmiten ainoastaan sillä verkkokerroksella, jolla reititin itse operoi. Reitittimissä ei aina kuitenkaan suorituskykysyistä johtuen kannata käyttää ainakaan erityisen suuria suodatuslistoja. (Cisco Systems, 2006b)

Langattomat verkkoyhteydet eli WLAN-verkot mahdollistavat vaivattoman työskentelyn esimerkiksi kannettavilla työkoneilla organisaation työtiloissa. Ne toimivat myös erinomaisena välineenä Internet-yhteyden tarjoamiseen organisaation vierailijoille. Langattomien verkkojen ongelmana on kuitenkin se, että ne ovat kuitenkin helposti myös kutsumattomien vieraiden saavutettavissa. Jotkin langattomien verkkojen linkkikerroksen suojausmekanismit (esimerkiksi WEP) ovat turvallisuustasoltaan heikkoja (Lehtonen et al., 2006) ja niiden sijasta suositellaan käytettäväksi monimutkaisempia suojauksia (esimerkiksi WPA2) tai jotain korkeamman tason suojausta, kuten salattua VPN-yhteyttä.

Koska vieraita ei tulisi koskaan päästää organisaation yksityiseen verkkoon käsiksi, eikä langaton verkko ole käytännössä suositeltava keino suojeltavien tietojärjestelmien verkkoihin liittymiseksi, kannattaa langattomat lähiverkot eriyttää kokonaan organisaation yksityisestä verkosta (Hakala et al., 2006, s. 295–296). Tällöin langattomat yhteydet voidaan toteuttaa kokonaisuudessaan pelkästään erillisenä vierailijoille soveltuvana, suojattuna Internet-yhteyskäytävänä. Samaan vierailijoille tarkoitettuun verkkoon voidaan tarvittaessa kytkeä langallisen verkon pistokkeita esimerkiksi neuvotteluhuonekäyttöön. Mikäli omat työntekijät tarvitsevat langattoman pääsyn organisaation verkkoon, voidaan se järjestää kuten muutkin etäyhteydet ulkopuolisista verkoista. Kuva 9 havainnollistaa verkon rakennetta segmentoimisen ja vierailijaverkon hyödyntämisen jälkeen.



Kuva 9. Esimerkki verkon rakenteesta.

4.1.2 Palvelimet ja työkoneet

Palomuureilla voidaan suojella tietokoneita asiattomalta verkkoliikenteeltä. Verkkojen reunalla sijaitsevat palomuurit eivät kuitenkaan suojaa sellaisilta uhilta, jotka tulevat verkkosegmentin sisäpuolelta. Nykyisissä Windows-käyttöjärjestelmissä ja Linux-jakeluissa on kuitenkin mukana ohjelmistot, joilla palomuurin voi toteuttaa myös jokaisella palvelimella erikseen (Hakala et al., 2006, s. 204 & 214). Laitekohtaisen palomuurin ansiosta palvelinten ja työkoneiden suojaaminen voidaan toteuttaa yksittäisen tietokoneen tasolla, jolloin voidaan suojautua myös tilanteilta joissa vihamielinen käyttäjä tai haittaohjelma pääsee käsiksi yrityksen verkkoon. Laitekohtainen palomuuri mahdollistaa myös kannettavien tietokoneiden kytkemisen vieraisiin verkkoihin etäyhteyttä varten siten, että tietokone on suojattu avoimessa verkossa vaanivilta vaaroilta.

Palomuurin ongelmana on kuitenkin se, että sillä voidaan suojautua ainoastaan sellaiselta liikenteeltä, joka voidaan estää tarpeettomana. Mikäli jossain tarpeellisessa palvelussa, jonka liikennöintiä ei ole voitu estää, esiintyy haavoittuvuus, on palvelinkohtainenkin palomuuri hyödytön (Anderson, 2001, s. 368–369). Tämän vuoksi palomuurin hyödyntämisen lisäksi tulisi kuitenkin aina huolehtia myös haavoittuvuuksien mahdollisimman nopeasta paikkaamisesta.

Viruksilta ja muilta haittaohjelmilta suojautuminen pohjautuu käytännössä kahteen tavoitteeseen: haittaohjelmien järjestelmään pääsyn estämiseen sekä suojauksista huolimatta järjestelmään päässeiden haittaohjelmien havaitsemiseen, tunnistamiseen ja poistamiseen (Stallings, 2006, s. 610). ISO 17799 -standardin (2006, s. 92) mukaan näihin tavoitteisiin

päästään estämällä hyväksymättömän ohjelmakoodin suorittaminen ja ottamalla käyttöön virustorjuntaohjelmisto järjestelmän tietokoneissa. Ohjelmien esikatselu ja ohjelmakoodin hyväksyttäminen mahdollistaa hyväksymättömien ohjelmien rajoittamisen, mutta ei estä hyväksytyissä ohjelmissa olevien havaitsemattomien haavoittuvuuksien hyödyntämistä. Virustorjunta taas ei tarjoa suoraa turvaa, mutta sen ajantasaisten tietokantojen avulla haitalliset ohjelmat voidaan useimmissa tapauksissa havaita ennen niiden tahatonta suorittamista.

Käytännössä parhaat toimenpiteet tietoverkkoihin kytkettyjen tietokoneiden suojaamiseksi ovat ohjelmistojen ylläpito ajantasaisilla päivityksillä, ohjelmien suoritusoikeuksien rajoittaminen sekä tietoverkkojen segmentointi mahdollisten vahinkojen rajoittamiseksi. Laitekohtaisilla palomuureilla voidaan parantaa verkkoturvallisuuden tasoa sulkemalla pois kaikki tarpeeton liikenne, jolloin koneelle ei muodostu yllättäviä aukkoja. Virustorjunta-ohjelmistolla voidaan taas pyrkiä estämään haitallisten ohjelmien tahatonta leviämistä.

4.1.3 Virtuaaliset yksityisverkot

Virtuaaliset yksityisverkot eli VPN-verkot ovat loogisia tietoverkkoja, jotka on rakennettu olemassa olevien tietoverkkojen päälle. Yksityisellä verkolla tarkoitetaan sitä, että liikennöinti verkossa on tarkoitettu ainoastaan siihen määritellyille osapuolille, ja että verkon osoitteistus ja reititys ovat erillisiä alla olevasta verkosta. Virtuaalisen verkosta tekee se, että se on muodostettu olemassa olevan verkon päälle ilman fyysistä olemusta. Virtuaalisen yksityisverkon voi muodostaa kahden tai useamman yksityisen verkon, laitteen tai sovelluksen välille. (Huston, 1999, s. 454–457)

Syitä virtuaalisten yksityisverkkojen käytölle on useita. Niiden avulla voidaan muun muassa hyödyntää tietoliikenneresursseja tehokkaammin, saavuttaa kustannussäästöjä organisaation toimipisteiden välisten yhteyksien muodostamisessa ja toteuttaa liikennöinnin yksityisyyttä (Huston, 1999, s. 457–458). Yksi yleisesti käytetty sovellus on etätyöskentelyn mahdollistaminen julkisten verkkojen kautta VPN-yhteyden avulla. Pelkkä virtuaalinen yksityisverkko ei kuitenkaan määritelmänsä mukaisesti tarjoa varsinaista suojaa siinä käydylle tietoliikenteelle, vaan se ainoastaan mahdollistaa yksityisen liikenteen julkisessa verkossa. Välitetty tieto on kenen hyvänsä salakuunneltavissa tai muutettavissa ja liikenteeseen osallistuminen mahdollista aivan kuten minkä tahansa normaalin verkko-liikenteen kanssa, kunhan vain pääsee käsiksi sopivaan verkon solmukohtaan.

Virtuaalisen yksityisverkon muodostamiseen on monia keinoja, jotka mahdollistavat verkkojen muodostamisen muun muassa erilaisissa ympäristöissä. Ne voidaan jakaa kahteen päämenetelmään: reititystietojen määrittelyyn ja tunnelointiin. Reititystietojen määrittelyssä virtuaalinen verkko muodostetaan lisäämällä taustalla olevan fyysisen verkon reititystietoihin tiedot siitä, kuinka yksityisen verkon liikenne tulisi ohjata. Tunneloinnissa yksityisen verkon liikenne liitetään kokonaisuudessaan julkisessa verkossa välitettävän liikenteen hyötykuormaksi. Tämän menetelmän etuna on, että liikenteen reititykseen voidaan käyttää julkisen verkon olemassa olevia reittejä ja ainoastaan tunnelin päissä olevien laitteiden tarvitsee tietää VPN-yhteyden olemassaolosta. Toinen tunneloinnin merkittävä etu on siinä, että sen avulla on helppo suojata julkisessa verkossa kulkevan yksityisen verkon liikenteen eheys ja luottamuksellisuus aina otsaketietoja myöten. (Huston, 1999, s. 463–475)

Yksi esimerkki tietojen suojaamisen mahdollistavasta virtuaalisen yksityisverkon muodostavasta tunneloivasta protokollakokonaisuudesta on IP-verkkojen päällä toimiva IPsec (Huston, 1999, s. 480–481). IPsec-suojausta käytetään muun muassa Cisco Systemsin verkkolaitteissa ja sille on tuki myös Windows-käyttöjärjestelmissä ja Linux-jakeluissa (Hakala, 2006, s. 290). Tämän tuen ansiosta IPsec-suojauksen avulla voidaan tarvittaessa turvata helposti paitsi julkisten verkkojen kautta välitettäviä yhteyksiä, niin myös organisaation yksityisen verkon sisällä muodostettavia yhteyksiä. Täten myös tietoliikenteen suojaaminen voidaan toteuttaa yksittäisen palvelimen ja työkoneen tasolla, aivan kuten konekohtaiset palomuuritkin.

Liikenteen turvaaminen IPsec-suojauksella vaatii ylimääräisiä resursseja – kuten prosessointiaikaa ja muistia – yhteyden muodostavilta laitteilta. Tarvittaessa palvelimiin voi kuitenkin hankkia esimerkiksi erityisen verkkosovittimen tai erillisen ohjaimen, joka mahdollistaa laitteistopohjaisen IPsec-suojauksen. Tällöin suojauksen käytöllä ei ole juurikaan vaikutusta palvelinten suorituskykyyn. (Microsoft, 2006)

4.2 Tietoaineiston suojaaminen

Tietoaineiston, kuten dokumenttien ja tietokantojen suojaaminen on välttämätöntä tiedon luottamuksellisuuden ja eheyden ylläpitämiseksi. Suojaaminen edellyttää käytännössä jonkinlaisten teknisten keinojen hyödyntämistä, ainakin kirjallisessa ja sähköisessä muodossa olevan tiedon osalta. Tietojen luottamuksellisuuden suojaamiseksi voidaan oikeudettomilta osapuolilta estää pääsy itse aineistoon tai salata aineisto sellaiseen muotoon, josta sitä ei voi tulkita ilman sellaista tietoa, jota vain oikeudellisilla on. Yksi

ratkaisu on hyödyntää molempia menetelmiä. Tiedon eheyden varmistamiseksi voidaan käyttää esimerkiksi digitaalista allekirjoitusta tai tarkistussummia.

4.2.1 Pääsynhallinta

Pääsynhallinnan tarkoituksena on erotella oikeudelliset ja oikeudettomat tahot siten, että oikeudellisille sallitaan pääsy niiden haluamaan resurssiin ja oikeudettomilta pääsy vastaavasti estetään (Whitman & Mattord, 2005, s. 135). Tietokoneen kirjautumislomake, tiedosto-oikeudet, lukolliset ovet ja kaapit, sekä vartija, joka päästää ohitseen ainoastaan kulkuun oikeutetut henkilöt, ovat kaikki esimerkkejä pääsynhallinnan mekanismeista. Pääsynhallinta tarvitsee oleellisena osana toimintaansa jonkin riittävän luotettavan menetelmän käyttäjän tunnistamiseen. Jos käyttäjää ei voida tunnistaa, ei myöskään oikeudellisten ja oikeudettomien tahojen erottaminen toisistaan onnistu (Whitman & Mattord, 2005, s. 332).

Käyttäjän tunnistamiseen pyrkivät menetelmät perustuvat käytännössä johonkin kolmesta eri vaihtoehdosta. Ensimmäinen vaihtoehto on tunnistaa käyttäjä jonkin käyttäjällä hallussa olevan esineen perusteella. Tällainen esine voi olla esimerkiksi avain tai älykortti. Toinen vaihtoehto tunnistamiseen on hyödyntää jotain sellaista mitä käyttäjä tietää, esimerkiksi tunnuksen ja salasanan yhdistelmä. Kolmas vaihtoehto on perustaa päätös biometrisiin menetelmiin (Anderson, 2001, s. 36). Biometrisiä menetelmiä on kehitetty useita: tunnistettavina kohteina käytetään muun muassa kasvonmuotoja, kasvojen lämpöjälkeä, sormenjälkeä, kämmenenjälkeä, iiriskoodia, verkkokalvon jälkeä, käsialaa ja äänijälkeä (Jain, Hong & Pankanti, 2000).

Hallussa olevaan esineeseen tai biometrisen tunnistamiseen perustuvien menetelmien hyvä puoli on se, että se ne eivät vaadi tunnistettavalta henkilöltä monimutkaisten koodien tai salasanojen muistamista. Hallussa olevan esineen ongelma on se, että sen voi hävittää tai unohtaa, tai se voidaan varastaa. Biometrisen tunnistuksen huonona puolena on joidenkin menetelmien alttius virheellisille päätöksille, ihmisten varautuneisuus niitä kohtaan ja menetelmien riippuvaisuus ihmisten fyysisistä ominaisuuksista. (Anderson, 2001, s. 273–275)

Käyttäjän muistiin perustuva tunnus–salasanapari on sen alhaisten käyttöönotto-kustannusten vuoksi yleisimmin käyttäjän tunnistamisessa hyödynnetty menetelmä. Salasanojen hallinta muodostaa kuitenkin oleellisen käytännön ongelman, muun muassa siksi, että siihen sisältyy inhimillisiä rajoitteita. Ihminen saattaa vahingossa, tahallaan tai

hyväuskoisuuttaan luovuttaa salasanansa toisen henkilön haltuun. Salasanojen muistaminen voi myös olla hankalaa, mistä seuraa se, että salasana saatetaan kirjoittaa ylös tai salasanaksi valitaan niin helppo sana, että hyökkääjä kykenee arvaamaan sen. Lisäksi ongelmaksi voi muodostua se, että käyttäjällä saattaa tuhraantua aikaa pitkän ja monimutkaisen salasanan syöttämiseen, kun virheiden mahdollisuus kasvaa. (Anderson, 2001, s. 36)

Nämä inhimilliset rajoitteet käytännössä johtavat myös siihen, että salasanat ovat hyvä kohde erilaisille hyökkäyksille. Heikot salasanat voidaan murtaa sanakirjahyökkäyksillä ja huonosti turvallisuusasioista perillä olevilta ihmisiltä salasanoja voidaan urkkia helposti joko sosiaalisin keinoin tai koneellisesti. Adams ja Sasse (1999) havaitsivat tutkimuksessaan, että inhimillisten rajoitteiden huomioiminen on erittäin oleellinen osa toimivan salasanajärjestelmän toteuttamiseksi. Heidän havaintojensa mukaan monissa järjestelmissä käytetyt salasanojen uusimiskäytännöt todellisuudessa heikentävät tietoturvallisuutta, sillä ihmiset joutuvat tiheästi salasanoja uusiessaan valitsemaan helpommin muistettavia salasanoja, ja pahimmillaan jopa kirjoittamaan ne ylös. Useiden samanaikaisesti käytettävien salasanojen tarve heikentää niiden muistamista ja lisää kognitiivista kuormaa. Mitä harvempi kunkin salasanan käyttötarve on, sitä vähemmän ihmisellä voi salasanoja olla kerralla käytössä.

Kertakirjautuminen ja fyysiset kirjautumismekanismit kuten älykortit ovat suositeltavia apumekanismeja silloin, kun kirjautumista tarvitsevia järjestelmiä on useita. Tällöin voidaan minimoida tarvittavien salasanojen määrä minimiin ja käyttää järjestelmässä hyvinkin turvallisia salasanoja. Salasanaa vaihdettaessa käyttäjälle tulisi antaa rakentavia ohjeita hyvän salasanan valitsemisesta. Tämän avulla käyttäjille muistuu mieleen oikeat menetelmät salasanojen muodostamiseen ja tuloksena on parempi salasana. Tunnuskäytännöissä pitäisi myös huomioida käytetyt työskentelytavat. Henkilökohtaisia tunnuksia ja salasanoja pitäisi suosia ensisijaisesti, mutta tarvittaessa poikkeustilanteissa voidaan sallia myös yhteiskäyttötunnusten ja salasanojen luominen. Jos tunnuskäytännöt ovat liian jäykkiä, vaarana on että ihmiset ryhtyvät jakamaan henkilökohtaisia salasanojaan. Ihmisten heikko tietous turvallisuusasioista taas johtaa helposti siihen, että he saattavat kertoa salasanojansa niitä kysyville, jopa tuntemattomille puhelimen välityksellä. Tietoturvatietoisuuden lisäämisestä on siten hyötyä myös tässä suhteessa. (Adams & Sasse, 1999)

4.2.2 Tiedon salaus ja eheys

Toisinaan tietoa joudutaan salaamaan, jotta sen luottamuksellisuus ei vaarantuisi tai jotta sen eheydestä voidaan varmistua. Tietoliikenteessä tämä on hyvin tavallista, sillä tietoa joudutaan usein siirtämään turvattomien ja jopa julkisten yhteyksien kautta. Tietoaineiston suojaaminen riittävän vahvalla salauksella mahdollistaa muun muassa tiedon säilyttämisen sellaisessa paikassa, jossa se on tavallista alttiimpana varkaudelle, kuten esimerkiksi työkoneen kiintolevyllä – etenkin jos kyseessä on kannettava tietokone. Salauksella voidaan suojautua myös pääsynhallintaan liittyviltä heikkouksilta, kuten ohjelmistoaukoilta ja pääsyoikeuksien joutumiselta oikeudettoman osapuolen haltuun. Vaikka oikeudeton taho sattuisi saamaan pääsyn johonkin säilöön, jossa säilytetään suojeltavaa tietoa, ei luottamuksellisuus kuitenkaan vielä vaarannu mikäli tietoaineisto on riittävän hyvin salattu.

Tiedon salausmenetelmät jaetaan niiden toimintaperiaatteen mukaan symmetrisiin ja asymmetrisiin salauksiin. Tiedon salaaminen perustuu useimmissa tapauksissa siihen, että salausalgoritmille annetaan salattava tieto ja jokin salausavain. Symmetrisissä salauksissa tieto salataan ja salaus puretaan käyttämällä samaa salausavainta (Stallings, 2006, s. 29). Asymmetrisissä salauksissa käytetään sen sijaan kahta avainta: julkista ja salaista avainta. Kummalla tahansa avaimella muodostettu salaus voidaan purkaa ainoastaan toisella avaimella (Stallings, 2006, s. 258). Avainten nimet kuvastavat niiden käyttötarkoitusta, jossa toinen avain on tarkoitettu jaettavaksi julkisesti kaikille halukkaille ja toinen pidetään salassa.

Erilaisia salausalgoritmeja on olemassa runsaasti ja ne eriävät toisistaan enemmän tai vähemmän ainakin toteutustavan mukaan. Oikean algoritmin valinnalla on merkitystä: esimerkiksi hyvin raskaat salaukset eivät välttämättä sovellu reaaliaikaisiin sovelluksiin tai niiden vaatima laskentateho voi olla liikaa mobiililaitteille. Toiset algoritmit saattavat myös olla helpommin oikeudettomasti purettavissa kuin toiset, esimerkiksi DES-algoritmin käyttöä ei sellaisenaan enää suositella sen käyttämän liian pienen avainkoon vuoksi (Stallings, 2006, s. 82). Avointen salausmenetelmien taustalla on usein huomattavasti enemmän julkista testausta ja koska niiden toimintaperiaate on suunniteltu lähtökohtaisesti siten, että algoritmi on julkinen, on avoin algoritmi usein parempi vaihtoehto kuin salaiset algoritmit. Salaisena pidetyt salausalgoritmit ovat monesti tehokkaita ainoastaan siihen hetkeen asti, kunnes joku selvittää ja vuotaa algoritmin toimintaperiaatteen julkisuuteen (Schneier, 2004, s. 115–119).

Symmetrinen salaus sopii hyvin tiedon salaamiseen sellaisissa tapauksissa, jossa tieto halutaan säilöä yhden avaimen taakse. Se soveltuu siten hyvin muun muassa dokumenttien salaamiseen tietosäilössä. Jos kuitenkin symmetrisin keinoin salattua tietoa halutaan välittää jollekin muulle taholle, on tällä niin ikään oltava hallussa salauksessa käytetty avain. Tällaisessa käyttötarkoituksessa asymmetrinen salaus on parempi ratkaisu, sillä tällöin salausavainta ei tarvitse välittää erikseen tiedon vastaanottajalle. On kuitenkin huomattava, että julkinen avain täytyy silti välittää luotettavaa kanavaa pitkin, jotta kolmas osapuoli ei voi huijata antamalla omaa julkista avaintaan toisen osapuolen nimissä. (Stallings, 2006, s. 259)

Suojattaessa tiedon eheyttä käytetään algoritmia, joka laskee halutusta tiedosta tarkistussumman jollain luotettavalla menetelmällä. Laskemalla tarkistussumma samalla menetelmällä ja vertaamalla sitä alkuperäiseen tarkisteeseen voidaan varmistua siitä, onko viestin eheys vaarantunut vai ei (Whitman & Mattord, 2005, s. 12). Tämä tietysti edellyttää myös sitä, että alkuperäistä tarkistussummaa ei pääse muuttamaan. MAC-algoritmeilla (*message authentication code*) tarkistussumma lasketaan lähdetiedon ja salaisen avaimen pohjalta, aivan kuten symmetrisessä salauksessa. Tässä menetelmässä tiedon eheyden varmistaminen perustuu käytetyn salausavaimen luottamuksellisuuteen. Jos avaimen luottamuksellisuus ei ole vaarantunut, voidaan tiedon lähde rajata salausavaimen tunteviin henkilöihin (Stallings, 2006, s. 318).

Asymmetrinen salaus mahdollistaa digitaalisten allekirjoitusten käyttämisen, jonka avulla tiedon alkuperän ja eheyden määrittäminen onnistuu tarkemmin. Salattaessa tieto asymmetrisen avainparin salaisella avaimella, on se kenen tahansa purettavissa kyseisen parin julkisella avaimella. Tämän ansiosta viestin lähettäjä tai dokumentin laatija voi allekirjoittaa tiedon sisällön salaamalla koko viestin ja siitä luotettavalla menetelmällä lasketun tarkistussumman omalla salaisella avaimellaan. Tällöin julkisen avaimen haltijat voivat varmistua tiedon alkuperästä ja eheydestä (Stallings, 2006, s. 378). Luotettavana menetelmänä tarkistussummien laskemiseen voidaan pitää yhdensuuntaisia hajautus-funktioita, kuten esimerkiksi SHA- tai Whirlpool-menetelmät (Stallings, 2006, s. 352).

4.3 Tiedon saavutettavuuden varmistaminen

Tiedon saavutettavuuden varmistaminen on ehdoton lähtökohta organisaation tietojärjestelmien toiminalle. Tekniset laitteet ja niiden ohjelmistot tarvitsevat säännöllistä huoltoa, kehittämistä ja ne voivat toisinaan myös vikaantua tai ruuhkaantua. Tällöin

tarvitaan korjaustoimenpiteiden lisäksi myös jonkinlaisia varajärjestelyitä, mikäli tieto halutaan pitää saavutettavissa.

Toiminnan jatkuvuuden kannalta on usein hyvin tärkeää, että liiketoiminnassa käytettävä tieto ei häviä vakavienkaan vahingollisten tapahtumien yhteydessä. Organisaatiolle, jonka toiminta perustuu tiedon hallintaan ja käsittelemiseen, tiedon säilyvyys on elinehto. Varajärjestelmien ylläpito ja tiedon varmistaminen ovat keinoja, joilla voidaan oikein toteutettuna varautua erilaisiin tiedon saavutettavuutta uhkaaviin tuhoisiinkin tapahtumiin.

4.3.1 Tietojärjestelmien saavutettavuuden takaaminen

Tietojärjestelmän saavutettavuus koostuu aina sen toimintaan vaikuttavien osa-alueiden toimivuudesta. Eri lähteitä (Oggerino, 2001, s. 43–45; Jones, 2000, s. 26–32; Marcus & Stern, 2003, s. 20–28 & 31–60 & 264) yhdistelemällä järjestelmän saavutettavuuteen vaikuttavat tekijät voidaan jakaa seuraaviin osa-alueisiin:

- Tekninen toimivuus (verkko, laitteisto ja ohjelmisto)
- Järjestelmän suojaukset hyökkäyksiä ja onnettomuuksia vastaan
- Järjestelmän suunnittelu ja muuttaminen
- Järjestelmän ylläpito
- Vikatilanteiden havaitseminen ja niistä toipuminen

Vaadittavan saavutettavuuden tason ylläpitämiseksi on huolehdittava, että kaikkiin näihin osa-alueisiin liittyvät uhat ovat riittävällä tasolla hallinnassa. Tietojärjestelmän saavutettavuuden tason määrittämisessä tulisi aina lähteä siitä, mikä on kyseisen järjestelmän käyttötarkoitus ja sen vaatima palveluntaso. Määrittelyssä tulisi selvittää, minkälaiset katkokset tiedon saatavuudessa ovat haitallisia ja minkälaiset siedettäviä. Vastaukset näihin löytyvät organisaation tietoriskien hallinnan päätöksistä.

Laitteiden tekninen toimivuus riippuu sen komponenttien muodostaman kokonaisuuden yhteenlasketusta toimivuudesta. Väistämättä tähän sisältyy myös laitteiden sisältämän ohjelmiston toiminta. Jokaisella komponentilla on elinkaari, jonka kuljettuaan komponentti vikaantuu. Tämän jälkeen komponentti on korjattava tai vaihdettava uuteen. Aika, joka kuluu kunkin komponentin käyttöönotosta sen vikaantumiseen, on yksilöllinen ja sitä voidaan käytännössä ainoastaan arvioida komponentille tehtävien elinikäsimulaatioiden pohjalta. Tällainen arvo on komponentin *Mean Time To Failure* eli MTTF-arvo. Mitä suurempi MTTF-arvo on, sitä luotettavampi myös komponentti keskimäärin on (Storey,

1996, s. 164–166). On hyvä huomata, että MTTF-arvon sijasta käytetään usein virheellisesti *Mean Time Between Failures* eli MTBF-arvoa, joka määritelmänsä mukaisesti on komponentin vikaantumistiheyden ja korjaamisajan summa.

Sarjaan asennetut komponentit aiheuttavat aina koko toimintaketjun toimimattomuuden, mikäli yksikin komponentti vikaantuu. Jos esimerkiksi laitteessa on yksi virtalähde, lakkaavat laitteen muut toiminnot toimimasta kun virtalähde vikaantuu. Rinnakkain asennetut komponentit sen sijaan mahdollistavat toiminnan jatkumisen myös komponenttien vikaantuessa, kunhan toiminnan edellyttämä vähimmäismäärä komponentteja on vielä toimintakunnossa. Jos edellisen esimerkin laitteessa onkin kaksi virtalähdettä, jatkaa se toisen virtalähteen vikaantuessa toimintaansa, kunhan komponentit vain ovat riittävän tehokkaita toimimaan yksinään. (Storey, 1996, s. 167–177)

Monistamalla järjestelmän osia ja asentamalla niitä rinnakkain voidaan varautua yksittäisten tai jopa useampien järjestelmän komponenttien vikaantumiseen. Tällöin toiminta voi jatkua järjestelmän käyttäjän näkökulmasta normaalisti eikä tiedon saatavuuteen tule katkosta. Tällaista järjestelmän osaa kutsutaan vikasietoiseksi. Tiedon saatavuutta voidaan siten teknisesti parantaa valitsemalla luotettavampia komponentteja ja lisäämällä järjestelmän vikasietoisuutta.

Varautumista järjestelmää kohtaan tehtäviä tietoteknisiä hyökkäyksiä – kuten esimerkiksi tietomurtoja tai haittaohjelmia – varten pidetään tyypillisesti puhtaasti tiedon luottamuksellisuuden ja eheyden suojaamistoimenpiteenä. Käytännössä suojautumisella on selkeä merkitys myös tiedon saavutettavuudelle, sillä usein hyökkäyksistä seuraa tiedon saavuttamattomuutta. Syynä tähän voi olla esimerkiksi tiedon tuhoutuminen tai muuttuminen hyökkäyksen yhteydessä tai sen seurauksena, epävarmuus tiedon eheydestä tai järjestelmän eheyden menettäminen.

Koska järjestelmän ja sen sisältämien tietojen eheys on saatava varmistettua tietomurron jälkeen, voi saavutettavuustason ylläpitäminen olla haastavaa siivoustoimenpiteiden, esimerkiksi ohjelmistojen uudelleenasennusten aikana. Usein myös järjestelmän se osa, johon hyökkäys on kohdistunut, joudutaan eristämään ainakin joksikin aikaa muusta järjestelmästä (Valtiovarainministeriö, 2005, s. 51–56). Mikäli tällaiseen joudutaan varautumaan, onnistuu se käytännössä parhaiten hyödyntämällä varajärjestelmää, jonka eheydestä voidaan olla varmoja. Tämän edellytyksenä on se, että varajärjestelmä on ollut riittävällä tasolla eriytetty hyökkäyksen kohteeksi joutuneesta järjestelmästä; esimerkiksi replikoitua tietoa ei välttämättä voida käyttää.

Myös fyysisiin hyökkäyksiin varautuminen on osa järjestelmän saavutettavuuden takaamista. Eri lähteiden (Tate, Cartwright, Cronin & Dapprich, 2003, s. 8; Valtiovarainministeriö, 2002, s. 9–17) mukaan tietojärjestelmiin kohdistuu seuraavanlaisia varteenotettavia fyysisiä uhkia:

- luonnononnettomuudet,
- vahingonteko tai varkaus,
- tulipalo, lämpötilan nousu, räjähdykset tai tärinä,
- nestevuodot ja putkistotukokset,
- sähköverkon häiriöt,
- ilman epäpuhtaudet, kaasuvuodot, säteilyonnettomuudet,
- liikenneonnettomuudet ja
- sähkömagneettiset hyökkäykset.

Koska osa näistä uhista saattaa toteutuessaan hävittää kokonaisia rakennuksia ja järjestelmän toiminnan kannalta oleellisia työntekijöitä, tulisi tiedon kriittisyyden mukaan järjestelmien toimintoja ja mahdollisesti organisaation henkilöstöä hajauttaa ja kahdentaa toisaalla sijaitseviin kohteisiin. Tämäntyyppisten onnettomuuksien varalta organisaatiolla tulisi myös olla suunnitelma toiminnan jatkuvuudelle (Virtanen, 2004, s. 78–81).

Tietojärjestelmän suunnittelu ja sen muutosten hallinnan toimenpiteet vaikuttavat oleellisesti järjestelmän toiminnan ongelmattomuuteen. Lähtökohtaisesti saavutettavuuteen voidaan suunnitteluvaiheessa vaikuttaa muun muassa selkeydellä ja yksinkertaisuudella, palveluiden keskittämisellä toimintavarmoihin laitteisiin, kehitysympäristöjen eriyttämisellä, turvallisuusasioiden huomioimisella, riittävällä mitoituksella, laajennettavuuden huomioimisella, laitekannan nopealla huollettavuudella, teknisillä varmistuksilla kuten klustereiden tai kahdennusten avulla sekä aukottomalla järjestelmän seurannalla ja valvonnalla. Muutoksista aiheutuvat turhat katkokset voidaan estää muun muassa muutostöiden ennakkosuunnittelulla, muutosten vaikutusten ennakoimisella ja toiminnan testaamisella. (Marcus & Stern, 2003, s. 78–79, 81–84, 88–91, 93, 96 & 101–103)

Jokaisen tietojärjestelmän toiminnan edellytyksenä on jatkuva ylläpito (Marcus & Stern, 2003, s. 264). Ylläpitoa tarvitaan ainakin erilaisiin järjestelmässä suoritettaviin rutiinitoimenpiteisiin kuten varmuuskopiointiin, toiminnan seuraamiseen, huoltamiseen ja vikatilanteiden korjaamiseen. Ylläpito vastaa usein myös monista muista järjestelmän toimintaan liittyvistä käytännön asioista.

Suurimmat vaikutukset saavutettavuuteen ylläpidon osalta tulevat huoltotoimenpiteistä, inhimillisistä erehdyksistä, laiminlyönneistä, huolimattomuudesta ja tarvittavan asiantuntemuksen puutteesta. Kolmen viimeisen tekijän osalta kyse on ongelmasta, joka tulisi havaita ja ratkaista ajoissa. Inhimillisten erehdysten esiintymistä voidaan vähentää muun muassa järjestelmää yksinkertaistamalla (Marcus & Stern, 2003, s. 103), kurinalaisilla toimenpideohjeilla, automatisoinnilla ja kokemuksella (Kamoun, 2005) sekä toimenpiteiden rajoituksilla ja koulutuksella (Im & Baskerville, 2005).

Tiedon saavuttamattomuuteen johtavan vikatilanteen kesto riippuu pitkälti siitä miten vikaan on varauduttu. Kun komponentti vikaantuu, kuluu aikaa vikatilanteen havaitsemiseen, diagnosointiin ja vian korjaamiseen. Vian diagnosointi sisältää myös mahdollisen kohteeseen matkustamisen ja vian paikallistamiseen kuluvan ajan, ja vastaavasti vian korjaus sisältää muun muassa korvaavien komponenttien hankkimiseen sekä korjaajan hälyttämiseen ja paikalle saapumiseen kuluvan ajan. (Jones, 2001, s. 13; Oggerino, 2001, s. 12)

Mitä vähemmän mikäkin vikatilanteen vaihe kestää, sitä nopeammin järjestelmä saadaan toimintakuntoon ja sitä parempi on tiedon saavutettavuus. Vian havaitsemista voidaan nopeuttaa tehokkaalla valvonnalla. Diagnosointivaihetta voidaan nopeuttaa esimerkiksi vikatilanneohjeistuksella ja minimoimalla diagnosoinnin aloittamiseen kuluva aika esimerkiksi järjestämällä kohteeseen päivystys. Korjausta voidaan nopeuttaa esimerkiksi suosimalla nopeasti korjattavia laitteita ja varastoimalla tarvittavia varaosia.

4.3.2 Tietojen varmistaminen

Tiedon menetys on ongelma, joka voi kohdata jokaista järjestelmää. Tietoa voidaan menettää muun muassa levyrikon, levyjärjestelmän tuhoutumisen, korruptoitumisen, haittaohjelman, tulipalon tai inhimillisen erehdyksen vuoksi (Tate et al., 2003, s. 8). Myös tiedon hallitsematon muuttuminen johtaa käytännössä alkuperäisen tiedon menettämiseen. Tietojen varmistamisella pyritään hävityksen aiheuttajasta riippumatta suojautumaan tiedon katoamiselta ja pitkäkestoiselta saavuttamattomuudelta.

Yksittäisen, muuttumattoman tiedon varmistaminen on monesti yksinkertaista, sillä tällöin usein riittää tiedon kopioiminen sellaiseen olomuotoon, jossa se säilyy, sekä sijoittaminen turvalliseen säilöön, josta se on mahdollista ottaa käyttöön riittävän lyhyessä ajassa. Suojeltavan tiedon varmuuskopion säilyttämisessä on luonnollisesti huomioitava samat turvallisuusseikat kuin alkuperäisenkin tiedon kanssa. Varmuuskopiot tulisi joka

tapauksessa säilyttää aina vähintäänkin eri tiloissa alkuperäiseen tietoon nähden, jotta tieto olisi suojattu erilaisten onnettomuuksien (esimerkiksi tulipalon) varalta.

Käytännössä varmistettavia kohteita on kuitenkin lähes poikkeuksetta useita ja ne saattavat muuttua hyvinkin lyhyessä ajassa. Seurauksena varmuuskopioiden ottaminen hankaloituu, sillä mukaan tulee uusi ulottuvuus: aika. Tiedon varmistamiseen ja varmuuskopioiden suojaamiseen kuluu aikaa ja resursseja. Resursseja voidaan säästää harventamalla tietojen varmennusväliä, mutta samalla kasvaa myös varmistuskertojen välinen aika, jolloin tieto voi muuttua. Tällöin tiedon muuttumisnopeudesta riippuen varmuuskopioiden joukosta ei välttämättä enää löydy ajan tasalla olevaa tietoa.

Tiedon varmistamiseen käytetystä menetelmästä ja sen käyttötiheydestä riippuu, kuinka pitkälle menneeseen aikaan joudutaan palaamaan. Marcus ja Stern (2003, s. 55–57) esittävät viisi eri tiedonvarmistustapaa ja niiden vaikutukset palautettavan tiedon ikään tiedonmenetyshetkellä:

- Synkroninen replikointi tai peilaus: alle sekunnista sekunteihin
- Asynkroninen replikointi: sekunneista minuutteihin
- Säännöllinen replikointi: minuuteista tunteihin
- Nauhavarmistus: tunneista viikkoihin
- Ei varmistusta: kaikki data on menetetty

Replikoinnit ja peilaus ovat ylikirjoittavia varmistusmenetelmiä, eivätkä siitä syystä tarjoa ratkaisua hallitsemattomasti muuttuneen mutta teknisesti kunnossa olevan (esimerkiksi inhimillisen erehdyksen tai haittaohjelmien seurauksena) datan tapauksessa (Marcus & Stern, 2003, s. 106), ellei poikkeamaa ehditä huomata ajoissa ennen seuraavaa replikointia. Tästä syystä replikoinnin yhteydessä tulisi aina käyttää myös jotain arkistoivaa varmistusmenetelmää. Synkronisen replikoinnin ongelmana on lisäksi myös sen kirjoitusoperaatioiden suorituskykyä heikentävä vaikutus (Marcus & Stern, 2003, s. 56).

Nauhavarmistus on yksi yleisimmin käytetyistä menetelmistä tiedonvarmistukseen (Whitman & Mattord, 2005, s. 223). Sen etuna on se, että nauhat joille tieto tallennetaan, voidaan helposti vaihtaa ja kuljettaa suojaan. Tästä johtuen myös tiedon arkistointi on mahdollista eikä samoja nauhoja tarvitse käyttää heti uudelleen. Tällöin, mikäli tiedon menettäminen huomataan vasta normaalia pidemmän ajan kuluttua, voi sen pelastaminen olla vielä mahdollista. Nauhavarmistuksen huonona puolena voidaan pitää sen hitautta. Sen

kanssa voidaan käyttää myös menetelmää, jossa tiedot tallennetaan vastaavalla tavalla myös kiintolevylle. Tällöin varmistusten palauttaminen on tarvittaessa nopeampaa.

4.4 Yhteenveto

Tietoturvallisuuden toteuttamiseksi tarvitaan erilaisia kontrolleja. Kontrolleilla voidaan säädellä esimerkiksi ihmisten tai teknisten välineiden toimintaa tavoitteena saavuttaa liiketoiminnan kannalta haluttu suojaustaso. Tässä luvussa käsiteltiin kohdeorganisaation tietoturvallisuuden toteuttamisen kannalta tarpeellisia kontrolleja, jotka liittyvät tietoverkkojen ja tietoaineistojen suojaamiseen ja tiedon saavutettavuuden varmistamiseen. Tietoliikenteen suojaaminen on merkittävä osa tiedon suojaamista nykyaikaisessa tiedonkäsittelyssä, sillä suuri osa tiedon käsittelystä edellyttää tiedon liikkumista. Organisaation tietoaineiston, kuten dokumenttien ja tietokantojen suojaaminen on välttämätöntä niiden sisältämän tiedon luottamuksellisuuden ja eheyden ylläpitämiseksi. Tiedon saavutettavuuden varmistaminen on ehdoton lähtökohta organisaation tietojärjestelmien toiminalle. Toiminnan jatkuvuuden kannalta on myös tärkeää, että liiketoiminnassa käytettävä tieto ei häviä vakavienkaan vahingollisten tapahtumien yhteydessä. Tämän luvun sisällön avulla on tarkoitus pystyä ymmärtämään esiteltyjen tietoturvakontrollien toiminta ja niiden merkitys tietoturvallisuudelle.

5 TIETOTURVAKARTOITUS KOHDEORGANISAATIOSSA

Tässä luvussa käsitellään kohdeorganisaatiossa tehdyn tietoturvakartoituksen toteutusta. Luvussa esitellään kartoitustyön lähtökohdat ja tavoitteet, käytetyt tiedonkeruumenetelmät ja varsinaisen tiedonkeruun kulku. Lopuksi esitellään kartoitustyön tulokset.

5.1 Kartoituksen lähtökohdat

Kohdeorganisaatio on erään Suomessa toimivan suurikokoisen kansainvälisen kustannusalan yrityksen liiketoimintayksikkö. Organisaatio tuottaa Internet-palveluja sekä kuluttaja- että yritysasiakkaille ja se toimii yhdessä erään emoyhtiön kustantaman aikakauslehden kanssa. Tuotetut palvelut on keskitetty yhdelle verkkosivustolle. Kuluttaja-asiakkaille suunnatut palvelut ovat maksuttomia sisältöpalveluita, joskin osan palveluista käyttö edellyttää voimassaolevaa lehden tilausta. Yrittäjäasiakkaille myydään mainosnäyttöjä Internet-sivuille ja palvelua, jonka kautta yritykset saavat organisaation verkkosivuston kautta asiakaskontakteja.

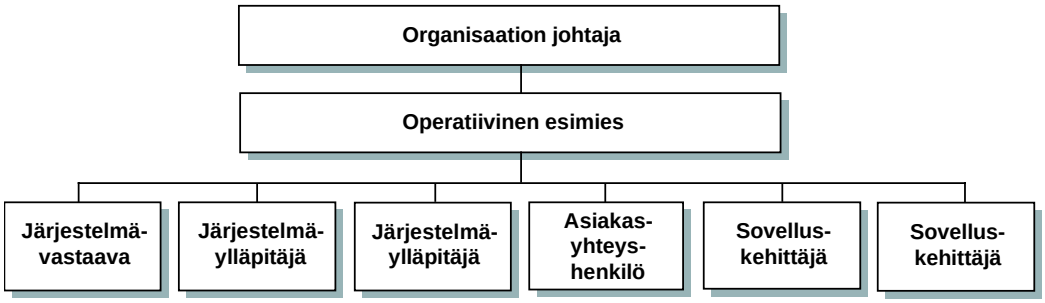
Kohdeorganisaatio tuottaa tarjoamansa palvelut kokonaisuudessaan itse ja palveluiden tuotantoon liittyvä ohjelmistokehitys on tehty ensisijaisesti organisaatioiden omien työntekijöiden toimesta. Organisaation oman tietojärjestelmän laitteisto sijaitsee kokonaisuudessaan emoyrityksen hallitsemassa laitesalissa, ja kyseisen järjestelmän teknisestä toteutuksesta ja ylläpidosta huolehtii organisaation omat työntekijät. Organisaatio tarjoaa asiakkailleen myös asiakaspalvelun, johon voi olla yhteydessä puhelimitse ja sähköpostilla. Tämän lisäksi organisaatio käyttää palveluidensa sisällöntuotantoon ja -hallintaan säännöllisesti muutamia freelance-työntekijöitä.

Kohdeorganisaation toiminta on täysin erillinen emoyrityksen tietojärjestelmistä, eikä yrityksen tietoteknisistä toiminnoista vastaava taho myöskään osallistu organisaation toiminnan ohjaamiseen. Emoyritys on ulkoistanut omien tietojärjestelmiensä sekä Internet-palvelujensa toteutuksen ja ylläpidon ulkopuolisille palveluntoimittajille. Emoyrityksen tietopalveluiden käyttöön liittyviä asioita käsitellään tämän tutkimuksen puitteissa ainoastaan silloin kun sille on tarvetta, pääpainon pysyessä kohdeorganisaation omassa järjestelmässä.

Emoyritys hallitsee kohdeorganisaation työtiloja ja kalusteita. Yritys tarjoaa organisaation käyttöön myös joitakin tietopalveluita, muun muassa SAP-liiketoimintajärjestelmän ja

peruspalvelut kuten yrityksen sähköpostin ja tiedostopalvelun. Kohdeorganisaation oman tietojärjestelmän palvelimien, Internet-yhteyden ja muiden komponenttien hankinta ja ylläpito kuuluu organisaatiolle itselleen. Peruspalveluiden osalta kohdeorganisaatio on omavarainen, joskin esimiehet käyttävät käytännön syistä myös yrityksen tarjoamia palveluita. Yritys on esittänyt vaatimuksen, että organisaation tietojärjestelmän täytyy olla toteutettu ja toimia lakien mukaisesti, ja että asiakasrekisterien tietoturvallisuudesta on pidettävä hyvää huolta.

Organisaation hallinnollisista toiminnoista vastaa yksikön päällikkö ja hänen alaisenaan toimiva operatiivinen esimies. Ohjelmistokehityksestä organisaatiossa vastasi tutkimuksen tekohetkellä kaksi henkilöä. Tietojärjestelmien ylläpitotiimiin kuului kolme työntekijää, joista yksi toimi järjestelmävastaavan[1] ja kaksi järjestelmäylläpitäjän roolissa. Järjestelmävastaava vastaa tietojärjestelmän ja siihen liittyvien asioiden suunnittelusta, toteutuksesta ja teknisestä toimivuudesta. Ylläpitäjät huolehtivat järjestelmävastaavan kanssa järjestelmälle tehtävien toimenpiteiden valmistelemisesta ja toteuttamisesta sekä erilaisten rutiinitoimenpiteiden tekemisestä. Organisaation asiakaspalvelutehtäviä hoitaa ensisijaisesti yksi henkilö, jonka tehtäviin kuuluu lisäksi myös sisällöntuotantoprosessiin liittyviä työvaiheita. Kuva 10 esittää organisaation rakenteen.



Kuva 10. Kohdeorganisaation organisaatiokaavio.

Koska yrityksen liiketoiminta perustuu Internet-palveluiden tarjoamiseen, on sen tulonlähde luontaisesti kytketty tietojärjestelmien toimivuuteen ja sen sisällön oikeellisuuteen. Järjestelmän toimivuuden ja liiketoiminnan kannalta myös tiedon luottamuksellisuudella on tärkeä rooli organisaation toiminnassa. Osaan organisaation tiedonkäsittelyyn sisältyy juridisia velvoitteita, joten vaatimustenmukaisuuden täyttäminen prosessien eri vaiheissa on myös tärkeää. Organisaatio haluaa lisäksi ylläpitää sen brändiin liittyvää tekniseen osaamiseen ja alan asiantuntevuuden mielikuvaa.

[1] Tutkimuksen tekijä toimi kirjoitushetkellä organisaation järjestelmävastaavana.

5.2 Kartoituksen tavoitteet

Tutkimuksen käytännön osan tavoitteena on selvittää kohdeorganisaation tietoturvallisuuden nykytila ja antaa esitys siitä, miten sitä voisi kehittää. Kohdeorganisaatiossa tehtävä tietoturvakartoitus ja sen pohjalta tehtävä nykytilan analyysi vastaa ensimmäiseen näistä tavoitteista. Nykytilan analyysiin pohjautuvat kehitysehdotukset vastaavat jälkimmäiseen tutkimuskysymykseen.

Yhtenä tutkimuksen käytännön osan syvällisemmistä tavoitteista on, että organisaatio pystyisi kartoituksen ja siitä tehtävän analyysin perusteella paikallistamaan kehitystä edellyttävät kohteensa ja tarvittaessa sen pohjalta myös käynnistämään organisaatiossa jatkuvan tietoturvallisuuden prosessin. Jotta tietoturvakartoituksen voitaisiin katsoa olevan riittävän kattavasti suoritettu ja siten täyttävän tutkimuksen tavoitteet, olisi sen hyvä pohjautua johonkin yleisesti hyväksyttyyn menettelyohjeeseen. ISO 17799 -standardi sisältää yleisesti hyväksyttyjä tietoturvahallinnan valvontatavoitteita, joita voidaan hyödyntää organisaatioiden tietoturvahallinnan käynnistämisessä, käyttöönottamisessa, ylläpidossa ja kehittämisessä. Standardi sisältää ohjeita ja yleisiä toimintaperiaatteita, ja sitä voidaan pitää käytännön ohjeistuksena organisaation tietoturvallisuuden kehittämiseksi (ISO 17799, 2006, s. 20). Tämän ansiosta standardi soveltuu erinomaisesti minkä tahansa organisaation tietoturvallisuuden tason kartoittamisen pohjaksi, ja siksi sitä on käytetty tämän tietoturvakartoituksen tiedonkeruun pohjana.

Kohdeorganisaation mukaan erityisen kiinnostavia tietoturvallisuuden aihealueita ovat

- turvallisuusjohtamisen menetelmät ja hallinnollinen tietoturvallisuus,
- tiedon käsittely- ja luokittelumenetelmät,
- tietoturvamenetelmät päivittäisessä työnteossa (ylläpito- ja ohjelmointityö), toteutettujen teknisten suojausten tila (järjestelmän tekniset suojaukset ja työ- ja tuotantotilojen suojaukset),
- käyttöoikeuksien ja pääsyn hallinta,
- työntekijöiden tietoturvaosaaminen ja asenteet tietoturvaa kohtaan ja
- tietoturvaan liittyvät ongelmatilanteet ja niiden hallinta.

Näille aihealueille on siten annettu kartoituksessa keskimääräistä enemmän painoarvoa.

5.3 Tiedonkeruumenetelmät

Tässä tutkimuksessa on käytetty viittä eri tiedonkeruumenetelmää: dokumentaation läpikäyntiä, järjestelmän läpikäyntiä, toimitilojen läpikäyntiä, työ- ja toimintatapa-tarkastelua ja haastattelua. Näitä menetelmiä hyödyntämällä tavoitteena oli saada aikaan kattava katsaus kohdeorganisaation tietoturvallisuuteen vaikuttavista asioista. Menetelmät valittiin siten, että niiden avulla saadaan kattavasti tietoa organisaation tietoturvan nykytilasta, jotta kartoituksen tavoitteet täyttyisivät.

Dokumentaation läpikäynti on menetelmä, jossa organisaation tuottama dokumentaatio käydään läpi tutkimuksen kannalta oleellisen materiaalin löytämiseksi. Tämän materiaalin pohjalta voitiin selvittää muun muassa miten tietoturvaan liittyviä asioita on organisaatiossa toteutettu, minkälaisia raportoituja poikkeamia on ollut ja minkälaisia tietoturvaan liittyviä asioita organisaatiossa on ylipäänsä dokumentoitu. Koska dokumentaation läpikäynnissä tarkoituksena oli etsiä kaikkia järjestelmän turvallisuuteen liittyviä seikkoja, ei läpikäyntiä varten ollut hyödyllistä määritellä erityisen tarkkoja rajauksia käsiteltäville dokumenteille, eikä erityisille tarkistuslistoille siten ollut tarvetta.

Järjestelmän läpikäynnillä tarkoitetaan menetelmää, jossa järjestelmän palvelimien ja verkkolaitteiden tietoturvallisuuteen liittyvät asetustiedostot ja muut tietoturvallisuuden tekijät käydään läpi. Samalla tutkitaan myös järjestelmää kokonaisuutena sekä järjestelmän sisältämiä teknisiä suojauksia. Menetelmän tarkoituksena on saada tieto siitä, ovatko järjestelmän tekniset suojaukset riittäviä ja oikein toteutettuja. Läpikäynnissä käytettiin ISO 17799 -standardia pohjana selvitettäville asioille.

Toimitilojen läpikäynnissä tarkoituksena on selvittää, miten toimitilojen tekniset suojaukset on toteutettu. Toimitiloihin luetaan mukaan kaikki organisaation toimintaan liittyvät tilat, kuten työhuoneet, kiinteistön sisäänkäynnit, kulku- ja säilytystilat sekä ennen kaikkea tuotantotilat kuten laitesali ja tietoliikenteen kytkentäpisteet. Myös toimitilojen läpikäynnissä käytettiin ISO 17799 -standardia pohjana selvitettäville asioille. Läpikäynti suoritettiin tutustumalla tiloihin käytännön tasolla.

Työ- ja toimintatapatarkastelulla tarkoitetaan menetelmää, jossa tutkimuksen tekijä tarkkailee organisaation työ- ja toimintatapoja ja kirjaa ylös tekemänsä havainnot. Tutkimuksen tekijä osallistui tutkimuksen aikana normaalisti organisaation toimintaan jokapäiväisessä työssä, ja koska tutkimuksen tekijä oli työskennellyt kohdeorganisaatiossa jo viiden vuoden ajan, voitiin tarkastelussa dokumentoida havaintoja myös tutkimuksen tekijän oman kokemuksen pohjalta. Tällä tavalla oli mahdollista saada vastauksia myös

kysymyksiin, joiden selvittäminen muilla keinoilla olisi ollut hankalaa tai jopa mahdotonta. Työ- ja toimintatapatarkastelulla pyrittiin myös keräämään organisaatiossa elävää hiljaista tietoa. Tällaisen tiedon selvittäminen esimerkiksi haastatteluilla ja dokumentointia tarkastelemalla on usein hankalaa, sillä kaikkea ei ole aina dokumentoitu eikä haastateltavilla välttämättä ole tietoa tai halua vastata kysymykseen todenmukaisesti tai riittävän laajasti. Työ- ja toimintatapatarkastelulla pyrittiin selvittämään asioita etenkin ISO 17799 -standardin näkökulmasta.

Haastatteluiden tarkoituksena oli selvittää ihmisten tiedossa olevia organisaation tietoturvallisuuteen liittyviä oleellisia asioita, heidän asenteitaan ja ajatuksiaan tietoturvallisuudesta sekä saada käsitys organisaation tietoturvaosaamisen tasosta. Haastatteluihin valittiin kaikki ne yrityksen työntekijät, joiden pääasiallisena työtehtävänä on osallistua kohdeorganisaation toimintaan. Näihin kuului haastatteluiden alkaessa tutkimuksen tekijän lisäksi seitsemän henkilöä: kaksi hallinnolliseen työhön osallistuvaa esimiestä, kaksi järjestelmäpuolen ylläpitäjää, kaksi ohjelmistokehittäjää ja yksi asiakaspalveluun ja sisällöntuotantoon osallistuva henkilö. Haastattelut pidettiin yksilöhaastatteluina ja ne olivat rakenteeltaan puolistrukturoituja.

Haastattelukysymykset muodostivat haastattelulle kolmiosaisen rakenteen. Ensimmäinen osa sisälsi yleisluontoisia kysymyksiä, jotka olivat yhteisiä kaikille työntekijöille. Toinen osa koostui työtehtäviin liittyvistä kysymyksistä, ja ne oli jaettu hallinnollisten, ylläpidollisten ja ohjelmistokehityksellisten työtehtävien mukaan. Viimeinen osa koostui jälleen kaikille yhteisistä kysymyksistä. Haastattelun kysymykset ryhmiteltiin siten, että jokaiseen kysymykseen on vastannut vähintään kaksi henkilöä. Haastattelukysymykset löytyvät liitteistä (Liite A: Haastattelukysymykset).

Organisaation työntekijät haastateltiin yhden viikon aikana. Haastattelusta kerrottiin kaikille työntekijöille yhteisesti haastatteluja edeltäneellä viikolla pidetyssä organisaation viikkopalaverissa. Palaverin jälkeen sovittiin kunkin henkilön kanssa sopiva aika haastattelulle. Jokaista haastattelua varten varattiin aikaa kaksi tuntia. Haastattelut pidettiin yrityksen neuvottelutiloissa. Haastateltavilta kysyttiin aluksi lupa haastattelun nauhoittamiseksi tutkimustyötä varten. Kunkin haastattelun aikana tehtiin yksityiskohtaiset muistiinpanot, jotka toimivat ensisijaisena lähteenä haastattelun tuloksia analysoitaessa. Nauhoitteita käytettiin asioiden ja sanamuotojen tarkistamiseen tuloksia laadittaessa.

Taulukko 3 havainnollistaa käytettyjä tiedonkeruumenetelmiä ja niillä kerättyä aineistoa. Menetelmien hyödyntämisessä on pyritty siihen, että jokaista aineistoryhmää varten olisi

käytetty vähintään kahta menetelmää tiedon hankkimiseksi. Tällä on tavoiteltu sitä, että saatu tieto voidaan vahvistaa toisella menetelmällä, ja samalla myös huomataan mahdolliset vallitsevat ristiriitaisuudet esimerkiksi käytäntöjen ja dokumentoinnin välillä. Suluissa oleva merkintä tarkoittaa sitä, että menetelmää on käytetty tiedonkeruussa toissijaisena menetelmänä. Tiedonkeruutyö on rajattu siten, että se kattaa ISO 17799 -standardin sisällön siltä osin kuin se on järkevästi sovellettavissa kohdeorganisaatioon. ISO 17799 -standardin sisältämien lukujen suhde tämän tutkimuksen tiedonkeruumenetelmiin ja käytetty osa-aluejaottelu löytyy liitteistä (Liite B: Tiedonkeruu ja jaottelu ISO 17799 -standardin osalta).

Taulukko 3. Käytetyt tiedonkeruumenetelmät.

Aineisto	Menetelmät				
	Dokumentaation läpikäynti	Järjestelmän läpikäynti	Toimitilojen läpikäynti	Työ- ja toimintatapatarkastelu	Haastattelu
Järjestelmän tekniset suojaukset	x	x		x	(x)
Työ- ja tuotantotilojen suojaukset	x		x	x	(x)
Tiedon käsittely- ja luokittelumenetelmät	x			x	x
Turvallisuusjohtamisen menetelmät ja hallinnollinen tietoturvallisuus	(x)			x	x
Tietoturvamenetelmät ohjelmointityössä	x			x	x
Tietoturvamenetelmät ylläpitotyössä	x			x	x
Käyttöoikeuksien ja pääsyn hallinta	x			x	x
Työntekijöiden tietoturvaosaaminen					x
Asenteet ja ajatukset tietoturvaa kohtaan				(x)	x
Tietoturvaan liittyvät ongelmatilanteet	x			x	x
Muut tietoturvallisuuteen liittyvät asiat	x	x	x	x	x

5.4 Kartoituksen tulokset

Tässä luvussa esitellään kartoituksen tulokset. Kerätty aineisto esitellään luvussa 2.3 esitetyn osa-aluejaottelun mukaan. Haastatteluihin on viitattu yksilöivällä tunnisteella (H1–H7).

5.4.1 Hallinnollinen tietoturvallisuus

Kohdeorganisaatiossa ei ole määritelty tietoturvapolitiikkaa. Tämä näkyy niin dokumentaation puuttumisesta kuin haastatteluvastauksistakin. Johdon sitoutuminen tietoturvallisuuteen ei ole erityisen näkyvää. Johto on kuitenkin suhtautunut aina hyvin avoimesti tarpeellisiin tietoturva-aloitteisiin, ja resursseja niiden toteuttamiseen on allokoitu liiketoiminnan tarpeiden mukaisesti. Tietoturvallisuuden tietoisuuden lisäämiseen ja ylläpitämiseen organisaatiolla ei ole käytäntöjä.

Organisaation tietoturvallisuuden tehtävien ja velvollisuuksien jakautumisessa on jonkin verran epäselvyyksiä, sillä vastuunjakoa ei ole tehty konkreettisella tasolla. Käytännössä osa työntekijöistä on ottanut vastuuta itselleen työtehtäviensä vastuualueiden mukaan, mutta yleisellä tasolla tätäkään ei ole erikseen edellytetty tai osoitettu. Tämä näkyy myös siinä, että lähes jokaisella haastatellulla oli oma yksilöllinen näkemyksensä siitä, kenelle vastuut kuuluvat. Käytännössä vastauksista on havaittavissa, että vastuu on käytännössä muotoutunut siten, että se on hajautunut henkilöstölle työtehtävien mukaan: jokainen vastaa siitä mitä tekee, mutta esimiehellä on lopullinen vastuu ylöspäin.

> *”Koko ylläpitotiimi [vastaa tietoturvallisuuden toteuttamisesta organisaatiossa], pääasiassa kai järjestelmävastaava [vastaa] isoista linjoista ja muut sitten [hallitsevat] pieniä yksityiskohtia. Totta kai [ohjelmoijat] omalta osaltaan vastaavat siitä, että koodi on edes jotenkin turvallista.”* (H3)

> *”Ei kukaan [ole yleisellä tasolla vastuussa], yksittäisistä asioista joku on vastuussa. Teknisellä tasolla [järjestelmävastaava], [eräs järjestelmäylläpitäjä] ja muut ovat vastuussa, [se] on osa sitä työtä, vaikka sitä ei ole erikseen sanottukaan, tietoturvajuttuja tai muuta. Ei ole sillain, että joku tietty ihminen on aina [vastuussa].”* (H2)

Tietoturvallisuuden kehittämiseen ja riskien kartoittamiseen liittyvät vastuukysymykset ovat niin ikään jokseenkin epäselviä. Varsinaista prosessia ei ole eikä tehtäviä ole eksplisiittisesti vastuutettu, vaikkakin hallinnollisilla esimiehillä on asianmukainen käsitys siitä, miten vastuu jakautuu. Tietoturvallisuuden kehittämistä ja siihen liittyvää riskikartoitusta tehdään joka tapauksessa jatkuvasti taustalla muun työn yhteydessä. Käytännössä kehitystyö pohjautuu henkilöstön oma-aloitteisuuteen.

> *”Vastuu on [organisaation johtajalla]. Käytännön vastuu on [järjestelmävastaavalla]. [Järjestelmävastaavan] tuntien tietää, että [riskien kartoitusta] tehdään ja asia nousee esille ajoittain.”* (H1)

Uusien tietojenkäsittelypalveluiden käyttöönoton hyväksymiseen ei ole olemassa erillistä prosessia, mutta käytännössä organisaatiossa toimitaan siltä osin ISO 17799 -standardin ohjeistuksen mukaisesti. Salassapitosopimuksia ei ole käytetty organisaation tiedon suojaamiseen. Yhteydenpitoa viranomaisiin ei ole ohjeistettu, vaan organisaatiossa on katsottu, että asianmukaiset yhteyskanavat voidaan luoda tarvittaessa. Yhteydenpitokanavat toiminnan kannalta oleellisiin palveluntarjoajiin on kuitenkin ohjeistettu. Yhteyksiä erityisryhmiin ei ole, eikä ulkopuolisen suorittamaa riippumatonta tietoturvallisuuden arviointia ole tehty.

Organisaatiolla on ollut tietoturvaan liittyviä ongelmatapauksia vain harvoin. Pääasiassa käsiteltävät tietoturvapoikkeamat ovat asiakkaisiin kohdistuvia hyökkäyksiä, joissa organisaation rooli on lähinnä avustava. Tyypillisimmät tapaukset liittyvät salasanojen vuotamiseen asiakkaan omalta taholta tai asiakkaiden käyttämien ohjelmistojen huonoon tietoturvallisuuden tasoon. Tämän lisäksi asiakkaiden tietoliikenneyhteyksien avulla on lähetetty roskapostia organisaation järjestelmän kautta. Organisaatiota kohtaan hyökätään toisinaan erilaisilla palvelunestohyökkäyksillä, mutta toistaiseksi ne on onnistuttu torjumaan ilman oleellista vaikutusta toiminnalle. Joskus harvoin organisaation työntekijöiden koneilta on löytynyt haittaohjelmia, mutta asianmukaisen virustorjunnan ansiosta näihin on ehditty reagoimaan ennen kuin kone on ehtinyt saastua. Ohjelmistotuotannon puolella on omasta koodista havaittu aikoinaan XSS-haavoittuvuuksia ja tietokantainjektion mahdollistavia aukkoja. Nämä ongelmat on kuitenkin korjattu heti kun ne on havaittu, ja yhtä tapausta lukuun ottamatta niitä ei oltu ehditty hyödyntämään.

> *”Siihen nähden miten lepsua tietoturva on [organisaatiossa], niin on mennyt hyvin kun ei ole tullut ongelmia, en tiedä johtuuko hyvästä tuurista tai väärästä tulkinnasta.”* (H6)

Tietoturvapoikkeamista ja -heikkouksista raportoimisesta ei ole olemassa kirjallista toimintaohjetta, mutta henkilöstöä on ohjeistettu suullisesti asiasta. Haastatelluista viisi seitsemästä mainitsi, että tällaisten tapausten varalta on annettu ohje olla yhteydessä asiasta järjestelmän ylläpitoon. Tämän lisäksi ylläpitotehtäviä hoitavilla työntekijöillä oli tiedossa joitakin tarkempia toimintaohjeita siitä, miten kyseisissä tilanteissa toimitaan. Tietoturvahäiriöiden hallintaa ei muilta osin ole organisaatiossa erikseen ohjeistettu, vaan toimenpiteet suoritetaan ja työt organisoidaan normaalisti, mutta korkeimmalla prioriteetilla. Erillisiä kirjallisia menettelyohjeita, varasuunnitelmia tai kirjausohjeita ei ole, vaan poikkeustilanteissa sovelletaan pääasiassa olemassa olevia, muussa ylläpidossa hyödynnettäviä menetelmiä. Todisteiden keräämistä ja säilytystä ei myöskään ole

ohjeistettu. Poikkeamista ja heikkouksista oppimista ei ole muodollisesti järjestetty erikseen, vaan siltä osin luotetaan ihmisten omaan kykyyn parantaa työtään. Ylläpitotiimi käsittelee kuitenkin säännönmukaisesti keskenään kaikenlaiset ilmi tulleet ongelmatilanteet.

Organisaatiossa ei erityisesti valvota tietoturvallisuuteen liittyvien käytäntöjen ja ohjeistuksien noudattamista erillisenä toimenpiteenä. Käytännössä puutteisiin ja laiminlyönteihin puututaan ainoastaan silloin, kun ne huomataan jonkin muun työprosessin yhteydessä. Johdon mukaan organisaatio tiedostaa sähköiseen maailmaan liittyvät riskit ja sen valveutunut henkilöstö pyrkii myös toimimaan sen mukaisesti, joten erillinen valvonta ei ole tarpeen. Toisaalta, myös ohjeiden puutteellisuuden todettiin olevan yksi este niiden noudattamisen valvomiselle. Tahallisia laiminlyöntejä ei ole ilmennyt, mutta tietämättömyydestä tai huolimattomuudesta johtuvia kylläkin.

5.4.2 Tietoaineistoturvallisuus ja pääsynhallinta

Organisaatiossa ei ole eksplisiittisesti ja kattavasti yksilöity suojattavia tietoaineistoja. Tästä johtuen niitä ei ole myöskään luetteloitu eikä niiden hyväksyttävää käyttöä ole määritelty. Haastatteluissa työntekijät kertoivat, että tiedolle ei käytännössä ole myöskään määritelty omistajaa. Vallitsevan käytännön mukaan tiedon omistaja on se henkilö, kuka tiedon on luonut tai se, kenen käyttöön tieto on luotu.

> *”Varmaan siis se henkilö [on tiedon omistaja], joka itse tietää olevansa omistaja, [hän] kuka on luonut sen. – – Se nyt on yhtä tyhjän kanssa jos muut eivät tiedä sitä.”* (H2)

> *”Tiedoista vastaa se joka ne on luonut tai se jonka käyttöön ne on luotu. Ulkopuolelta tulevasta tiedosta vastaa se joka on tiedot hankkinut käyttöönsä.”* (H1)

Tiedon luokittelusta kysyttäessä lähes kaikki haastateltavat olivat sitä mieltä, että tiedon luokittelua ei ole ohjeistettu. Kaksi haastateltavaa osasi kuitenkin mainita, että organisaation ongelmanratkaisujärjestelmässä luokitellaan automaattisesti asiakkaisiin liittyvät ongelmat sellaisiksi, että niiden käsittely on mahdollista ainoastaan niiltä henkilöiltä, joilla on siihen oikeudet. Tiedon luokitteluun ei ole olemassa kirjallisia ohjeita.

> *”[Tietojen luokittelemista] ei oikeastaan [ole ohjeistettu], aika paljon luotetaan ihmisten omaan päättelykykyyn tai luokittelukykyyn.”* (H6)

Myös luokittelemattoman tiedon osalta haastatellut olivat yhtä mieltä siitä, että sen käsittelyä ei ole ohjeistettu. Haastatteluiden pohjalta voidaan todeta, että vaikka

organisaatiossa ei olekaan erikseen määritelty miten luokittelematonta tietoa käsitellään, niin lähes kaikki haastatellut kuitenkin mainitsivat, että tiedon luovuttamista – ainakin ulkopuolisille – edeltää aina jonkinlainen omalähtöinen arviointi siitä, voiko tietoa luovuttaa. Tältäkin osin siis työntekijöiden osaamiseen ja arviointikykyyn luotetaan.

> *"Ei ole ohjeistettu [luokittelemattoman tiedon käsittelyä], käytännöt ovat kunkin itsensä luomia ja siinä on helvetillinen tietoturva-aukko."* (H1)

> *"Yrityksen sisäinen tieto luokittuu omassa mielessä johonkin tiettyyn luokkaan ja käy ulkopuolisessa kommunikaatiossa tietyn sensuurin läpi."* (H5)

Emoyhtiö tarjoaa tiedon hävittämiseen erilaisia menetelmiä. Papereita voidaan hävittää joko silppuamalla tai lukitun tietoturvasäiliön kautta. Myös levykkeille ja cd-levyille on hävittämiseen tarkoitettu tietoturvasäiliö. Säiliöt tyhjentää tiedon hävittämiseen erikoitunut yritys, joka hävittää tiedot turvallisesti. Organisaation käytöstä poistettavista laitteista poistetaan kiintolevyt ennen laitteiden toimittamista kierrätykseen. Mikäli näin ei voida toimia, tai jos levyä tarvitaan vielä jossain myöhemmässä käytössä, tyhjennetään levyt ohjelmalla, joka ylikirjoittaa levyllä olevat tiedot vähintään kolmesti. Kiintolevyt ja nauhavarmistukseen käytetyt nauhat hävitetään lopulta tiedon hävittämiseen erikoistuneen yrityksen kautta. Takuun aikana tai huoltosopimusten piiriin kuuluvat hajonneet kiintolevyt luovutetaan laitevalmistajalle tai sen edustajalle, joka huolehtii tietojen hävittämisestä erillistä maksua vastaan. Muistitikuille, matkapuhelimille tai muille vastaaville tallennusvälineille ei ole olemassa hävitysohjeita.

Yhtä lukuun ottamatta kaikki haastatelluista tiesivät, että paperilla olevan tiedon voi hävittää tietoturvalaatikoita käyttämällä. Myös silppuri mainittiin hävitysmenetelmänä. Haastatelluista vain esimiehet tiesivät yrityksenlaajuisesta ohjeistuksesta fyysisessä olomuodossa olevan tiedon hävittämiseksi. Sähköisestä tiedon hävittämisestä ei yrityksessä eikä organisaation sisällä ole olemassa ohjeita, mutta muutama työntekijä tiesi, että ylläpito ylikirjoittaa käytöstä poistuneita kiintolevyjä. Kannettavilta muistivälineiltä kuten muistitikuilta ja muilta käytössä olevilta tallennusvälineiltä tietoa poistetaan käytännössä ainoastaan normaaleilla käyttöjärjestelmän poistotoiminnoilla. Vain yksi haastatelluista työntekijöistä tiesi, että cd-levyjä ja levykkeitä varten on olemassa oma hävityssäiliönsä. Kaksi työntekijää mainitsi myös, että tietoa joutuu hävittämään niin harvoin, että hävittämiseen liittyviä asioita ei ole joko tullut vastaan tai niitä ei muista.

> *”Fyysisessä [kontekstissa käytössä] on [tiedon hävittämiseen] arkaluontoisten papereiden kierrätyslaatikoita. Vähemmän arkaluontoista [tietoa heitetään]*

roskikseen. Sähköisellä puolella [käytössä on] delete-nappi ja Windowsin roskakori." (H6)

Organisaatiossa ei ole katselmoitu pääsyoikeuksiin liittyviä vaatimuksia liiketoiminnan kannalta, eikä tällaisia vaatimuksia ole myöskään kirjattu yksittäisinä vaatimuksina. Käyttöoikeuksien hallinta jakautuu organisaatiossa kahteen eri kokonaisuuteen: organisaation omat käyttöoikeudet ja asiakkaiden käyttöoikeudet. Omien käyttöoikeuksien hallinnalla tarkoitetaan organisaation omien työntekijöiden, yhteistyökumppaneiden, sopimuskumppanien ja teknisten tunnusten käyttöoikeuksien hallintaa. Näitä oikeuksia hallitaan organisaation sisäisten menettelyjen kautta käsin. Käyttäjien lukumäärä on noin 100 kappaletta. Erilaisia palveluita, joiden käyttöoikeuksia hallitaan, on useita kymmeniä.

Asiakkaiden käyttöoikeuksilla tarkoitetaan tietylle asiakasryhmälle tarjottavien palveluiden pääsynhallintaan liittyvien käyttöoikeuksien hallintaa. Emoyritys toimittaa organisaatiolle säännöllisesti listan voimassaolevista asiakkuuksista, jonka pohjalta organisaatio päivittää omat tietokantansa ja suorittaa tarvittavat muutokset järjestelmään koneellisesti. Asiakkaiden lukumäärä on yli 100 000. Asiakkaiden käyttöoikeudet on rajattu selkeästi asiakasjärjestelmiin, asiakkaiden oikeuksien hallinta on selvästi dokumentoitu ja palvelut on toteutettu kyseisen dokumentaation mukaisesti. Tämän tutkimuksen puitteissa asiakasjärjestelmien käyttöoikeuksia ei tarkastella erikseen, sillä ISO 17799 -standardi ei sovellu siihen tarkoitukseen erityisen hyvin.

Organisaation omien oikeuksien hallinta on toteutettu siten, että kaikilla käyttäjillä on henkilökohtaiset tunnukset. Yhteiskäyttötunnuksia käytetään pääasiassa ylläpidossa teknisistä syistä. Tällaisia ovat pääkäyttäjien oikeudet, tuotantojärjestelmien julkaisu-tunnukset ja tekniset tunnukset, joita tarvitaan palveluiden toteuttamiseksi. Yhteiskäyttö-tunnuksia ei ole dokumentoitu. Käyttäjän valtuutuksien ja oikeuksien tarkoituksen-mukaisuuden tarkistamisesta on olemassa kirjallinen ohjeistus. Käyttöoikeuksia ei jaeta käyttäjille kirjallisena, eikä heiltä vaadita allekirjoitettua sitoumusta käyttöoikeuksien myöntämiseksi. Tarpeettomien käyttäjätunnusten säännöllisestä läpikäynnistä ei ole olemassa käytäntöä, vaan sitä tehdään satunnaisesti. Pääkäyttäjien oikeudet on pääsääntöisesti ainoastaan järjestelmän ylläpidolla. Pääkäyttäjän valtuutuksia ei ole erikseen dokumentoitu. Järjestelmän sovelluskehittäjillä on joissain tapauksissa pääsy tietyille palvelimille pääkäyttäjän oikeuksilla julkaisutoimenpiteitä ja suorituskykymittauksia varten. Työkoneiden osalta kaikilla työntekijöillä on täydet oikeudet oman työkoneensa hallintaan. Windows-järjestelmissä pääkäyttäjän oikeudet on liitetty tavallisiin käyttäjätunnuksiin, kun

taas Linux-järjestelmien puolella pääkäyttäjän oikeudet on eriytetty tavallisista käyttäjätunnuksista. Pääkäyttäjän oikeuksiin liittyviä muutoksia ei kirjata.

Käyttäjiltä ei edellytetä allekirjoitettua sitoumusta salasanan salassapidosta käyttöoikeuksia myönnettäessä. Käyttäjätunnusta luotaessa sille annetaan tilapäinen salasana, joka on tarkoitettu vaihdettavaksi tunnuksen käyttöönoton yhteydessä. Organisaatiossa on ohjeistettu kirjallisesti, että käytettävien tilapäisten salasanojen on oltava turvallisia. Käyttäjän henkilöllisyyttä ei todeta erikseen käyttöoikeutta myönnettäessä, vaan käyttöoikeuksien tilaaja vastaa henkilön oikeellisuuden tarkistamisesta. Kirjallisen ohjeen mukaan tilapäisen salasanan vastaanottamisesta ja vaihtamisesta vaaditaan kuittaus silloin, kun salasana toimitetaan käyttäjälle sähköpostilla tai muulla vastaavalla epäturvallisella menetelmällä. Salasanoja ei säilytetä salaamattomana, paitsi joissain tapauksissa teknisten tunnusten kohdalla (esim. asetustiedostossa) kun se on palvelun toteuttamiseksi välttämätöntä. Oletussalasanojen muuttamisesta on olemassa kirjallinen ohje. Käyttöoikeuksien säännöllisin väliajoin suoritettavasta uudelleenarvioinnista ei ole olemassa käytäntöä.

Organisaatiossa ei ole olemassa erityistä salasanapolitiikkaa, eikä käyttäjiä ole myöskään ohjeistettu salasanan valitsemisesta. Yksi haastatelluista muisteli, että suullisesti olisi ohjeistettu valitsemaan pitkä ja monimutkainen salasana. Organisaatiossa on perinteisesti luotettu siihen, että työntekijät osaavat valita turvallisen salasanan ja vaihtavat sitä riittävän usein. Linux-palvelimissa on käytössä tekninen rajoitus, joka ei hyväksy selkeästi huonoja salasanoja. Käytännössä rajoitukset ovat kuitenkin melko alkeellisia, ja pääkäyttäjä pystyy joka tapauksessa halutessaan pakottamaan käyttäjälle huonon salasanan. Muilta osin organisaation omille salasanoille ei ole teknisiä rajoituksia.

Emoyhtiön järjestelmien salasanapolitiikat koskevat osaa organisaation työntekijöistä jopa päivittäin, suurinta osaa kuitenkin harvemmin. Emoyhtiöllä on omien tietojärjestelmiensä osalta käytössä yksiselitteinen salasanapolitiikka, joka määrittää salasanan vähimmäispituuden, edellyttää siinä olevan isoja ja pieniä kirjaimia sekä numeroita, määrittää salasanan pisimmän mahdollisen vaihtovälin, sekä rajoittaa samojen salasanojen uudelleenkäyttöä. Yhtiön puolelta on ohjeistettu, että salasanaksi ei suositella mitään sellaista, mikä voisi olla jotenkin jonkun muun arvattavissa tai pääteltävissä. Lisäksi on käsketty, että muistiin kirjoitettua salasanaa ei saa säilyttää sellaisessa paikassa, mistä joku muu sen voisi löytää. Yrityksen SAP-liiketoimintajärjestelmän salasanapolitiikka on vieläkin tiukempi ja edellyttää salasanan vaihtamista haastateltujen mukaan jopa kuukauden välein. Kaksi haastateltua mainitsi, että tämä johtaa käytännössä siihen, että salasana on

tiheän vaihtamisen ja epäsäännöllisen käytön vuoksi kirjoitettava ylös, jos sen aikoo muistaa seuraavalla käyttökerralla.

Kukaan haastatelluista hallinnolliseen työhön osallistumattomasta viidestä työntekijästä ei ollut sitä mieltä, että organisaation nykyinen salasanakäytäntö olisi sellaisenaan hyvä. Yhtä lukuun ottamatta jokainen heistä myös toivoi, että salasanapolitiikka muotoiltaisiin kirjallisena. Molemmat esimiehet totesivat omassa vastauksessaan, että salasanapolitiikkaa voisi parantaa jonkin verran nykyisestä, mutta että nykyinenkin käytäntö on periaatteessa riittävä. Toinen heistä nosti esille myös ohjeistuksen parantamisen kehitysmahdollisuutena.

> *”Se mikä tulee väistämättä mieleen, niin järjestelmän omat salasanat jotka on koodattu sisään, [niillä] ei ole vanhentumisrajoja ja useissa paikoissa on samat salasanat käytössä koko organisaatiossa olon ajan, ja tässä tapauksessa jopa maksimissaan yli 10 vuotta.”* (H5)

> *”[Organisaation] käytäntö on [surkea], kun voi olla mitä tahansa salasanoja kenellä tahansa.”* (H3).

Haastateltuja pyydettiin myös kuvailemaan, minkälaisia salasanoja heillä on käytössä. Vastausten perusteella kaikilla organisaation jäsenillä on sisäisen ohjeistuksen puuttumisesta huolimatta käytössä turvalliseksi luokiteltavat salasanat. Kukaan ei myöskään sanonut joutuvansa kirjoittamaan salasanoja ylös. Myös salasanojen keksimiseen käytetyt menetelmät ovat kaikilla riittävän turvallisia.

Työntekijöitä ei ole ohjeistettu valvomattomien koneiden lukitsemiskäytännöistä. Käytännössä muutaman kuukauden aikana suoritettu käytännön tutkimus osoittaa, että kaikki organisaation hallinnolliseen työhön osallistumattomat työntekijät lukitsevat koneensa aina vähintäänkin silloin, kun he poistuvat huoneesta jossa kone sijaitsee. Toinen esimiehistä jätti koneensa toisinaan lukitsematta jättäessään koneensa valvomatta. Esimiehillä on käytössään henkilökohtaiset huoneet. Organisaatiossa ei ole ohjeistettu puhtaan pöydän politiikkaa, eikä sellainen myöskään käytännössä toteudu. Esimiehillä on käytössään henkilökohtaiset tulostimet ja työntekijöiden kummassakin työhuoneessa on omat verkkotulostimet.

Organisaation palveluiden pääsynhallinta perustuu pitkäaikaiseen hallitsemattomaan kehitykseen. Pääsynhallintaa on kehitetty sekä tietojärjestelmien ylläpitäjien että sovelluskehittäjien toimesta, käytännössä kummatkin omista lähtökohdistaan omiin tarpeisiinsa. Osittain tästä johtuen organisaation tietojärjestelmiin tarvitaan jopa kuusi eri tunnusta, hieman työtehtävistä ja tarvittavista palveluista riippuen. Viimeisen kahden

vuoden ajan tilannetta on pyritty parantamaan yksinkertaisilla linjauksiin liittyvillä muutoksilla, esimerkiksi sillä, että pääsyoikeuksia jaetaan nyt ainoastaan keskitetysti järjestelmän ylläpidon toimesta. Käyttöoikeudet jaetaan ensisijaisesti siten, että käyttäjillä on ainoastaan työtehtävien edellyttämät oikeudet. Joissain tapauksissa, etenkin vanhojen palveluiden kanssa, käyttäjä saattaa saada oikeuksia myös muihin vastaaviin palveluihin. Tätä ei kuitenkaan ole pidetty ongelmallisena, sillä oikeusryhmät on pilkottu melko pieniin kokonaisuuksiin ja riskialttiit palvelut on eriytetty erillisten oikeuksien taakse. Verkkopalveluita ja niihin liittyviä pääsyoikeuksia ei ole kattavasti dokumentoitu, vaan dokumentaatio on luotu ainoastaan joidenkin palveluiden osalta. Yhtä ylläpitopalvelua lukuun ottamatta kirjautumisessa edellytetään aina salattua yhteyttä, mikäli yhteys muodostetaan julkisen verkon kautta.

Kaksi haastateltua mainitsi järjestelmään liittyvien lukuisten eri käyttötunnusten aiheuttavan toisinaan ylimääräistä vaivaa työtehtävien suorittamiselle. Lisäksi kaksi työntekijää mainitsi, että käyttöoikeuksia joutuu oikeuksien jakokäytännön vuoksi pyytämään etenkin alkuvaiheessa useaan otteeseen, ennen kuin käytössä on riittävät oikeudet kaikkialle mihin tarvitseekin. Lisäksi yksi haastatelluista piti ongelmallisena sitä, että sovelluskehittäjillä ei ole aina pääsyä joihinkin heidän kehittämiinsä sovelluksiin niiden tuotantoon käyttöönoton jälkeen, vaikka kyseisiä sovelluksia joutuu kuitenkin toisinaan päivittämään.

Organisaation tietoverkko on jaettu loogisesti yhteen työkoneverkkoon, kahteen palvelinverkkoon, yhteen asetustenhallintaverkkoon, vierailijoille ja työntekijöiden omille tietokoneille tarkoitettuun verkkoon, sekä ulkopuoliseen julkiseen verkkoon. Organisaatiolla ei ole käytössään langattomia lähiverkkoja. Verkkoyhteyksiä työkoneilta ei juuri ole rajoitettu ja ainoastaan välttämättömät estot on toteutettu. Palvelinten osalta verkkoliikennettä on rajoitettu mahdollisuuksien mukaan siten, että välttämätön liikennöinti ulkomaailmaan täytyy tehdä välityspalvelimien kautta. Verkkojen välistä reititystä valvotaan siten, että ulkopuolisista tai niihin verrattavista verkoista tulevaa liikennettä sallitaan ainoastaan palveluiden toteuttamiseksi. Sisäisessä liikenteessä verkkojen välinen liikenne on järjestetty siten, että ainoastaan tarpeelliseksi katsotut yhteydet voidaan muodostaa. Esimerkiksi työkoneverkkoon ei ole pääsyä palvelinverkoista käsin. Laitteiston tunnistusta ei käytetä yhteyksien todentamiseen. Organisaation tietojärjestelmässä ei ole vianmääritys- tai asetustenhallintayhteyksiä ulkopuoliselle tukihenkilöstölle.

Käyttöjärjestelmiin sisäänkirjautuminen on organisaatiossa toteutettu mahdollisimman minimaalisesti: tietoa kirjauduttavasta järjestelmästä tai ohjeviestejä ei näytetä, kuten ei myöskään oikeudettoman käytön erikseen kieltäviä varoituksia. Epäonnistuneiden

kirjautumisyritysten määrä on Linux-palvelimilla rajoitettu kolmeen, mutta tunnuksen lukitus ei ole käytössä. Poikkeuksellisilta vaikuttavat epäonnistuneet kirjautumisyritykset ilmoitetaan erikseen ylläpidolle automaattisesti. Sisäänkirjautumisen jälkeen ei ilmoiteta epäonnistuneiden kirjautumisyritysten määrää, mutta Linux-järjestelmissä kerrotaan kuitenkin edellisen kirjautumisen ajankohta. Syötettävää salasanaa ei näytetä koskaan selväkielisenä, eikä järjestelmään kirjautumiseen käytettäviä salasanoja siirretä salaamattomana. Käyttämättömillä istunnoilla ei ole käytössä aikakatkaisua Windows-palvelinten etäyhteyksiä lukuun ottamatta. Myöskään yhteysaikoihin liittyviä rajoituksia ei ole käytössä, sillä online-palveluiden toteuttamisessa tarvitaan ympärivuorokautisia yhteyksiä. Käyttäjien pääsyn rajoittamisesta sovellusten tietoihin ja järjestelmätoimintoihin ei ole erillistä ohjetta, vaan oikeudet tietoihin ja toimintoihin jaetaan tapauskohtaisesti. Arkaluontoiset sovellukset, kuten tietokantasovellukset, on organisaatiossa eriytetty omiin palvelimiinsa.

Matkakäyttöön tarkoitettuja laitteita on organisaatiossa muutamia. Ylläpidon käytössä olevia etäylläpitoon tarkoitettuja kannettavia tietokoneita ei ole erityisesti suojattu. Näillä koneilla ei kuitenkaan säilytetä mitään tietoa, vaan ne on tarkoitettu ainoastaan etähallintaan. Muut organisaation hallussa olevat tietokoneet ovat emoyhtiön hallitsemia ja niissä on käytössä koko kiintolevyn salaava toiminnallisuus. Muita suojauskeinoja ei käytetä, eikä kannettavien laitteiden varmuuskopiointia ole ohjeistettu erikseen. Organisaation työntekijät on ohjeistettu tallentamaan kaikki tärkeät tiedot säännöllisesti organisaation verkkolevyille, josta tiedot varmistetaan edelleen. Etätyöskentely on mahdollistettu ainoastaan ylläpidolle, joka käytännön syistä tarvitsee ympärivuorokautisen pääsyn järjestelmään. Näiden etäyhteyspisteiden virustorjunnan järjestäminen on edellytetty organisaation toimesta, muilta osin turvallisuustoimet ovat etäkäyttäjän vastuulla.

5.4.3 Toimitilaturvallisuus

Organisaation tuotantolaitteisto on sijoitettu yhteen palvelinsaliin emoyrityksen toimitiloihin. Emoyhtiö vuokraa toimitilansa kiinteistön omistajalta, joka itse toimii samassa kiinteistössä. Kiinteistön sisällä laitesali on sijoitettu siten, että sillä on erittäin hyvä suoja erilaisia fyysisiä hyökkäyksiä ja onnettomuuksia vastaan. Sali on vertikaalisesti katsoen sijoitettu kolmannelle ja horisontaalisesti katsottuna toiselle sisäkkäiselle turvallisuusvyöhykkeelle. Laitesalin sijainti on ilmaistu kyltein ensimmäisellä ja toisella vyöhykkeellä. Toiselle vyöhykkeelle pääsy on jo hyvin rajoitettu, eikä alueelle ole oikeuksia esimerkiksi kiinteistön siivoajilla. Kolmannelle vyöhykkeelle pääsy on rajattu

ainoastaan ylläpidolle, organisaation esimiehille ja turvallisuussyistä myös kiinteistön päivystävälle vartiopäällikölle. Ulkopuoliset pääsevät laitesaliin ainoastaan saatettuna. Kiinteistössä on ympärivuorokautinen paikallisvartiointi, kulunvalvontajärjestelmä ja tallentava videovalvonta. Kiinteistön vartiointiin kuuluu myös miehittämättömien, lukittujen alueiden säännöllinen tarkistaminen.

Kiinteistössä on myös ympärivuorokautinen kiinteistövalvonta, joka huolehtii jäähdytyksen ja sähkönsyötön toiminnasta sekä vesi- ja paloilmaisinten seurannasta ja niihin liittyvien vahinkojen rajoittamisesta. Kiinteistö on kytketty automaattiseen paloilmoitinjärjestelmään ja lähin paloasema sijaitsee alle kilometrin etäisyydellä. Laitetiloissa on käytössä sekä optisia ilmaisimia että optinen linjailmaisinjärjestelmä. Linjailmaisimet on asennettu korotetun lattian alle ja laitesalin kattoon, jäähdytysilmanoton yhteyteen. Tavalliset optiset ilmaisimet on sijoitettu kattoon sopiville paikoille. Laitetiloissa on yksi 12 kg:n hiilidioksidisammutin ja kuiva-asennettu sprinklerijärjestelmä. Tiloissa on olemassa myös valmius kemiallisen sammutusjärjestelmän käytölle, mutta se ei ole käytössä. Työtiloissa on optiset paloilmaisimet, sprinklerijärjestelmä ja käsisammutuskalustoa.

Laitesalin jäähdytysjärjestelmän puhaltimet on kahdennettu, sähkönsyöttö varmistettu, ja laitesalin tulo- ja poistoilman lämpötiloja valvotaan aktiivisesti useassa mittauspisteessä. Tiloissa on lisäksi erillinen ilmanvaihtojärjestelmä. Salin kosteusanturit on sijoitettu korotetun lattian päälle ja alle. Tilojen läpi ei kuljeteta nesteitä. Laitesalin sähkönsyöttö on järjestetty kahdennetun UPS-järjestelmän kautta. UPS-järjestelmää syötetään ensisijaisesti julkisesta sähköverkosta, jonka palvelukatkosten aikana sähköä tuotetaan automaattisesti kiinteistön omien dieselgeneraattoreiden avulla. Organisaation tietojärjestelmien valvonta-järjestelmälle tuleva sähkö kulkee laitesalissa vielä yhden erillisen UPS-järjestelmän kautta. Kiinteistön varavoimalaitteistoa koestetaan kahden kuukauden välein. Laitetilan sähkön-syötön pääkytkin sijaitsee sisäänkäynnin välittömässä läheisyydessä. Hätävalaistusta huoneessa ei ole, mutta päävalaistus on kytketty varavoimalähteen taakse. Tiloissa on myös taskulamppu, ja poistumistiet on merkitty paikallisten vaatimusten edellyttämällä tavalla.

Tietoliikenneyhteydet on kaapeloitu siten, että ne eivät kulje kiinteistön sisällä tai ulkopuolella samaa reittiä toistensa kanssa. Laitesalin ulkopuolella kaapelointi on toteutettu pääasiassa valokuituyhteyksin, jonka salakuunteleminen ei onnistu ilman kaapelin katkaisemista. Työtiloissa kaapeloinnin viimeiset metrit on toteutettu kupariyhteyksillä ilman erityisiä suojaputkia. Kaapelit kulkevat osan matkasta yrityksen käytäviä pitkin kaapelihyllyissä välikaton sisällä. Kaapelointi ei kulje julkisten tilojen kautta. Laitesalissa olevat laitteet ja niiden sähkökaapelit on merkitty niiden yksilöimiseksi. Verkkokaapeleita

ei ole merkitty, mutta ne on dokumentoitu erittäin tarkalla tasolla, jotta kaapeleiden ongelmaton yksilöity käsittely onnistuu. Kaapeleiden kytkeminen on ohjeistettu kirjallisesti ylläpitohenkilökunnalle.

Organisaatio tai sen emoyritys ei toiminnallaan nosta ulkopuolisten hyökkäysten uhkaa, eikä satunnaisen murtoyrityksenkään todennäköisyys vaikuta kovin suurelta. Laitesalin sijainti, rakennuksen koko ja rakennustapa suojaavat laitesalia useimmilta rakennuksen ulkopuolisilta onnettomuuksilta. Luonnononnettomuuksien, sähkömagneettisen hyökkäyksien ja liikenneonnettomuuksien aiheuttamien ongelmien todennäköisyys on arvioitu hyvin pieneksi. Myös tärinän ja ilman mukana kulkevien epäpuhtauksien aiheuttamaa laitesalin toiminnan keskeytymistä pidetään melko epätodennäköisenä. Laitetilojen palokuorma on pyritty minimoimaan eikä alueella säilytetä vaarallisia tai tulenarkoja aineita. Kameroiden käyttöä turva-alueilla ei ole erityisesti kielletty. Myöskään syömisestä tai juomisesta turva-alueilla ei ole olemassa ohjeita. Tupakointi on kielletty koko kiinteistössä muualla kuin merkityillä alueilla. Näitä alueita ei ole lainkaan turva-alueen lähistöllä.

Yrityksessä on käytössä kuvalliset henkilökortit, joita on pidettävä jatkuvasti esillä. Vierailla on erillinen vieraskortti, jonka luovuttaminen ja palauttaminen kirjataan. Työntekijöitä on ohjeistettu, että vieraita ei saa jättää valvomatta, ja että henkilökortittomat henkilöt ja saattamattomat vieraat tulisi aina saattaa yrityksen aulaan. Viisi haastatelluista vastasi yrityksen ohjeistuksen mukaisesti kysymykseen siitä, miten tulisi toimia jos tapaa yrityksen käytäviltä kulkuluvattoman, epäilyttävältä näyttävän henkilön. Loput kaksi haastateltua kertoi, että ilmapiiri yrityksessä on tämän käytännön osalta hieman lepsu. Kolme haastateltavaa lisäsi vastaukseensa, että henkilön tulisi kuitenkin käyttäytyä erityisen epäilyttävästi, jotta asiaan tulisi kiinnitettyä huomiota. Kaksi henkilöä mainitsi toimivansa aina yrityksen ohjeiden mukaan. Käytännössä koko emoyrityksen tasolta toimintaa tarkkailtaessa on selvää, että vain pieni osa yrityksen työntekijöistä on aktiivisesti kiinnostunut siitä, että tiloissa ei liiku henkilökortittomia ihmisiä. Yrityksessä on myös yleinen tapa päästää kulunvalvotuista ovista ja hisseistä kerralla useita ihmisiä työtiloihin – jopa tuntemattomia. Laitesalien osalta tätä ongelmaa ei ole.

> *”Todennäköisesti en toimisi mitenkään [jos näkisin epäilyttävästi käyttäytyvän henkilökortittoman ihmisen yrityksen työtiloissa] – ellei se olisi täysin denan näköinen tai täysin out of place – niin sitten voi tiedustella mikä se jannu oikein on. Täällä näkee kaikennäköistä suhaajaa.”* (H7)

Kaksi haastateltua kritisoi sitä, että emoyhtiön toimitiloissa ei ole lukittavia työtiloja. Käytännössä kuka tahansa jolla on pääsy työtiloihin voi käydä toisten työhuoneissa. Paperit,

tietokoneet ynnä muut pitäisi siten säilyttää lukittavissa kaapeissa, mutta esimerkiksi pöytämallista tietokonetta ei lukkojen taakse saa lainkaan.

> *”Lukolliset kaapit on tietoturvan kannalta aika ongelma, täytyy sanoa että niihin ei ole aina laittanut sitä tietoturvatavaraa mikä pitäisi laittaa yöksi kaappiin. Voi unohtua pöydälle. Yritetään säästää [huoneiden lukituksessa], mutta ei tiedä onko se loppujen lopuksi viisasta.”* (H2)

Aulasta ja muilta julkisilta alueilta, kuten tavarantoimitukselle tarkoitetuista tiloista yrityksen työtiloihin pääsemiseksi tarvitaan kulkuoikeus. Saapuvaa tavaraa ei erikseen tarkasteta postikeskuksessa tai aulassa ennen käyttökohteisiin siirtämistä. Kaikki saapuneet lähetykset rekisteröidään. Tavarantoimitukselle varattuja alueita ei ole rajoitettu tunnistettuihin kulkuluvan saaneisiin henkilöihin, vaan tiloihin pääsee kuka vain ilmoittamalla ovipuhelimella asiansa.

5.4.4 Henkilöstöturvallisuus

Työntekijöiden, toimittajien ja ulkopuolisten käyttäjien turvallisuusrooleja ja -vastuita ei ole määritelty eikä dokumentoitu. Työntekijöiden valinnassa tarkistetaan pääsääntöisesti muun muassa entisten työpaikkojen paikkansapitävyys, ansioluettelon oikeellisuus soveltuvin osin ja hakijan henkilöllisyys. Koulutuksen tai ammatillisen pätevyyden paikkansapitävyyden osalta on uskottu tutkintotodistusta. Turvallisuusselvityksiä ei tehdä eikä ulkopuolisille käyttäjille tai toimittajille tehdä myöskään taustatarkistuksia. Työsopimukseen kirjattavat ehdot eivät vastaa ISO 17799 -standardin toteuttamisohjeita, joskin suurin osa standardin vaatimuksista on Suomessa tarpeettomia paikallisen lainsäädännön vuoksi.

Johto ei edellytä tai järjestä erillistä tietoturvakoulutusta uudelle työntekijälle. Ylläpidosta organisaatiossa vastaavat henkilöt kertovat tyypillisesti uudelle henkilölle ohjeistusta siitä, mikä on sallittua ja mikä ei käyttöoikeuksien luovuttamisen yhteydessä, mutta mitään johdonmukaista tai ennalta määrättyä perehdytysohjetta ei ole olemassa. Muilta osin uusille työntekijöille kerrotaan, että yrityksen asiat ovat salassa pidettävää tietoa ja että työvälineet ovat henkilökohtaisia välineitä. Joidenkin tietoturvaan läheisesti liittyvien asioiden kuten etätyön osalta annetaan tarvittaessa erillinen opastus. Tietoturvallisuusvastuita ei eksplisiittisesti selvitetä työntekijälle.

> *”Ei [järjestetä uusille työntekijöille] spesifiä koulutusta. Katsotaan, että perustason ohjeistus riittää ja tai että se tieto mitä kukin yleensä käsittelee ei vaadi sen kummempaa tietoturvaa.”* (H1)

Tietoturvaosaamisen kehittämisestä ja ylläpitämisestä ei myöskään ole käytäntöjä organisaatiossa. Käytännössä tietoturvallisuuteen liittyvän osaamisen oletetaan olevan jokaisella työntekijällä riittävä omien tehtäviensä suorittamiseksi ilman erillistä koulutusta, ja mikäli näin ei ole, niin työntekijä selvittää omatoimisesti, miten asiat tulisi toteuttaa turvallisesti. Erillisiä sanktioita tietoturvallisuussäännösten rikkomisesta ei ole määritelty.

> *”Eipä oikeastaan [kehitetä tietoturvaosaamista]. – – Se kehittyy siinä missä kaikki muukin osaaminen tällä alalla. Oppimista tää on koko ajan. – – Ensinnäkin kukaan ei ole erikseen vastuussa, toisekseen sitä ei nähdä niin tärkeänä kuin muita koulutusasioita. Jos pitäisi valita tietoturvakoulutuksen ja muun koulutuksen väliltä, niin äkkiseltään se on se muu koulutus.”* (H2)

> *”Yleisesti ottaen ei [kehitetä tietoturvaosaamista]. Jos kehitetään niin satunnaisesti ja tilannesidonnaisesti.”* (H1)

Haastatteluiden aikana pyrittiin kartoittamaan jonkin verran myös työntekijöiden ymmärrystä tietoturvallisuudesta. Useimmat haastatelluista hahmottelivat tietoturvallisuuden tarkoittavan sitä, että estetään organisaation ja emoyrityksen tietojen leviämistä oikeudettomille osapuolille. Yksi haastateltu osasi laajentaa käsitettä vielä sisältämään sen, että organisaation hallitsema tieto ei muutu hallitsemattomasti. Jokainen haastatelluista sanoi kokevansa, että hänellä on riittävät valmiudet niiden tietoturvallisuuteen liittyvien päätösten tekemiseen, joita hän joutuu työssään tekemään. Haastatteluiden perusteella kuitenkin voidaan sanoa, että useimpien työntekijöiden tietoturvaosaaminen keskittyy lähinnä omaan asiantuntemusalueeseen liittyviin asioihin.

> *”Haastattelun aikana oli mielenkiintoista huomata kuinka vähän [tietoturvallisuudesta] tietääkään oikeastaan, rupesi ihan mietityttämään mitenkä se nyt oikeastaan meneekään.”* (H7)

Vastuiden viestinnästä työsuhteen päättymisen tai oleellisen muuttumisen osalta ei ole olemassa käytäntöä tai ohjeistusta, vaan organisaatiossa on toimittu tältä osin tapauskohtaisesti. Työntekijöitä ohjeistetaan palauttamaan kaikki organisaatiolle kuuluva omaisuus työsuhteen päättyessä, suojattavat kohteet mukaan lukien, mutta koska luovutetuista tiedoista ja työvälineistä ei ole erillistä rekisteriä, on prosessi esimiesten oman muistin ja työntekijän rehellisyyden varassa. Kulkuoikeudet poistetaan kaikilta työntekijöiltä työsuhteen päättyessä. Työntekijän hallitsemaa muistinvaraista tietoa pyritään siirtämään dokumentaatioon mahdollisimman tehokkaasti heti siitä lähtien, kun tieto tulevasta työsuhteen muutoksesta saavuttaa organisaation. Tähän ei ole erillistä toimintamallia, vaan dokumentointi hoidetaan aina tapauskohtaisesti, poistuvan työntekijän

toimesta ja esimiehen johdolla. Työntekijän poistumiseen liittyvien riskien hallintaan ei organisaatiolla ole olemassa käytäntöjä. Käyttöoikeuksien poistaminen on hoidettu epäjärjestäytyneesti, käytännössä aina järjestelmävastaavan aloitteesta. Järjestelmävastaava ei kuitenkaan ole tekemisissä henkilöstöasioiden kanssa, joten oikeuksien hallinta on riippuvainen siitä, onko hän tietoinen työsuhteen tai yhteistyön päättymisestä. Työtehtävien muuttuessa organisaation sisällä ei käyttöoikeuksia pääsääntöisesti arvioida uudelleen, vaikka siitä on ohjeistettu kirjallisesti. Yhteiskäyttötunnusten salasanoja ei myöskään pääsääntöisesti muuteta työntekijän poistuessa. Ylläpidolla on olemassa ajantasaiset ohjeet siitä miten käyttöoikeuksien kanssa toimitaan, kun jokin työntekijä poistuu organisaation palveluksesta. Urakoitsijoiden ja muiden ulkopuolisten poistumiseen liittyviä käytäntöjä ei ole olemassa.

Yleinen asenne tietoturvaa kohtaan organisaatiossa oli haastattelujen perusteella varsin myönteinen. Kaikki haastateltavat olivat sitä mieltä, että tietoturvallisuus on tärkeä asia. Haastatelluista viisi sanoi suhtautuvansa tietoturvallisuuteen vakavasti ja loput kaksi henkilöä olivat sitä mieltä, että tietoturvallisuus on periaatteessa vakava asia, mutta on tilannekohtaista kuinka vakavasti siihen tarvitsee suhtautua. Neljä ihmistä oli sitä mieltä, että työpaikalla vallitsee hyvä asenne tietoturvaa kohtaan, ja loppujen kolmen henkilön mielestä tietoturvaan suhtaudutaan jossain määrin hieman liian huolettomasti. Yhtä henkilöä lukuun ottamatta kaikki haastatellut olivat sitä mieltä, että myös käytännön tasolla näkyy, että organisaatio panostaa tietoturvallisuuteen. Yksi haastatelluista oli myös sitä mieltä, että organisaation asenne tietoturvallisuuteen on terveempi kuin emoyrityksen tietohallinnolla.

> *”Kokonaisuudessaan tekee mieli sanoa että [emoyhtiössä] ei panosteta [tietoturvallisuuteen]. Epäilen että kyse on enemmänkin kohtaanto-ongelmasta, eli lyödään hyttystä pesäpallomailalla ja yritetään kärpäslätkällä torjua norsua. [Kohdeorganisaatiossa] tietoturva-asiat ovat hyvin, panee joskus miettimään onko meillä päälaellaan kääntynyt kohtaanto-ongelma eli ammutaan tankilla norsua.”* (H1)

5.4.5 Tietoliikenne- ja käyttötoimintoturvallisuus

Tietojenkäsittelypalveluiden menettelyohjeita ei ole kattavasti dokumentoitu, toisin sanoen läheskään kaikista toimenpiteistä ei ole olemassa menettelyohjeita. Ylläpidon osalta tyypillisten vikatilanteiden korjaamiseksi on olemassa menettelyohjeet, mutta muilta osin menettelyohjeita on tehty ainoastaan silloin, kun sille on ollut jotain erityistä tarvetta. Muutokset organisaation tietojärjestelmiin suoritetaan pääasiassa ylläpidon toimesta;

sovelluskehittäjät suorittavat kuitenkin joitakin itse tuotettuun ohjelmakoodiin liittyviä päivityksiä ja käyttöönottoja. Mikäli sovelluskehittäjien tekemällä muutoksella on epäilty olevan jotain oleellista vaikutusta järjestelmän toimintaan tai muutoksen vaikutukset eivät ole aivan selvillä, ovat sovelluskehittäjät tyypillisesti olleet yhteydessä ylläpitoon ennen muutosta. Ylläpidon tekemät muutokset arvioidaan pääsääntöisesti siten, että muutosta hakeva ylläpitäjä arvioi ensin muutostyön suuruuden. Mikäli muutoksen vaikutusalue on riittävän suuri, kysyy hän joko järjestelmävastaavalta tai kerää koko ylläpidon kokoon. Tämän jälkeen järjestelmävastaavan johdolla päätetään milloin ja miten muutos järjestelmään tehdään. Tässä yhteydessä päätetään myös tiedottamisesta asiakkaille. Pienimuotoiset muutokset ylläpitäjä tekee omatoimisesti. Kaikki järjestelmän muutokset – mukaan lukien myös sovelluskehittäjien tekemät kirjastopäivitykset – kirjataan vähintäänkin ylläpidon tapahtumaseurantajärjestelmään. Tarvittaessa muutokset dokumentoidaan tarkemmin. Muutoksiin liittyvä testaaminen mitoitetaan aina tapauskohtaisesti siten, että muutoksen kohteen kriittisyyden mukaan lisätään ennakkotestauksen määrää, mikäli mahdollista. Kriittisten sovellusten toimivuus tarkistetaan aina käyttöjärjestelmään tehtävien päivitysten yhteydessä.

Tehtävien eriyttämistä ei käytännössä ole juurikaan toteutettu organisaatiossa muuten kuin että sovelluskehitys, ylläpito, asiakaspalvelu ja hallinto on jaettu omiksi vastuualueiksi. Esimerkiksi tietojärjestelmien ylläpidossa ei juuri ole sellaisia toimintoja, joita ylläpitäjä ei voisi käytännössä tehdä ilman toisten konkreettista valtuutusta. Pienellä työntekijämäärällä toiminnan jatkuvuuden takaamiseksi täydet käyttöoikeudet on oltava koko ylläpidolla, vaikka päivittäisessä työssä kyseiset henkilöt eivät kaikkia järjestelmän osa-alueita ylläpitäisikään. Tuotanto- ja kehitysjärjestelmien toimintoja on pyritty eriyttämään mahdollisimman paljon, mutta käytännössä molemmat sijaitsevat samassa verkkosegmentissä ja toisinaan sovelluskehityksessä käytetään tuotantojärjestelmän tietokantoja testikantojen sijaan.

Organisaation tuotantoon liittyviä ulkopuolisia palveluita ovat lähinnä Internet-yhteys ja talotekniikka. Talotekniikan osalta palvelun toimintaa seurataan jatkuvasti, ja kriittiset tekijät – esimerkiksi laitesalin lämpötila tai sähkönsyöttö – on liitetty organisaation valvontajärjestelmään. Internet-yhteyden toimivuudelle on sovittu toimittajan kanssa liiketoiminnan kannalta sopiva saavutettavuuden taso. Yhteyden toimivuutta valvotaan ja suorituskykyä seurataan myös koko ajan. Palveluntarjoajan katastrofisuunnitelmia ei ole selvitetty, eikä sopimuksissa niitä myöskään edellytetä. Myöskään ulkopuolisten toimittajien palveluiden muutosten hallintaan liittyviä toimenpiteitä ei ole erikseen

määritelty, vaan organisaatiossa on toimittu aina tapauskohtaisesti, mikäli toimittaja on muutoksesta ilmoittanut.

Organisaation tietojärjestelmien kapasiteetin hallinta pohjautuu jatkuvaan nykytilanteen seurantaan ja tulevaisuuden tarpeiden arvioimiseen. Uusia järjestelmiä tai niiden osia suunniteltaessa oikeaa resurssien mitoitusta pidetään tärkeänä osana suunnittelutyötä. Vaatimuksia ei kuitenkaan tyypillisesti ole kirjattu ylös, vaikka niitä onkin käsitelty päätöksiä tehtäessä. Järjestelmää käyttöönotettaessa ei tehdä mitään formaalia hyväksyntää, vaan järjestelmä otetaan käyttöön, mikäli sen havaitaan toimivan testeissä tarkoitetun mukaisesti.

Työasemissa on käytössä keskitetyn hallinnan takana oleva haittaohjelmilta suojaava ohjelmisto. Ohjelman tietokannat päivitetään automaattisesti aina kun kone on verkossa, ja uusi päivitys on saatavilla. Ohjelma paitsi tutkii onko tietokoneella olevissa tiedostoissa viruksia, niin myös suojaa koneen ulkopuolelta tulevilta asiattomilta yhteydenotoilta. Verkkosivuja ei suodateta haittaohjelmien varalta, mutta sähköpostin liitetiedostot kylläkin. Menettelyohjeita ei ole luotu eikä vastuita ole määritelty siltä osin, miten toimitaan mikäli jokin haittaohjelma pääsee järjestelmään. Myöskään erillistä jatkuvuussuunnitelmaa haittaohjelman aiheuttamien vahinkojen varalta ei ole. Haittaohjelmiin liittyvän tiedon keräämisestä ei ole erillisiä kirjattuja menettelytapoja, mutta niitä seurataan ylläpidon suorittaman haavoittuvuustietojen seurannan yhteydessä. Tiedon hankkimisessa käytetään ensisijaisesti ainoastaan hyvämaineisia lähteitä. Liikkuvan koodin suorittamista ei ole erikseen rajoitettu, mutta selaimet eivät oletusasetuksillaan suorita kyseisiä ohjelmia ilman erillistä lupaa.

Organisaation tietoverkot on suojattu asianmukaisilla palomuureilla ja pääsy verkkoon on teknisesti rajattu siten, että työkoneverkkoon ei voi omatoimisesti lisätä uusia laitteita. Julkisissa verkoissa kulkeva luottamuksellinen liikenne siirretään aina salattuna. Organisaation palvelinten välinen liikenne on pääsääntöisesti salaamatonta, joskin jotkin palvelut kuten esimerkiksi käyttöoikeuksien varmentaminen välitetään luontaisesti suojattuna. Käyttäjille suunnatut palvelut on toteutettu pääosin salaavilla sovellustason protokollilla. Verkon valvonta hoidetaan kirjaamalla liikennöintisäännöistä poikkeavat tapahtumat. Tietomurtohälytintä organisaatiolla ei ole käytössä. Tietoverkkojen suojauksia on käsitelty myös luvussa 5.4.2 sivulla 67.

Organisaation työntekijät kertoivat haastattelujen yhteydessä siirtävänsä tietoa sähköpostissa ja sen liitteinä, suojatulla tiedonsiirtoyhteydellä, paperilla, cd-levyillä,

muistitikulla, pikaviestimillä ja levyjakojen kautta käyttöjärjestelmään kuuluvilla työkaluilla. Suojattavien kohteiden siirtämisestä pois työpaikalta ei ole olemassa erillistä ohjeistusta eikä virallista käytäntöä. Tiedon siirtoa organisaation tietojärjestelmien ulkopuolelle tehdään kuitenkin hyvin vähän. Käytännössä yleisin tähän tarkoitukseen käytetty siirtomenetelmä on muistitikku. Laitteiden viemisestä toimitilojen ulkopuolelle ei myöskään ole erityistä ohjeistusta tai muuta menettelyä. Organisaation käyttämät matkapuhelimet ja kannettavat tietokoneet kuuluvat ylläpidon kahta tietokonetta lukuun ottamatta emoyrityksen hallintaan. Tietovälineiden hävittämistä on käsitelty tarkemmin luvussa 5.4.2 sivulla 63. Tiedon käsittelystä tai varastoimisesta ei ole annettu erillisiä ohjeita. Järjestelmän dokumentaatiota on rajoitettu osittain pelkästään ylläpidon käyttöön, mutta suurin osa dokumentaatiosta on kuitenkin kaikkien työntekijöiden luettavissa.

Tiedonvaihtoon liittyviä menettelytapoja ei ole ohjeistettu organisaatiossa, vaan käytäntönä on ollut, että työntekijöiden tietoturvaosaamiseen luotetaan myös tältä osin. Fyysisten tietovälineiden kuljetuksesta ei ole ohjeistusta eikä käytäntöjä, koska siirron tarvetta on niin vähän, että tilanteet voidaan käsitellä tapauskohtaisesti. Pääsääntöisesti tietovälineet on kuljetettu henkilökohtaisesti kohteeseen. Sähköiseen viestintään käytetään pääasiassa suojaamattomia yhteyksiä. Jonkin verran luotetaan siihen, että paikallisesti lähetetyt sähköpostit säilyvät suojassa ulkopuolisilta, mutta pääsääntöisesti mitään kriittistä tietoa ei kuitenkaan välitetä suojaamattomassa muodossa. Eräs työntekijä mainitsi haastattelussa, että hän toisinaan joutuu vastoin omaa tietosuojakäsitystään lähettämään luottamuksellista materiaalia sähköpostilla, kun ei ole vaihtoehtoja.

> *”Usein tilanne on se, että vaikka tieto on luottamuksellista ja periaatteessa kyllä tietää, että sitä ei pitäisi sähköpostilla lähettää, niin käytännössä se on ainoa tapa lähettää se eteenpäin. Sähköposti on aika hasardi – – kuinka paljon sähköpostissa oikeasti liikkuu luottamuksellista tietoa yritystenkin välillä, [tiedot makaavat] ihmisten koneilla ja sitten joku virus lähettää ne kerralla eteenpäin. Siinähän sitä sitten ollaan. – – Monta kertaa kyllä miettii, että tämä on tosi hasardia lähettää [tämä tieto] sähköpostilla, mutta ei ole muutakaan vaihtoehtoa.”* (H2)

Pikaviestimiä organisaatiossa käytetään paljon, mutta ei mihinkään arkaluontoiseen viestintään. Pikaviestimiä ja sähköpostia käytetään myös henkilökohtaiseen keskusteluun työhön liittymättömien henkilöiden kanssa. Lankapuhelimeen ja matkapuhelimeen luotetaan jonkin verran muita sähköisiä viestintävälineitä enemmän, ja niitä saatetaan käyttää tärkeään tiedonvaihtoon, mikäli keskustelua ei voida käydä kasvotusten. Arkaluontoista ja kriittistä tiedonvaihtoa tehdään käytännössä ainoastaan kasvotusten. Muita käytössä olevia viestimiä ovat IRC-keskustelukanava, jota osa henkilökunnasta

käyttää työhön liittymättömään kommunikointiin muiden työntekijöiden kanssa, sekä faksi, jota käytetään työasioiden hoitamiseen, mutta ei arkaluontoisiin asioihin. Haastatteluiden yhteydessä selvisi myös, että toisinaan hallinnon ulkopuolisten työntekijöiden viestintää hankaloittaa se, että ei ole yksiselitteistä, mitä tietoa saa milloinkin välittää niille henkilöille, jotka tekevät organisaatiolle freelance-työtä.

Tiedonvaihto asiakkaiden kanssa on koettu ongelmattomaksi, sillä organisaatiolla on käytössään riittävän luotettava menetelmä asiakkaiden tunnistamiseksi silloin, kun sille on tarvetta. Pääsääntöisesti asiakkaiden kanssa käydyt keskustelut ovat sellaisia, joissa asiakkaalle ei luovuteta mitään suojattavaa tietoa tai ei suoriteta erityisiä toimenpiteitä. Lisäksi käytössä olevat toimintatavat tukevat turvallista toimintaa, esimerkiksi kadonneen salasanan tilalle lähetetään aina kirjekuoressa uusi salasana asiakkaan aiemmin ilmoittamaan postisoitteeseen, eikä uutta salasanaa voi saada selville puhelimessa. Asiakasyhteydenotot ohjataan organisaation sisällä aina sen omaan asiakaspalveluun, mikäli yhteys edellyttää jotain toimenpiteitä. Näin toimenpiteitä suorittaa ainoastaan kokenut ja asianmukaisesti koulutettu asiakaspalvelija.

Järjestelmän toimintojen tarkkaileminen on järjestetty keskitetysti. Käyttäjätoimintojen tapahtumalokit tallennetaan sekä paikallisesti että erilliselle lokipalvelimelle, josta epäilyttäviä lokitietoja seulotaan automaattisesti. Samalla lokitietojen väärentäminen on hankalaa, sillä tiedot tallennetaan lähdepalvelimen lisäksi erikseen suojatulle palvelimelle. Tälle palvelimelle on pääsy ainoastaan järjestelmän pääkäyttäjillä, ja sen levytilan käyttöä valvotaan aktiivisesti, jotta kirjaukseen käytetty tila ei pääse täyttymään. Järjestelmässä on käytössä keskitetty kellojen hallinta, jonka perusteella kaikki palvelimet ja useimmat verkkolaitteet päivittävät kellonaikansa. Tapahtumalokeihin tallennetaan sisäänkirjautumiset ja niiden yritykset yksityiskohtineen, mutta ei juurikaan muita tietoja. Eri palveluiden käytön tarkkailun taso riippuu runsaasti palvelusta. Kaikki www-pohjaisten palveluiden käyttö kirjataan riittävällä tasolla normaaleihin www-palvelimen tekemiin lokitiedostoihin, samoin kaikkien ulkopuolisten palveluiden toiminnot. Järjestelmässä kirjataan myös luvaton liikennöinti verkkosegmenttien välillä. Pääkäyttäjien toimintoja ei erityisesti kirjata lokeihin. Häiriöiden kirjaaminen on hyvin tapauskohtaista, eikä varsinaista prosessia niiden käsittelemiseen ole. Tyypillisesti yksinkertaiset häiriöt käsitellään kirjaamatta, isommat tai ratkeamattomat ongelmat sen sijaan kirjataan yleensä aina. Jälkikatselmusta ei useimmiten järjestetä kuin merkittävien korjaustoimenpiteiden jälkeen.

Järjestelmän ylläpitoon liittyvä toiminta organisaatiossa on hyvin järjestäytynyttä. Tietojärjestelmiin tehdään runsaasti ennakoivaa ylläpitotyötä. Enimmäkseen ennakoiva työ

kohdistuu ohjelmistojen päivittämiseen ja suorituskykyyn liittyvien mittareiden trendien ja olemassa olevan kapasiteetin riittävyyden säännölliseen tarkistamiseen. Samalla jatkuvasti tutkitaan kehitysmahdollisuuksia toiminnan parantamiseksi tulevaisuudessa. Organisaatiossa piirretään seurantaa varten kuvaajia noin 1500 eri järjestelmän mittarista. Tämän lisäksi ylläpito seuraa jatkuvasti muun muassa ohjelmien päivitystarpeita, lokitiedostoja ja järjestelmän toimintaa yleisesti.

> *”[Ennakoiva ylläpito] on jatkuva prosessi. Ei sitä voi tehdä vain ``kerran viikossa´´.”* (H3)

Vikatilanteita varten organisaatiossa on käytössä valvontajärjestelmä, joka valvoo noin neljää sataa eri kohdetta. Valvonnan piiriin kuuluu paitsi järjestelmän toimintaan liittyviä mittareita, niin myös asiakkaan toimintaa simuloivia valvontatoimenpiteitä. Mikäli jokin mittari ajautuu hälytysrajan yli tai jonkin palvelun asiakassimulaatio ei mene virheettä läpi, hälytetään kellonajasta riippumatta tilanteen vakavuuden mukaan päivystävä ylläpitäjä. Päivystäjä tekee päätöksen siitä, minkälaisia korjaustoimenpiteitä vikatilanne vaatii, ja aloittaa sen jälkeen tarvittavat toimenpiteet. Ylläpidolla on kirjalliset toimintaohjeet erilaisten vikatilanteiden varalta. Osa organisaation palveluiden toteuttamiseen liittyvistä laitteista on lisäksi kahdennettu. Tämä mahdollistaa toiminnan jatkumisen näiden palveluiden osalta ilman, että se näkyy käyttäjälle. Tällaisia palveluita ovat esimerkiksi Internet-yhteys, tietokantapalvelut, käyttäjähakemistopalvelu ja osa www-palvelimista. Varmistukset on tehty liiketoiminnan kannalta kriittisimpiin palveluihin.

Inhimillisten virheiden osuutta ylläpitotyössä pyritään välttämään sillä, että tuotantojärjestelmiin liittyvät työt käydään läpi yleensä vähintään kahden ylläpitäjän voimin. Tarvittaessa töihin haetaan vielä hyväksyntä järjestelmävastaavalta tai organisaation esimiehiltä. Huoltokatkot ja muut projektiluontoiset toimenpiteet suunnitellaan askeltasolla etukäteen, ja palaaminen toimenpidettä edeltävään tilaan mietitään tällöin myös erikseen. Asetustiedostot säilytetään versiohallinnassa, joten vanhat asetukset ovat aina saatavilla ja tehdyt muutokset kirjautuvat järjestelmään automaattisesti. Organisaation testausjärjestelmässä voidaan useimmissa tapauksissa tehdä testauksia ennen toimenpiteiden suorittamista. Haastatteluiden perusteella ylläpitäjillä on myös henkilökohtaisia menettelytapoja inhimillisten virheiden vähentämiseksi, esimerkiksi voimakkaiden järjestelmäkomentojen antamisen yhteydessä tehtävä komennon parametrien oikeellisuuden varmistaminen.

Tietoturvallisuuden ylläpitämiseksi ylläpitotyössä on ainoastaan muutamia kirjallisia ohjeita. Suullisia ohjeita on annettu ylläpitäjille tarpeen mukaan. Haastatteluissa ylläpitäjät

eivät muistaneet juurikaan suullisia ohjeita, mutta käytännössä osasivat kuitenkin esimerkinomaisesti haastattelun yhteydessä esille nostetut aiemmin ohjeistetut asiat. Kirjallisista ohjeista osattiin mainita muun muassa oikeudenhallintaan liittyvä ohjeistus. Annettuja ohjeita noudatetaan ylläpitäjien mielestä, mutta kumpikaan ei muista että noudattamista olisi näkyvästi valvottu. Toinen ylläpitäjä tosin mainitsi uskovansa, että ainakin järjestelmävastaava seuraa tilannetta taustalta. Käytännössä toimintaa valvotaan tältä osin mahdollisuuksien mukaan jatkuvasti.

5.4.6 Laitteisto- ja ohjelmistoturvallisuus

Organisaatiossa ei ole määritelty liiketoiminnan asettamia vaatimuksia tietojärjestelmien turvallisuudelle, eikä turvamekanismeja ei ole määritelty liiketoiminnan ehtojen pohjalta. Organisaatiossa ei myöskään käytetä salakirjoitusmekanismeja. Tietoa salataan ainoastaan teknisissä yhteyksissä, jossa salaaminen tehdään automaattisesti. Tällaisia ovat muun muassa käyttäjätunnusten salasanatiedot ja tietoliikenneyhteydet. Tiedon salaamisesta ei ole olemassa ohjeistusta.

Organisaation tuotantojärjestelmässä ajetaan ainoastaan suoritusvalmista, ei kehitysvaiheessa olevaa koodia. Kaikki koodi testataan ennen tuotantoon siirtämistä. Testaamisesta ei ole olemassa kirjallisia ohjeita eikä vaatimuksia testaukselle ole määritelty. Ohjelmistokoodin vanhat versiot ovat tallessa versionhallintajärjestelmässä, vanhat suoritusvalmiit ohjelmat tai ohjelmakirjastot siirretään talteen päivitysten yhteydessä. Yleensä muutoksia tehtäessä on olemassa valmis paluustrategia, mutta sitä ei ole edellytetty. Ohjelmistoja pyritään päivittämään mahdollisuuksien mukaan siten, että valmistajan tuki säilyy. Testiaineistona käytetään tyypillisesti tuotantoaineistoa. Testiaineisto on suojattu samalla tavalla kuin tuotantoaineistokin, mutta sen käyttöä ei valvota millään erityisillä toimenpiteillä. Testiaineiston tuhoamisesta ei ole olemassa ohjeita eikä tuotantoaineiston kopiointia testijärjestelmiin kirjata. Ohjelmien lähdekoodi on suojattu tuotantopalvelimilla ja versionhallintajärjestelmässä normaaleilla pääsynrajoituksilla. Lähdekoodin hakua tai käyttöä ei kirjata. Muutoksenhallinta on järjestetty koko organisaation tietojärjestelmien osalta siten, kuten luvussa 5.4.5 sivulla 73 on mainittu.

Tietovuotojen tarkkaileminen on järjestetty organisaatiossa paikallisen lainsäädännön puitteissa. Tietoliikenteen ja palvelinten osalta seurataan sellaisia suoritusarvoja, jotka eivät yksilöidy kehenkään työntekijään tai sopimuskumppaniin. Järjestelmässä käytetään pääsääntöisesti ainoastaan yleisesti luotettavina pidettyjä ohjelmistoja. Piiloyhteyksiä ei valvota eikä standardinmukaisia kommunikaatiomenettelyitä ole lähdetty muuttamaan.

Ulkoistettua ohjelmistokehitystä organisaatiossa on jonkin verran, käytännössä sen osuus on kuitenkin melko pieni sisällä tehtyyn ohjelmistokehitykseen verrattuna. Tällöin ohjelmistot tilataan hyvin tunnetulta yhteistyökumppanilta, joka vastaa omalta osaltaan kehitystyöhön liittyvistä edellytyksistä – kuten esimerkiksi lisensseistä. Koodin omistajuus on määritelty kumppanien välisissä sopimuksissa. Muita vaatimuksia kuten esimerkiksi koodin laadullisia edellytyksiä ei tyypillisesti ole esitetty. Asennusta edeltävässä testauksessa ei erityisesti etsitä koodissa olevia tietoturva-aukkoja.

Infrastruktuurin ohjelmistojen teknisten haavoittuvuuksien hallinta on järjestelmän ylläpidon vastuulla. Tietojärjestelmien haavoittuvuuksista hankitaan tietoa muun muassa kaupallisen palvelun kautta. Tämän lisäksi ylläpito seuraa aktiivisesti erilaisia ohjelmistojen haavoittuvuuksiin liittyviä postituslistoja, foorumeita ja weblogeja. Haavoittuvuuksien hallintaan liittyviä rooleja ja vastuita ei ole eritelty normaalista vastuunjaosta. Myöskään haavoittuvuuksien seuraamiseen käytettäviä tietolähteitä ei ole dokumentoitu. Tietoturva-aukosta kertovaan ilmoitukseen reagoimiseen kuluvaa aikaa ei ole ennalta määritelty. Ylläpito tutkii haavoittuvuuden vakavuuden, arvioi sen hyödyntämisen todennäköisyyden, arvioi päivityksen riskit ja tekee päivittämiseen tai muihin estotoimenpiteisiin liittyvät päätökset tapauskohtaisesti näiden tietojen perusteella. Korjaustiedostot testataan pääsääntöisesti aina ennen niiden käyttöönottoa. Tehdyt päivitykset kirjataan ylläpidon tapahtumaseurantaan. Haavoittuvuuksien hallintaprosessia ei arvioida säännöllisesti.

Organisaation laitteita huolletaan aina laitetoimittajan ohjeistuksen mukaisesti. Ainoastaan ne henkilöt, joilla on osaaminen laitteiden huoltamiseen, osallistuvat huoltotoimenpiteisiin. Laitevioista ja kaikista huoltotoimenpiteistä pidetään kirjaa. Ulkopuolisen huoltohenkilökunnan osalta ei ole tehty erillistä päätöstä siitä, mitä huoltohenkilökunta saa tehdä. Jos ulkopuolinen henkilö on huoltamassa laitteistoa, on paikalla kuitenkin aina vähintään yksi organisaation ylläpitäjä valvomassa toimintaa.

Ohjelmistokehityksessä on käytössä muutamia yleisiä käytäntöjä tietoturvallisuuden suojaamiseksi. Omia tai asiakkaiden salasanoja ei kuljeteta salaamattomana julkisessa verkossa, ja SQL-injektioita tai XSS-hyökkäyksiä mahdollistavia aukkoja ei saa olla julkisessa käytössä olevassa koodissa. Näistä asioista on huolehdittu systemaattisesti lähinnä sen jälkeen, kun toimintaohjeet on useampi vuosi sitten otettu käyttöön. Ohjelmakoodia ajalta, jolloin ohjeita ei vielä ollut, ei ole tarkistettu kattavasti mahdollisten aukkojen varalta. Sovellusten turvallisuuden varmistaminen riippuu käytännössä kehittäjän omasta aktiivisuudesta, eikä siihen ole käytössä automatisoituja työkaluja. Testaukseen ei myöskään ole tarjolla valmiita testisyötteitä, joiden avulla sovellusten turvallisuutta voisi

kokeilla, eikä sovelluksilta edellytetä ennalta määrättyjä tietoturvaan liittyviä testejä. Kirjastokoodin tuotannossa on käytäntö, että toisen sovelluskehittäjän on tarkistettava ja hyväksyttävä tehdyt muutokset, ennen kuin uusi koodi voidaan ottaa käyttöön tuotannossa. Tämä menettely on käytännössä vähentänyt myös tietoturva-aukkoja. Ensisijaisesti testaaminen on joka tapauksessa pääasiallisen kehittäjän vastuulla. Ohjelmistokehittäjille tarkoitettua tietoturvaohjeistusta on olemassa vain muutaman yksittäisen asian osalta – kuten esimerkiksi XSS-aukkojen estämisestä – ja kaikki muu informaatio on kulkenut organisaatiossa ainoastaan suullisena perimätietona sovelluskehittäjältä toiselle.

> *”[Kohdeorganisaatio] ei ole mielestäni korkean turvallisuustason kohde, siinä suhteessa ollaan [ohjelmistokehityksen turvallisuudessa] aika ajan tasalla. Erillinen tietoturvakoulutus tai päivitys ei olisi mikään huono asia. Jos oltaisiin töissä verkkopankissa niin tilanne olisi aivan toisenlainen, nykytietämyksellä ei pärjäisi siellä.”* (H5)

5.4.7 Liiketoiminnan jatkuvuuden hallinta

Organisaatiolla ei ole olemassa liiketoiminnan jatkuvuuden ylläpitoprosessia eikä myöskään jatkuvuussuunnitelmaa. Haastatteluiden perusteella kattavaa riskikartoitusta tai konkreettisia suunnitelmia onnettomuuksien tai muiden toimintaa lamaannuttavien tapahtumien varalta ei ole tehty, mutta asiaa on kuitenkin mietitty organisaation sisällä. Koska organisaatio on osa isoa ja vakavaraista kansainvälistä yritystä, luottaa se siihen, että toiminnan uudelleenkäynnistämiseen on tarvittaessa saatavissa rahaa ja resursseja niin kauan, kun toiminnan jatkaminen on ylipäänsä järkevää. Onnettomuuksiin ennalta varautumattomuuden vaikutusta tuotantokatkoksen pituuteen ei ole katsottu toiminnan jatkuvuuden kannalta merkitykselliseksi.

> *”Ei kauheasti [ole varauduttu toiminnan lamaannuttaviin tapahtumiin], ainakaan kirjallisesti, on kumminkin pohdittu, ei mitään kirjallisia ohjeita, silloin se tulee vasta kunnolla pohdittua.”* (H2)

Henkilöstön muistinvaraista ja kokemusperäistä tietoa yrityksen toimintaan liittyvistä asioista on pyritty varmistamaan jakamalla tietoa säännöllisesti työntekijöiden välillä. Etenkin järjestelmän ylläpitoon osallistuvien henkilöiden välillä tiedon ja osaamisen jakamista tehdään jatkuvasti. Järjestelmät on dokumentoitu osin erittäin kattavasti mutta osin vain välttävällä tasolla. Näkemys asiasta kuitenkin on, että tarvittaessa myös ulkopuolinen taho pystyy jatkamaan järjestelmien toimintaa – ainakin jollain tasolla – mikäli henkilöstö syystä tai toisesta estyy tekemään työtään.

”Jos esim. 90 prosenttia työntekijöistä katoaa niin sitten ollaan kusessa. Ne jotka on jäljellä [onnettomuuden jälkeen] niin rakentaa [järjestelmän] uudestaan.” (H2)

”Järjestelmistä on dokumentit; osin hyvät, osin erinomaiset, osin heikot. Järjestelmän jatkettu ylläpito on mahdollisuuksien rajoissa. Jokainen on tärkeä ja yksittäisen henkilön menettäminen tuo erilaisia ongelmia.” (H1)

Tietojärjestelmän sisältävien tietojen varmuuskopiointi on organisoitu siten, että kaikki tiedot varmistetaan säännöllisesti. Varmistukset testataan kerran kuukaudessa. Varmuuskopioita säilytetään pääkäyttöpaikalla murtosuojatussa dataturvakaapissa, joka suojaa tietoja myös mahdollisen tulipalon sattuessa. Varmuuskopioiden laajuus ja varmistusten välille jäävä aika on sovitettu vastaamaan liiketoiminnan vaatimuksia. Varmuuskopiointi ja siihen liittyvät toimenpiteet on dokumentoitu.

5.4.8 Vaatimustenmukaisuus

Organisaatiossa ei ole erikseen kartoitettu lainsäädännön toiminnalle asettamia vaatimuksia ainakaan viimeisen viiden vuoden aikana, eikä lakien noudattamisesta toiminnassa ole annettu erillisiä ohjeita. Organisaation laatimat sopimukset ja käyttöehdot on säännönmukaisesti tarkastutettu emoyhtiön lakiosastolla ennen niiden käyttämistä liiketoiminnassa. Pääsääntöisesti organisaatiossa on toimittu siten, että mikäli jossain yhteydessä on tiedostettu, että jokin asia tai toimenpide on lailla säädelty, se on otettu tarkempaan käsittelyyn vaatimusten selvittämiseksi ja täyttämiseksi. Organisaation käytännön pyrkimyksenä on ollut noudattaa lakeja poikkeuksetta.

Ohjelmistolisenssien tapauksessa organisaation käytännön toimintaa ohjaava esimies huolehtii siitä, että organisaatiolla on käytössään asianmukaiset lisenssit ja että hankittavat lisenssit vastaavat käyttötarkoitusta. Lisenssiehtojen noudattamista ei valvota muilla keinoilla, mutta omatoimisesta asentamisesta on annettu työntekijöille kieltävä suullinen ohjeistus rajoitettujen käyttöoikeuksien lisensseillä varustettujen ohjelmistojen osalta. Edelleenjaeltaviin ohjelmistoihin hankitaan levitysluvat, mikäli ohjelmistojen käyttöoikeudet sitä edellyttävät. Tähän on myös olemassa kirjalliset ohjeet, luparekisteri ja valmis anomuslomake. Muilta osin tekijänoikeuksien noudattamisesta on työntekijöitä yleensä ohjeistettu tarpeen mukaan.

Organisaation arkistoituja tallenteita säilytetään lukituissa tiloissa, joihin on rajattu pääsy. Tiedot on varastoitu siten, että niihin päästään tiedon tarpeellisuuteen nähden käsiksi kohtuullisessa ajassa. Tallenteiden arkistoimisesta ei ole erillisiä ohjeita, joskin tiedon

arkistoinnista vastaavat henkilöt on ohjeistettu suullisesti siitä miten tietoa arkistoidaan. Tallenteiden suojaamisessa ei ole huomioitu tallennusmedioiden heikkenemistä, sillä arkistoitujen tallenteiden säilytystarve on yleensä enimmillään kaksi vuotta käytöstä poistamisen jälkeen.

Organisaation kannalta oleellisiin tietosuojaan ja henkilötietojen yksityisyyteen liittyviin lakeihin kuuluvat ainakin Henkilötietolaki organisaation hallinnoimien henkilörekisterien vuoksi, Sähköisen viestinnän tietosuojalaki organisaation asiakkailleen tarjoamien palveluiden (mm. sähköposti) luonteen vuoksi ja Laki yksityisyyden suojasta työelämässä sen tietoturvallisuuteen liittyvien pykälien osalta. Organisaation käyttämät henkilörekisterit ovat lainmukaisia. Henkilörekisterien käytöstä tai hallinnoinnista ei ole olemassa kirjallisia ohjeita, mutta organisaation toimintatavat vastaavat sitä miten laissa on määrätty. Sähköisen viestinnän tietosuojalain pohjalta ei myöskään ole olemassa kirjallisia toimintaohjeita, mutta organisaation vakiintuneet toimintatavat ovat niin ikään lainmukaisia. Työnantajalle kuuluvien sähköpostiviestien avaamiseen liittyvistä oikeuksista ja velvollisuuksista on tiedotettu järjestelmän pääkäyttäjiä, mutta varsinaista kirjallista ohjeistusta asiasta ei ole annettu. Toiminta on myös tältä osin ollut lainmukaista.

> *”[Emoyhtiö vaatii], että asiakkaitten tiedot eivät saa tulla julkiseksi ja että niitä ei käytetä sellaisiin tarkoituksiin joihin niitä ei saa käyttää. [On toimittava] niin että lain kirjain täyttyy.”* (H1)

Organisaatiossa ei valvota teknisin välinein työntekijöiden tietoliikennettä, viestintää tai tietojenkäsittelypalveluiden mahdollista luvatonta käyttöä. Sähköpostin ja tietoliikenne-yhteyksien käyttäminen omaan tarkoitukseen on sallittua niin kauan, kun siitä ei aiheudu organisaatiolle haittaa. Organisaation salausmekanismien käyttö noudattaa paikallisia lainsäädäntöjä.

6 TIETOTURVALLISUUDEN NYKYTILA KOHDEORGANISAATIOSSA JA KEHITYSSUUNNITELMA

Edellisessä luvussa esiteltiin kohdeorganisaatiossa tehdyn tietoturvakartoituksen tulokset. Tässä luvussa vedetään yhteen kartoituksen tärkeimmät tulokset ja esitetään analyysi organisaation tietoturvallisuuden nykytilasta. Tämän lisäksi annetaan kehitysehdotuksia organisaation tietoturvallisuuden nykytilan kehittämiseksi. Luvun lopussa esitetään pohdintoja kehityssuunnitelmasta ja sen toteuttamisesta.

6.1 Nykytilan analyysi

Kartoitustyön tiedonkeruuvaiheessa kasatun aineiston analysoimiseen sovelletaan pääsääntöisesti ISO 17799 -standardin ohjeita ja määritelmiä. Tämän lisäksi hyödynnetään myös tämän tutkimuksen kirjallisessa osiossa muusta alan kirjallisuudesta kerättyä tietoa. Sekä ISO 17799 -standardia että muiden lähteiden suosituksia, määräyksiä ja ohjeita tulkitaan nimenomaisesti kohdeorganisaation tarpeiden näkökulmasta. Liitteissä on esitetty taulukkomuotoinen yhteenveto kartoituksessa läpikäydyistä osa-alueista ja niiden nykytilasta yrityksessä (Liite C: Yhteenveto kohdeorganisaation tietoturvallisuuden nykytilasta).

6.1.1 Yleiset havainnot

Kohdeorganisaation toimintamallit ja ratkaisut ovat syntyneet pääsääntöisesti tarpeen mukaan ilman järjestäytyneempiä tuotantoprosesseja, toisinaan jopa improvisoidusti ja ennalta valmistelematta. Tämä vastaa tilannetta, joka usein on pienissä ja keskikokoisissa yrityksissä, joissa organisaation käytettävissä olevat rajoittuneemmat resurssit ohjaavat vahvasti tarvekeskeiseen toimintamalliin. Toimintatavoista heijastuu myös kohde-organisaation toiminnan autonominen luonne, sillä emoyritys ei juuri ole edellyttänyt organisaatiolta järjestelmällisempää tiedon suojaamiseen liittyvää toimintaa. Käytännössä organisaatiossa on siten toteutettu lähinnä sellaisia kontrolleja, joiden työntekijät ovat itse katsoneet olevan toiminnan kannalta tarpeellisia.

Tällaisessa toimintatavassa on usein se ongelma, että varsinainen tietoturvallisuustyö on ainakin jossain määrin vinoutunutta: resursseja kohdistetaan yksipuolisesti jonkin tietyn osa-alueen parantamiseksi, vaikka akuutimpi tarve saattaisi olla muualla. Tämä näkyy myös

kohdeorganisaatiossa, joka sijoittuu tietoturvallisuustyön kehittyneisyyttä mittaavalla asteikolla selvästi ensimmäiselle tasolle, teknologia-aallon vaiheeseen (Kuva 1, s. 20). Vaikka organisaatiossa tiedostetaan tietoturvallisuuden tarpeet ja tehdään jatkuvasti työtä tietoturvallisuuden kehittämiseksi, on toiminta pohjautunut kuitenkin ensisijaisesti teknisiin ratkaisuihin hallinnollisen työn osuuden jäädessä vähemmälle huomiolle. Tämän kartoituksen myötä organisaatiolla on mahdollisuus ottaa askel asteikon toiselle tasolle, hallinnollisen aallon vaiheeseen, ryhtymällä kehittämään organisaation tietoturvallisuuden hallintaan liittyviä prosesseja.

6.1.2 Positiiviset havainnot

Kartoituksessa havaittiin runsaasti tietoturvallisuuden kannalta hyvin toteutettuja asioita. Tekniset suojaukset ovat melko hyvällä tolalla ja vaikka organisaatiossa ei juuri ole virallisia toimintatapoja ja dokumentoituja käytäntöjä, on jokapäiväinen toiminta ja erikoistilanteiden hallinta hoidettu hyvin. Etenkin tiedon saavutettavuuteen on panostettu, mikä näkyy hyvin organisaation ylläpitotoiminnassa ja jossain määrin myös järjestelmän teknisissä varmistuksissa. Laitteiston elinkaari on huomioitu kauttaaltaan ja tiedon suojaamiseen liittyvät perusasiat ovat kunnossa.

Kohdeorganisaatiossa on viime vuosien aikana ryhdytty kehittämään tietoturvallisuutta myös hallinnollisesta näkökulmasta. Vaikkakin työ on tältä osin ollut pienimuotoista ja sitä on tehty enimmäkseen kiireellisempien töiden ohessa, osoittaa suuntaus, että organisaatiossa on ymmärretty tietoturvallisuuden merkitys laajemmin kuin ainoastaan teknisinä kontrolleina. Kohdeorganisaation työntekijät ymmärtävät tietoturvallisuuden merkityksen ja osaavat riittävissä määrin oma-aloitteisesti huomioida sen tarpeen jokapäiväisessä työssään. Henkilöstön suhtautuminen tietoturvallisuutta kohtaan on myös hyvä ja turvallisuus koetaankin tärkeäksi osaksi toimintaa.

6.1.3 Havaitut ongelmakohdat

Organisaation tietoturvallisuuteen liittyvät suurimmat ongelmakohdat kohdistuvat pääasiassa hallinnolliselle puolelle. Selkeitä puutteita havaittiin erityisesti tietoturvatyön organisoimisessa ja vastuunjaossa, strategisessa suunnittelussa ja dokumentoinnissa, sekä tietoturvahäiriöiden ja parannuskohteiden hallinnan organisoimisessa. Nämä puutteet ovat ymmärrettäviä organisaation pienen koon, sen rajallisten resurssien ja vähäisten ulkopuolisten vaatimusten valossa. Ongelmallista on kuitenkin se, että muun muassa liiketoiminnan vaatimukset tietoturvallisuudelle ja organisaation tietoturvapolitiikka ovat

kokonaan dokumentoimatta. Tästä johtuen organisaation tietoturvallisuuteen liittyvä proaktiivinen toiminta pohjautuu työntekijöiden aloitteellisuuteen, mikä puolestaan aiheuttaa sen, että tietoturvallisuustyö ei käytössä olevilla resursseilla voi vastata täysin liiketoiminnan tarpeita. Organisaation tulisi siten keskittää resursseja erityisesti tietoturvallisuuden hallinnoimiseen.

Tietoaineistoturvallisuuden osalta selviä puutteita löytyi suojattavien kohteiden tunnistamisessa, luetteloimisessa ja niiden omistajien määrittelyssä, tiedon luokittelun määrittelyssä ja ohjeistamisessa sekä liiketoiminnan pääsynhallinnalle asettamien vaatimusten määrittelemisessä. Myös tietojärjestelmien käyttäjien velvollisuuksiin liittyvissä asioissa oli puutteita mm. organisaation salasanapolitiikan muodossa. Henkilöstöturvallisuuden osalta suurimmat puutteet johtuvat työntekijöiden tietoturvakoulutuksen puutteellisuudesta ja työsuhteen päättymiseen liittyvien prosessien puuttumisesta.

Tietoliikenne- ja käyttötoimintojen osa-alueella selkeitä puutteita löytyi liikuteltavien laitteiden turvallisuuden hallinnasta ja tietovälineiden käsittelyyn ja tiedon vaihtoon liittyvästä ohjeistamisesta. Laitteisto- ja ohjelmistoturvallisuuden osa-alueen ongelmakohtiin kuuluvat liiketoiminnan näkökulmasta tehdyn tietojärjestelmien turvallisuusvaatimusten määrittelyn, salakirjoitusmekanismien ja ohjelmointityön tietoturvamenetelmien hallinnan puuttuminen. Liiketoiminnan jatkuvuuden hallinnan kannalta puutteita on jatkuvuussuunnitelmassa ja varajärjestelyiden toteuttamisessa.

Tutkimusta varten tehdyissä haastatteluissa kohdeorganisaation työntekijät kaipasivat enemmän konkreettista ohjeistusta siitä miten tietoturvallisuuteen liittyvissä asioissa tulisi toimia. Työntekijöillä on kiinnostusta organisaation tietoturvallisuuden kohentamiseen, mutta he pystyvät tällä hetkellä toimimaan ainoastaan heidän oma-aloitteisesti kehittämiensä kykyjen puitteissa. Organisaatiossa ei ole osattu hyödyntää tätä tilannetta tietoturvakoulutuksien muodossa.

6.2 Kehityssuunnitelma

Kohdeorganisaatiolle tehdyssä kehityssuunnitelmassa on otettu huomioon organisaation pieni koko ja sen rajalliset resurssit ja keskitytty siitä syystä enimmäkseen tärkeimpiin kokonaisuuksiin. Kohdeorganisaation kehittämisen kannalta ensiarvoista on saada oma tietoturvallisuustyö käyntiin ja suurimmat puutteet korjattua, minkä jälkeen organisaatio voi omatoimisesti hyödyntää kartoituksessa kerättyä yksityiskohtaisempaa sisältöä. Tällä

tavalla muutosten läpivienti on helpompaa ja tulokset parempia. Tietoturvallisuuden prosessin käynnistämisen jälkeen pienemmät ongelmat korjaantuvat luonnostaan prosessin mukana.

6.2.1 Tietoturvatyö ja vastuunjako

Organisaation toiminta perustuu pitkälti siihen, että se luottaa henkilöstön ammatilliseen osaamiseen ja työntekijöiden kyvykkyyteen ja haluun kehittää organisaation toimintaa oman työn ohessa. Etenkin tietoturvallisuuden osalta tämä toimintamalli on hyvin haasteellinen ja riskialtis, sillä vaikka tämänhetkinen henkilöstö pystyisikin takaamaan liiketoiminnan kannalta riittävän turvallisuuden tason organisaatiolle, ei se ole millään tavalla tae siitä, että näin olisi myös tulevaisuudessa. Koska kohdeorganisaatiolla on työssä pääasiassa työelämänsä alkupuolella olevia nuoria työntekijöitä, on tavallista että henkilöstössä tapahtuu vaihtelua ajan kuluessa. Tällöin paitsi menetetään osaamista, myös altistutaan sille että korvaavien työntekijöiden osaamisen taso ei välttämättä ole riittävä. Etenkin avainosaajien kohdalla on olemassa lisäksi verrattain suuri riski siitä, että henkilön poistumisen seurauksena organisaatiossa joudutaan eräänlaiseen tietoturvallisuuden taantumatilaan. Organisaation nykyisestä toimintamallista tulisi pyrkiä eroon, jotta tietoturvallisuutta voitaisiin kehittää vastaamaan liiketoiminnan vaatimuksia ja samalla varmistua siitä, että turvallisuuden taso on riittävä myös tulevaisuudessa.

Vastauksena organisaation toiminnan nykytilaan tulisi käynnistää selkeä ohjelma, jonka kautta organisaatiossa otetaan käyttöön tietoturvallisuuden prosessi. Tätä varten organisaation johdon tulisi selvittää itselleen tietoturvatyöhön liittyvät vastuut ja muuttaa tarpeen vaatiessa organisaatiorakennetta siten, että tietoturvallisuustyön edellyttämä vastuunjako voidaan toteuttaa mahdollisimman tehokkaalla tavalla. Vastuutus tulisi tehdä siten, että jokaiselle organisaation työntekijälle on selvää mitkä hänen vastuunsa ovat ja miten ne vaikuttavat hänen työtehtäviinsä. Samalla johdon tulisi antaa täysipainoinen tuki näiden velvoitteiden noudattamiselle.

Vastuunjaolla ja siihen liittyvän selkeän vastuiden selvittämisen jälkeen organisaation toimijat tietävät mikä heidän roolinsa on organisaation tietoturvallisuustyössä. Tietoturvallisuuden prosessin käynnistämisellä tavoitellaan sitä, että tietoturvallisuus saadaan integroitua organisaation tavoitteelliseen työhön, jolloin organisaatio pystyy toimimaan liiketoiminnan vaatimusten mukaisesti muuttuvissa olosuhteissa. Nämä kaksi asiaa toimivat edellytyksenä sille, että organisaatio kykenee huolehtimaan omasta tietoturvallisuudestaan nyt ja tulevaisuudessa.

6.2.2 Dokumentointi ja koulutus

Organisaatio tarvitsee tietoturvallisuustyölleen selkeät suuntaviivat. Nämä saavutetaan luomalla organisaatiolle tietoturvapolitiikka ja -suunnitelma, jotka kertovat kuinka organisaatiossa tehdään tietoturvallisuustyötä ja kuinka se palvelee liiketoiminnan tarpeita. Politiikan ja suunnitelman lisäksi organisaatiolla täytyy olla työtehtäväkohtaisia tietoturvaohjeita, jotta henkilöstö kykenisi toimimaan liiketoiminnan edellyttämällä tavalla. Yksityiskohtainen ohjeistus on tehokas tapa vähentää tietämättömyydestä johtuvia virheellisiä toimintatapoja. Tarkat ohjeet ovat lisäksi usein paras tapa saada organisaation valitsemia käytäntöjä sisällytetyksi tavanomaisiin työtehtäviin, sillä tyypillisesti abstraktimmalla tasolla olevaa ohjeistusta – kuten esimerkiksi tietoturvapolitiikkaa – ei mielletä samalla tavalla käskeväksi ohjeistukseksi kuin suoria ohjeita.

Kohdeorganisaation tulisi kehittää lisäksi myös muun tietoturvallisuuteen liittyvän dokumentaation luomista ja ylläpitämistä. Esimerkiksi suojeltavien kohteiden luetteloiminen on edellytyksenä sille, että voidaan todeta kohteiden olevan tunnistettu. Dokumentoiminen on paitsi keino todentaa että tietoturvallisuustyötä on tehty, myös apuväline tietoturvallisuuden kehittämisessä. Jatkuvan dokumentoinnin avulla tietoturvatyön kehittäminen on oleellisesti helpompaa, sillä tällöin kehitystyön vaatima informaatio on kerätty valmiiksi käsittelyä varten.

Organisaation koko henkilöstön kouluttaminen tietoturvatyöhön on oleellinen toimenpide, jotta he voisivat ymmärtää mitä työhön kuuluu ja miksi sitä tehdään, ja ennen kaikkea jotta jokainen työntekijä osaisi toimia edellytysten mukaisesti omassa työssään. Koulutus on yksinkertainen tapa lisätä työntekijöiden sitoumusta tietoturvatyöhön silloin, kun henkilöstöllä on jo valmiiksi myönteinen asenne tietoturvaa kohtaan. Koulutus aktivoi työntekijät hyödyntämään opittuja asioita omassa työssään. Mikäli koulutukset ajoitetaan siten, että organisaatiolle on luotu oma tietoturvapolitiikka ja -suunnitelma sekä työtehtäväkohtaista tietoturvaohjeistusta, voidaan aktivoituminen hyödyntää parhaiten. Tällöin henkilöstö ymmärtää varmemmin annetut ohjeet ja myös todennäköisemmin lähtee toimimaan ohjeiden mukaisesti. Tehokas aloituspotku tietoturvallisuustyölle luo kestäviä toimintatapoja ja toimii perustana sille, että tietoturvallisuus saadaan konkreettiseksi osaksi jokapäiväistä työtä.

6.2.3 Liiketoiminnan vaatimusten määrittäminen

Jotta kohdeorganisaation tekemä tietoturvallisuustyö voitaisiin kohdistaa mahdollisimman tehokkaasti oikeisiin parannuskohteisiin, tulisi organisaation muodollisesti määritellä liiketoiminnan edellyttämät vaatimukset tietoturvallisuudelle. Tämän määrittelyn avulla riskianalyysien tekeminen ja kontrollien suunnitteleminen helpottuu, kun liiketoiminnan vaatimukset ohjaavat tietoturvatyötä. Toimenpiteet kohdistuvat tällöin sopivassa määrin oikeisiin kohteisiin ja toiminta on tehokkaampaa.

Liiketoiminnan asettamien vaatimusten puuttumisen aiheuttamat suurimmat yksittäiset ongelmat havaittiin kartoituksessa pääsynhallinnan ja tietojärjestelmien turvallisuus-vaatimusten aihepiireistä. Liiketoiminnan vaatimusten perusteella tulisi määrittää ne periaatteet, joiden perusteella pääsynhallinta asettaa yksittäisten käyttäjien ja käyttäjä-ryhmien käyttöoikeudet. Tietojärjestelmien turvallisuuden osalta tulisi määrittää liike-toiminnan asettamat edellytykset tietojärjestelmien suojausmekanismeille.

6.2.4 Tietoaineistoturvallisuuden kehittäminen

Tietoaineistoturvallisuuden puutteet tulivat hyvin selvästi esiin kartoituksen yhteydessä. Kohdeorganisaatiossa ei ole olemassa minkäänlaista kokonaisvaltaista tiedon elinkaaren hallintaan pureutuvaa prosessia. Organisaatiossa ei ole käytäntöjä eikä ohjeistusta suojattavien kohteiden tunnistamiseen ja luetteloimiseen, tiedon omistajan määrittelemiseen tai tiedon luokitteluun. Tilanteen korjaamiseksi tulisi organisaatiossa käynnistää työryhmä, jonka tehtävänä on luoda tietoaineistoturvallisuuden näkökulmasta tiedon elinkaarta ohjaava prosessi kaikkine siihen liittyvine vaiheineen. Erilaiset tiedon luomiseen, käsittelyyn ja tuhoamiseen liittyvät asiat tulisi ohjeistaa siten, että kaikki organisaation työntekijät pystyvät ohjeistuksen avulla toimimaan oikein.

6.2.5 Salasanapolitiikan luominen

Henkilöstön haastatteluista kävi selväksi, että organisaatiossa on akuutti tarve salasanapolitiikalle. Koska organisaation salasanajärjestelyt eivät käytännössä rajoita, ohjaa tai opasta salasanojen muodostamista, käyttöä tai vaihtamista, on kohdeorganisaatioon muodostunut huonon salasanakulttuurin uhka: salasanoja ei vaihdeta riittävän usein, salasanoiksi valitaan liian helppoja sanoja tai samoja salasanoja käytetään useissa eri järjestelmissä. Käytännössä riski on erityisen suuri avustajien ja sidosryhmien salasanojen osalta, mutta myös organisaation omat työntekijät muodostavat riskin laajempien

käyttöoikeuksiensa kautta. Organisaation tulisi luoda itselleen sellainen salasanapolitiikka, joka yksiselitteisesti määrittelee, millaisia salasanoja käyttäjien pitää luoda ja kuinka usein niitä täytyy vaihtaa, sekä kieltää salasanojen uusiokäytön ja monistamisen. Mahdollisuuksien mukaan salasanapolitiikkaa pitäisi valvoa teknisesti. Salasanapolitiikka tulee ohjeistaa ja ohjeiden olla helposti saatavissa. Jos mahdollista, ohjeet tulisi asettaa näkyville salasananvaihtolomakkeen yhteyteen.

6.2.6 Tietoturvahäiriöiden ja parannuskohteiden hallinta

Kohdeorganisaatiossa on käytäntönä käsitellä tietoturvahäiriöt ja niihin rinnastettavat parannustarpeet samalla tavalla kuin miten organisaatiossa käsitellään muutkin toimintahäiriöt ja ongelmat. Ongelmana tässä toimintatavassa on, että se sallii henkilö-riippuvaisen tulkinnanvaraisuuden poikkeamien raportoimisessa ja käsittelyssä ja toisaalta se ei huomioi tietoturvapoikkeamien erityistä luonnetta, joka vaatii formaalimman käsittelytavan. Organisaation tulisi kehittää muodollinen tapa käsitellä tietoturvahäiriöitä ja parannuskohteita, jotta raportointi ja poikkeamien käsittely tapahtuisi ennalta määritellyllä, tietoturvallisuuden prosessia tukevalla tavalla.

Organisaation tulisi tuottaa toimintaohjeet erilaisten tietoturvapoikkeamien varalta, jotta henkilöstö pystyisi toimimaan oikein poikkeustilanteissa ja jotta kaikki toiminnan kannalta oleelliset toimenpiteet tulisi tehtyä ajallaan. Ohjeiden tulisi sisältää ainakin raportoimiseen ja kirjaamiseen sekä vahinkojen ehkäisemiseen tai lievittämiseen liittyviä toimintaohjeita. Poikkeamien ja parannuskohteiden käsittelemistä varten tulisi kohdeorganisaatioon perustaa pysyvä päätösvaltainen työryhmä, joka kokoontuu tarvittaessa.

6.2.7 Jatkuvuussuunnitelman kehittäminen

Vaikka kohdeorganisaatio onkin osa isoa yritystä, joka tukee organisaation toimintaa poikkeustilanteissa niin paljon kuin on taloudellisesti kannattavaa, olisi organisaatiolla hyvä olla sen liiketoiminnan erilaisuuden vuoksi kokonaisuudessaan oma jatkuvuussuunnitelma. Kunnollisen testatun jatkuvuussuunnitelman avulla voidaan vähentää oleellisesti poikkeustilanteissa tuotantoon palaamiseen kuluvaa aikaa, koska usein jo pelkkä suunnitelman luominen paljastaa erilaisia selvitystä vaativia kohteita, joiden ennakko-selvityksellä voidaan lyhentää poikkeustilanteissa tehtävän työn määrää. Suunnitelman testaus paljastaa myös usein sellaisia asioita tai puutteita suunnitelmassa, joita suunnittelutyöryhmä ei ole osannut ennakoida. Koska kyseessä on pieni organisaatio, tulisi jatkuvuussuunnitelmassa huomioida myös yksittäisten henkilöiden puuttumisen

vaikutukset. Myös tarve varajärjestelmille ja -järjestelyille tulisi selvittää ja tarvittaessa järjestää niiden olemassaolo. Varajärjestelmien ja -järjestelyiden olemassaololla varaudutaan poikkeustilanteisiin siten, että tuotantoa voidaan jatkaa joko täydellisesti tai osittain mahdollisessa häiriötilanteessa.

6.2.8 Muita ehdotuksia

Työsuhteen päättymiseen ja muuttumiseen liittyvissä tilanteiden hallinnassa havaittiin kohdeorganisaatiossa olevan puutteita siltä osin, että viesti työsuhteen muutoksista ei aina saavuttanut organisaation pääsynhallinnasta vastaavia tahoja. Tämän seurauksena yrityksen palveluksesta poistuneille tai yrityksen sisällä toisiin tehtäviin siirtyneille henkilöille saattoi jäädä vanhojen työtehtävien mukaisia käyttöoikeuksia pitkäksikin aikaa. Työsuhteen päättymisten ja muutosten hallitsemiseen tulisi kehittää prosessi, jonka avulla voitaisiin varmistua siitä, että muutokseen liittyvät toimenpiteet tulisivat tehdyksi kaikissa tapauksissa.

Kartoituksen yhteydessä havaittiin selkeitä puutteita kohdeorganisaation toimitilojen ulkopuolelle siirrettävien laitteiden turvallisuuteen liittyvässä ohjeistuksessa. Vaikka toimitilojen ulkopuolella olevat laitteet eivät ole erityisen keskeisessä asemassa organisaation toiminnassa, tulisi aiheeseen kuitenkin luoda selkeät kirjalliset ohjeet, jotta käytännöt olisivat henkilöstön tiedossa. Ohjeistuksessa tulisi kiinnittää huomiota niin etätyöskentelyyn käytettävien tietokoneiden turvallisuusvaatimuksiin kuin myös suojattavien kohteiden toimitilojen ulkopuolelle kuljettamiseen liittyviin seikkoihin.

Myös tietovälineiden käsittelyyn ja tiedon vaihtoon liittyvissä toimintatavoissa oli havaittavissa puutteita. Siirrettävien tietovälineiden hallintaan ja tiedon hävittämiseen tulisi luoda ohjeistus ja muistitikkujen turvalliseen hävittämiseen pitäisi luoda asianmukainen käytäntö. Lisäksi tiedon vaihtoon liittyvät toimintatavat tulisi ohjeistaa, jotta organisaation henkilöstöllä olisi yhteiset pelisäännöt ja ymmärrys siitä miten ja mihin mitäkin viestimiä voi käyttää.

Organisaatiossa tulisi ottaa käyttöön salakirjoitusmekanismit, joiden avulla valikoitua tietoa voitaisiin salakirjoittaa tiedon luottamuksellisuuden edistämiseksi. Kaikkien käytettävissä olevien salausmekanismien käytön tulisi olla ohjeistettua ja kaikilla organisaation työntekijöillä tulisi olla mahdollisuus käyttää niitä. Tiedon salaamisella voidaan myös vastata tiedon välittämiseen liittyviin ongelmiin, esimerkiksi silloin kun organisaatiossa täytyy lähettää luottamuksellista materiaalia sähköpostin välityksellä. Ongelmaksi tällöin

muodostuu lähinnä se, että ulkopuolisilla tahoilla ei tyypillisesti ole käytettävissä sopivia salausmekanismeja omissa viestintävälineissään, jolloin salaus monesti ohitetaan. Eräs oivallinen ratkaisu sähköpostien salaamiseen ulkopuolisten kanssa viestittäessä on pystyttää sellainen oma sähköpostipalvelin, jolta ulkopuoliset henkilöt voivat käydä lukemassa heille osoitetun luottamuksellisen viestin suojatun yhteyden läpi.

Ohjelmointityöhön liittyvien tietoturvamenetelmien hallinnan kehitys tulisi ottaa työn alle, jotta ohjelmistokehityksen tietoturvallisuuden tasoa voidaan nostaa nykyisestä riittävälle tasolle. Hallinnan kehitystyössä tulisi kiinnittää huomiota työhön liittyvään ohjeistukseen, koodin tarkistamiseen ja tietoturvalliseen ohjelmointitapaan. Tietoturvamenetelmien noudattamista tulisi valvoa säännöllisesti ja ohjelmistokoodin tarkistuskäytäntö tulisi ulottaa koskemaan kaikkea sellaista koodia jolla voi olla vaikutusta tietoturvallisuuteen.

Organisaation vaatimustenmukaisuuden todettiin olevan kunnossa ja organisaation katsottiin noudattavan kaikkia paikallisia lakeja. Kohdeorganisaation toiminnan kannalta oleellista laeista olisi kuitenkin hyvä suorittaa kattava kartoitus tämän tietoturvakartoituksen lisäksi erillisenä projektina. Syynä tähän on se, että lakiasioissa tulisi niiden luonteen ja niihin liittyvien vastuukysymysten vuoksi tukeutua aina oikeusoppineen apuun.

6.3 Pohdinta

Taulukko 4 käy läpi kehityssuunnitelmassa esitetyt toimenpiteet esittäen kullekin toimenpide-ehdotukselle tärkeysasteen, arvion tarvittavista resursseista toimenpiteen toteuttamiseksi ja suositellun aikataulun toimenpiteen aloittamiselle. Aikatauluehdotus on suhteutettu siten, että nollakohtana käytetään muutostyön aloittamisen ajankohtaa. Resurssintarvearvio on annettu kolmiportaisella asteikolla siten, että työvaiheet ovat keskenään vertailukelpoisia. Asteikko on suhteutettu organisaation tämänhetkiseen kokoon.

Taulukko 4. Kehityssuunnitelman toimenpide-ehdotukset.

Toimenpide-ehdotus	Tärkeysaste	Resurssi-tarve	Tekijät ja resurssi-tarpeen osuus	Aikataulu
Tietoturvatyö ja vastuunjako	erittäin tärkeä	suuri	johto ja järjestelmä-vastaava (95%), muu organisaatio (5%)	heti
Dokumentointi ja koulutus	erittäin tärkeä	suuri	johto ja järjestelmä-vastaava (70%), muu organisaatio (30%)	samanaikaisesti tietoturvatyön käynnistämisen kanssa
Liiketoiminnan vaatimusten määrittäminen	erittäin tärkeä	keskisuuri	johto (100%)	heti
Tietoaineistoturvallisuuden kehittäminen	tärkeä	keskisuuri	johto ja järjestelmä-vastaava (75%), muu organisaatio (25%)	heti kun tietoturvatyö on saatu käyntiin

Toimenpide-ehdotus	Tärkeysaste	Resurssi-tarve	Tekijät ja resurssi-tarpeen osuus	Aikataulu
Salasanapolitiikan luominen	erittäin tärkeä	pieni	ylläpito (80%), johto (20%)	heti
Tietoturvahäiriöiden ja parannuskohteiden hallinta	tärkeä	keskisuuri	johto (35%), ylläpito (50%), sovelluskehittäjät (15%)	1 vuoden aikana
Jatkuvuussuunnitelman kehittäminen	hyödyllinen	keskisuuri	johto ja järjestelmä-vastaava (80%), muu organisaatio (20%)	1 vuoden kuluttua
Työsuhteen päättymisen hallinta	tärkeä	pieni	johto (100%)	6 kk kuluessa
Toimitilojen ulkopuolelle siirrettävien laitteiden turvallisuuden hallinta	hyödyllinen	pieni	johto (95%), muu organisaatio (5%)	1 vuoden aikana
Tietovälineiden käsittelyn ja tiedon vaihdon ohjeistaminen	hyödyllinen	pieni	johto (90%), muu organisaatio (10%)	6 kk kuluessa
Salakirjoitusmekanismien käyttöönotto	hyödyllinen	pieni	ylläpito (95%), johto (5%)	1 vuoden aikana
Ohjelmointityöhön liittyvien tietoturvamenetelmien hallinnan kehitys	tärkeä	suuri	johto (40%), sovelluskehittäjät (60%)	1 vuoden aikana
Organisaation vaatimustenmukaisuuden ulkopuolinen kartoitus	hyödyllinen	pieni	johto (10%), muu organisaatio (25%), ulkop. taho (65%)	1 vuoden aikana

Esitetyn suunnitelman toteutuminen on pitkälti kiinni siitä, pystyykö kohdeorganisaatio sitoutumaan riittävällä tasolla esitettyjen asioiden korjaamiseen ja tietoturvallisuuden prosessin käynnistämiseen. Jatkuva tietoturvallisuustyö ja etenkin sen käynnistäminen on etenkin pienikokoiselle organisaatiolle aina melkoinen työ ja edellyttää tyypillisesti jonkintasoista resurssillista uhrausta. Mikäli organisaatio haluaa panostaa tietoturvallisuuteen nyt ja tulevaisuudessa, tulisi sen huomioida, että esitetyt toimenpiteet ovat välttämättömiä paitsi kehittymisen kannalta niin myös siksi, että organisaation toiminta pystyisi jatkossa vastaamaan sille asetettuihin liiketoiminnallisiin vaatimuksiin. Käytännössä tämän tutkimuksen tietoturvakartoituksen ja kehitysehdotusten myötä kohdeorganisaatiolle otollisinta olisi tietoturvallisuuden prosessin käynnistäminen ja ehdotettujen korjaustoimenpiteiden suorittaminen seuraavan vuoden aikana. Suunnitelman toteutumisen kannalta olisi suositeltavaa, että kohdeorganisaatiossa tehtäisiin alustavat toimenpide-suunnitelmat jokaisesta korjaustoimenpiteestä ennen esitetyn suunnitelman toteuttamista. Tällöin myös ne korjaustoimenpiteet, jotka eivät edellytä välittömiä muutoksia, tulevat huomioiduksi organisaation kehitystyössä.

Suunnitelma on kehitetty siten, että se on toteutettavissa kohdeorganisaatiossa sellaisenaan eikä se edellytä kohtuuttomia toimenpiteitä organisaation pienestä koosta huolimatta. Esitetyt toimenpiteet on suunniteltu siten, että ne ovat myös rahallisen panostuksen tarpeen

suhteen linjassa organisaation koon kanssa. Kehitysehdotuksissa on huomioitu myös se, että muutokset onnistuvat nykyisellä henkilöstömäärällä. Pitkällä tähtäimellä katsottuna organisaation kehittymisen kannalta olisi järkevää muutaman vuoden kuluttua nimittää tietoturvallisuudesta ja työprosesseista vastaava esimies, jonka tehtäviin kuuluisi muun muassa tietoturvallisuuden prosessin ja tietoturvatyön ohjaaminen. Tämä olisi ajankohtaista etenkin, jos organisaatio kasvaa nykyisestään enemmän kuin muutamalla työntekijällä.

7 YHTEENVETO

Tässä luvussa käydään läpi mitä tämän tutkimuksen tavoitteena on ollut ja kuinka asetetut tavoitteet ovat täyttyneet. Lisäksi luvussa esitellään mitä tutkimuksessa on käyty läpi ja mitä siinä on todettu. Lopuksi pohditaan tutkimuksen luotettavuutta ja sovellettavuutta ja ehdotetaan aiheita jatkotutkimukselle.

7.1 Johtopäätökset

Tässä tutkimuksessa keskityttiin tietoturvallisuuden aihepiiriin. Tutkimuksen lähtökohtana oli kohdeorganisaation tarve ja halu kehittää omaa tietoturvallisuuden tasoaan. Kohde-organisaatio on erään Suomessa toimivan suurikokoisen kustannusalan yrityksen liiketoimintayksikkö, joka tuottaa Internet-palveluja sekä kuluttaja- että yritysasiakkaille. Kuluttaja-asiakkaille suunnatut palvelut ovat pääasiassa maksuttomia sisältöpalveluita. Yrittäjäasiakkaille myydään mainosnäyttöjä Internet-sivuille ja palvelua, jonka kautta yritykset saavat asiakaskontakteja. Tutkimuksen teoreettisena tavoitteena oli selvittää, minkälaisista tekijöistä organisaation tietoturvallisuus muodostuu ja miten sitä voidaan hallita. Käytännön tavoitteena oli kartoittaa kohdeorganisaation tietoturvallisuuden nykytaso ja luoda kartoituksen perusteella suunnitelma organisaation tietoturvallisuuden kehittämiseksi.

Tutkimuksen teoriaosassa avattiin tietoturvallisuuden käsitteistöä, pohdittiin tietoturvallisuuden merkitystä organisaatioille ja muodostettiin tietoturvallisuuden osa-aluejako tietoturvatyön helpottamiseksi. Katsauksessa eriteltiin organisaation toimijoiden tehtäviä ja vastuita tietoturvallisuuden toteuttamisessa. Tietoturvallisuuden hallintaa tarkasteltiin prosessina, jossa organisaation tietoturvastrategia ja riskienhallinta ohjaavat toiminnan kehittämistä. Lisäksi tutustuttiin ISO 17799 -standardiin, joka määrittelee yleisiä toiminta-periaatteita organisaation tietoturvallisuuden hallintaan. Katsauksen lopuksi tutkittiin erilaisia tietoturvallisuuden kontrolleja tietoverkkojen, tietoaineiston ja saavutettavuuden suojaamiseksi.

Tutkimuksen käytännön osassa tehtiin kattava tietoturvakartoitus kohdeorganisaatiolle. Kartoituksen pohjana käytettiin ISO 17799 -standardia ja kartoitustyön painopisteiksi valittiin kohdeorganisaation kannalta tärkeitä aihealueita. Tutkimuksessa käytettiin viittä eri tiedonkeruumenetelmää: Dokumentaation läpikäynnissä tutkittiin kauttaaltaan organisaation tietojärjestelmien dokumentaatiot, järjestelmän läpikäynnissä tutkittiin järjestelmän teknisiä

suojauksia ja toimitilojen läpikäynnissä tutkittiin työ- ja tuotantotilojen teknisiä suojauksia. Työ- ja toimintatapatarkastelussa tehtiin havaintoja käytännön toiminnasta ja tutkittiin dokumentoimattomia käytäntöjä ja työtapoja. Puolistrukturoiduilla yksilöhaastatteluilla selvitettiin työntekijöiden tiedossa olevia organisaation tietoturvallisuuteen liittyviä oleellisia asioita, heidän asenteitaan ja ajatuksiaan tietoturvallisuudesta sekä organisaation tietoturvaosaamisen tasoa.

Kartoituksessa havaittiin monia tietoturvallisuuden kannalta hyvin toteutettuja asioita. Tekniset suojaukset, jokapäiväinen toiminta ja erikoistilanteiden hallinta on hoidettu hyvin ja etenkin tiedon saavutettavuuteen on panostettu. Organisaation tietoturvallisuuteen liittyvät suurimmat ongelmakohdat kohdistuvat pääasiassa hallinnolliselle puolelle. Selkeitä puutteita havaittiin erityisesti tietoturvatyön organisoimisessa ja vastuunjaossa, strategisessa suunnittelussa ja dokumentoinnissa sekä tietoturvahäiriöiden ja parannuskohteiden hallinnan organisoimisessa.

Kartoituksen tulosten pohjalta tehtiin kohdeorganisaatiolle 13-kohtainen kehityssuunnitelma, joka sisältää tarvittavat toimenpiteet, perustelut kunkin toimenpiteen tärkeydestä, aikatauluehdotuksen ja arvion jokaisen kohdan osalta sen läpiviemiseen tarvittavista resursseista. Ehdotettuja toimenpiteitä olivat muun muassa tietoturvatyön organisointi, dokumentoinnin ja koulutuksen parantaminen, liiketoiminnan vaatimusten määrittäminen ja tietoaineistoturvallisuuden kehittäminen. Kehitysehdotukset on suunniteltu siten, että kohdeorganisaatio pystyy realistisesti toteuttamaan muutokset joutumatta tekemään merkittäviä uhrauksia. Esitetyt toimenpiteet edellyttävät organisaatiolta halua sitoutua muutokseen ja aluksi selvästi näkyvän määrän työaikaa muutosten toteuttamiseen. Kun ehdotetut muutokset on saatu toteutettua, on tietoturvallisuustyö tehokkaampaa ja tietoturvallisuuden ylläpitämiseen tarvittavien resurssien määrä pienenee. Suurin haaste kehitystyön toteutumiselle on organisaation halu sitoutua muutokseen ja prosessin ylläpitämiseen sen käynnistämisen jälkeen.

Yhteenvetona voidaan todeta, että tehty tutkimus vastasi hyvin asetettuihin tutkimuskysymyksiin, ja sen puitteissa muodostettiin hyvä yleiskuva organisaatioiden tietoturvallisuuteen liittyvistä asioista. Tutkimuksen pohjalta kohdeorganisaatio voi lähteä kehittämään omaa tietoturvallisuuttaan ja annettujen kehitysehdotusten ja -aikataulun pohjalta korjata suurimmat kartoituksessa havaitut puutteet. Tämän kehitystyön myötä organisaatio pystyy tulevaisuudessa ylläpitämään riittävää tietoturvallisuuden tasoa ja siten vastaamaan liiketoiminnan edellyttämiin vaatimuksiin. Jos ehdotettuja muutoksia ei toteuteta, on uhkana että organisaatio tulee jatkossa menettämään kykynsä toimia nykyisellä

tasolla ja että suojattavat kohteet vaarantuvat riittämättömän tietoturvatyön myötä. Vähintäänkin muutosten toteuttamatta jättäminen tulee olemaan esteenä organisaation tietoturvatyön kehittymiselle ja myös resurssien oikean kohdentamisen myötä saatava hyöty jää saavuttamatta.

7.2 Tutkimuksen luotettavuus ja sovellettavuus

Kohdeorganisaation nykytilan kartoituksessa käytettiin useita eri menetelmiä tutkittujen asioiden selvittämiseksi. Jokaista yksittäistä tarkastelukohdetta pyrittiin lähestymään mahdollisuuksien mukaan vähintään kahdella eri tutkimusmenetelmällä, jotta saataisiin kattava näkemys eri osa-alueista ja voitaisiin vähentää yksittäisistä tutkimusmenetelmistä mahdollisesti johtuvia virheitä. Tutkimuksen aikana ei osoittautunut, että eri menetelmillä kerätty aineisto olisi ollut keskenään ristiriitaista, vaan löydökset tukivat toinen toisiaan. Koska kartoituksessa on käytetty pohjana yleisesti siihen käyttöön sovellettua ja kattavana pidettyä ISO 17799 -standardia, voidaan katsoa, että tutkimuksen aihepiiriä on käsitelty riittävän laajasti. Kartoitukseen liitettiin kuitenkin myös ISO 17799 -standardin ulkopuolelta joitakin kohdeorganisaation kannalta kiinnostavia aiheita.

Tuloksien luotettavuutta tarkasteltaessa on huomioitava, että tutkimuksen tekijä on toiminut usean vuoden ajan organisaation työntekijänä. Vaikka tekijä on tutkimuksen aikana tietoisesti pyrkinyt puolueettomaan tarkasteluun, on mahdollista, että yksittäisillä tutkimus-alueilla saatu tulos saattaa heijastella tekijän omaa käsitystä asiasta. Tekijän läheinen suhde kohdeorganisaatioon on helpottanut aineiston keruuta ja pääsyä eri tietoaineistoihin. Haastattelutilanteissa tutun haastattelijan läsnäolo on voinut rentouttaa tilannetta, jolloin haastatellut ovat saattaneet kertoa organisaation nykytilasta avoimemmin kuin jos haastattelija olisi ollut tuntematon, organisaation ulkopuolinen henkilö. Toisaalta on myös mahdollista, että yksittäiset haastatellut henkilöt ovat saattaneet esimerkiksi kielteisten seuraamusten pelossa vastata tai jättää kertomatta jotain siten, että asian todellinen tila on vääristynyt. Rinnakkaisten tutkimusmenetelmien ja riittävän kattavan haastatteluryhmän ansiosta on kuitenkin vähäinen todennäköisyys, että tällaista tulosten vääristymistä olisi päässyt esiintymään. Tältä pohjalta voidaan todeta, että tutkimus antaa kattavan ja luotettavan kuvan kohdeorganisaation tietoturvallisuuden nykytilasta.

Tämän tutkimuksen sisältö on ensisijaisesti suunniteltu Suomessa toimivan organisaation tarpeisiin, eikä siinä ole huomioitu ulkomaisten organisaatioiden tarpeita tai poikkeavaa lainsäädäntöä. Teoriaosuuden tulokset ovat hyödyllisiä kaikille tietoturvallisuuden kehitystyötä suunnitteleville tai arvioiville, ja ne ovat sovellettavissa myös muunlaisiin

organisaatioihin. Esitetyn teorian hallitseminen antaa tietoturvallisuuden hallinnan kannalta välttämättömän osaamisen tietoturvallisuuteen liittyvistä asioista, ja ISO 17799 -standardiin kytketty tietoturvallisuuden osa-aluejaottelu muodostaa sopivan alustan käytännössä minkälaisen tahansa organisaation tietoturvatyön kehitystyölle. Käytännön osan tietoturva-kartoituksen tulokset on tarkoitettu ensisijaisesti kohdeorganisaatiolle, joka voi tutkimuksen avulla käynnistää oman tietoturvallisuuden prosessinsa ja parantaa tietoturvallisuuden tasoaan kartoituksen havaintojen ja ehdotusten pohjalta. Koska samankaltaisia ongelmia todennäköisesti esiintyy myös muissa pienissä ja keskisuurissa organisaatioissa, voivat esitetyt kehitysehdotukset olla hyödyllisiä muillekin: kohdeorganisaation tilaa voi esimerkiksi peilata omaan organisaatioon ja käyttää sitä soveltuvin osin vertailukohtana oman organisaation tarkastelussa.

7.3 Jatkotutkimuksen aiheet

Koska tietoturvallisuuden tutkimuskenttä on hyvin laaja, keskityttiin tässä tutkimuksessa erityisesti kohdeorganisaation kannalta oleellisiin asioihin. Etenkin tietoturvakontrollien osalta laajemmalle jatkotutkimukselle on lähes rajattomasti mahdollisuuksia. Tähän osioon on poimittu muutama aihe, jotka erottuivat kiinnostavuudellaan ja tarpeellisuudellaan muiden joukosta.

Tässä tutkimuksessa havaittiin, että kohdeorganisaatiolla oli ongelmia etenkin tietoturvallisuuden vastuuttamisessa ja organisoimisessa sekä tietoturvatyön hallinnassa. Pienikokoisella organisaatiolla ei tyypillisesti ole resursseja ja tarvittavaa osaamista näiden asioiden järjestämiseksi. Jatkotutkimuksella voitaisiin selvittää, pystyttäisiinkö tilannetta parantamaan kehittämällä erityisesti rajallisilla resursseilla toimivien organisaatioiden käyttöön sopivia menetelmiä. Esimerkkinä voisi olla hyvin kevyt ja helposti omaksuttava laajalti yksinkertaistettu prosessi, jonka avulla tietoturvallisuustyön ohjaaminen onnistuisi pienissäkin organisaatioissa.

Tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja saavutettavuuden ylläpitämistä. Nämä kolme käsitettä ovat kuitenkin jossain määrin keskenään ristiriidassa, sillä luottamuksellisuuden ja eheyden suojaaminen johtaa tyypillisesti saavutettavuuden heikkenemiseen. Jatkotutkimuksella voitaisiin selvittää, kuinka näiden suojeltavien ominaisuuksien välille voidaan löytää optimaalinen ja kustannustietoinen tasapaino siten, että liiketoiminnan vaatimukset täyttyvät vaativammissakin tapauksissa.

Tietoturvallisuuden prosessin yhtenä tehtävänä on seurata asetettujen kontrollien ja tehtyjen toimenpiteiden onnistumista ja hyödyllisyyttä kehitystyötä varten. Jotta onnistumista voitaisiin arvioida, tarvitaan organisaation käyttöön useita erilaisia mittareita. Koska tämän tutkimuksen puitteissa ei ollut mahdollista käsitellä sopivien mittareiden valitsemista, olisi sitä hyödyllistä tutkia tarkemmin.

Kansainväliset organisaatiot törmäävät väistämättä toiminnassaan siihen, että eri valtioiden lainsäädännöt poikkeavat joskus hyvinkin oleellisesti toisistaan. Yksi haaste näille organisaatioille onkin noudattaa kunkin maan lainsäädäntöä samanaikaisesti siltä osin kuin niitä on sovellettava toiminnassa. Myös yhden valtion sisällä toimiva organisaatio voi törmätä kansainvälisyyden tuomiin ongelmiin tietoturvallisuuden osalta. Esimerkiksi ylläpitopalveluiden ostaminen eri puolilla maapalloa *follow the sun* -periaatteella toimivalta organisaatiolta voi olla ongelmallista yksityishenkilöiden kanssa toimivalle organisaatiolle, sillä suomalainen lainsäädäntö sisältää rajoituksia henkilötietojen siirtämiselle Euroopan unionin jäsenmaiden ulkopuolelle. Kansainvälisen toiminnan tietoturvallisuudelle tuomat haasteet olisi oivallinen aihe jatkotutkimukselle.

LÄHTEET

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 41–46. New York, NY, Yhdysvallat: ACM Press. ISSN: 0001-0782.

Anderson, R. (2001). *Security Engineering*. Yhdysvallat: John Wiley & Sons, Inc. ISBN: 0-471-38922-6.

Cisco Systems (2006a). *Inter-Switch Link and IEEE 802.1Q Frame Format*. Yhdysvallat: Cisco Systems. Viitattu: 3.6.2007, `http://www.cisco.com/warp/public/473/741_4.pdf`

Cisco Systems (2006b). *Protecting Your Core: Infrastructure Protection Access Control Lists*. Yhdysvallat: Cisco Systems. Viitattu: 3.6.2007, `http://www.cisco.com/warp/public/707/iacl.pdf`

Covert, E., & Nielsen, F. (2005). Measuring Risk Using Existing Frameworks. *Information systems security*, *14*(1), 21–25. New York, NY, Yhdysvallat: Auerbach Publications. ISSN: 1065-898X.

Crosby, L. A. (1991). Expanding the role of CSM in total quality. *International Journal of Service Industry Management*, *2*(2), 5–19. Bradford, Iso-Britannia: MCB University Press. ISSN: 0956-4233.

Dourish, P., Grinter, R. E., Delgado de la Flor, R., & Joseph, M. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, *8*, 391–401. Lontoo, Iso-Britannia: Springer-Verlag. ISSN: 1617-4909.

Hakala, M., Vainio, M., & Vuorinen, O. (2006). Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland. ISBN: 951-846-273-9.

Hansche, S. D. (2004). Making security awareness happen. Kirjassa H. F. Tipton & M. Krause (toim.), *Information Security Handbook* (5. painos, s. 999-1009). Boca Raton, FL, Yhdysvallat: Auerbach Publications. ISBN: 0-8493-1997-8.

Herbig, P., & Milewicz, J. (1997). The relationship of reputation and credibility to brand success. *Pricing Strategy & Practice*, *5*(1), 25–29. Bradford, Iso-Britannia: MCB University Press. ISSN: 0968-4905.

Huston, G. (1999). *ISP survival guide: strategies for running a competitive ISP*. Yhdysvallat: John Wiley & Sons. ISBN: 0-471-31499-4.

Im, G. P., & Baskerville, R. L. (2005). A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error. Teoksessa: *The DATA BASE for Advances in Information Systems*, *36*(4), 68–79. New York, NY, Yhdysvallat: ACM Press. ISSN: 0095-0033.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, *43*(2), 90–98. New York, NY, Yhdysvallat: ACM Press. ISSN: 0001-0782.

Jones, V. C. (2001). *High Availability Networking with Cisco*. Yhdysvallat: Addison-Wesley. ISBN: 0-201-70455-2.

Järvinen, P. (2001). *Tietoturva & yksityisyys*. Jyväskylä: Docendo Finland. ISBN: 951-846-152-X.

Kairab, S. (2005). *A practical guide to security assessments*. Boca Raton, FL, Yhdysvallat: Auerbach Publications. ISBN: 0-8493-1706-1.

Kamoun, F. (2005). Toward best maintenance practices in communications network management. *International Journal of Network Management*, 15(5), 321–334. New York, NY, Yhdysvallat: John Wiley & Sons. ISSN: 1099-1190.

Kyrölä, T. (2001). *Esimies ja tietoriskien hallinta*. Helsinki: Werner Söderström. ISBN: 951-0-25645-5.

Lehtonen, S., Ahonen, P., Savola, R., Uusitalo, I., Karjalainen, K., Kuusela, E., et al. (2006). *LUOTI-julkaisuja 9/2006: Langattomien verkkojen tietoturva*, 13–20. Helsinki. ISBN: 952-201-728-5.

Lonka, H., Hjelt, M., Vanhanen, J., Raivio, T., Vaahtoranta, T., Visuri, P., et al. (2002). *Riskien hallinta Suomessa, Esiselvitys*, 8–14. Helsinki: Edita Prima. ISBN: 951-37-3801-9.

Marcus, E., & Stern, H. (2003). *Blueprints for High Availability* (2. painos). Indianapolis, IN, Yhdysvallat: Wiley Publishing. ISBN: 0-471-43026-9.

Microsoft (2006). *Server and Domain Isolation Using IPsec and Group Policy, Chapter 7: Troubleshooting IPsec*. Yhdysvallat: Microsoft. Viitattu: 3.6.2007, http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/ipsecch7.mspx

Miettinen, J. E. (1999). *Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan.* Helsinki: Kauppakaari. ISBN: 952-14-0229-6.

Miettinen, J. E. (2002). *Yritysturvallisuuden käsikirja*. Helsinki: Kauppakaari. ISBN: 952-14-0559-7.

Oggerino, C. (2001). *High Availability Network Fundamentals*. Indianapolis, IN, Yhdysvallat: Cisco Press. ISBN: 1-58713-017-3.

Parker, D. B. (1997). The strategic values of information security in business. *Computers & Security*, 16, 572–582. Amsterdam, Hollanti: Elsevier. ISSN: 0167-4048.

Siponen, M. T. (2000a). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. Bradford, Iso-Britannia: MCB University Press. ISSN: 0968-5227.

Siponen, M. T. (2000b). Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Information Management & Computer Security*, *8*(5), 197–209. Bradford, Iso-Britannia: MCB University Press. ISSN: 0968-5227.

Schneier, B. (2004). *Secrets and lies*. Indianapolis, IN, Yhdysvallat: Wiley Publishing. ISBN: 0-471-45380-3.

Spears, J. (2006). The effects of user participation in identifying information security risk in business processes. *Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research: Forty four years of computer personnel research: achievements, challenges & the future*, 351–352. New York, NY, Yhdysvallat: ACM Press. ISBN: 1-59593-349-2.

Stallings, W. (2006). *Cryptography and network security* (4. painos). Upper Saddle River, NJ, Yhdysvallat: Pearson Education. ISBN: 0-13-187316-4.

Storey, N. (1996). *Safety Critical Computer Systems*. Yhdysvallat: Addison-Wesley. ISBN: 0-201-42787-7.

Suomen Standardoimisliitto SFS (2006), ISO/IEC 17799:fi -standardi. Helsinki.

Suominen, A. (2003). *Riskienhallinta* (3. painos). Helsinki: Werner Söderström. ISBN: 951-0-26878-X.

Tate, J., Cartwright, B., Cronin, J., & Dapprich, C. (2003). *IBM SAN Survival Guide Featuring the IBM 3534 and 2109* (2. painos). Yhdysvallat: IBM Redbooks. ISBN: 0-738-49985-4.

Tipton, H. F., & Krause, M. (2004). *Information Security Handbook* (5. painos, toim.). Boca Raton, FL, Yhdysvallat.: Auerbach Publications. ISBN: 0-8493-1997-8.

Valtiovarainministeriö (2002). *Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002*. Suomi. ISBN: 951-804-293-4.

Valtiovarainministeriö (2003). *Valtionhallinnon tietoturvakäsitteistö, VAHTI 4/2003*. Suomi. ISBN: 951-804-404-8.

Valtiovarainministeriö (2005). *Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005*. Suomi. ISBN: 951-804-521-6.

Virtanen, T. (2002). *Four views on security*. Espoo: Otamedia. ISBN: 951-22-6160-X.

Virtanen, T. (2004). Oppimateriaali Teknillisen korkeakoulun kurssille T-110.260 Yritysturvallisuuden perusteet. Espoo: Edita Prima Oy.

von Solms, B. (2000). Information security – the third wave? *Computers & Security*, 19, 615–620. Amsterdam, Hollanti: Elsevier. ISSN: 0167-4048.

von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers & Security*, 23, 273–279. Amsterdam, Hollanti: Elsevier. ISSN: 0167-4048.

Vorster, A., & Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*, 95–103. Pretoria, Etelä-Afrikka: SAICSIT. ISBN: 1-59593-258-5.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23, 191–198. Amsterdam, Hollanti: Elsevier. ISSN: 0167-4048.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM*, *46*(8), 91–95. New York, NY, Yhdysvallat: ACM Press. ISSN: 0001-0782.

Whitman, M. E., & Mattord, H. J. (2005). *Principles of information security* (2. painos). Boston, MA, Yhdysvallat: Thomson Course Technology. ISBN: 0-619-21625-5.

LIITTEET

LIITE A: HAASTATTELUKYSYMYKSET

LIITE B: TIEDONKERUU JA JAOTTELU ISO 17799 -STANDARDIN OSALTA

LIITE C: YHTEENVETO KOHDEORGANISAATION TIETOTURVALLISUUDEN NYKYTILASTA

LIITE A: HAASTATTELUKYSYMYKSET

1. Mikä on nykyinen työkuvasi? Kuvaile lyhyesti minkälaisia tehtäviä siihen kuuluu.
2. Mitä mielestäsi tietoturvallisuudella tarkoitetaan?
    a. Mihin asioihin se liittyy?
    b. Missä kaikkialla tietoturvallisuuteen liittyviin asioihin törmää?
3. Minkälaisia tietoturvallisuuteen liittyviä asioita kohtaat työssäsi?
    a. Kuinka usein?
4. Minkälaisia tietoturvallisuuteen liittyviä päätöksiä joudut työssäsi tekemään?
    a. Koetko että sinulla on riittävät valmiudet niiden tekemiseen?
5. Minkälaista tietoa käsittelet työssäsi? Kategoriat: Yrityksen sisäinen viestintä, yrityksen muu viestintä, tuotekehitys, hallinto (projektisuunnitelmat, toisten tuntilistat, strategia, markkinointi, henkilöstöasiat, ym.), sisäiset dokumentit, esitykset ja raportit sekä organisaation ulkopuolisille tahoille osoitetut dokumentit, esitykset ja raportit.
6. Minkälaisia viestimiä käytät työssäsi/työpaikalla? (esim. puhelin, matkapuhelin, faksi, pikaviestin, sähköposti, IRC)
    a. Minkälaista kommunikointia käyt milläkin välineellä?
7. Mitä tiedonsiirto- ja tallennusvälineitä käytät työssäsi tai työpaikalla? (esim. levyke, cd, usb-tikku, kannettava tietokone)
    a. Entä mitä tiedonsiirto-ohjelmia tai -protokollia käytät työssäsi tai työpaikalla? (esim. sftp, ftp, sähköposti)
8. Tiedätkö onko työpaikallanne ohjeistettu tiedon luokittelusta? (esim. luottamuksellinen, salainen)
    a. Jos on, niin miten tietoa luokitellaan työpaikalla? Millaisia käytäntöjä luokitellun tiedon käsittelemiseksi on?
9. Miten luokittelematonta tietoa käsitellään työpaikallanne?
10. Onko luokittelemattoman tiedon käsittelyä ohjeistettu?
11. Onko tiedolle määritelty omistajaa työpaikallanne?
    a. Missä tilanteissa ja kuinka usein näin toimitaan?
    b. Jos ei, niin kuka vastaa näistä tiedoista?
12. Salataanko työpaikallanne tietoa teknisillä apuvälineillä (esim. PGP)?
    a. Jos, niin miten tietoa salataan?
    b. Minkälaista tietoa salataan?
13. Onko tiedon salaamista ohjeistettu? Toimitko ohjeiden mukaan?

14. Miten tietoa hävitetään?
    a. Onko asiaa ohjeistettu? Toimitko ohjeiden mukaan?
15. Minkälaiset oikeudet sinulla on työkoneesi hallintaan?
    a. Onko sinulla oikeuksia hallita muita koneita? Jos on, mitä varten?
16. Onko teillä käytössä kaikissa tilanteissa henkilökohtaiset tunnukset ja salasanat?
    a. Jos ei, niin missä tilanteissa ei ja miksi?
17. Miten salasanojen muodostaminen on ohjeistettu? (luominen, uusiminen, kompleksisuus)
    a. Valvotaanko sitä?
    b. Toimitko ohjeiden mukaan?
18. Minkälaisia salasanoja sinulla on käytössä?
    a. Onko kaikkiin koneisiin sama salasana, kaikkiin eri vai jotain siltä väliltä?
    b. Miten itse keksit salasanasi?
    c. Onko nykyinen salasanakäytäntö hyvä?

Hallinto

19. Kuka on vastuussa riskien kartoittamisesta ja arvioinnista?
    a. Tehdäänkö sitä ja missä yhteydessä?
20. Ketkä osallistuvat tietoturvallisuuden kehittämiseen liittyviin päätöksiin? (suunnitelmat, investoinnit, tietoturvapolitiikka)
21. Onko organisaatiolla tietoturvapolitiikkaa?
    a. Jos on, mitkä sen tavoitteet ovat?
22. Mitä vaatimuksia emoyritys on esittänyt organisaatiolle tietoturvallisuuden suhteen?
23. Valvotaanko organisaatiossa tietoturvallisuuteen liittyvien käytäntöjen ja ohjeistuksien noudattamista?
    a. Jos valvotaan, miten?
24. Tarkistetaanko uusien työntekijöiden taustat?
    a. Jos tarkistetaan, miten?
    b. Jos ei, miksi ei?
25. Järjestetäänkö uusille työntekijöille ohjeistusta tai koulutusta tietoturvallisuudesta?
    a. Jos ei, miksi?
26. Kehitetäänkö nykyisten työntekijöiden tietoturvallisuusosaamista jotenkin?

a. Jos kehitetään, niin miten ja kuinka usein?

b. Jos ei, miksi?

27. Miten toiminnan lamaannuttaviin tapahtumiin on varauduttu? (esim. työntekijän katoaminen, onnettomuus laitesalissa)

Ylläpito

28. Mitä ohjeita on käytössä tietoturvallisuuden ylläpitämiseksi ylläpitotyössä?

    a. Ovatko ne ajantasaisia?

    b. Noudatetaanko niitä? Valvotaanko noudattamista?

29. Miten varmistetaan, että järjestelmässä ei ole tietoturva-aukkoja?

30. Miten huolehditaan siitä, että ohjelmistot ovat ajan tasalla?

    a. Miten saadaan tieto uusista päivityksistä?

31. Minkälaisia teknisiä ratkaisuja on käytössä järjestelmän saavutettavuuden varmistamiseksi?

32. Miten vikatilanteisiin on varauduttu?

    a. Miten niihin reagoidaan?

33. Tehdäänkö järjestelmissä ennakoivaa ylläpitotyötä?

    a. Jos, niin millaista ja miten usein?

34. Miten järjestelmään tehtävät muutokset hallitaan? (esim. testaus, muutosten kirjaaminen, luvat muutoksiin)

35. Miten ylläpitotyössä pyritään välttämään inhimillisiä virheitä?

36. Kuinka vierailu ja huoltotyöt on järjestetty laitetiloissa?

37. Miten tiedon hävittämisestä huolehditaan tietokoneita uusittaessa tai kiintolevyjä ja muita vastaavia tallennusvälineitä hävitettäessä?

Ohjelmointi

38. Minkälaisia tietoturvaan liittyviä käytäntöjä ja menetelmiä on käytössä ohjelmointityössä? (esim. syötteiden tarkistaminen)

39. Miten varmistetaan, että kehitetyssä ohjelmakoodissa ei ole tietoturva-aukkoja? (esim. lähdekoodin tarkistus, testaaminen)

40. Mitä ohjeita on käytössä tietoturvallisuuden ylläpitämiseksi ohjelmointityössä?

    a. Ovatko ne ajantasaisia?

    b. Noudatetaanko niitä? Valvotaanko noudattamista?

Loput yhteiset kysymykset

41. Oletko työssäsi yhteydessä asiakkaisiin? Millaisissa asioissa?
    a. Onko asiakkaan tunnistamiselle joskus tarvetta? Milloin?
    b. Kuinka asiakkaan tunnistamisesta huolehditaan organisaatiossa?
    c. Näetkö asiakasyhteydenotoissa joitakin riskejä? (esim. asiattomat toimeksiannot, salasanautelut)
    d. Onko asiakasyhteydenottojen hoitamista ohjeistettu? Noudatatko ohjeita?
42. Kuka on vastuussa tietoturvallisuuden toteuttamisesta organisaatiossa?
43. Muistatko tietoturvaan liittyviä ongelmatapauksia?
    a. Miten niihin reagoitiin?
    b. Ovatko jotkut toistuneet? Kuinka usein?
44. Onko annettu ohjeita miten tietoturvaan liittyvät ongelmatilanteet käsitellään?
    a. Noudatetaanko niitä?
45. Jos havaitset ongelman, mahdollisen tietoturva-aukon tai epäilyttävää toimintaa, miten reagoit?
    a. Jos työpaikan käytävällä häärii kulkuluvaton, epäilyttävältä vaikuttava henkilö, miten toimit?
46. Onko tietoturvallisuuden suojaustoimenpiteistä joskus haittaa työnteolle? Minkälaista haittaa?
    a. Onko tilannetta pyritty korjaamaan? Miten?
47. Onko nykyään käytössä tai onko aikaisemmin ollut sellaisia tietoturvamekanismeja jotka tuntuvat turhilta tai liioitelluilta? Jos, niin kuvaile lyhyesti niitä ja kerro mitä niissä on ongelmallista.
48. Minkälainen asenne mielestäsi työpaikalla vallitsee tietoturvallisuuden suhteen?
    a. Panostetaanko siihen? Näkyykö se jotenkin käytännössä?
    b. Miten itse suhtaudut tietoturvaan?
49. Voitaisiinko jotain tehdä paremmin kuin miten se tehdään nyt?

LIITE B: TIEDONKERUU JA JAOTTELU ISO 17799 -STANDARDIN OSALTA

Käytetyt lyhenteet:

D	Dokumentaation läpikäynti
H	Haastattelu
T	Työ- ja toimintatapatarkastelu
JL	Järjestelmän läpikäynti
TL	Toimitilojen läpikäynti
HA	Hallinnollinen turvallisuus
HE	Henkilöstöturvallisuus
LJ	Liiketoiminnan jatkuvuuden hallinta
LO	Laitteisto- ja ohjelmistoturvalisuus
TK	Tietoliikenne- ja käyttötoimintoturvallisuus
TO	Toimitilaturvallisuus
TP	Tietoaineistoturvallisuus ja pääsynhallinta
VA	Vaatimustenmukaisuus
ei sov.	ei sovellu kohdeorganisaatioon

Luku	Otsikko	Menetelmät	Aihealue
5	**Turvallisuuspolitiikka**		
5.1	**Tietoturvapolitiikka**		
5.1.1	Tietoturvapolitiikan määrittelyasiakirja	H/D/T	HA
5.1.2	Tietoturvapolitiikan katselmointi	D/T	HA

6	**Tietoturvallisuuden organisoiminen**		
6.1	**Sisäinen organisaatio**		
6.1.1	Johdon sitoutuminen tietoturvallisuuteen	D/T	HT
6.1.2	Tietoturvallisuuden koordinointi	H/D/T	HT
6.1.3	Tietoturvallisuutta koskevien vastuiden jako	D/T	HT
6.1.4	Tietojenkäsittelypalveluja koskeva hyväksymisprosessi	D/T	HT
6.1.5	Salassapitositoumus	D/T	HT
6.1.6	Yhteydet viranomaisiin	D/T	HT
6.1.7	Yhteydet erityisintressiryhmiin	D/T	HT
6.1.8	Tietoturvallisuuden riippumaton arviointi	D/T	HT
6.2	*Ulkopuoliset tahot*	*ei sov.*	

7	**Suojeltavien kohteiden hallinta**		
7.1	**Vastuu suojattavista kohteista**		
7.1.1	Suojattavien kohteiden luetteloiminen	D/T	TP
7.1.2	Suojattavien kohteiden omistajuus	H/D/T	TP
7.1.3	Suojattavien kohteiden hyväksyttävä käyttö	D/T	TP
7.2	**Tiedon luokitus**		
7.2.1	Luokitusohjeita	H/D/T	TP
7.2.2	Tiedon merkitseminen ja käsittely	H/D/T	TP

8	**Henkilöstöturvallisuus**		
8.1	**Ennen työsuhteen alkua**		
8.1.1	Roolit ja vastuut	D/T	HE

Luku	Otsikko	Menetelmät	Aihealue
8.1.2	Valinta	H/D/T	HE
8.1.3	Työsopimuksen ehdot	D/T	HE
8.2	**Työsuhteen aikana**		
8.2.1	Johdon vastuu	H/D/T	HE
8.2.2	Tietoturvatietoisuus, -koulutus ja -harjoittelu	H/D/T	HE
8.2.3	Sanktiomenettelyt	D/T	HE
8.3	**Työsuhteen päättyminen tai muuttuminen**		
8.3.1	Päättämisvastuut	D/T	HE
8.3.2	Suojattavien kohteiden palauttaminen	D/T	HE
8.3.3	Käyttöoikeuksien poistaminen	D/T	HE

9	Fyysinen turvallisuus ja ympäristön turvallisuus		
9.1	**Turva-alueet**		
9.1.1	Fyysinen turva-alue	TL/D	TO
9.1.2	Kulunvalvonta	TL/H/D	TO
9.1.3	Toimistojen, tilojen ja laitteiden suojaus	TL/D	TO
9.1.4	Suojaus ulkoisia ja ympäristön aiheuttamia uhkia vastaan	TL/D	TO
9.1.5	Turva-alueilla työskentely	TL/D	TO
9.1.6	Julkinen pääsy, toimitukset ja kuormausalueet	TL/D	TO
9.2	**Laiteturvallisuus**		
9.2.1	Laitteiden sijoitus ja suojaus	TL/D	TO
9.2.2	Peruspalvelut	TL/D	TO
9.2.3	Kaapeloinnin turvallisuus	TL/D	TO
9.2.4	Laitteiden huolto	D/T	LO
9.2.5	Toimitilojen ulkopuolelle vietävien laitteiden turvallisuus	D/T	TK
9.2.6	Laitteistojen turvallinen käytöstä poistaminen ja kierrättäminen	H/D/T	TP
9.2.7	Suojattavien kohteiden siirtäminen pois työpaikalta	D/T	TK

10	Tietoliikenteen ja käyttötoimintojen hallinta		
10.1	**Menettelyohjeet ja velvollisuudet**		
10.1.1	Kirjalliset menettelyohjeet	D	TK
10.1.2	Muutosten hallinta	H/D/T	TK
10.1.3	Tehtävien eriyttäminen	D/T	TK
10.1.4	Kehitettävänä, testattavana ja tuotannossa olevien palveluiden eriyttäminen	D/T	TK
10.2	**Ulkopuolisten palvelujen toimittamisen hallinta**		
10.2.1	Palvelujen toimittaminen	D/T	TK
10.2.2	Ulkopuolisten palvelujen tarkkailu ja katselmointi	D/T	TK
10.2.3	Ulkopuolisten palvelujen muutosten hallinta	D/T	TK
10.3	**Järjestelmän suunnittelu ja hyväksyntä**		
10.3.1	Kapasiteetin hallinta	D/T	TK
10.3.2	Järjestelmän hyväksyntä	D/T	TK
10.4	**Suojaus haittaohjelmia ja liikkuvia ohjelmia vastaan**		
10.4.1	Turvamekanismit haittaohjelmien torjunnassa	JL/D/T	TK
10.4.2	Turvamekanismit liikkuvien ohjelmien torjunnassa	JL/D/T	TK
10.5	**Varmuuskopiointi**		
10.5.1	Tietojen varmuuskopiointi	JL/D/T	LJ
10.6	**Verkon turvallisuuden hallinta**		
10.6.1	Verkon turvamekanismit	JL/D/T	TK
10.6.2	Verkkopalvelujen turvaaminen	JL/D/T	TK
10.7	**Tietovälineiden käsittely**		
10.7.1	Siirrettävien tietovälineiden hallinta	H/D/T	TK

Luku	Otsikko	Menetelmät	Aihealue
10.7.2	Tietovälineiden poistaminen käytöstä	H/D/T	TK
10.7.3	Tietojen käsittelyohjeet	H/D/T	TK
10.7.4	Järjestelmän dokumentoinnin turvaaminen	JL/D/T	TK
10.8	**Tiedon vaihto**		
10.8.1	Tiedonvaihtoperiaatteet ja -menettelytavat	JL/D/T	TK
10.8.2	*Tiedonvaihtosopimukset*	*ei sov.*	
10.8.3	Fyysiset tietovälineet kuljetuksen aikana	D/T	TK
10.8.4	Sähköinen viestintä	H/JL/D/T	TK
10.8.5	*Liiketoiminnan tietojärjestelmät*	*ei sov.*	
10.9	***Verkkoasiointipalvelut***	*ei sov.*	
10.10	**Tarkkailu**		
10.10.1	Tapahtumalokit	JL/D	TK
10.10.2	Järjestelmän käytön tarkkailu	JL/D/T	TK
10.10.3	Lokitietojen suojaus	JL/D	TK
10.10.4	Pääkäyttäjä- ja operaatiolokit	JL/D	TK
10.10.5	Häiriöiden kirjaus	JL/D/T	TK
10.10.6	Kellojen synkronointi	JL/D	TK

11	**Pääsyoikeuksien valvonta**		
11.1	**Liiketoiminnan asettamat vaatimukset pääsynvalvonnalle**		
11.1.1	Pääsynvalvonnan toimintaperiaatteet	D/T	TP
11.2	**Käyttöoikeuksien hallinta**		
11.2.1	Käyttäjien rekisteröinti	D/T	TP
11.2.2	Pääkäyttäjän oikeuksien hallinta	D/T	TP
11.2.3	Käyttäjän salasanojen hallinta	D/T	TP
11.2.4	Käyttöoikeuksien uudelleenarviointi	D/T	TP
11.3	**Käyttäjän velvollisuudet**		
11.3.1	Salasanan käyttö	D/T	TP
11.3.2	Valvomattomat käyttäjien laitteet	D/T	TP
11.3.3	Puhtaan pöydän ja puhtaan näytön politiikka	D/T	TP
11.4	**Verkkoon pääsyn hallinta**		
11.4.1	Verkkopalvelujen käytön periaatteet	D/T	TP
11.4.2	Ulkopuolisia yhteyksiä käyttävien henkilöiden todentaminen	JL/D/T	TP
11.4.3	Laitteiden tunnistus verkossa	JL/D/T	TP
11.4.4	Etähuoltoyhteyksien suojaus	JL/D/T	TP
11.4.5	Verkkojen looginen jaottelu	JL/D/T	TP
11.4.6	Verkkoyhteyksien valvonta	JL/D/T	TP
11.4.7	Verkon reitityksen valvonta	JL/D/T	TP
11.5	**Käyttöjärjestelmään pääsyn valvonta**		
11.5.1	Turvalliset sisäänkirjausmenettelyt	JL/D/T	TP
11.5.2	Käyttäjän tunnistaminen ja todentaminen	JL/D/T	TP
11.5.3	Salasanojen hallintajärjestelmä	JL/D/T	TP
11.5.4	Järjestelmän apuohjelmien käyttö	JL/D/T	TP
11.5.5	Istunnon aikakatkaisu	JL/D/T	TP
11.5.6	Yhteysajan rajoittaminen	JL/D/T	TP
11.6	**Sovellukseen ja tietoon pääsyn valvonta**		
11.6.1	Tietojen käytön rajoittaminen	JL/D/T	TP
11.6.2	Arkaluonteisen sovelluksen eristäminen	JL/D/T	TP
11.7	**Tietokoneen matkakäyttö ja etätyö**		
11.7.1	Tietokoneen matkakäyttö ja tietoliikenne	JL/D/T	TP
11.7.2	Etätyö	JL/D/T	TP

Luku	Otsikko	Menetelmät	Aihealue
12	**Tietojärjestelmien hankinta, kehitys ja ylläpito**		
12.1	**Tietojärjestelmien turvallisuusvaatimukset**		
12.1.1	Turvallisuusvaatimusten analysointi ja määrittely	D/T	LO
12.2	***Virheetön tietojenkäsittely sovelluksissa***	*ei sov.*	
12.3	**Salakirjoitusmekanismi**		
12.3.1	Salakirjoitusmekanismien käytön periaatteet	D/T	LO
12.3.2	Salausavainten hallinta	JL/D/T	LO
12.4	**Järjestelmätietojen turvallisuus**		
12.4.1	Tuotannossa olevan ohjelmiston hallinta	JL/D/T	LO
12.4.2	Järjestelmän testiaineistojen suojaus	JL/D/T	LO
12.4.3	Ohjelmien lähdekoodiin pääsyn hallinta	JL/D/T	LO
12.5	**Kehitys- ja tukiprosessien turvallisuus**		
12.5.1	Muutosten valvontamenettelyt	H/D/T	LO
12.5.2	Käyttöjärjestelmän muutosten jälkeinen sovellusten tekninen tarkastus	D/T	LO
12.5.3	Ohjelmistopakettien muutoksia koskevat rajoitukset	D/T	LO
12.5.4	Tietovuodot	JL/D/T	LO
12.5.5	Ulkoistettu ohjelmistokehitys	D/T	LO
12.6	**Teknisten haavoittuvuuksien hallinta**		
12.6.1	Teknisten haavoittuvuuksien valvonta	D/T	LO

13	**Tietoturvahäiriöiden hallinta**		
13.1	**Tietoturvatapahtumista ja -heikkouksista raportoiminen**		
13.1.1	Tietoturvatapahtumien raportointi	H/D/T	HA
13.1.2	Turvallisuuden heikkouksista raportoiminen	H/D/T	HA
13.2	**Tietoturvahäiriöiden ja parannuskohteiden hallinta**		
13.2.1	Vastuut ja menettely	D/T	HA
13.2.2	Tietoturvahäiriöistä oppiminen	D/T	HA
13.2.3	Todisteiden kokoaminen	D/T	HA

14	**Liiketoiminnan jatkuvuuden hallinta**		
14.1	**Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia**		
14.1.1	Tietoturvallisuuden sisällyttäminen liiketoiminnan jatkuvuuden hallintaprosessiin	D/T	LJ
14.1.2	Liiketoiminnan jatkuvuus ja riskien arviointi	D/T	LJ
14.1.3	Tietoturvallisuuden sisältävien jatkuvuussuunnitelmien kehittäminen ja toteuttaminen	D/T	LJ
14.1.4	Liiketoiminnan jatkuvuussuunnittelun puitteet	D/T	LJ
14.1.5	Liiketoiminnan jatkuvuussuunnitelmien testaus, ylläpito ja uudelleenarviointi	D/T	LJ

15	**Vaatimustenmukaisuus**		
15.1	**Lakisääteisten vaatimusten noudattaminen**		
15.1.1	Sovellettavan lainsäädännön tunnistaminen	D/T	VA
15.1.2	Aineettomat oikeudet	D/T	VA
15.1.3	Organisaation tallenteiden suojaus	D/T	VA
15.1.4	Tietosuoja ja henkilötietojen yksityisyys	D/T	VA
15.1.5	Tietojenkäsittelypalvelujen väärinkäytön estäminen	D/T	VA
15.1.6	Salakirjoitusmekanismeja koskevat säädökset	D/T	VA
15.2	***Turvallisuuspolitiikan ja -standardien noudattaminen ja tekninen vaatimustenmukaisuus***	*ei sov.*	
15.3	***Tietojärjestelmän tarkastusnäkökohtia***	*ei sov.*	

LIITE C: YHTEENVETO KOHDEORGANISAATION TIETOTURVALLISUUDEN NYKYTILASTA

Käytetty arviointiasteikko:

0	Ei toteutettu
1	Osittain toteutettu
2	Lähes toteutettu
3	Toteutettu

Hallinnollinen turvallisuus	
5.1 Tietoturvapolitiikka	0
Tietoturvapolitiikkaa ei ole eikä sen tekemistä ole aloitettu.	
6.1 Sisäinen organisaatio	1
Sisäistä organisointia tietoturvatehtävien osalta ei ole käytännössä suoritettu ja vastuukysymykset ovat pääosin epäselviä. Organisaation työntekijät ovat kuitenkin ottaneet oma-aloitteisesti vastuuta tietoturvallisuudesta omilla tehtäväalueillaan.	
13.1 Tietoturvatapahtumista ja -heikkouksista raportoiminen	2
Raportoimisesta ei ole kirjallisia ohjeita, mutta työntekijät ovat tietoisia oikeasta toimintatavasta.	
13.2 Tietoturvahäiriöiden ja parannuskohteiden hallinta	1
Tietoturvahäiriöiden osalta ei ole erillisiä toimenpideohjeita, vaan ne käsitellään samalla prosessilla kuin kaikki muutkin reaktiivisia toimenpiteitä vaativat tapahtumat: ensisijaisesti vakiintuneiden käytäntöjen mukaan, tarpeen mukaan myös improvisoiden. Poikkeamat käsitellään tyypillisesti ainoastaan ylläpidon sisäisessä palaverissa. Parannuskohteiden hallinnalle ei ole olemassa vakiintunutta käytäntöä.	

Tietoaineistoturvallisuus ja pääsynhallinta	
7.1 Vastuu suojattavista kohteista	0
Suojattavia kohteita ei ole eksplisiittisesti yksilöity eikä luetteloitu. Tiedon omistajaa ei myöskään ole määritelty.	
7.2 Tiedon luokitus	0
Tiedon luokittelua ei ole ohjeistettu eikä organisaatiossa ole käytössä vakiintunutta luokittelutapaa. Myöskään luokittelemattoman tiedon käsittelyä ei ole ohjeistettu.	
9.2 Laiteturvallisuus	3
Laitteiden käytöstä poistaminen on järjestetty asianmukaisesti.	
11.1 Liiketoiminnan asettamat vaatimukset pääsynvalvonnalle	0
Liiketoiminnan vaatimuksia pääsynvalvonnalle ei ole määritelty.	

11.2 Käyttöoikeuksien hallinta	2
Käyttöoikeuksien hallinta on järjestetty pääosin asianmukaisesti. Yhteiskäyttötunnuksista ei kuitenkaan pidetä kirjaa, eikä pääkäyttäjien valtuuksia ole kirjattu. Sovelluskehittäjillä on pääsy joihinkin palvelimiin pääkäyttäjän oikeuksilla. Käyttöoikeuksia ei arvioida uudelleen säännöllisesti.	
11.3 Käyttäjän velvollisuudet	1
Käyttäjille ei ole määritelty erillistä salasanapolitiikkaa eikä salasanojen muodostamista ole ohjeistettu, vaan organisaatiossa on luotettu siihen, että asiantuntija-asemassa olevat työntekijät osaavat valita turvallisen salasanan. Työntekijät lukitsevat pääsääntöisesti työasemansa poistuessaan sen äärestä, vaikka sitä ei olekaan ohjeistettu. Puhtaan näytön ja työpöydän politiikkaa ei organisaatiossa ole käytössä.	
11.4 Verkkoon pääsyn hallinta	2
Palveluihin pääsy on rajattu riittävällä tasolla niille, joille on erityisesti myönnetty käyttöoikeudet. Pääsynhallintaa ei kuitenkaan ole dokumentoitu kattavasti. Etäkäyttöyhteydet on rajattu vain muutamalle käyttäjälle. Laitteiston automaattista tunnistamista ei ole käytössä. Langattomia lähiverkkoja tai ulkopuolisten toimittajien tarvitsemia etähuoltoyhteyksiä ei ole. Verkkojen jaottelu on riittävää ja tarkoituksenmukaista. Sovellusten käyttöä ei ole juurikaan rajoitettu. Verkkojen välisen liikenteen valvonta on järjestetty sopivalla tasolla.	
11.5 Käyttöjärjestelmään pääsyn valvonta	2
Sisäänkirjautumismenettelyt on toteutettu melko yksinkertaisesti, mutta kokonaisuuden huomioiden riittävällä tavalla. Pääsynvalvontaan käytetään pääsääntöisesti henkilökohtaisia käyttäjätunnuksia ja käytössä oleville yhteiskäyttötunnuksille on olemassa riittävät perusteet. Salasanojen hallinta on toteutettu puutteellisesti siltä osin, että järjestelmä ei käytännössä edellytä hyvien salasanojen käyttöä.	
11.6 Sovellukseen ja tietoon pääsyn valvonta	3
Sovellustason pääsynhallinta on hoidettu riittävällä tasolla. Arkaluonteiset sovellukset on asianmukaisesti eriytetty.	
11.7 Tietokoneen matkakäyttö ja etätyö	2
Organisaatiossa etätyömahdollisuus on rajoitettu ainoastaan ylläpidon käyttöön. Etäyhteyksien ottamiseen käytetään toisinaan muita kuin yrityksen hallitsemia koneita eikä koneen tunnistamista käytetä. Etäkäyttöön tarkoitettujen koneiden kiintolevyjä ei ole suojattu. Etälaitteiden virustorjunta on järjestetty.	

Toimitilaturvallisuus	
9.1 Turva-alueet	3
Turva-alueiden suojaaminen on hoidettu asianmukaisesti. Emoyrityksen työntekijöiden kevytmielinen suhtautuminen työtilojen kulunhallintaan on kuitenkin lievä riski.	
9.2 Laiteturvallisuus	2
Laiteturvallisuus on järjestetty pääosin esimerkillisesti. Tuotantotilojen osalta kemiallisen palosammutinjärjestelmän puuttuminen luo toiminnallisen riskin, joka voi suurella todennäköisyydellä realisoitua pitkänä käyttökatkona ja suurena taloudellisena menetyksenä mahdollisen tulipalon sattuessa.	

Henkilöstöturvallisuus	
8.1 Ennen työsuhteen alkua	2
Henkilöstön tai ulkopuolisten työntekijöiden turvallisuusrooleja ja -vastuita ei ole määritelty. Henkilökunnan valintaprosessi on hyvä, joskaan taustatarkistuksia ei juuri tehdä. Työsopimusten sisältö on paikallisen lainsäädännön huomioiden riittävä. Salassapitosopimuksia ei allekirjoituteta.	
8.2 Työsuhteen aikana	1
Tietoturvakoulutusta uusille työntekijöille ei järjestetä, eikä työntekijöiden tietoturvaosaamista kehitetä eikä ylläpidetä. Johto ei huolehdi siitä, että työntekijöillä on riittävät taidot ja motivaatio tietoturvallisuuden ylläpitämiseen. Organisaatiossa kaikilla on omasta mielestään riittävä osaamisen taso omien työtehtäviensä suorittamiseen.	
8.3 Työsuhteen päättyminen tai muuttuminen	1
Vastuiden viestinnästä työsuhteen päättymisen tai oleellisen muuttumisen osalta ei ole olemassa käytäntöä tai ohjeistusta. Poistuminen on hoidettu pääosin epäorganisoidusti, ilman erillistä ohjeistusta. Käyttöoikeudet poistetaan ainoastaan silloin, kun tieto poistumisesta saavuttaa organisaation tietojärjestelmän ylläpidon. Yhteiskäyttötunnusten salasanoja ei muuteta aina kun työntekijä poistuu. Osa poistumiseen liittyvistä työvaiheista on kuitenkin organisoitu ja dokumentoitu asianmukaisesti.	

Tietoliikenne- ja käyttötoimintoturvallisuus	
9.2 Laiteturvallisuus	0
Toimitilojen ulkopuolelle vietyjen laitteiden turvallisuudesta tai suojattavien kohteiden siirtämisestä toimitilojen ulkopuolelle ei ole olemassa ohjeistusta eikä asianmukaista käytäntöä.	
10.1 Menettelyohjeet ja velvollisuudet	2
Tietojenkäsittelypalvelujen menettelyohjeita ei ole kattavasti dokumentoitu. Muutostenhallinta on järjestetty pääosin asianmukaisesti. Kaikki muutokset kirjataan ja muutoksen suuruudesta riippuen esivalmistelujen määrää lisätään tarpeen mukaan. Muutoksen suuruuden arvioimista ei ole kuitenkaan ohjeistettu eikä organisaationlaajuista yhtenäistä muutosprosessia ole määritelty. Työtehtävien eriyttäminen on toteutettu organisaation koon huomioiden riittävällä tasolla. Testi- ja tuotantoympäristöt on pääosin erotettu toisistaan, mutta muutamia yhteisiä tekijöitä on olemassa.	
10.2 Ulkopuolisten palvelujen toimittamisen hallinta	3
Ulkopuolisten palvelujen toimittamisen hallinta on toteutettu organisaation liiketoimintaan nähden riittävällä tasolla.	
10.3 Järjestelmän suunnittelu ja hyväksyntä	2
Kapasiteetinhallinta on hoidettu organisaatiossa hyvin. Uusien järjestelmien, järjestelmäpäivitysten tai uusien versioiden käyttöönottoa varten ei ole käytössä formaalia hyväksymisprosessia.	
10.4 Suojaus haittaohjelmia ja liikkuvia ohjelmia vastaan	2
Tekninen suojautuminen haittaohjelmilta on toteutettu riittävän kattavasti, joskin verkkosivujen suodatus ei kuulu organisaation suojausmekanismeihin. Menettelyohjeet ja jatkuvuussuunnitelma puuttuvat.	
10.6 Verkon turvallisuuden hallinta	2
Tietoverkkojen turvallisuuden hallinta on toteutettu organisaatiossa pääasiassa riittävällä tasolla. Käyttäjille tarkoitetut palvelut on toteutettu lähtökohtaisesti turvallisilla suojatuilla sovellustason protokollilla, mutta palvelinten välinen kommunikointi on pääosin salaamatonta. Organisaatiolla ei ole käytössä tietomurtohälytintä.	

10.7 Tietovälineiden käsittely	1
Siirrettävien tietovälineiden hallintaan ei ole määritelty menettelytapoja. Tiedon hävittäminen on järjestetty organisaatiossa pääosin oikein hyvin, mutta työntekijöiden ohjeistaminen puuttuu. Lisäksi muistitikkujen hävittämistä ei ole järjestetty. Tiedon käsittelyä ei ole ohjeistettu käytännössä lainkaan. Järjestelmän dokumentaatio on pääosin kaikkien työntekijöiden luettavissa, joskin osa siitä on rajoitettu ainoastaan järjestelmän ylläpidon käyttöön.	
10.8 Tiedon vaihto	1
Tiedonvaihtoon liittyviä menettelytapoja ei ole ohjeistettu organisaatiossa. Pääsääntöisesti organisaatiossa pyritään välttämään arkaluontoisen tiedon välittämistä sähköisesti suojaamattomassa muodossa, mutta käytännössä esimerkiksi sisäisessä sähköpostissa välitetään joskus tällaista tietoa. Asiakasyhteyksien osalta tiedonvaihto on järjestetty keskitetysti asiakaspalvelun kautta.	
10.10 Tarkkailu	2
Järjestelmän tarkkailu on järjestetty melko kattavasti. Palvelinten tapahtumalokit kerätään keskitetylle lokipalvelimelle ja niistä etsitään ohjelmallisesti poikkeavuuksia. Kirjaaminen tehdään pääsääntöisesti toimintaan nähden riittävällä tasolla, mutta pääkäyttäjien toimenpiteitä ei kirjata ylös. Häiriöitä ei aina kirjata ylös eikä jälkikatselmusta järjestetä tyypillisesti kuin merkittävien korjaustoimenpiteiden jälkeen.	
Tietoturvamenetelmät ylläpitotyössä	2
Järjestelmän saavutettavuuteen ja vikatilanteiden hallintaan liittyvä ylläpitotyö on järjestetty erittäin hyvin. Kirjallinen ohjeistus on kuitenkin osittain puutteellista.	

Laitteisto- ja ohjelmistoturvallisuus	
9.2 Laiteturvallisuus	3
Laitteiden huolto on järjestetty asianmukaisesti ja riittävällä laajuudella tietoturvallisuuden takaamiseksi.	
12.1 Tietojärjestelmien turvallisuusvaatimukset	0
Tietojärjestelmien turvallisuusvaatimuksia ei ole määritelty liiketoiminnan näkökulmasta.	
12.3 Salakirjoitusmekanismi	0
Salakirjoitusmekanismeja ei ole käytössä.	
12.4 Järjestelmätietojen turvallisuus	2
Tuotannossa ajetaan ainoastaan testattua ja tuotantovalmista koodia. Tuotannossa olevan ohjelmiston muutoshallinta on järjestetty melko hyvin, mutta käytännössä muutokset tuotantoon tehdään kokonaisuutta tarkastellen hallitusti ainoastaan silloin, kun kyse on suuresta muutoksesta. Testiaineistona käytetään tyypillisesti tuotantoaineistoa. Testiaineiston hallintaan ei ole olemassa ohjeita eikä virallista käytäntöä. Ohjelmakoodiin pääsyn hallinta on toteutettu riittävällä tasolla organisaation koon huomioiden.	
12.5 Kehitys- ja tukiprosessien turvallisuus	2
Järjestelmän ylläpidolla on käytössä hyvin kattava ja käytännössä toimiva järjestelmän ja sovellusten saavutettavuuden huomioiva muutostenhallintaprosessi. Sovelluskehittäjien tekemien muutosten riski arvioidaan kuitenkin pelkästään heidän itsensä toimesta. Sovelluskehittäjät ottavat omatoimisesti tuotantoon suurimman osan tekemistään muutoksista. Mitä pienempi muutos, sitä vähemmän käyttöönottoon liittyviin riskeihin on varauduttu ja sitä vähemmän muutosta on myös testattu.	
12.6 Teknisten haavoittuvuuksien hallinta	2
Ohjelmistojen teknisten haavoittuvuuksien hallinta on toteutettu melko hyvin. Aihepiiriin liittyvä dokumentaatio on kuitenkin puutteellista ja hallintaan ei ole määritelty erillistä prosessia.	

Tietoturvamenetelmät ohjelmointityössä	1

Käytetyt menetelmät perustuvat puhtaasti työntekijöiden omaan aktiivisuuteen. Tietoturvallista toimintaa ei ole yleisellä tasolla ohjeistettu, vaan käytössä on ainoastaan muutamia ohjeistettuja menettelytapoja. Koodin tarkistuttaminen toisella ohjelmoijalla vähentää tietoturva-aukkoja, mutta menettely on käytössä ainoastaan kirjastokoodin osalta.

Liiketoiminnan jatkuvuuden hallinta	
10.5 Varmuuskopiointi	3

Varmuuskopiointi on järjestetty kattavasti ja luotettavasti ja se vastaa liiketoiminnan asettamia vaatimuksia.

14.1 Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia	1

Liiketoiminnan jatkuvuussuunnitelmaa ei ole tehty, eikä varajärjestelyitä ole olemassa. Organisaatiossa tehdään aktiivisesti tiedon ja osaamisen jakamista. Organisaation taloudellinen asema on poikkeustilanteessa turvattu emoyrityksen toimesta, mikäli liiketoiminnan jatkaminen koetaan kannattavaksi.

Vaatimustenmukaisuus	
15.1 Lakisääteisten vaatimusten noudattaminen	3

Organisaation lakisääteisten vaatimusten noudattaminen vaikuttaisi olevan kunnossa. Lainsäädännön toiminnalle asettamia vaatimuksia ei ole kuitenkaan systemaattisesti kartoitettu viimeisen viiden vuoden aikana. Organisaatio pyrkii poikkeuksetta noudattamaan paikallisia lakeja kaikessa toiminnassaan.