OULUN SEUDUN
AMMATTIKORKEAKOULU

Petteri Huovinen

MUISTIX OY:N TIETOTURVATARKASTELU

MUISTIX OY:N TIETOTURVATARKASTELU

Petteri Huovinen
Opinnäytetyö
Syksy 2013
Tietotekniikan koulutusohjelma
Oulun seudun ammattikorkeakoulu
Raahen tekniikan ja talouden kampus

TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu, Raahen tekniikan ja talouden kampus
Tietotekniikan koulutusohjelma

Tekijä: Petteri Huovinen
Opinnäytetyön nimi: Muistix Oy:n tietoturvatarkastelu
Työn ohjaaja: Juha Huhtala
Työn valmistumislukukausi ja -vuosi: Syksy 2013 Sivumäärä: 36 + 1 liitettä

Tämä insinöörityön tehtiin Muistix Oy:lle. Työssä selvitettiin, mitä kaikkia asioita tietoturvaan sisältyy ja missä ovat toimeksiantajayrityksen tietoturvan kriittisimmät kohdat.

Työn julkisessa osassa käsitellään tietoturvaa teoriatasolla sekä selvitetään tietoturvan peruskäsitteitä ja osa-alueita. Tämä osuus on luonteeltaan yleinen ja käy mainiosti pohjaksi muidenkin organisaatioiden tietoturvallisuuden kehittämisen pohjaksi. Materiaalina on käytetty tietoturvastandardeja sekä alan kirjallisuutta. Tämän raportin pohjalta rakennetaan toimeksiantajayritykselle tietoturvajärjestelyt.

Tuloksena saatiin kattava teoriapaketti tietoturvasta sekä yrityksen käyttöön tieturvatarkastelun raportti, jonka pohjalta on helppo lähteä kehittämään yrityksen tietoturva-asioita. Tietoturvatarkastelun raportti on salainen.

Asiasanat: tietoturva, tietoturvapolitiikka, tietoturvakartoitus, tietovuoto

ABSTRACT

Oulu University of Applied Sciences
Information Technology

Author: Petteri Huovinen
Title of thesis: An information security check for Muistix Ltd.
Supervisor: Juha Huhtala
Term and year when the thesis was submitted: Autumn 2013 Pages: 35 + 1 appendices

---

This Bachelor's thesis was made for Muistix Ltd. The main purpose was examine things, that are related to information security and what are the most critical part in target organization when talking about information security

Public part goes through information security in theory. It clarifies terms which are related to information security and what are sectors for that. This part can be used also in other organizations for the base of the information security.

As a result, there is good document of information security and information security check report for the organization. With that it is easy to start improve organizations information security.

Keywords: information security, Information security policy, data seepage

ALKUSANAT

Suuret kiitokset yhteistyöstä, ajatuksista ja neuvoista Arto Ruhalle ja ohjaavalle opettajalle Juha Huhtalalle sekä Tuula Hopeavuorelle kielellisestä ohjauksesta.

Suurimmat kiitokset Helena, että uskoit ja jaksoit potkia opiskelussa eteenpäin!

Raahessa 20.11.2013

Petteri Huovinen

SISÄLLYS

1 JOHDANTO

Tietoturvalla ymmärretään hyvin useasti vain virustorjunta ja palomuuri. Usein onkin niin, että näiden toiminnot riittävät turvaamaan keskivertokansalaisen tietoturvan. Laajemmalti ajateltuna totuus on kuitenkin toinen. Pelkkä palomuuri ja virustorjunta eivät organisaation tietoturvaksi riitä, vaan on oltava jotakin vahvempaa tietämystä ja tekniikkaa. Tietoturva, tai ennemmin tietoturvallisuus, onkin siis paljon laajempi käsite.

Yleisesti tietoturvallisuuden tarkoituksena on suojata organisaation tietojärjestelmää ja siihen tallennettuja tietoja, organisaation palveluita sekä tietoliikennettä. Yritysmaailmassa, mukaan lukien yhdistykset, organisaatiot ja muut vastaavat, lähes kaikki toiminnot tapahtuvat välillisesti tai välittömästi tietoverkossa tietokoneella, älypuhelimella tai muulla älylaitteella joko aivan perinteistä kaapelia pitkin tai mobiilisti pilvipalveluina. Erilaisissa tietoverkoissa, niin organisaatioiden sisäisissä kuin internetissäkin, liikkuu valtavat määrät tietoa. Usein mukana on tietoja, joita lakikin velvoittaa turvaamaan.

Enenevässä määrin kiinnitetään huomiota tietoturvallisuuteen, niin kansainvälisesti kuin kotimaassakin. Suurten yritysten budjetista lohkeaa suurempi osa tietoturvallisuuden kehittämiseen ja ylläpitoon kuin pienillä yrityksillä. Toisinpäin ajateltuna taas pienillä yrityksillä toimenpiteet tietoturvallisuuden parantamiseen ovat rahallisesti pienemmät ja suojeltavaakin voi olla vähemmän. Voidaan myös todeta, ettei hyvä tietoturva välttämättä vaadi isoja investointeja

Kun seuraa tiedotusvälineiden otsikoita haittaohjelmista, tietomurroista ja muista tietokoneajan ongelmista, lähes poikkeuksetta jokaisessa tapauksessa on kyse ihmisen tekemästä tahallisesta tai tahattomasta virheestä. Me ihmiset emme kuitenkaan toimi niin kuin ohjeet ja säännöt määrittävät: avaamme epämääräisiä liitetiedostoja sähköpostista ja selaamme www-sivuja, joita ei pitäisi. Tällöin toimimme annettujen ohjeiden vastaisesti ja tämä saattaa vaarantaa organisaatiomme, mutta myös oman tietoturvamme. Silloin tarvitsemme avuksi teknistä laitteistoa, joka oikein suunniteltuna, konfiguroituna, asennettuna ja ylläpidettynä auttaa meitä torjumaan tietoturvaongelmia.

Tämän opinnäytetyön tarkoituksena on tarkastella Muistix Oy:n tietoturvaa sekä erilaisia suoria tai välillisiä riskejä, jotka kohdistuvat tietoteknisiin seikkoihin. Havaittuihin ongelmakohtiin on tarkoitus miettiä ratkaisuja, joilla riskien aiheuttamiin ongelmiin osattaisiin varautua tai niiltä voitaisiin välttyä kokonaan. Tässä tutkimuksessa pyritään selvittämään myös ratkaisujen aiheuttamia kustannuksia yritykselle sekä miettiä, millaisia kustannuksia aiheutuu siinä tapauksessa, että riskeihin ei varauduta. Lisäpotkua tämän työn tekemiseen antoi yrityksessä tapahtunut RAID-levypakan rikko, josta aiheutui aika suuria ongelmia. Sitä ongelmaa ratkoessa heräsi kysymys niin minulla kuin yrityksen johdollakin: Mitä muuta voi sattua?

2 TIETOTURVALLISUUDEN MÄÄRITELMÄT

Eri organisaatiot ja kirjallisuus tarjoavat tietoturvallisuuden perustaksi toisistaan poikkeavia määrityksiä. Ajatus kaikissa on kuitenkin sama eli organisaation tärkein omaisuus on tieto. Tämän tiedon halutaan olevan luotettavaa, oikeassa muodossa sekä saatavilla nopeasti vain ja ainoastaan siihen oikeutetuille tahoille. (1, s. 4.)

Klassisessa tiedon arvoon perustuvassa määritelmässä tietoturvallisuus koostuu kolmesta osa-alueesta, jotka ovat luottamuksellisuus, käytettävyys ja eheys. Tämä määritelmä ei kuitenkaan huomioi riittävästi laitteistojen sekä tietoliikenne- ja tietojärjestelmien arvoa eikä myöskään tiedon omistajan tai tuottajan identiteettiä. Sen vuoksi tietoturvallisuuden määritelmää on laajennettu. Laajennetussa tietoturvallisuuden määritelmässä kolme ensimmäistä kohtaa saadaan klassisesta määritelmästä ja näihin määritelmiin lisätään kiistämättömyys sekä pääsynvalvonta. (1, s. 5.)

2.1 Luottamuksellisuus

Luottamuksellisuus (confidentiality) tarkoittaa sitä, että tietojärjestelmän tietoja pääsevät katsomaan vain sellaiset henkilöt, jotka ovat oikeutettuja tietoja tarkastelemaan (1, s. 4). Järkevää on määritellä pääsy siten, että henkilöllä on pääsy vain sellaisiin tietoihin, joita hän omassa työtehtävässään tarvitsee.

Yleisesti käytettävät tiedon luottamuksellisuutta osoittavat merkintätavat ovat

1. luottamuksellinen
2. salainen
3. erittäin salainen.

Tätä luokitusta käytetään myös valtionhallinnossa. (2.)

On tärkeää, että kaikki organisaation työntekijät tietävät luokittelusta ja sitoutuvat noudattamaan niihin liittyviä käytäntöjä eivätkä näin saata luottamuksellista tai salaista tietoa sellaisen henkilön tietoon, jolla ei ole siihen oikeutta. Jos näin käy, on tiedon luottamuksellisuus menetetty.

Luottamuksellisuutta ylläpidetään suojaamalla tietojärjestelmien laitteet ja tietovarastot käyttäjätunnusten, salasanojen, käyttörajoitusten sekä salakirjoitusmenetelmien avulla. (1, s. 4.)

2.2 Käytettävyys

Tietoturvasta puhuttaessa käytettävyys (availability) tarkoittaa sitä, että tieto on käytettävissä silloin, kun siihen oikeutetut henkilöt tai palvelut sitä tarvitsevat (3, s. 23). Yleisesti käytettävyyttä voidaan ajatella ominaisuutena, joka kertoo, kuinka varmasti palvelu, laite, ohjelma tai järjestelmä on tarvittaessa käytettävissä (4; 5).

Käytettävyysvaatimusta tarkemmin ajatellessa huomataan, että käytettävyys on riippuvainen hyvin monesta eri tekijästä, kuten tiedon luottamuksellisuudesta, laitteiston määrästä, ohjelmistolisensseistä, tietoliikennekapasiteetista, käyttäjän toimista, huolto- ja tukitoimintojen tehokkuudesta sekä laitteisto-, ohjelmisto-, ja tietoliikennehäiriöistä. Tämä taas asettaa tietoturvan koko tietojärjestelmien käytön ja suunnittelun perustaksi. (3, s. 23.)

Käytettävyyden takaamiseksi onkin huolehdittava laitteistojen riittävästä tehokkuudesta ja siitä, että ohjelmistot ovat sopivia tallennetun tiedon käsittelyyn. Inhimillisen virheen vuoksi on pyrittävä tiedon automaattiseen jalostukseen mahdollisimman pitkälle.

2.3 Eheys

Eheydellä (integrity) tarkoitetaan sitä, että tiedot pitävät paikkansa eivätkä ne muutu tai tuhoudu inhimillisen toiminnan, tietoturvahyökkäyksen tai laitteisto- tai järjestelmävian seurauksena. Jos tieto kuitenkin muuttuu, on se pystyttävä havaitsemaan. (6, s. 26.)

Ilman eheyttä eli tiedon paikkansapitävyyttä oikean alkuperäisen tiedon kanssa ollaan todella hataralla pohjalla. Tällöin asiantilan vastaavuus väitteen ja todellisuuden kanssa ei ole yhtäpitävä eikä esimerkiksi nykypäivän elektroninen kaupankäynti ole mahdollista. (3, s. 10.)

Eheyden ylläpitämiseen pyritään ensisijaisesti ohjelmistoteknisillä ratkaisuilla. Ohjelmoinnissa syötteille asetetaan vaatimuksia ja rajoitteita, esimerkiksi numerokenttiin ei voi syöttää kirjaimia eikä päinvastoin. Syötettävä tieto voidaan myös rajata tiettyyn merkkimäärään. Tiedonsiirto-operaatioiden yhteydessä esimerkiksi varmistussummat tai tiivisteet ovat käyttökelpoisia. Laitteistotasolla eheyttä varmistamaan käytetään virheenkorjaavia muisteja ja väyliä. (1, s. 5.)

2.4 Kiistämättömyys

Kiistämättömyys (non-repudiation) tarkoittaa tietojärjestelmän ominaisuutta tunnistaa ja tallentaa järjestelmää käyttävän henkilön tiedot. Tähän on yleensä kaksi eri syytä: ensinnäkin halutaan varmistaa, keneltä tieto on peräisin, ja toisekseen, kuka tietoa käyttää. Tiedon käyttäjän identiteetillä on merkitystä etenkin silloin, kun käyttö on luvatonta ja järjestelmän omistaja joutuu harkitsemaan mahdollisia oikeudellisia toimenpiteitä. (1, s. 5.)

Kiistämättömyyden varmistamiseen on kehitetty useita menetelmiä ja lisää tulee jatkuvasti. Tunnistusmekanismit liittyvät salausmenetelmiin tai biometrisiin tunnisteisiin. Salaustekniikoita käyttävissä tunnistusmenetelmissä käytetään älykortteja tai muita mukana kuljetettavia laitteita, joihin on tallennettu henkilötiedot ja käyttölupa eli sertifikaatti, joka on voimassa vain määritellyn ajan. Biometrisessä tunnistuksessa käytetään laitteita ja järjestelmiä, joissa tunnistus tapahtuu esimerkiksi sormenjäljestä tai silmänpohjasta. (1, s. 5; 7.)

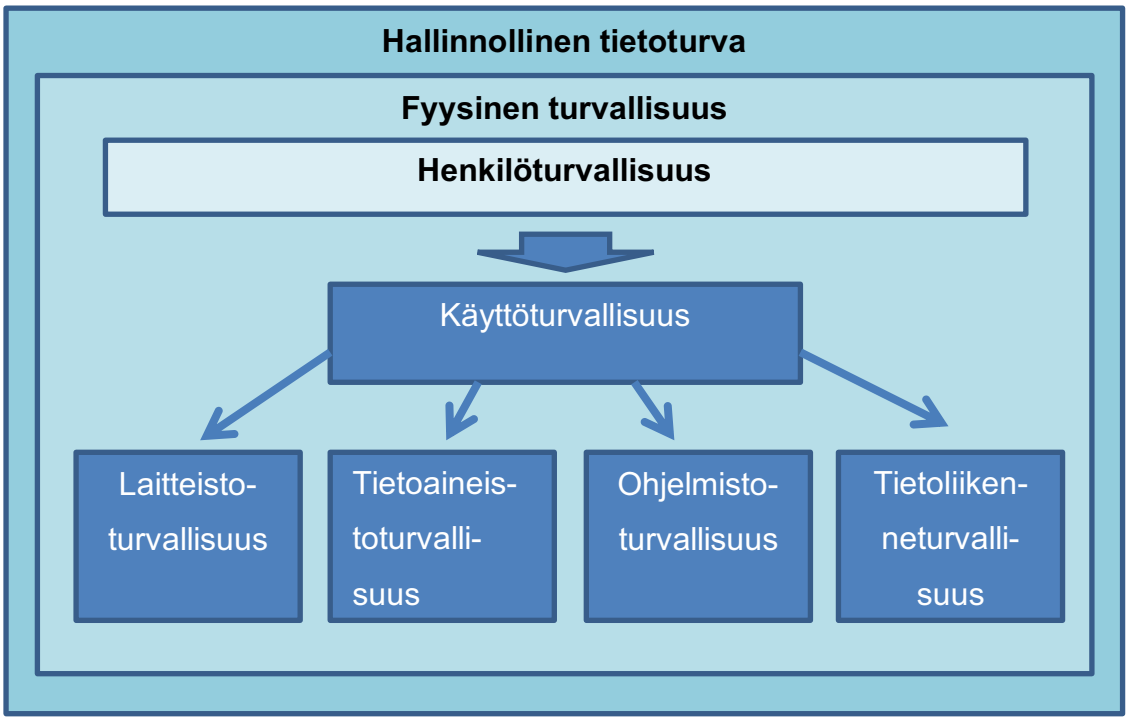
2.5 Pääsynvalvonta

Menetelmiä, joilla rajoitetaan tietojärjestelmän käyttöä, kutsutaan pääsynvalvonnaksi. Pääsynvalvontaan ei kuulu varsinainen tietoihin pääsy, vaan se kuuluu luottamuksellisuuden ylläpitoon. Organisaatiolla on kuitenkin tarve estää tai ainakin rajoittaa ulkopuolisia tai omaa henkilökuntaansa käyttämästä organisaation laitteita omiin käyttötarkoituksiinsa. Jos näin kuitenkin toimitaan, se kuormittaa laitteistoa ja tietoverkkoa. Tämä voi heikentää saatavuutta tai pahimmassa tapauksessa estää sen kokonaan. Luvaton käyttö saattaa altistaa myös tietojärjestelmän esimerkiksi haittaohjelmille ja viruksille, jolloin voi aiheutua eheys- ja luottamuksellisuusongelmia. (1, s. 5.)

Pääsynvalvontaan on syytä panostaa yhä enemmän, sillä langattomien verkkojen yleistyttyä ulkopuoliset käyttäjät pyrkivät käyttämään organisaation langattomia yhteyksiä omiin tarpeisiinsa. Tietoisuus langattomien verkkojen turvallisuudesta tai turvattomuudesta on lisääntynyt. Tästä johtuen langattomissa verkoissa ja laitteissa otetaan käyttöön vahvempia salauksia jo kiitettävästi. Tiedonsiirto- ja -käsittelykapasiteetti ovat kehittyneet, eikä siis verkon hidastuvuus vahvojen salauksien takia ole enää peruste olla käyttämättä niitä.

3 TIETOTURVALLISUUDEN OSA-ALUEET

Laadittaessa organisaatiolle tietoturvapolitiikkaa, tietoturvasuunnitelmaa tai tietoturvaohjetta on tarpeen jaotella tietoturvan osa-alueet omiin kokonaisuuksiinsa. Tällöin saatavasta dokumentista tulee rakenteelta ja sisällöltään selkeä. Kuvassa 1 on esitetty tavallisin ja selkeä tapa jaotella tietoturvan osa-alueet kahdeksaan erilliseen osioon. (1, s. 10.)



KUVA 1. Tietoturvan osa-alueet. (3, s.26 mukaillen.)

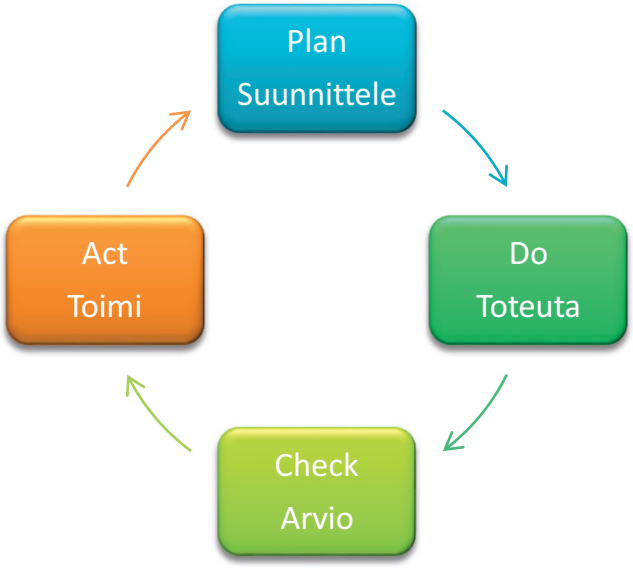
3.1 Hallinnollinen tietoturva

Hallinnollisella tietoturvallisuudella tarkoitetaan toimenpiteitä, jotka määrittävät turvallisuutta parantavat toimenpiteet ja yleiset suuntaviivat sekä luovat toimintamallin, jossa pyritään välttämään ja estämään tietoturvaan liittyvät riskit. Hallinnollisella tietoturvallisuudella varmistetaan myös kehittäminen, ohjaaminen ja johtaminen organisaation muilla tietoturvan osa-alueilla. Samalla on varmistuttava siitä, että eri osa-alueet ovat riittävällä tasolla. Ilman kunnollista suunnittelua ja hallinnointia tietoturvallisuusjärjestelyt voivat sisältää suuria puutteita tai ne keskittyvät epäolennaisiin seikkoihin. (3, s. 48.)

Hallinnollisen tietoturvan tehtävänä on päättää vastuualueiden jakamisesta, esimerkiksi kuka vastaa tietoturva- ja toipumissuunnitelmasta ja kenellä on vastuu suurien kriittisten kohteiden valmiussuunnitelmasta. (3, s. 49.)

Organisaation suuruudesta riippuu myös hallinnollisen tietoturvan laajuus. Pienempään organisaatioon hallinnolliseksi tietoturvaksi voi riittää, että toimitaan lakien ja asetusten puitteissa (1, s. 11). Esimerkkiä mainittakoon henkilötietojen säilytys ja käsittely. Johdon sitoutumisella tietoturvallisuuden kehittämiseen organisaatio pystyy kuitenkin varautumaan sekä reagoimaan riskeihin ja ongelmakohtiin huomattavasti paremmin (3, s 49). Tärkeimpänä tehtävänä hallinnollisella tietoturvalla on luoda sellaiset toimintatavat, joilla tietoturva saadaan mukaan päivittäisiin toimintoihin niin johdon kuin työntekijöidenkin tasolla.

Tietoturvan kehittäminen ja ylläpito vaativat jatkuvaa arviointia ja turvauhkien analysointia ja se muodostaakin oman prosessinsa. Tietoturvallisuuden hallintajärjestelmää (Information Security Management System, ISMS) ohjaavalle järjestelmälle löytyy asetetut vaatimukset standardista ISO/IEC 27001. Sen mukaisesti tietoturvallisuuden johtaminen ja hallinta on prosessi, jossa tietoturvallisuuden hallintajärjestelmää kehitetään vastaamaan organisaation toimintojen ja toimintaympäristön muutoksia. Kuvassa 2 on prosessin perustana oleva PDCA-malli (Plan-Do-Check-Act). Tämän mallin mukaan tietoturvallisuuden hallinta toteutetaan tietyn vaihejaon mukaisesti, eli ensin suunnitellaan, sitten toteutetaan ja seurataan vaikutuksia. Jos havaitaan muutostarpeita, niin korjataan ja tehdään muutoksia. Tämä PDCA-mallin mukaisen toiminnan tulee siis olla katkeamatonta. (4; 5.)



Kuva 2. Tietoturvallisuuden hallintaprosessin mukainen PDCA-malli

3.1.1 Tietoturvapolitiikka

Tietoturvapolitiikan laadinta kuuluu organisaatiossa ylimmän johdon vastuulle. Se tehdään aika pitkälle aikavälille, joka on tavallisesti 5–10 vuotta. Sen sisältämän ohjeistuksen tulee olla käyttökelpoista tietojärjestelmien ylläpitäjille ja toimintaprosesseista vastaaville henkilöille koko tuon ajan. Toki sitä tarkastellaan vuosittain, jotta se vastaisi turvallisuustarpeita ja organisaation senhetkistä toimintaa. (1, s. 7.)

Tietoturvapolitiikka tulee kirjoittaa siinä muodossa, että sitä lukiessaan ei tarvitse olla tietotekniikan tai hallinnon ammattilainen, sillä se on tarkoitettu organisaation koko henkilöstölle, asiakkaille ja yhteistyökumppaneille. Asiakkaille ja yhteistyökumppaneille se on osoituksena pyrkimyksestä suojata omat ja sidosryhmiensä tiedot. Tietoturvapolitiikan julkisuuden takia dokumenttiin ei saa sisällyttää sellaista tietoa, joka altistaa organisaation hyökkäyksille tai tietomurroille. Liitteeksi voidaan lisätä asiakirjoja, joissa kuvataan tarkemmin käytännöt, tekniset ratkaisut sekä menettelytavat ongelmien ilmetessä. Nämä liitteet ovat yleensä luottamuksellisia tai salaisia. (1, s. 9.)

Tietoturvapolitiikan tulee olla sisällöltään tarpeeksi laaja, koska se on merkittävin organisaation tieturvakäytäntöjä ja tietoturvallisuus prosesseja ohjaava do-

kumentti. Usein sen sisältö jää kuitenkin varsin yleisluonteiseksi eikä se sisällä kaikkia asioita, joihin sen pitäisi ottaa kantaa. Kuvassa 3 on määritetty asiat, joihin hyvässä tietoturvapolitiikassa otetaan kantaa. (1, s. 8.)

KUVA 3. Hyvän tietoturvapolitiikan sisältö (1, s. 8.)

3.1.2 Tietoturvasuunnitelma

Tietoturvasuunnitelmassa on konkreettiset käytänteet, joita käyttämällä pyritään määritettyyn tietoturvallisuuden tasoon. Dokumentissa esitellään tarkasti käytettävät työtavat sekä käytettävät tekniset ratkaisut. (1, s. 9.)

Tietoturvasuunnitelman lähtökohtana ovat organisaation tietoturvapolitiikan asettamat reunaehdot sekä yleiset suuntaviivat. Sitä on päivitettävä jatkuvasti organisaation toimintojen muutosten sekä uuden teknologian käyttöönoton vuoksi. Isompi kokonaisvaltainen tietoturvasuunnitelman laadintaväli on yleensä 2–5 vuotta. Tietoturvasuunnitelma laaditaan yhdessä organisaation turvallisuudesta sekä tietohallinnosta vastaavien henkilöiden kanssa. Koska suunnitelma sisältää tarkkoja kuvauksia sekä tietoja, määritellään dokumentti luottamukselliseksi ja salaiseksi. (1, s. 9.)

3.1.3 Tietoturvaohje

Tietoturvasuunnitelmaa voidaan suoraan käyttää tietoturvaohjeena vain joissakin tapauksissa. Sen sisältämien salassa pidettävien sekä yksityiskohtaisten teknisten tieto-osuuksien vuoksi siitä ei usein kuitenkaan ole käytännön hyötyä järjestelmän peruskäyttäjälle. Tällöin tietoturvasuunnitelman pohjalta laaditaan tietoturvaohje, jossa käytännön esimerkein perustellen pyritään luomaan hyviä ohjeita käyttäjän tarpeisiin. Hyvä ohjeistus kertoo, miksi ohje on annettu ja mikä sen merkitys on työntekijälle itselleen. Tällöin käyttäjä motivoituu ja sisäistää ohjeet huomattavasti paremmin. Nämä ohjeet luokitellaan luottamuksellisiksi tai salaisiksi. (1, s. 10.)

3.2 Fyysinen turvallisuus

Organisaation on syytä varautua palo-, vesi- ja sähkövahinkoihin, sillä toteutuessaan ne saattavat tuhota toimitiloja, laitteita sekä organisaation toiminnan kannalta elintärkeää tietoa (1, s. 11). Materiaalivalinnoilla ja rakenteilla vaikutetaan merkittävästi vesi- ja palo vahinkojen minimointiin (3, s. 97).

Esimerkkinä laitteiden suojauksesta voidaan mainita palvelimen sijoituspaikka. Palvelin on syytä sijoittaa turva-alueelle, jossa on erityisesti otettu huomioon kulunvalvonta, ilmanlaatu, lämpötila ja ilmanvaihtoasiat. Jollei palvelinta ole fyysisesti hyvin suojattu, organisaation on mahdoton varmistaa sen eheys, luottamuksellisuus ja saatavuus. Tästä johtuen laitteiden fyysinen suojaus onkin erittäin tärkeä osa tietoturvaa. (3, s. 97–98.)

Työtehtävän ollessa sen laatuinen, että fyysisen väkivallan mahdollisuus on olemassa, työhuoneiden suunnittelussa on otettava huomioon myös tämä seikka. Laitevarkauksiin on varauduttava huolehtimalla, ettei työpöydillä loju muistitikkuja, puhelimia ja muuta helposti varastettavaa. On muistettava, että myös tulosteet ja muu paperilla oleva tieto voi olla erittäin arvokasta tai kuulua salassa pidettäviin tietoihin ja niiden joutuminen vääriin käsiin voi aiheuttaa monenlaisia ongelmia. Murtoihin ja ilkivaltaan varaudutaan vartioinnilla ja rikosilmoitinjärjestelmällä sekä kameravalvonnalla. (5, s. 19.)

Fyysisen turvallisuuden vaatimukset ja laajuus vaihtelevat suuresti organisaation toimialan sekä laajuuden mukaan.

3.3 Henkilöturvallisuus

Henkilöturvallisuudella tarkoitetaan toimenpiteitä, joissa tarkastellaan organisaation tietojärjestelmän ja tietojen suojausta ihmisten tahallisilta tai tahattomilta uhilta. On myös huomioitava, millaiset henkilöt pääsevät varmistamaan tietoturvallisuutta. Siihen kuuluvat myös organisaation varamiesjärjestelyt, vastuiden ja oikeuksien määrittelyt sekä koulutuksen järjestäminen tietojärjestelmiin liittyen. Henkilöturvallisuus ei kuitenkaan rajoitu pelkästään omaan henkilökuntaan, vaan asiaa on tarkasteltava laajemmin. Huomioon on otettava myös kaikki muut organisaation toimintaan liittyvät henkilöt, kuten esimerkiksi asiakkaat, vierailijat ja ulkopuoliset työntekijät. (6, s. 18.)

Aiempaa tärkeämmäksi on muodostunut uuden työntekijän taustatietojen tarkistaminen ennen sopimussuhteen alkamista. Tällä toimenpiteellä vähennetään riskiä, jossa uusi työntekijä osoittautuukin epäpäteväksi tai jopa rikolliseksi. Julkisuudessa on ollut tapauksia, joissa muun muassa opettaja, lääkäri ja sairaanhoitaja on toiminut työsuhteessa, vaikka hänellä ei ole ollut pätevyyttä, tai jopa siten, että todistus on ollut väärennetty. (6, s. 162.)

Työtehtävästä ja organisaation toimialasta riippuen työntekijälle voidaan tehdä myös turvallisuusselvitys, jossa Suojelupoliisi selvittää työntekijän taustat. Tällaista järeämpää turvallisuustarkastelua pyydettäessä perusteena on oltava val-

tion turvallisuuden kannalta oleellinen asia tai huomattava taloudellinen intressi. (8.)

3.4 Laitteistoturvallisuus

Laitteistoturvallisuudesta löytyy paljon yhteneväisyyksiä fyysisen turvallisuuden kanssa, mutta siihen kuuluu myös sellaisia seikkoja, jotka eivät taas kuulu fyysisen turvallisuuden piiriin. Laitteistoturvallisuus on todella laaja käsite, sillä siihen kuuluu kaikki organisaation käyttämät tietotekniset laitteet. Tavoitteena laitteistoturvallisuudessa on toimintojen jatkuminen ja omaisuuden vahingoittumisen sekä häviämisen estäminen. (6, s. 221.)

Laitteistoturvallisuuteen kuuluu laitteistojen tarkoituksenmukainen mitoittaminen, toiminnan testaaminen sekä huoltotoimintojen ja varaosien asianmukainen järjestäminen. Laitteistoturvallisuuden piiriin kuuluvat myös laitteiden käyttämisestä johtuvien vaaratekijöiden, esimerkiksi sähköiskun, tai muun vaaran arviointi ja riskien minimointi. (1. s. 12.)

Laitteistoon kohdistuu useita riskejä, joihin organisaatiossa tulee varautua. Näitä riskejä ovat esimerkiksi vesi, tulipalo, savu, tärinä, kemialliset vaikutukset, pöly, lämpö, sähköhäiriöt ja sähkömagneettinen säteily (3, s. 96). Näissäkin maalaisjärjenkäytöllä päästää hyviin lopputuloksiin, kun esimerkkinä kemiallisten vaikutusten estämiseksi kielletään syöminen ja juominen tietokoneiden lähellä. Tulipalojen varalle on asennettava tarkoitukseen sopiva paloilmaisinjärjestelmä ja kohteet on varustettava asianmukaisella alkusammutuskalustolla. On muistettava, että vesi ja jauhesammuttimet eivät sovellu tietoteknisten laitteiden sammuttamiseen, vaan sammutusaineeksi on valittava esimerkiksi hiilidioksidisammutin. Alkusammutuskoulutukseen on myös panostettava, sillä hyvästäkään alkusammutuskalustosta ei ole mitään hyötyä, jollei sitä osata käyttää.

Ennaltaehkäisevä huolto on erittäin tärkeää, koska sillä saadaan laitteille lisää elinikää. Se on tärkeää myös jatkuvan käytettävyyden ja tiedon eheyden kannalta. Huollot on suunniteltava valmistajan antamien huolto-ohjeiden sekä huoltovälien mukaisesti ja huollon saa suorittaa vain siihen pätevä henkilö.

Yksinkertaisin tapa suojata laitteet on pääsynvalvonta. Tällä estetään laitteen luvaton käyttö. On huomioitava, että käyttö ei välttämättä tapahdu suoraan laitteeseen kirjautumalla, vaan käyttö voi tapahtua myös etäyhteyden avulla. Pääsynvalvonta toteutetaan yleisesti vaatimalla käyttöön oikeuttava käyttäjätunnus ja salasana. (6, s. 222–223.)

Kriittisimpien kohteiden käytettävyys ja hallinta on varmistettava. Esimerkiksi palvelimien virransaanti on järkevää turvata kahdella erillisellä virransyötöllä tai ainakin kytkeä palvelin UPS-laitteeseen. Tämä mahdollistaa palvelimen hallitun alasajon virtakatkon aikana. UPS:n käyttäminen on järkevää myös muissa vähänkin kriittisimmissä kohteissa. (6, s. 224.)

Verkon aktiivilaite, palvelin tai jokin muu laite voi olla organisaatiossa erittäin tärkeässä asemassa. Tuleekin miettiä, miten toimitaan jonkin tärkeän laitteen vikaantuessa. Kuinka kauan organisaatio voi toimia odottaessaan uutta laitetta? Onko ratkaisuna hankkia vastaava laite ja konfiguroida se valmiiksi jopa siten, että toisen vikaantuessa se ottaa huolehtiakseen rikkoutuneen laitteen tehtävät? (6, s. 223–224.)

Laitteistosta tulee pitää rekisteriä, josta saadaan selville laitteen merkki, malli, sarjanumero ja sijoituspaikka. Ongelmien selvittämisessä auttaa, jos laitteesta on arkistoituna tarkat käyttöohjeet sekä muuta tärkeää dokumentaatiota. Tällaista dokumentaatiota voi olla esimerkiksi tekninen rakenne. (6, s. 223.)

Osa tietoteknisistä laitteista vanhenee suhteellisen nopeasti tai käyttöaika on muuten lyhyt. Tämä aiheuttaa sen, että käytöstä poistettuja laitteita on myös hävitettävä. Laitteita hävitettäessä on huolehdittava siitä, etteivät organisaation salassa pidettävät tai muutoin arkaluontoiset tiedot joudu ulkopuolisten käsiin. Näitä tietoja on voinut tallentua muistikorteille, muistitikuille, tulostimiin, puhelimiin sekä tietokoneiden kovalevyille. Usein peruskäyttäjä ei tiedosta sitä, että kiintolevyn sisältö on usein luettavissa, vaikka itse tietokone ei enää toimisikaan.

3.5 Tietoliikenneturvallisuus

Kaikki viestijärjestelmät, LAN- ja WAN-yhteydet sekä muut tiedonsiirtoratkaisut kuuluvat tietoliikenneturvallisuuden piiriin. Tavoitteena on turvata organisaation tietoliikenteen ongelmaton toiminta ja tiedon suojaaminen tiedon käsittelyn, varastoinnin ja siirron aikana, niin omassa kuin yleisessäkin verkossa. Pyrkimyksenä on siis tietoliikenteen luotettava toiminta ja se, ettei tieto päädy ulkopuolisen tahon käsiin. (3, s. 108.)

Huolellisessa suunnittelussa on huomioitava verkon ja kapasiteetin riittävyys, mutta myös tietomurtojen ja palvelunestohyökkäysten torjuminen. Tietoverkon käyttö ei useinkaan ole tasaista vaan ruuhkia syntyy (3, s. 138). Tällöinkin tärkeät tiedot tulee olla käytettävissä. Esimerkkinä voidaan mainita esimerkiksi sairaanhoidon kriittiset toiminnot, joissa tieto on saatava välittömästi.

Tietoliikennettä uhkaa tyypillisesti yhteyskatkot, verkon käytön estyminen, tietovuodot, luvaton käyttö sekä eheysvirheet. Katkoja voivat aiheuttaa kaapelirikko tai jonkin yhteyden muodostamiseen tarvittavan laitteen rikkoutuminen syystä tai toisesta. (3, s. 108–109, s. 115.)

Tietovuodon mahdollisuus on olemassa, jos luvaton käyttäjä on keksinyt keinon päästä verkkoon käsiksi (3, s. 112, s. 139). Vaikka hänellä ei olisikaan varsinaisesti pääsyä tiedostoihin, hän voi kuitenkin saada tietoa lokitiedostoista ja puskureista sekä suoritta verkon salakuuntelua. Tietovuotojen ehkäisemiseksi liittimet ja kaapelit on suojattava fyysisesti luvattomalta käytöltä sekä käyttämättömät liitinrasiat on jätettävä kytkemättä ristikytkentäpaneeliin. Lisäksi verkon aktiivilaitteiden käyttämättömät portit on myös syytä sulkea (3, s. 112). Huomiota on kiinnitettävä myös organisaation WLAN-verkon suojaukseen.

Viat laitteistossa tai käytettävässä ohjelmistossa voivat aiheuttaa verkon hidastumista tai pahimmassa tapauksessa sen käyttö voi estyä kokonaan. Verkko voi myös ylikuormittua pahimpina ruuhkahetkinä. Näitä ruuhkautumisia voidaan estää mitoittamalla ja suunnittelemalla verkko tiedonsiirtokapasiteetiltaan riittäväksi. (3, s.138.)

Organisaation verkossa olevat palvelut ja verkon käyttäminen mahdollistetaan järkevästi palomuurilla. Palomuuriin tehdään määritykset organisaatiossa määritellyn verkonkäyttöpolitiikan mukaisesti. Oikein konfiguroidulla palomuurilla voidaan estää palvelunestohyökkäykset. Tämä taas puolestaan turvaa verkon käytettävyyttä. (9, s. 105–107.)

Palomuureja on kahta laatua: ohjelmallinen tai erillisenä laitteena toimiva palomuuri. Laitteistopalomuurin edut ohjelmallisiin palomuureihin verrattuna ovat erittäin merkittäviä. Sillä voidaan suojata koko organisaation verkko ulkoapäin tulevalta haitalliselta liikenteeltä. Tällöin myös sen ylläpito on helppoa ja ylläpidolliset toimet hyödyttävät välittömästi kaikkia verkon käyttäjiä. Haittaohjelmat eivät myöskään voi sammuttaa laitteistopalomuuria. Sopivalla laitteistopalomuurilla on helppo toteuttaa turvalliset VPN-yhteydet, jotta käyttäjät pääsevät turvallisesti organisaation sisäverkkoon. Ohjelmallinen palomuuri kannattaa kuitenkin pitää päällä työasemissa, sillä se tarkkailee organisaation sisäisen verkon liikennettä. (9, s. 109–111.)

Laitteistopalomuuri kerää haluttua lokitiedostoa, josta nähdään tietoa yksittäisen koneen tai koko verkon liikenteestä. Tiedoista nähdään tarkasti verkkoliikenteen määrä, laatu, muutokset ja havaitut tietoturvauhat. Lokien tarkkailu onkin yksi rautapalomuurin haittapuolia, koska se vaatii asiantuntevan henkilön ottamaan vastaan hälytyksiä sekä ylläpitämään ja päivittämään haluttuja liikennöintisääntöjä. (9, s. 110.)

3.6 Käyttöturvallisuus

Käyttöturvallisuus koostuu organisaation järjestelmien turvallisesta käytöstä, käyttöympäristöstä, tietojenkäsittelytapahtumien valvonnasta sekä jatkuvuuden turvaamisesta. Turvallisella käytöllä tarkoitetaan, että järjestelmän asennus on asianmukainen ja ylläpito on jatkuvaa sekä huolellista. Käyttöympäristön turvallisuus koostuu fyysisestä turvallisuudesta ja laitteistoturvallisuudesta sekä näiden jatkuvasta ylläpidosta ja valvonnasta. Tietojenkäsittelytapahtumia valvotaan lokitiedostojen ja muiden vastaavien apuvälineiden avulla. Jatkuvuuden turvaaminen on mahdollista, kun organisaatiolta löytyy asianmukainen toipumis-

suunnitelma, hyvä dokumentaatio, toimiva pääsynvalvonta ja riittävät lokitiedot sekä edellisten tietojen suojaaminen. (3, s. 213.)

3.7 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus käsittää tietojärjestelmissä käytettävien ohjelmistoihin liittyvät asiat. Näihin kuuluvat muun muassa lisenssien ja ohjelmistoversioiden hallinta (6, s. 21). Ohjelmistoturvallisuus voi kuulostaa tietoturvallisuuden näkökannalta vähäpätöiseltä asialta, mutta näin ei kuitenkaan ole. Esimerkkinä virusturvaohjelmiston lisenssin päättyminen voi aiheuttaa sen, että ohjelma lakkaa toimimasta ja altistaa koko tietojärjestelmän viruksille ja haittaohjelmille.

Ohjelmistojen on oltava käyttötarkoitukseensa nähden sopivia sekä niiden on oltava yhteensopivia myös muiden järjestelmässä olevien ohjelmistojen kanssa. Ennen ohjelmiston päivitystä tai uuden ohjelmistoversion asennusta on varmistuttava niiden toimivuudesta, jotta vältyttäisiin suuremmilta ongelmilta.

Virustorjuntaohjelmisto on yksi tärkeimmistä ohjelmistoista koko tietojärjestelmässä. Virustorjuntaohjelmistot pyrkivät suojaamaan käyttäjän viruksilta sekä muilta haittaohjelmilta. Näitä haittaohjelmia ovat madot, Troijan hevoset ja vakoiluohjelmat. Nämä aiheuttavat erinäisiä ongelmia koneelle, johon ne ovat asentuneet, mutta ne aiheuttavat ongelmia myös koko organisaatiolle.

Käyttöjärjestelmän tietoturva-aukkoja hyväkseen käyttävät verkkomadot pyrkivät levittymään muihin verkossa oleviin koneisiin välittömästi järjestelmään päästyään. Ylläpidon tuleekin seurata maailman virustilannetta ja huolehtia käyttöjärjestelmien sekä virustorjunta ohjelmistojen tunnistetietokantojen päivityksistä. (9. s. 27, s. 29, s. 47.)

Vaikka virustorjunnan löytämistä viruksista tai muista haittaohjelmista aiheutunut hälytys menisikin ylläpidon tietoon välittömästi, on käyttäjällä suuri rooli näissä tapauksissa. Tietokoneen ja ohjelmistojen epänormaaliin käyttäytymiseen sekä ilmoituksiin on kiinnitettävä huomiota aina ja tarvittaessa raportoitava ylläpidolle.

Organisaation ohjelmistoturvallisuuden tärkeimmät perussuojausmenetelmät ovat ohjelmiston pääsynvalvonta, tapahtumatietojen seuranta, varmuuskopiointi, asianmukainen ohjelmistodokumentaatio sekä asianmukaisesti laaditut ylläpito- ja huoltosopimukset. (6, s. 226.)

Yhtenä tärkeimmistä ohjelmistoturvallisuuden suojausmekanismeista pidetään ohjelmiston pääsynvalvontaa. Sen avulla pystytään välttämään luvattomien käyttäjien pääsy tietojärjestelmiin. Käyttäjällä on oltava oikeat tunnukset päästäkseen käyttämään ohjelmistoa. Kriittisiin ohjelmistoihin voidaan myös määritellä eri käyttäjäryhmiä, joilla on eriasteisia oikeuksia ohjelman toiminnoissa. Useat ohjelmistot keräävät lokitietoja, joita voidaan käyttää esimerkiksi ongelmatilanteen tai väärinkäyttötapausten selvittelyyn. (6, s. 226.)

Yleisin ja ehkäpä tärkein suojaustekniikka on ohjelmien ja tietojen varmuuskopiointi. Tällä varmistetaan, että organisaatiolla on käytössään mahdollisimman ajantasainen tieto ohjelmista sekä tiedoista, vaikka alkuperäiset tiedot vaurioituvat tai tuhoutuvat syystä tai toisesta. Palvelimen varmuuskopiointi määritellään usein automaattiseksi toiminnoksi, joka suoritetaan säännöllisesti. Tämä ei kuitenkaan välttämättä onnistu yksittäisellä työasemalla. Tällöin käyttäjän on itse huolehdittava varmuuskopioinnista. Varmuuskopiointi on järkevintä suorittaa silloin, kun tiedostoja ei käytetä ja verkossa on vähiten käyttäjiä eli esimerkiksi iltaisin. Tällöin voidaan varmuuskopioida esimerkiksi vain päivän aikana muuttuneet tiedot. Viikoittain voidaan suorittaa koko järjestelmän varmuuskopiointi. (6, s. 227.)

Varmuuskopiot tulee säilyttää fyysisesti erillään alkuperäisistä tiedoista ja ohjelmista, jotta ne säilyvät vahingoittumattomina myös onnettomuustilanteissa (6, s. 227). Ne on myös tarpeen tullen osattava palauttaa ja sitä tuleekin testata säännöllisesti.

Ohjelmistot, joita organisaatio käyttää, tulee listata asianmukaisesti. On sanomattakin selvää, että ohjelmistojen tulee olla laillisesti hankittuja ja ne kannattaa myös rekisteröidä. Rekisteröinti voi olla vaatimuksena, jotta esimerkiksi ohjelmistojen päivitys olisi mahdollista. Ohjelmistolisenssien hallinnalla pystytään

varmistamaa lisenssien ajantasaisuus ja ohjelmistojen häiriötön toiminta. (6. s. 228.)

3.8 Tietoaineistoturvallisuus

Tietoaineistoturvallisuus on tiedostojen, asiakirjojen ja muiden tietovälineiden suojausta, turvaluokitusta sekä tietovälineiden hallintaa, säilytystä ja käsittelyä asianmukaisesti kaikissa tiedonkäsittelyprosessien ja tiedon eri vaiheissa (6, s. 241). Tietoaineistoturvallisuus sopii erityisen hyvin sähköisen materiaaliin, mutta ne ovat täysin sopivia myös paperisten asiakirjojen käsittelyssä. Tärkeimpänä päämääränä on tiedon tuhoutumisen tai tahattoman muuttumisen estäminen. Tietoaineistoturvallisuuteen kuuluu erottamattomasti tiedon varmistaminen, asianmukainen säilytys ja hävittäminen.

Hyvin usein käyttäjä itse on syyllinen tiedostojen tuhoutumiseen. Muita syitä voivat olla esimerkiksi tietovälineiden väärä käsittely tai virhetilanne ohjelmistossa tai laitteistossa. Tiedon täydelliseen häviämiseen varaudutaan asianmukaisella varmuuskopioinnilla ja varmuuskopioiden säilyttämisellä.

Organisaation tietoaineisto on järkevä tunnistaa ja luokitella. Kun näin on menetelty, on huomattavasti helpompi toteuttaa tarvittavat suojaustoimenpiteet. Helposti tunnistettavissa on sellainen tieto, jonka esimerkiksi laki määrää salassa pidettäviksi. Salassa pidettäviin tai luottamuksellisiin tietoihin kuuluvat myös kaikki ne tiedot, jotka ulkopuolisen käsiin joutuessaan olisivat haitaksi organisaatiolla. Monet yritykset luokittelevat tiedot julkisiin, sisäisiin, luottamuksellisiin ja salaisiin tietoihin. Tällaisella luokittelulla saadaan luotua jo varsin monipuolinen jaotteluperiaate (6. s. 243). Omalle organisaatiolle sopivan jaottelun löytäminen voi olla hankalaa. Apuna voi käyttää VAHTI-työryhmän julkaisemia ohjeita erityyppisten asiakirjojen luokitteluun, käsittelyyn ja säilyttämiseen (2).

4 ORGANISAATION TIETOTURVAKARTOITUS

Niin kuin aiemmista luvuissa on huomattu, tietoturvallisuus on erittäin laaja aihe ja koostuu useasta eri osa-alueesta. Tietoturvallisuuden kartoittaminen vaatii tietoa ja taitoa, eikä se välttämättä onnistu organisaation omalta henkilöstöltä. Toteutustavasta riippuen se aiheuttaa myös kustannuksia. Ulkopuolisen riippumattoman arvioijan käyttö on perusteltua, koska tällöin saadaan varmasti puolueeton lausunto organisaation tietoturvallisuuden nykytilasta. Ulkopuolisen arvioitsijan käyttö voi olla myös riskitekijä, esimerkiksi tietovuotojen muodossa. Tärkeää on muistaa, että kartoitus on tehtävä jokaiselle organisaatiolle erikseen, koska jokainen organisaatio on erilainen tavoitteiltaan ja suojattavat tiedot voivat olla erilaisia.

4.1 Tietoturvakartoituksen toteuttaminen

Tietoturvakartoitus antaa organisaatiolle tietoa, millainen organisaation tietoturvallisuuden taso on juuri sillä hetkellä. Kartoituksen pohjalta pyritään selvittämään, millaisia muutoksia tietoturvan parantamiseksi on mahdollista tehdä ja miten.

Suunnitteluvaiheessa kartoitetaan nykytilanne tietoturvallisuuden osa-alue kerrallaan. Tällöin tehdään myös riskien arviointi. Tuloksena suunnitteluvaiheesta muodostuu dokumentti, jonka pohjalta muutoksia tietoturvallisuuden parantamiseksi ryhdytään tekemään.

Riskien arviointiin kuuluvat riskianalyysi ja riskin merkityksen arviointi. Tällä toiminnolla saadaan selville organisaation toimintaan liittyvät vaarojen mahdollisuudet, olivatpa ne sitten tahattomia tai tahallisia, ja niistä mahdollisesti aiheutuvat seuraukset. Optimaalinen tilanne olisi, että tuloksena vaarat voitaisiin tunnistaa ja hallita ennen kuin mitään ongelmaa edes ehtii tapahtua. (10.)

Riskianalyysillä pyritään saamaan selville riskin suuruus vahingon esiintymistaajuuden ja seurausten vakavuuden arvioinnista. Esimerkkinä voisi olla kiintolevyn vikaantumistaajuus ja millaiset seuraukset tiedon tai järjestelmän käytettävyyden menettämisestä voi seurata. (10.)

4.2 Nykyisen tilanteen kartoitus

Nykyisen tilanteen kartoituksessa on järkevää käsitellä jokainen tieturvallisuuden osa-alue omana yksikkönään. Tällöin saatavasta dokumentista saadaan selkeä ja sen perusteella on helppo tehdä tarvittavat muutokset.

Tietoturvakartoituksessa on pyrittävä selvittämää organisaation tietoturvan nykytilanne myös haastattelemalla. Runkona haastattelussa voidaan käyttää tietoturvakartoitusta varten laadittua apukysymyslistaa, joka on liitteenä 1 (11). Apukysymyslistan pohjana käytettiin www.tietoturvaopas.fi-sivustolta saatavaa kysymyslistaa, jota täydennettiin kattavammaksi. Näihin kysymyksiin vastaamalla saadaan jo varsin hyvä kuva organisaation tietoturvasta tai sen puutteesta.

4.2.1 Hallinnollinen tietoturva

Hallinnollisen tietoturvallisuuden kartoittamisella selvitetään, miten organisaatiossa hallinnoidaan tietoturvallisuuden hoitamista ja miten se on organisoitu. Peruslähtökohtana organisaation tietoturvassa on, että tehtävät ja vastuualueet on määritelty huolellisesti ja toteutumista valvotaan. Ohjenuorana organisaation omaan toimintaan ja myös ulospäin, esimerkiksi yhteistyökumppaneille, toimii järkevästi laadittu tietoturvapolitiikka. Minimissään hallinnollinen tietoturva selvittää ovatko organisaation toimintatavat voimassa olevan lainsäädännön mukaisia. Tärkeintä on kuitenkin saada tietoturva jalkautettua jokapäiväiseen toimintaan. (3, s. 48–50.)

4.2.2 Fyysinen turvallisuus

Organisaation on varauduttava palo-, vesi- ja sähkövahinkoihin. Myös murtoihin ja ilkivaltaan on varauduttava vartioinnilla, rikosilmoitinjärjestelmällä sekä kameravalvonnalla (6, s. 19). Myös organisaation tärkeimmät tietotekniset kohteet on suojattava fyysisesti siten, ettei kuka tahansa pääse käyttämään tietojärjestelmiä tai varastamaan tietokoneita tai muita laitteita.

4.2.3 Henkilöturvallisuus

Henkilöturvallisuutta kartoitettaessa tulee kiinnittää huomiota henkilöstön toimenkuviin, käyttöoikeuksiin ja koulutukseen. On mietittävä miten toimitaan uutta

henkilökuntaa palkattaessa tai miten toimitaan kun organisaatiosta eroaa tai erotetaan henkilö. Toimintamallit on selvitettävä myös vierailijoiden valvomiseksi, jotteivät esimerkiksi tuotannon koneet tai laitteet aiheuta vaaraa vierailijoille. (3, s. 18–19, s. 161.)

4.2.4 Laitteistoturvallisuus

Kartoituksessa huomioidaan laitteet, joita käytetään tietojenkäsittelyssä tai tietoliikenteessä. Niiden on oltava turvallisia sekä niiden suunnittelussa on otettava huomioon määritellyt turvallisuutta tukevat ominaisuudet. Käytettävien laitteiden on siis oltava luotettavia ja toiminnaltaan varmoja. Näissä laitteissa tietoturvallisuus on otettu huomioon jo valmistusvaiheessa. (6, s. 21.)

4.2.5 Tietoliikenneturvallisuus

Tietoliikenneturvallisuutta kartoitettaessa kiinnitetään huomiota organisaatiossa käytettävien verkojen turvalliseen käyttöön. Tietoliikenteen tulee olla suojassa silloin, kun tietoa siirretään, varastoidaan ja käsitellään yleisessä verkossa tai organisaation omassa suojatussa verkossa (6, s. 20). Ulkopuolisen käyttäjän pääsy organisaation verkkoon on estettävä esimerkiksi suojaamalla liittimet ja kaapelit.

4.2.6 Käyttöturvallisuus

Käyttöturvallisuuden kartoituksessa tarkastellaan järjestelmien turvallista käyttöä, käyttöympäristöä ja tietojenkäsittelytapahtumien valvontaa. Pienessä organisaatiossa valvonta saattaa olla hankala toteuttaa, koska valvontatoimenpiteet tehdään oman varsinaisen toimen ohessa silloin kun ehditään. (3, s. 213–214.)

4.2.7 Ohjelmistoturvallisuus

Kartoitettaessa ohjelmistoturvallisuutta selvitetään miten organisaatiossa hallitaan lisenssejä ja ohjelmistoja. Kartoituksessa kiinnitetään huomiota esimerkiksi sellaisiin asioihin kuin, mitä ohjelmistoja organisaatiossa käytetään, onko kaikki ohjelmistot laillisesti hankittuja, miten ohjelmisto soveltuu organisaation käyttötarkoitukseen ja niin edelleen.

4.2.8 Tietoaineistoturvallisuus

Tietoaineistoturvallisuutta kartoitettaessa selvitetään, miten organisaation tiedostot ja tiedot on suojattu. Tärkeimpänä päämääränä on estää tiedon tuhoutuminen, tahaton muuttuminen tai valtuuttamaton muuttaminen. Tietoaineistoturvallisuuteen kuuluu myös erottamattomasti tiedon varmistaminen, asianmukainen säilytys ja hävittäminen.

5 TOIMEKSIANTAJAN TIETOTURVATARKASTELU

Toimeksiantajan tietoturvatarkastelua ei tässä opinnäytetyössä käsitellä, koska tiedot sisältävät luottamuksellista tietoa.

6 LOPPUSANAT

Ryhtyessäni alussa miettimään työn määrittelyn mukaisesti, mitä riskejä organisaation tietoteknisiin laitteistoihin ja ratkaisuihin kohdistuu, olin ihmeissäni. Pala palalta kaikki ajattelemani riskit kääntyivät tietoturvallisuuteen. Tietoturvaoppaita, tietoturvastandardeja, alan julkaisuja ja tietoturva-ammattilaisten artikkeleita lukiessani sain mielestäni koottua kattavan teoriaosuuden ja ohjenuoran, jonka perusteella toimeksiantajayritys voi tietoturvaansa lähteä kehittämään.

Tämän dokumentin pohjalta toimeksiantajayritykselle alettiin tehdä tietoturvasuunnitelmaa ja riskikartoitusta. Suurimmat riskikohteet saatiin tunnistettua ja niihin reagoitiin välittömästi. Muihin riskeihin puututaan mahdollisimman nopealla aikataululla. Työ riskien määrittämisen sekä tietoturvasuunnitelman kanssa jatkuu edelleen.

Toimeksiantajan toimialasta ja pitkistä asiakassuhteista johtuen tietoaineistoa on todella paljon ja aineisto on todella monipuolista. Tämän tietomäärän tehokas käyttö, varastointi ja asianmukainen varmuuskopiointi kustannustehokkaasti ovat haastavia tehtäviä. Tietoaineiston menettäminen olisi rahallisesti mitattuna todella huomattava. Riittävä tietoturvallisuus ei kuitenkaan vaadi ihmeitä rahallisesti laitteistotasolla, mutta suunnitteluun ja toteutukseen se vaatii rutkasti työtunteja ja uusien asioiden opettelua.

Kaikissa organisaatioissa tulisi olla laadittuna tietoturva-ohjeistus. Ohjeistuksesta on turha tehdä usean sadan sivun opusta. Tällöin olennaisin tieto jää varmasti huomaamatta. Ajattelisin, että tärkeimmät ohjeet työntekijän näkökulmasta käsittelisivät internetin käyttöä, hyvän salasanan ominaisuuksia, tietoaineiston käsittelyä sekä muiden työvälineiden käyttöä (siirrettävät USB-muistit, älylaitteet, puhelimet, jne.). Niin kuin kaikessa ohjeistuksessa, on hyvä perustella, miksi jokin asia on kielletty tai miksi täytyy toimia juuri siten kuin on ohjeistettu.

Aiheena tietoturvallisuus on todella ajankohtainen. Erilaisia tietovuotoja ja urkinta tapauksia uutisoidaan lähes viikoittain. Suurimpana uutisena kesän ja syksyn aika on ollut NSA:n (National Security Agency) suorittama kansainvälinen sähköinen vakoilu-uutinen. On huhuttu, että niin ohjelmisto- kuin laitevalmistajatkin

olisivat jättäneet NSA:n painostuksesta tietoturva-aukkoja mahdollistamaan tehokkaan sähköisen vakoilun. Tästäkin huolimatta tietoturvasta on huolehdittava ja ylläpidettävä jatkuvasti ja tehokkaasti.

LÄHTEET

1. Hakala, Mika – Vainio, Mika – Vuorinen, Olli 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

2. Valtiovarainministeriö. 2000. Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/6206_fi.pdf VM 5/01/2000. Hakupäivä 4.10.2013.

3. Paavilainen, Juhani 1998. Tietoturva. Jyväskylä: Suomen Atk- Kustannus.

4. ISO/IEC 17799. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Helsinki: Suomen Standardisoimisliitto SFS.

5. ISO/IEC 27001. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS.

6. Miettinen, Juha E. 1999. Tietoturvallisuuden johtaminen: Näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari.

7. Hakkarainen, Marko 2012. Biometriset tunnisteet nykypäivänä. Saatavissa: https://jop.cs.tut.fi/twiki/bin/view/Tietoturva/Tutkielmat/BiometrisetTunnisteetNykypaivana. Hakupäivä 5.10.2013.

8. 8.3.2002/177 Laki turvallisuusselvityksistä.

9. Järvinen, Petteri 2006. Paranna tietoturvaasi. Jyväskylä: Docendo.

10. Malmén, Yngve – Wessberg, Nina 2004. Mitä tarkoitetaan riskillä, riskianalyysillä, riskin arvioinnilla ja riskien hallinnalla? Saatavissa: http://www.nbcsec.fi/spt/artikkeleita/art-01.pdf. Hakupäivä 6.10.2013.

11. Turvallisesti netissä – Kansalliset tietoturvatalkoot. Tietoturvakartoitus kysymyslista. Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tietoturvakartoitus_kysymyslista.pdf. Hakupäivä 18.10.2013.

Tietoturvakartoituksen apukysymyslista

Hallinnollinen tietoturva:

- Onko organisaatiolla selkeä yritysjohdon hyväksymä tietoturvapolitiikka?
- Tietoturvan valvonta?
- Miten henkilöstön koulutus ja opastus on järjestetty?
- Kenen vastuulla on henkilöstön koulutus ja opastus?
- Kenellä on vastuu turvallisuussuunnitelmasta?
- Kuka vastaa toipumissuunnitelmasta?
- Kuka vastaa valmiussuunnittelusta?
- Noudatetaanko lainsäädäntöä?
- Onko päätetty miltä osin toiminta vakuutetaan?
- miten huolehditaan tärkeiden tehtävien varahenkilöjärjestelyistä?

Fyysinen turvallisuus

- Miten varmuuskopiointi on hoidettu?
- Onko vesivahinkoihin varauduttu? Miten?
- Jos kiinteistössä syttyy tulipalo, voivatko tiedot tuhoutua ja liiketoiminta pysähtyä?
- Onko sähkökatkoksiin varauduttu? Miten?
- Onko ilkivaltaa ja murtoja vastaan suojauduttu? Miten
- Miten vanhat laitteet hävitetään (erityisesti muistia sisältävät laitteet)?
- Jos yrityksen tietokone varastetaan, voiko joku hyödyntää siinä olevaa tietoa?

Henkilöturvallisuus

- Kenellä on vastuu organisaation tietoturva koulutuksesta?
- Kenellä on vastuu henkilöstön valvonnasta?
- jos työntekijä irtisanotaan, voiko hän tuhota tärkeitä tietoja tai viedä ne eteenpäin ja hyötyä niistä?
- Onko organisaation henkilöstöllä vaitiolovelvollisuus?

Laitteistoturvallisuus

- Miten fyysisistä laitteista huolehditaan?
- Kuka vastaa niiden ylläpidosta?
- Miten työasemien varmuuskopiointi on hoidettu

- Onko organisaatiolla kannettavia laitteita (kannettavat tietokoneet, puhelimet, tabletit yms.)?
- Kuinka niiden varmuuskopiointi on hoidettu?
- Säilytetäänkö varmuuskopiot eri kiinteistössä?
- Jos tietokone ei tunnista käyttäjää, voiko konetta käyttää?

Tietoliikenneturvallisuus

- Millainen on verkkoyhteys?
- Miten verkkoa on rajoitettu?
- Onko käytössä pilvipalveluja?

Käyttöturvallisuus

- Käyttääkö organisaatio kulunvalvontaa (oma henkilöstö, vierailijat)?
- Missä laitteistojen dokumentointi säilytetään?
- Onko organisaation verkossa etäkäyttömahdollisuus?

Ohjelmistoturvallisuus

- Onko työntekijöillä oikeuksia asentaa ohjelmia?
- Onko organisaation käytössä ilmaisohjelmia?
- Onko organisaation käytössä piraattiohjelmia?
- Onko ohjelmista olemassa lisenssit?
- Kuka vastaa lisenssien hoidosta?
- Miten lisenssipäivitykset hoidetaan?
- Miten ohjelmistotuki toimii?

Tietoaineistoturvallisuus

- Kuka vastaa tietojen suojauksesta (käyttöoikeudet, varmuuskopiointi, palautus, tuhoaminen)?
- Missä asiakirjoja säilytetään?
- Miten asiakirjoja säilytetään?

Henkilötietojen käsittely

- Käsitteleekö yritys henkilötietoja?
- Onko henkilötietojen käsittelyn tarkoitus ja siihen liittyvät prosessit suunniteltu henkilötietolain (523/1999) 6§ edellyttämällä tavalla?
- Onko henkilötietojen suojaamisesta huolehdittu kaikissa niiden käsittelyvaiheissa (sekä sähköisen että manuaalisen aineiston osalta)?

(11.)