Tanja Kantanen

Yrityksen tietoturvakartoitus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

21.11.2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Tanja Kantanen Yrityksen tietoturvakartoitus 59 sivua + 5 liitettä 21.11.2013
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Ohjelmistotekniikka
Ohjaaja(t)	Consultant Manager Petri Kiviaho Lehtori Ilpo Kuivanen

Insinöörityössä tutkitaan tietoturvakartoituksen laatimista ja sen toteutusta varten huomioitavia asioita. Kartoituksen tarkoituksena on selvittää yrityksen tämänhetkinen tietoturvan taso. Kartoituksen perusteella saadaan tietoa kehittämistä vaativista osa-alueista ja voidaan laatia korjausehdotukset.

Työn teoriaosuudessa on käyty läpi tietoturvan peruskäsitteet ja osa-alueet sekä tietoturvaan liittyvät ISO/IEC 27001 -standardi ja Puolustusvoimien luoma Kansallinen turvallisuusauditointikriteeristö KATAKRI. Teoriaa on syvennetty liittämällä tietoturva yrityksen liiketoimintaan ja käymällä läpi tietoturvaan liittyvää Suomen lainsäädäntöä.

Tietoturvakartoitus on aloitettu kartoittamalla suojattavat kohteet. Saatujen tulosten pohjalta on tehty syventävä kartoitus. Näiden lisäksi on toteutettu laajempi kartoitus, joka yhdistää ISO/IEC 27001 -standardin ja KATAKRI:n aihealueet haastattelukysymyksiksi. Kartoituksen tulokset on luokiteltu salaisiksi niiden arkaluontoisuuden takia.

Tämä työ luo kattavan pohjan yrityksen tietoturvakartoituksen laatimiselle, sen tavoitteena on olla hyödyksi tietoturvakäsikirjan kehittämisessä ja yrityksen tietoturvatason parantamisessa.

Avainsanat	tietoturva, tietoturvakartoitus, ISO/IEC 27001, KATAKRI, VAHTI

Author(s) Title Number of Pages Date	Tanja Kantanen Information Security Survey for a Business 59 pages + 5 appendices 21 November 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Software Engineering
Instructor(s)	Petri Kiviaho, Consultant Manager Ilpo Kuivanen, Senior Lecturer

The thesis studies the preparation and implementation of the information security survey. The purpose of the survey is to assess the company's current level of security. The survey is used to identify the areas that need to be improved and its findings can be used to make suggestions for correction.

The theoretical part consists of the basic security concepts and aspects of information security, as well as a related ISO/IEC 27001 standard and the National Security Auditing Criteria (KATAKRI) that has been created by the Finnish Armed Forces. The theoretical parts are deepened by connecting the information security to the company's business activities and by going through the security-related Finnish legislation.

The information security survey starts by identifying the securable objects. The study is continued with an in-depth survey based on the results of the first survey. The full information security survey was carried out by incorporating the related areas from ISO/IEC 27001 and KATAKRI into the interview questions. The results of the study have been classified as confidential due to their sensitive nature.

The thesis provides a comprehensive basis for performing an information security survey of a company. It aims to improve company’s information security and to upgrade the best practices included in the information security hand book.

Keywords	Information Security, Information Security Survey, ISO/IEC 27001, KATAKRI, VAHTI

Sisällys

Liitteet

Liite 1. Voimassa olevat VAHTI-ohjeistukset, jotka liittyvät yrityksen tietoturvaan.

Lyhenteet

AD	Active Directory, Windowsin hakemistopalvelu, jollaa hallinnoidaan laitteita ja käyttäjiä sekä heidän käyttöoikeustasojaan.
KATAKRI	Kansallinen turvallisuusauditointikriteeristö.
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä.

1 Johdanto

Opinnäytetyön tarkoituksena on selvittää yrityksen tietoturvan taso ja parannusta vaativat osa-alueet sekä toimia lähtökohtana tietoturvakäsikirjan kehittämiselle. Toimeksiantajan pyynnöstä työhön liitettiin kiinteänä osana tietoturvastandardi ISO/IEC 27001 ja Kansallinen turvallisuusauditointikriteeristö KATAKRI.

Työ kattoi aluksi tietoturvakartoituksen, tietoturvakäsikirjan ja tietoturvakoulutuksen. Alueen laajuudesta johtuen sovimme kuitenkin työn toimeksiantajan kanssa, että rajaan tämän insinöörityön aiheeksi vain tietoturvakartoituksen. Kartoitusta varten tehtävät selvitykset oli kuitenkin tehtävä sillä tarkkuudella ja huolellisuudella, että niistä on hyötyä tietoturvakäsikirjan päivittämisen kannalta. Tämän työn valmistuttua tarkoitukseni on kuitenkin jatkaa käsikirjan kehittämisen ja koulutuksen suunnittelun kanssa.

Työn haastavuus oli sen laajuudessa. Tietoturvasta ja tietoturvakartoituksesta on kirjoitettu hyvin paljon erilaisia materiaaleja. Suurin osa niistä on erilaisilla jaotteluilla ja sisällöillä. Lisäksi monet tietoturvakartoituksesta kirjoitetut materiaalit ja kartoituksen avuksi tarkoitetut työvälineet ovat maksullisia. Näistä kaikista materiaaleista oli paikoitellen haastavaa löytää ne osiot, jotka ovat oleellisia kyseessä olevan yrityksen kohdalla. Oman haasteensa loivat myös valittujen taustamateriaalien poikkeavat tietoturvan osa-alueiden jaottelut.

Työn aluksi käydään läpi tietoturvallisuuden peruskäsitteitä ja osa-alueita sekä valittuja tietoturvaan liittyviä standardeja ja kriteeristöjä. Tämän jälkeen jatketaan käsittelemällä hieman, mitä tietoturva on liiketoiminnassa ja millaisia lakeja vaikuttaa tietoturvan toteutukseen. Lopuksi käydään läpi sitä, kuinka tietoturvakartoituksessa käytetyt kysymykset valittiin ja kuinka kartoitus toteutettiin.

Aloittaessani tämän työn työstämisen asetin muutamia tavoitteita. Tekemääni työtä tulisi voida käyttää suoraan hyödyksi tietoturvakäsikirjan kehittämisessä ja yrityksen tietoturvatason parantamisessa. Henkilökohtaisiksi tavoitteikseni asetin tietoturvaosaamiseni kehittämisen ja sen, että pyrin ottamaan tietoturvanäkökulmat huomioon kaikissa työtehtävissäni ja tiedottamaan jatkossa kollegoitani tietoturva-asioista.

Työn toimeksiantaja on Rongo Oy, joka on suomalainen 2006 perustettu informaation hallintaan erikoistunut asiantuntijayritys. Yrityksen palvelut kattavat tietovarastoinnin, mastertietojen ja liiketoimintatietojen hallinnan, suorituskyvyn johtamisen, ennakoivan analytiikan ja ylläpidon. Rongo on pk-yritys, jolla on toimipisteet Espoossa ja Tampereella.

2 Tietoturvan peruskäsitteet

Tietoturva koostuu klassisen määritelmän mukaan kolmesta osa-alueesta: luottamuksellisuudesta, eheydestä ja saatavuudesta. Näiden lisäksi tietoturva yleensä laajennetaan käsittämään kiistämättömyyttä, todentamista ja pääsynvalvontaa, sillä klassista määrittelyä ei pidetä enää tarpeeksi kattavana. Näiden osa-alueiden tarkoituksena on pitää tietoihin, tietojärjestelmiin ja palveluihin kohdistuvat riskit hallinnassa. [Hakala ym. 2006: 4-5; Henkilöstön tietoturvaohje, VAHTI 10/2006: 10.]

Tietoturvaan liittyy näiden lisäksi myös tietosuoja, sillä tietoturva tarjoaa keinoja ja toimintamalleja tietosuojan toteuttamiseen. Tietoturvalla ja tietosuojalla on siis yhteisiä piirteitä ja niiden erottaminen toisistaan voi olla paikoitellen hankalaa. [Laaksonen ym. 2006: 17.]

2.1 Luottamuksellisuus, eheys ja saatavuus

Luottamuksellisuudella (engl. confidentiality) tarkoitetaan sitä, että tieto annetaan vain ja ainoastaan niiden henkilöiden tai järjestelmien saataville, joilla on siihen oikeus. Tällöin sivullisten ei pidä pystyä käsittelemään, muuttamaan tai poistamaan tietoja. Tiedon luottamuksellisuudella ylläpidetään henkilöiden ja tahojen yksityisyyttä järjestelmissä, joissa säilytetään heidän tietojaan. Järjestelmän luottamuksellisuus toteutetaan yleensä käyttäjätunnus-salasana -yhdistelmällä, käyttöoikeuksien rajaamisella ja tiedon salauksella. [Hakala ym. 2006: 4; Järvinen 2012: 10; Henkilöstön tietoturvaohje, VAHTI 10/2006 2006: 10.]

Eheys (engl. integrity) tarkoittaa tiedon oikeellisuutta. Tiedon pitää siis olla loogista (sisäinen eheys) ja paikkansapitävää (ulkoinen eheys). Tieto ei saa muuttua vahingossa tai esimerkiksi hyökkäyksen seurauksena, eikä se saa sisältää tahallisia tai tahattomia virheitä tai lisäyksiä. Tiedon eheys rikkoutuu esimerkiksi hakkerien muokatessa nettisivuja tai sähköpostin mukana leviävien viruksien takia. Tiedon eheyttä ylläpidetään pääasiassa ohjelmallisin toteutuksin, esimerkiksi rajoittamalla ja tarkistamalla annettuja syötteitä sekä käyttämällä virheiden korjaus- ja tunnistusmekanismeja. [Hakala ym. 2006: 4-5; Järvinen 2012: 10; Tietoturva 2004.]

Saatavuudella (käytettävyys, engl. availability) tarkoitetaan, että tieto on saatavilla silloin, kun sitä tarvitaan. Käytännössä tällä tarkoitetaan järjestelmän laitteiston ja tietoliikenneyhteyksien toimintaa. Hyvänä esimerkkinä tästä on pankkien toiminta: pankkitililtä pitää pystyä nostamaan rahaa silloin, kun sille on tarve, internetpankin olisi suotavaa olla aina auki. [Hakala ym. 2006: 4; Information security 2001.]

2.2 Kiistämättömyys ja todentaminen

Kiistämättömyydellä (engl. non-repudiation) tarkoitetaan sekä palvelua, joka tarjoaa todisteen tiedon eheydestä ja lähteestä, että todentamista, jonka oikeellisuudesta on korkea varmuus ja jota ei voida jälkikäteen kumota [McCullagh ja Caelli 2000]. Kiistämättömyydellä pyritään siihen, että järjestelmän käyttäjät pystytään tunnistamaan tilanteissa, joissa on tapahtunut väärinkäytöksiä mahdollisia oikeustoimia varten [Hakala ym. 2006: 5].

Todentamisella (engl. authentication) varmistetaan käyttäjän väittämä identiteetti. Yleisimmin tämä tapahtuu esimerkiksi pankissa näytettäessä henkilökorttia, passia tai ajokorttia, jolloin virkailija voi verrata annetun tunnistusvälineen tietoja edessään olevaan henkilöön. [Information security 2001.]

Todentamiseen voidaan käyttää kolmea erilaista todentamismetodia: jotain minkä käyttäjä tietää, omistaa tai on. Jotain käyttäjän tietämää voi olla esimerkiksi salasana, pin-koodi tai kuvio. Omistettuihin asioihin kuuluvat esimerkiksi avain, henkilökortti, passi, sähköinen avainkortti tai puhelinliittymä. Todentamisessa käytettäviä henkilön ominaisuuksia ovat yleensä biometriset tunnisteet, joita ovat esimerkiksi sormenjäljet, kasvojen tunnistus, äänitunniste ja verkkokalvotutkimus. [Information security 2001; Multi-factor authentication 2009.]

Kaksivaiheisessa todentamisessa (engl. two-factor authentication) yhdistetään kaksi aiemmin mainittua todentamismetodia luomaan vahvempi todennus. Sillä tavoin pyritään varmistamaan se, että käyttäjä todella on se joka hän väittää olevansa. Kaksivaiheinen todentaminen ei ole mikään uusi keksintö vaan sitä on käytetty jo pitkään. Perinteinen esimerkki tästä on asiointi pankkiautomaatilla. Pankkiautomaatilla ensimmäiseksi annetaan pankkikortti (omistettava asia) ja sen jälkeen näppäillään pin-koodi (tiedetty asia). [Multi-factor authentication 2009.]

Tietojärjestelmiä ja internetpalveluita käytettäessä kaksivaiheisessa todentamisessa käyttäjätunnus ja salasana -yhdistelmä muodostaa yleensä ensimmäisen vaiheen. Toisena vaiheena voidaan käyttää esimerkiksi jotain seuraavista:

- tekstiviestitse saatavaa koodia
- automaattipuhelua, johon syötetään ennalta tiedetty koodi
- vaihtuvaa koodia, joka saadaan fyysisestä avainlukugeneraattorista (esimerkiksi RSA-avain)
- vaihtuvaa koodia, joka saadaan puhelimessa olevasta ohjelmasta (esimerkiksi Googlen Authenticator)
- vaihtuva koodi tunnusluku- tai salasanalistasta.

Kaksivaiheisen todentamisen hyöty on, että se pienentää salasanojen käytön riskiä. Salasanojen käyttöön liittyy kaksi suurta käyttäjäriskiä. Salasanat voivat olla liian helppoja, jolloin ne on helppo muistaa, mutta samalla myös helppoja murtaa. Salasanat voivat olla myös liian vaikeita, jolloin ne unohtuvat helposti ja käyttäjät todennäköisesti käyttävät samaa salasanaa monessa eri paikassa tai kirjoittavat ne ylös suojaamattomassa muodossa. Kaksivaiheien todentamisen vahvuus on kuitenkin siinä, että mikäli joku saa selville käyttäjätunnuksen ja salasanan, ei hän pääse niillä kuitenkaan suoraan sisälle järjestelmään. [Thomas 2013.]

Monet palvelut ovat alkaneet mahdollistaa kaksivaiheisen todentamisen käyttöä. Esimerkkeinä suurten ihmismäärien käyttämistä palveluista ovat Google, Facebook, Twitter, Dropbox, Apple ja Microsoft. [Higgins 2013.]

2.3 Tietosuoja

Tietosuojalla tarkoitetaan ihmisten henkilötietojen keräämiseen, tallentamiseen ja käsittelyyn, eli henkilötietorekisteriin, liittyvien asioiden turvaamista. Tietosuojan tarkoituksena on taata henkilöiden yksityisyys ja estää, ettei heidän tietojaan käytetä muuhun tarkoitukseen kuin mihin ne on kerätty. Tietosuojaa ylläpidetään tietoturvan keinoin ja toimintamallein, jonka takia se paikoitellen sekoitetaan tietoturvaan. Tietosuoja ja sen kattavuus määritellään henkilötietolaissa ja laissa yksityisyyden suojasta työelämässä,

joita käsitellään jäljempänä. Tietosuojan ylläpitämistä valvoo tietosuojavaltuutettu ja hänen virastonsa, jotka voivat puuttua tarvittaessa tietosuojarikkomuksiin. [Järvinen 2012: 12; Laaksonen ym. 2006: 17; Suomi.fi 2010.]

Tietosuojaan liittyvät kiinteästi liittyvät henkilötiedot, henkilörekisteri ja henkilörekisterin pitäjä. Termit on selitetty esimerkein taulukossa 1. Lyhyesti kerrottuna henkilötieto yksilöi ihmisen, ne koskevat rekisteröityä henkilöä. Henkilötietoja voidaan kerätä henkilörekisteriin esimerkiksi luetteloksi ja henkilörekisterinpitäjän velvollisuuksiin kuuluu huolehtia henkilörekisteristä. [Laaksonen ym. 2006: 17, 32-34.]

Taulukko 1. Tietosuojaan liittyvä termistö. [Henkilötietolaki (523/1999): 3, 8 §; Laaksonen ym. 2006: 17, 32-34, 35, 37.]

Termi	**Selitys**	**Esimerkit**
Henkilötieto	Sellainen tieto, joilla luonnollinen henkilö voidaan yksilöidä. Tällaisia tietoja ovat sellaiset, jotka voidaan liittää henkilöön tai tämän perheeseen tai samassa taloudessa asuviin henkilöihin.	Nimi, henkilötunnus, syntymäaika, osoite tai DNA.
Rekisteröity henkilö	Henkilö, jota henkilötieto koskee ja joka on jollain tahdonilmaisulla hyväksynyt henkilötietojensa käsittelyn. Rekisteröityä henkilöä on informoitava henkilötietojen käsittelystä ja heillä tulee olla mahdollisuus tarkastaa tietojensa oikeellisuus.	Hyväksyntä on esimerkiksi rekisteröityminen internetkauppaan ja siinä yhteydessä käyttöehtoihin suostuminen.
Henkilörekisteri	Tietojoukko, joka koostuu henkilötiedoista, jotka ovat käyttötarkoituksensa vuoksi yhteenkuuluvia. Tämä tietojoukko voidaan järjestää kortistoksi, luetteloksi tai muuksi vastaavaksi rakenteeksi, josta on helppo löytää henkilöä koskevia tietoja.	Asiakasrekisteri, palkkahallinnon rekisteri, hakemistopalvelu (kuten Windowsin Active Directory), jossa on kaikkien yrityksen työntekijöiden henkilötiedot tai yhdistyksen jäsenrekisteri.
Henkilörekisterinpitäjä	Taho, jota varten rekisteri perustetaan ja joka hallinnoi sitä tai jonka tehtäväksi se on lailla määrätty.	Yritys, yhdistys tai virasto. Mikäli esimerkiksi yritys hoitaa rekisterin käsittelyn ei rekisterinpitäjä ole henkilö vaan yritys.

Tietosuojaan kuuluu aiemmin mainittujen lisäksi henkilörekisteriseloste. Seloste tulisi luoda tehdä ennen henkilörekisterin luomista. Henkilörekisteriselosteen on tarkoitus vastata seuraaviin kysymyksiin [Henkilötietolaki (523/1999): 10 §; Laaksonen ym. 2006: 35-36, 39.]:

- Minkä takia henkilötietoja halutaan alkaa käsitellä?
- Kuka omistaa käsiteltävät henkilötiedot eli kuka hallinnollisesti vastaa niiden käytettävyydestä, eheydestä ja luottamuksellisuudesta?
- Miten henkilötietojen käsittely toteutetaan?
- Miten henkilötiedot hankitaan rekisteriä varten?
- Mitä henkilötietoja rekisteriin kerätään?
- Luovutetaanko henkilötietoja ja mahdolliset tarkennukset aiheesta?
- Siirretäänkö henkilötietoja EU- tai ETA-maiden ulkopuolelle ja mahdolliset tarkennukset aiheesta?
- Miten rekisterin tietoturva toteutetaan?

Tietoturvan osalta rekisteriselosteen tulisi olla yleisluontoinen, jotta järjestelmän yksityiskohdat eivät paljastuisi siitä. Rekisteriseloste tulee myös uusia, mikäli tietoturvan toteutus muuttuu olennaisesti. [Laaksonen ym. 2006: 39.]

Erilaisia henkilörekistereitä on paljon, mutta yritykset eivät aina tiedosta kaikkia rekistereitä, joita heillä on käytössään. Tietoturvallisuuden suunnittelussa ja ylläpitämisessä onkin tärkeä tunnistaa erilaiset rekisterit. Yrityksestä löytyy yleensä normaalien asiakas- ja palkkahallinnon rekisterien lisäksi Windowsin Active Directory (AD) tai muu vastaava hakemistopalvelu sekä mahdollisesti eri palveluiden tuottamat lokitiedot. Poikkeuksena muihin henkilörekistereihin työnantaja saa kerätä yrityksen tarpeisiin työntekijöidensä henkilötietoja rekisteriksi. Yritys ei tarvitse tällöin työntekijän lupaa tietojen keräämiseen, mutta tietojen niiden täytyy olla tarpeellisia työsuhteen kannalta. Hyväksynnästä huolimatta henkilöstä ei saa kerätä käsittelytarkoituksen kannalta tarpeettomia tietoja. Mikäli rekisterit kuitenkin sisältävät tietoja, joista yksittäinen käyttäjä on tunnistettavissa, ovat ne henkilörekistereitä ja vaativat henkilörekisteriselosteet, kuten muutkin henkilörekisterit. [Laaksonen ym. 2006: 32-35, 37.]

3 Tietoturvastandardit ja -kriteeristöt

Insinöörityön lähtökohtana oli käyttää kolmea ennalta määriteltyä tietoturvastandardia ja kriteeristöä. Nämä ovat ISO/IEC 27001 -standardi, Puolustusministeriön KATAKRI-auditointityökalu ja soveltuvat Valtiovarainministeriön VAHTI-ohjeistukset. Näitä kriteeristöjä käytetään määrittelemään tarvittava tietoturvataso ja vaatimukset tietoturvalle kartoituksen kohteena olevassa yrityksessä. Kriteeristöt esitellään seuraavissa luvuissa.

3.1 ISO/IEC 27001

ISO/IEC 27001 on standardi, joka on luotu tietoturvallisuuden hallintajärjestelmän malliksi. Standardin ovat julkaisseet International Organization for Standardization (ISO) ja International Electrotechnical Commission (IEC). Standardi kuuluu ISO/IEC 27000 -sarjaan, joka tarjoaa parhaat käytännöt tietoturvan hallintaan, riskien hallintaan ja muihin kontrolleihin tietoturvan hallintajärjestelmään liittyen. [ISO/IEC 27000-series 2007.]

Standardin virallinen nimi on “ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements”. Standardi on käännetty suomeksi ja käännös on nimeltään ”ISO/IEC 27001:fi, Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.”. Suomenkielinen standardiversio sisältää myös englanninkielisen standardin tekstit, ja ne ovat luettavissa rinnakkain.

Standardi sisältää seuraavat osa-alueet [ISO/IEC 27001:fi 2006: 32-56.]:

- turvallisuuspolitiikka
- tietoturvallisuuden organisoiminen
- suojattavien kohteiden hallinta
- henkilöstöturvallisuus
- fyysinen turvallisuus ja ympäristön turvallisuus
- tietoliikenteen ja käyttötoimintojen hallinta
- pääsyoikeuksien valvonta
- tietojärjestelmien hankinta, kehitys ja ylläpito

- tietoturvahäiriöiden hallinta
- liiketoiminnan jatkuvuuden hallinta
- vaatimustenmukaisuus.

Tämän insinöörityön kirjoituksen aikana standardista on ollut tekeillä uusi ISO/IEC 27001:2013 -versio, jota ei ole vielä julkaistu. Uudessa versiossa keskitytään enemmän tietoturvallisuuden hallintajärjestelmän toiminnan arviointiin ja lisätään uutena alueena toimintojen ulkoistaminen. Myös muita osa-alueita päivitetään. [ISO/IEC 27001:2013 2013.]

3.2 Kansallinen turvallisuusauditointikriteeristö (KATAKRI)

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) on Puolustusministeriön julkaisema auditointityökalu, jonka tavoitteena on yhtenäistää viranomaisten toteuttamat turvallisuustason todentamisen tarkastukset yrityksissä tai muissa yhteisöissä. Sen on tarkoitus auttaa myös muita, esimerkiksi yrityksiä ja yhteisöjä, omassa sisäisessä turvallisuustyössään. Tämän takia julkaisuun on lisätty erilliset elinkeinoelämän suositukset. [Kansallinen turvallisuusauditointikriteeristö (KATAKRI) 2011.]

KATAKRI on neljä osaa [Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009: 1.]:

- hallinnollinen turvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoturvallisuus.

Jokainen osio on jaettu osa-alueisiin, jokaisessa osa-alueessa on omat tarkentavat kysymyksensä. Kysymyksiin vastaavat vaatimustasot on eritelty kolmeen viranomaistasoon: perustasoon, korotettuun tasoon ja korkeaan taso. Viranomaistasoja vastaavat turvallisuusluokkamerkinnät ovat käyttö rajoitettu, luottamuksellinen ja salainen. [Kansallinen turvallisuusauditointikriteeristö (KATAKRI) 2011.]

KATAKRI:sta on tällä hetkellä tekeillä uusi versio, jonka odotetaan valmistuvan vuoden 2013 aikana. Uudesta versiosta on tarkoitus tulla käytettävämpi ja siihen lisätään uutena asiana moduulit. Käytettävyyttä parannetaan siten, että siinä huomioidaan paremmin tarkasteltavan tahon koko, ja suojausedellytykset suhteutetaan tarkasteltavan tahon riskitasoon. Moduuli-ajattelussa tietoturvallisuus siirrettäisiin päätasolta yhdeksi moduuliksi muiden rinnalle. Muita mahdollisia moduuleita voisivat suunnitelman mukaan olla logistiikkaketjun turvallisuus ja pelastusturvallisuus. [Evwaraye 2012: 8, 10-13.]

3.3 Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI)

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) on asetettu Valtiovarainministeriön päätöksellä vastaamaan hallinnon tietoturvallisuuden yhteistyöstä, ohjauksesta ja kehittämisestä. Käytännössä VAHTI esimerkiksi kehittää, ylläpitää, seuraa ja arvioi valtiohallinnon tietoturvaa sekä edistää tietoturvallisuuden integrointia ja tietoturvakulttuuria valtiohallinnossa. [Tietoturvallisuus 2013.]

VAHTI on luonut paljon erilaisia ohjeita ja oppaita tietoturvan kehittämiseen. VAHTI-ohjeistukset sisältävät vaatimuksia Valtiohallinnon tietoturvalle ja suosituksia elinkeinoelämän tarpeisiksi. Tietoturvakartoituksen, -käsikirjan ja -koulutuksen kannalta kiinnostavimmat on lueteltu liitteessä 1 olevassa taulukossa. Taulukkoon on kerätty voimassa olevat ohjeistukset viimeiseltä kymmeneltä vuodelta.

Tietoturvakartoituksen kannalta oleellisimmat VAHTI-ohjeistukset ovat riskienhallinnasta kertovat ICT-varautumisen vaatimukset (VAHTI 2/2012), Johdon tietoturvaopas (VAHTI 2/2011), Tietoturvallisuuden arviointi valtionhallinnossa (VAHTI 8/2006), Tietoturvapoikkeamatilanteiden hallinta (VAHTI 3/2005), Tietoturvatavoitteiden asettaminen ja mittaaminen (VAHTI 6/2006) sekä Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta (VAHTI 2/2008).

Suurin osa muista listatuista ohjeistuksista käsittelevät tarkemmin jotain tiettyä tietoturvan osa-aluetta, kuten toimitiloja, salausta tai älypuhelimia. Niitä voidaan käyttää hyödyksi tutkittaessa kyseisen aihealueen tietoturvatasoa, mutta niistä on todennäköisesti enemmän hyötyä silloin, kun luodaan ohjeistuksia ja toimintatapoja. Monet ohjeistuksista sisältävät hieman päällekkäisiä tietoja muiden ohjeistusten kanssa, sillä ne on tehty käyttöä helpottaen itsenäisiksi teoksiksi.

4 Tietoturvan osa-alueet

Tietoturva koostuu eri osa-alueista, jotka yhdessä luovat kokonaisvaltaisen käsityksen tietoturvasta. Hallinnolliset toimenpiteet, käyttöturvallisuus, pääsynhallinta ja fyysisesti toteutettavat suojamekanismit luovat viitekehyksen muille osa-alueille. Tietoliikenneverkon, laitteistojen, ohjelmistojen ja tietoaineistojen tietoturva ovat henkilöstön vastuualuetta. Kaikkien osa-alueiden toteuttaminen mahdollistaa kattavien tietoturvakäytäntöjen muodostamisen organisaatiolle.

Monilla käytettävistä lähteistä on oma tapansa jaotella tietoturva. Taulukossa 2 on lueteltu KATAKRI:n, ISO/IEC 27001 -standardin ja Tietoturvakäsikirjan jaottelut tietoturvalle sekä niistä tehty jaottelu tälle insinöörityölle.

Taulukko 2. Tietoturvan osa-alueet. [Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009: 1; ISO/IEC 27001:fi 2006: 32-56; Hakala ym. 2006: 10-12.]

Tietoturvan osa-alue	**KATAKRI**	**ISO/IEC 27001:fi**	**Hakkala ym. 2006**
Hallinnollinen tietoturvallisuus	Hallinnollinen tietoturvallisuus	Turvallisuuspolitiikka Tietoturvallisuuden organisoiminen Suojattavien kohteiden hallinta	Hallinnollinen turvallisuus
Henkilöstöturvallisuus	Henkilöstöturvallisuus	Henkilöstöturvallisuus	Henkilöstöturvallisuus
Fyysinen turvallisuus	Fyysinen turvallisuus	Fyysinen turvallisuus ja ympäristön turvallisuus	Fyysinen turvallisuus
Tietoliikenteen turvallisuus	Tietoturvallisuus: Tietoliikenneturvallisuus, osa-alue I400	Tietoliikenteen ja käyttötoimintojen hallinta	Tietoliikenteen turvallisuus
Laitteistoturvallisuus	Tietoturvallisuus: Tietojärjestelmäturvallisuus, osa-alue I500	Tietoliikenteen ja käyttötoimintojen hallinta -osiossa	Laitteistoturvallisuus
Ohjelmistoturvallisuus	Tietoturvallisuus: Tietojärjestelmäturvallisuus, osa-alue I500	Tietoliikenteen ja käyttötoimintojen hallinta -osiossa	Ohjelmistoturvallisuus
Tietoaineistoturvallisuus	Tietoturvallisuus: Tietoaineistoturvallisuus, osa-alue I600		Tietoaineistoturvallisuus
Käyttöturvallisuus	Tietoturvallisuus: Käyttöturvallisuus, osa-alue I700		
Pääsynvalvonta		Pääsyoikeuksien valvonta	

Kaikissa käytetyistä lähteistä löytyy omat osuutensa hallinnolliselle turvallisuudelle, henkilöstöturvallisuudelle, fyysiselle turvallisuudelle ja tietoliikenteen turvallisuudelle. Näiden lisäksi kaikissa lähteissä on käsitelty laitteisto- ja ohjelmistoturvallisuutta, joko omana osionaan tai jonkin toisen osion sisällä. Osassa lähteistä on käsitelty vielä tietoaineistoturvallisuutta ja käyttöturvalisuutta sekä pääsynvalvontaa. Näistä tietoaineistoturvallisuus päädyttiin nostamaan omaksi osiokseen, sillä kartoituksen kohteena olevan yrityksen liiketoiminta pohjautuu tietotyöhön. Käyttöturvallisuus taas otettiin omaksi osiokseen, jotta riskien hallinta olisi keskitettyä. Pääsynvalvonta on taas kartoituksen kohteena olevassa yrityksessä toteutettu keskitetysti tai samankaltaisia käytäntöjä käyttäen, joten sen koostaminen yhdeksi alueeksi on loogista.

Seuraavissa luvuissa käydään tarkemmin läpi tietoturvallisuuden osa-alueet ja mitä niihin sisältyy.

4.1 Hallinnollinen tietoturvallisuus

Hallinnollinen tietoturvallisuus (engl. administrative controls) koostuu hyväksytyistä käytännöistä, toimintatavoista, standardeista ja suosituksista. Ne luovat puitteet yrityksen pyörittämiselle ja ihmisten johtamiselle ja niillä pyritään varmistamaan tietoturvan kehittäminen ja johtaminen. Hallinnolliseen tietoturvaan voidaan lukea taulukon 3 mukaiset asiat. [Hakala ym. 2006: 10-11; Information security 2001.]

Taulukko 3. Hallinnollisen tietoturvallisuuden aihealueet. [ISO/IEC 27001:fi 2006: 32-34, 40, 44; Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009: 8-19, 21, 28-46.]

Aihealue	**Sisältö**
Tietoturvapolitiikka	Turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt. Yrityksen johto hyväksyy ja katselmoi säännöllisesti.
Tietoturvallisuuden tavoitteet	Tavoitteiden määrittely yrityksen toiminnoille ja hierarkiatasoille. Tavoitteiden saavuttamisen mittaaminen ja aikataulutus.
Tietoturvallisuuden toimintaohjelma	Menetelmät ja vastuut tietoturvallisuuden tavoitteiden saavuttamiseksi.
Tietoturvallisuuden koordinointi	Turvallisuusorganisaation luonti ja vastuiden jakaminen. Resursointi, roolien tiedotus ja sitouttaminen.
Tiedon luokitus	Tiedon luokittelun luominen ja ohjeistus.

Suojattavien kohteiden hallinta	Suojattavien kohteiden luetteloiminen sekä niiden omistajien ja hyväksyttävän käytön määrittäminen.
Tehtävien eriyttäminen	Tehtävien jakaminen eri ihmisille siten, ettei vaarallisia yhdistelmiä synny ja kriittiset päätökset vaativat useamman henkilön hyväksynnän.
Riskien hallinta	Sisäisten ja ulkoisten riskien tunnistus, arviointi ja kontrollit, toimenpiteiden toteuttamisen ja tehokkuuden valvominen, riskien priorisointi ja tietoturvan arviointi. Tulosten hyödyntäminen turvallisuuskoulutuksissa. Riskien hallinnan osa-alueiden läpikäynti säännöllisesti.
Jatkuvuuden hallinta	Menetelmät poikkeusten havaitsemiseksi ja korjausten tekemiseksi, korjauksista aiheutuvien riskien arvioinniksi ja toimenpiteiden vaikutusten analysointi hallittujen tietojärjestelmämuutosten varmistamiseksi. Vastuut kriisi- ja poikkeustilanteissa toimimisessa.
Tietoturvallisuuden raportointi	Turvallisuusjärjestelmän toimivuuden tarkastus säännöllisesti, seurantatarkastusten dokumentointi ja tulosten käyttö tietoturvan parantamiseen.
Tietoturvakoulutus	Tietoturvakoulutusten käytännöt, järjestys ja sisältöjen valikointi.
Järjestelmien suunnittelu, kehitys ja muutostenhallinta	Järjestelmän hankinta-, kehitys- ja ylläpitoprosessit, vaatimusten mukaisuus ja kapasiteetin hallinta sekä järjestelmän hyväksyntä.
Ulkopuolisten palveluiden hallinta	Ulkoistettujen palveluiden hallinta, tarkkailu, katselmointi ja muutostenhallinta. Turvallisuudesta huolehtiminen asiakassuhteissa ja kolmansien osapuolten sopimuksissa.
Tiedonvaihto	Tiedonvaihtoperiatteet, -menettelytavat ja -sopimukset, fyysiset tietovälineet kuljetuksen aikana, sähköinen viestintä ja liiketoiminnan tietojärjestelmät.
Dokumentaation hallinta	Turvallisuusdokumenttien tekomenetelmät, säilytysajat ja -paikat.

Hallinnolliseen tietoturvallisuuteen kuuluvat esimerkiksi tietoturvan koordinointi, tietoturvapolitiikka, tietoturvan kehittäminen, riskien ja jatkuvuuden hallinta, järjestelmien muutosten hallinta ja ulkoistus, tietoturvakoulutukset ja dokumentaation hallinta. Siihen liittyvät myös lainsäädännön ja yksityisoikeudellisten sopimusten vaikutusten arviointi tietoturvakäytäntöihin.

Hallinnollisen tietoturvan suunnittelua aloitettaessa olisi syytä määrittää sen kattavuus ja mahdolliset rajaukset, jotta saadaan kokonaiskuva siitä, mitä se pitää sisällään. Hallintakokonaisuutta suunniteltaessa tulisi pohtia seuraavia: kattaako se koko toiminnan, mitkä ovat laajuuteen vaikuttavat ulkoiset vaatimukset, onko yrityksellä muita huomioitavia johtamisjärjestelmiä (esimerkiksi riskienhallinta tai laadunhallinta), ovatko hallinnasta vastaavat henkilöt muissa rooleissa organisaatiossa ja mitkä ovat erityishuomiota vaativat kriittiset toiminnot. [Nummi 2011: 14.]

4.2 Henkilöstöturvallisuus

Osassa lähteistä puhutaan henkilöturvallisuudesta ja osassa henkilöstöturvallisuudesta. Valitsin henkilöstöturvallisuuden, koska se on näistä kahdesta laajempi käsite. Henkilöturvallisuudella tarkoitetaan henkilöihin kohdistuvien riskien hallintaa, kun taas henkilöstöturvallisuus sisältää myös henkilöistä aiheutuvien riskien hallinnan. Henkilöstöturvallisuuteen luetaan myös yhteistyökumppanien valinta ja siihen liittyvät toimet. Henkilöstöturvallisuuden aihealueet on lueteltu sisältöineen taulukossa 4. [Laaksonen ym. 2006: 138-139; Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008: 11-12.]

Taulukko 4. Henkilöstöturvallisuuden aihealueet. [ISO/IEC 27001:fi 2006: 36; Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009: 47, 49-59; Laaksonen ym. 2006: 139; Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008: 22.]

Aihealue	**Sisältö**
Henkilöstön hallinta	Henkilöstön listaaminen ja merkinnät saaduista koulutuksista.
Rekrytointiprosessi	Henkilöiden roolit ja vastuut rekrytoitaessa, riittävän osaamisen varmistaminen, mahdolliset henkilö- ja soveltuvuustestit, henkilöiden taustatietojen selvittäminen sekä henkilön valinta.
Työsuhteen solmiminen	Työsopimuksen ehdot, salassapito- ja vaitiolosopimukset, koeaika sekä muut työsuhteen solmimiseen liittyvät asiat.
Toimenpiteet työsuhteen alussa	Perehdytys yritykseen, tehtäviin ja tietoturvaan.
Toimenpiteet työsuhteen aikana	Sijaisuusjärjestelyt, työhyvinvoinnista huolehtiminen, tietoturvakoulutukset ja erilaiset sanktiomenettelyt.
Työsuhteen päättyminen tai muuttaminen	Päättämisvastuut, suojattavien kohteiden palauttaminen ja käyttöoikeuksien poistaminen.
Henkilöstöstä johtuvien riskien arviointi	Riskikartoituksen tekeminen ja avainhenkilöstön käytettävyyden arviointi.
Yhteistyökumppanien valinta	Yrityksen taustatietojen selvittäminen.

Henkilöstöturvallisuuteen kuuluvat tietojärjestelmän käyttäjien toimintakyvyn varmistamiseen liittyvät toimet. Niitä ovat esimerkiksi varamiesjärjestelyt, tietojärjestelmiin liittyvien koulutusten järjestäminen sekä erikoistapauksissa henkilöiden taustatietojen, kuten rikosrekisterin, selvittäminen. Henkilöstöturvallisuuteen sisältyy myös erilaiset sopimukset, esimerkiksi työsopimukset ja salassapitosopimukset. [Hakala ym. 2006: 11; Laaksonen ym. 2006: 141.]

VAHTI 2/2008 sisältää esimerkin henkilöstöriskikartoituksen laatimisesta. Riskikartoituksella saa helposti käsityksen siitä, millä tasolla henkilöstöturvallisuus on ja mitä osa-alueita pitäisi parantaa. [Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008: 57-58.]

4.3 Fyysinen turvallisuus

Fyysiseen turvallisuus (engl. physical security) sisältää rakennusten ja niiden sisätilojen sekä niissä olevien laitteiden suojaamisen erilaisilta fyysisiltä uhkilta. Fyysinen turvallisuus luo siis pohjan kaikille muille suojaustoiminnoille. Erilaisia uhkia ovat esimerkiksi murto, ilkivalta, vesivahinko, tulipalo, sähkö- ja lämmitysjärjestelmien toimintahäiriö. Näitä uhkia torjutaan esimerkiksi ovilla ja lukoilla, lämmitys- ja ilmastointilaitteilla sekä savu- ja palovaroittimilla. [Hakala ym. 2006: 11; Laaksonen ym. 2006: 125.]

Fyysisen turvallisuuteen luetaan alueen ja rakennusten turvalisuus, tilojen tärkeysluokitus, tiloissa liikkuminen, turvallisuustekniset järjestelmät ja huoltotoimenpiteet. Näiden sisältämät yksityiskohtaisemmat asiat on lueteltu tarkemmin taulukossa 5.

Taulukko 5. Fyysisen turvallisuuden aihealueet. [ISO/IEC 27001:fi 2006: 38; Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009: 60-65, 67, 68-72)

Aihealue	**Sisältö**
Alueen turvallisuus	Pysäköintitilat, piha-alue, lastausalueet, portit ja ajoesteet.
Rakennusten turvallisuus	Julkinen pääsy, toimistojen ja tilojen suojaus, ovet ja ikkunat sekä niiden lukitukset, äänieristys, säilytystilat ja kassakaapit, turva-alueet ja niissä työskentely.
Tilojen tärkeysluokittelu	Tilojen tärkeysluokittelun luominen ja tilojen jaottelu niihin.
Tiloissa liikkuminen	Yleiset kulkuväylät, hätäpoistumistiet, ulkopuolisten vierailijoiden saapuminen.
Turvallisuustekniset järjestelmät	Rikoshälytin-, kulunvalvonta-, videovalvonta-, savu- ja palovaroitinjärjestelmät sekä ilmastointilaitteisto.
Huoltotoimet	Laitteistojen ja laitetilojen huolto-, asennus ja siivoustoimet.

Fyysisen turvallisuuden suunnitteluun on hyvä ottaa mukaan toimitilojen tärkeysluokitus, sillä kaikki tilat eivät ole samanarvoisia, eivätkä tarvitse samanlaista suojausta. Siinä voidaan käyttää apuna esimerkiksi valtiohallinnon toimitilojen turvallisuusvyöhykejakoa,

jossa tilat jaetaan turvallisuusvyöhykkeisiin sen perusteella, millaista tietoa siellä käsitellään tai säilytetään. Tämän luokittelu on yhteneväinen salassa pidettävien asiakirjojen luokitteluun, jota käsitellään luvussa 6.2. Laki viranomaisten toiminnan julkisuudesta (julkisuuslaki). Asiakirjojen luokittelu on käyty läpi tarkemmin taulukossa 13. Turvallisuusvyöhykkeiden jako on esitelty taulukossa 6. [Toimitilojen tietoturvaohje, VAHTI 2/2013: 21-22.]

Taulukko 6. Valtiohallinnon toimitilojen turvallisuusvyöhykejako. [Toimitilojen tietoturvaohje, VAHTI 2/2013: 21-22.]

Turvallisuusvyöhyke	**Tiedon suojaustaso-luokka**	**Käsiteltävät ja säilytettävät tiedot**
Julkinen tila (VALKOINEN)	Ei suojaustasoa	Julkiset asiakirjat ja satunnaisesti suojaustason IV asiakirjat
Perustason tila (VIHREÄ)	Suojaustaso IV	Suojaustason IV asiakirjat
Korotetun tason tila (KELTAINEN)	Suojaustaso III	Suojaustason III asiakirjat
Korkean tason tila (SININEN)	Suojaustaso II	Suojaustason II asiakirjat
Erittäin korkean tason tila (PUNAINEN)	Suojaustaso I	Suojaustason I asiakirjat

Tietohallinto on yleensä mukana fyysisen turvallisuuden suunnittelussa, mahdollisten kolmannen osapuolen toimijoiden kanssa. Kiinteistöhuolto ja vartiointialan ammattilaiset huolehtivat yleensä fyysisen turvallisuuden ylläpidosta. [Hakala ym. 2006: 11.]

4.4 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus (engl. communication security) kattaa tiedonsiirron ja viestinnän turvallisuuden. Käytännössä tämä tarkoittaa, etteivät viestintäverkoissa välitettävät asiat paljastu asiaankuulumattomille ja etteivät ne pääse muuttamaan tai tuhoamaan välitettäviä asioita. Tämän lisäksi tietoliikenneturvallisuus sisältää tarvittavat todentamis- ja kiistämättömyysmenettelyt, joilla turvataan viestintäverkon turvallisuus. [Hakala ym. 2006: 12; Laaksonen ym. 2006: 66-67.]

Tietoliikenneturvallisuuteen liittyvät tietoliikenneverkkojen rakenne, turvallisuus ja suodatus, verkkoasiointipalvelut ja verkkoon pääsyn valvonta. Aihealueet on käyty läpi tarkemmin taulukossa 7.

Taulukko 7. Tietoliikenneturvallisuuden aihealueet. [ISO/IEC 27001:fi 2006: 42-48; Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009: 75-81, 82-84, 95.]

Aihealue	**Sisältö**
Tietoliikenneverkko	Tietoliikenneverkon rakenteet.
Tietoliikenneverkon turvallisuus	Tietoliikenneverkon turvallisuus ja turvamekanismit, verkkopalvelujen ja kaapeloinnin turvaaminen, palomuurin, VPN-yhteyden ja langattomien verkkojen konfigurointi, laitteiden ja ohjelmien oletusasetusten muuttaminen ja istuntojen hallinta.
Tietoliikenneverkon suodatus	Palomuurin ja muiden laitteiden suodatusasetukset.
Verkkoasiointipalvelut	Verkkoasiointi, verkon kautta välitetyt tapahtumat, julkinen informaatio.
Verkkoon pääsyn valvonta	Verkkopalvelujen käytön periaatteet, laitteiden ja käyttäjien tunnistus ja todentaminen, etähuoltoyhteyksien suojaus, verkkojen looginen jaottelu, verkon reitityksen valvonta.

Verkon turvallisuutta voidaan parantaa monin teknisin toteutuksin. Tällainen on esimerkiksi verkon rakenteiden huolellinen suunnittelu ja toteutus siten, että luodaan sisäverkko, joka on rajattu palomuurilla ulkoverkosta. Sisäverkko on hyvä vielä rajata pienempii kokonaisuuksiin erilaisten toimintojen, laitteiden ja tietoturvavaatimusten mukaan. [Hakala ym. 2006: 181-182.]

4.5 Laitteistoturvallisuus

Laitteistoturvallisuuteen kuuluu kaikkien yrityksen teknisten laitteiden suojaaminen. Tämän lisäksi siihen sisältyy muun muassa laitteiston hallinta, tietokoneiden ja muiden laitteiden käyttöönotto, toiminnan testaus ja huoltotoimenpiteiden järjestäminen, laitteiston turvallisuus, suojaus ja varmuuskopiointi, varautuminen laitteiston kulumiseen ja vanhentumiseen sekä käyttöjärjestelmään pääsyn valvonta. Laitteistoturvallisuuden aihealueet on kerrottu tarkemmin taulukossa 8. [Hakala ym. 2006: 12.]

Taulukko 8. Laitteistoturvallisuuden aihealueet. [ISO/IEC 27001:fi 2006: 38-42, 46, 48; Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009: 81, 86, 92-94, 98, 114-115; Hakala ym. 2006: 141-145.]

Aihealue	**Sisältö**
Laitteistopolitiikka	Sallitut laitteet ja laitteiden hankintapolitiikka.
Laitteiston hallinta	Laitekirjanpito.

Laitteiden käyttöönotto	Uusien laitteiden käyttöönottomenetelmät ja kovettaminen.
Laitteiden turvallisuus	Laitteiden sijoitus, suojaus, salaus, huolto ja testaus, käyttämättömien laitteiden suojaus sekä puhtaan pöydän ja näytön periaate.
Käyttöjärjestelmään pääsyn valvonta	Turvalliset sisäänkirjautumismenettelyt, käyttäjän tunnistaminen ja todentaminen, salasanojen hallintajärjestelmä, järjestelmän apuohjelmien käyttö, istunnon aikakatkaisu ja yhteysajan rajoittaminen.
Laitteiden siirto	Toimitilojen ulkopuolelle sijoitettujen ja vietyjen laitteiden turvallisuus.
Laitteiden varmuuskopiointi	Toteutustapa, toteutusaika, toteuttaja ja sijoitus sekä varmuuskopioinnin palautuksen testaus.
Laitteiden suojaus häiriöiltä	Suojaustoimenpiteet sähkökatkoksia, tietoliikennekatkoksia ja muita häiriöitä ja riskejä varten.
Laitteiden poisto käytöstä	Turvallinen käytöstä poistaminen ja kierrättäminen.

Matkapuhelimet, ja varsinkin älypuhelimet, ovat nykyään niin kehittyneitä, että ne on syytä ottaa mukaan suunniteltaessa laitteistoturvallisuutta. Matkapuhelimet voivat aiheuttaa suuria riskejä, mikäli niiden tietoturvasta ei huolehdita asiaankuuluvasti. Niitä käytetään usein osana kaksivaiheista todentamista, ja työsähköpostitkin voivat tulla suoraan puhelimeen. Älypuhelinten suojausta käsitellään tarkemmin esimerkiksi ”Älypuhelimien tietoturvallisuus – hyvät käytännöt” -ohjeistuksessa [Älypuhelimien tietoturvallisuus - hyvät käytännöt, VAHTI 2/2007 2007] ja kirjassa ”Mobile Device Security for Dummies” [Campagna ym. 2011.]

4.6 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan ohjelmistojen ja lisenssien hallintaa ja ohjelmistopolitiikkaa. Siihen kuuluvat myös ohjelmistojen keskinäinen yhteensopivuus, toiminnan luotettavuus ja virheettömyys, ohjelmistopäivitykset, haittaohjelmien torjunta, tietojärjestelmien hankinta, kehitys ja ylläpito sekä tärkeiden ohjelmistojen varmuuskopiointi ja turvallinen säilytys. Ohjelmistoturvallisuuden aihealueet on kerrottu tarkemmin taulukossa 9. [Hakala ym. 2006: 11-12, 135-136; Laaksonen ym. 2006: 67.]

Taulukko 9. Ohjelmistoturvallisuuden aihealueet. [ISO/IEC 27001:fi 2006: 42, 48-52; Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009: 87, 92, 97; Hakala ym. 2006: 11-12; Laakso 2013.]

Aihealue	**Sisältö**
Ohjelmien, lisenssien ja ohjelmistosopimusten hallinta	Ohjelmien ja lisenssien käyttötarkoitukset, voimassaoloajat, laajuudet, määrät, versiot ja vastuuhenkilöt sekä ohjelmistoihin liittyvien sopimusten ja niiden kattavuuden sekä voimassaoloaikojen listaaminen.
Ohjelmistopolitiikka	Sallitut ja kielletyt ohjelmat, ohjelmistot ja sovellukset.
Ohjelmistojen ja sovellusten suojaus	Arkaluonteisten sovellusten eristäminen.
Haittaohjelmien torjunta	Turvamekanismit haittaohjelmien torjumiseen.
Järjestelmien hankinta, kehitys ja ylläpito	Turvallisuusvaatimukset, tietojen käsittely sovelluksissa, salakirjoitusmekanismit, järjestelmätiedostojen turvallisuus, kehitys- ja tukiprosessien turvallisuus sekä teknisten haavoittuvuuksien hallinta.
Ohjelmien ja sovellusten varmuuskopiointi	Toteutustapa, toteutusaika, toteuttaja ja sijoitus.

On hyvä tarkistaa, että ulkomailla valmistetut ohjelmistot noudattavat Suomen lainsäädäntöä. Ohjelmat saattavat esimerkiksi kerätä tarpeettomia tietoja tietojärjestelmän käyttäjistä, jolloin yksityisyydensuoja saattaa vaarantua. [Laaksonen ym. 2006: 67.]

4.7 Tietoaineistoturvallisuus

Tietoaineistoturvallisuuteen kuuluvat kaikki toimet, jotka liittyvät tietojen suojaamiseen. Käytännössä sillä tarkoitetaan tietoaineistojen hallintaa, turvallista käsittelyä, suojausta, säilytystä, varmuuskopiointia, tuhoamista sekä luokittelua. Näihin toimiin sisältyvät asiat on käyty läpi tarkemmin taulukossa 10. [Hakala ym. 2006: 11; Laaksonen ym. 2006: 67.]

Taulukko 10. Tietoaineistoturvallisuuden aihealueet. [ISO/IEC 27001:fi 2006: 34, 42, 48; Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009: 89-91, 99-106.]

Aihealue	**Sisältö**
Tietoaineistojen hallinta	Tietoaineistojen luetteloiminen, luokittelu ja omistajan määrittäminen.
Tietoaineistojen käsittely	Tiedon käsittely, säilytys, kopiointi, tulostus, sähköinen ja fyysinen välitys sekä hyväksyttävä käyttö.

Tietoaineistojen suojaus	Tietojen käytön rajoittaminen, salauskäytännöt sekä tietoaineistojen suojaus huoltotoimenpiteiden aikana ja muissa tilanteissa.
Tietoaineistojen varmuuskopiointi	Toteutustapa, toteutusaika, toteuttaja ja sijoitus.
Tietoaineistojen poistaminen käytöstä	Tietojen säilytyksen kesto, tietojen poistaminen käytöstä ja tuhoaminen.

Tietoaineistoturvallisuus ei koske vain sähköisiä aineistoja, vaan se kattaa myös paperiset dokumentit.

4.8 Käyttöturvallisuus

Käyttöturvallisuus kattaa riskien hallinnan ja niihin varautumisen. Käytännössä tämä tarkoittaa riskien-, liiketoiminnan jatkuvuuden tietoturvahäiriöiden hallintaa, tietoturvahaavoittuvuuksilta suojautumista sekä etätyöskentelyn toimintatapoja, tehtävien eriyttämistä ja varmuuskopioinnin riittävyyden varmistamista. Käyttöturvallisuuden aihealueet on kerrottu tarkemmin taulukossa 11. [Hakala ym. 2006: 12.]

Taulukko 11. Käyttöturvallisuuden aihealueet. [ISO/IEC 27001:fi 2006: 50-54; Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009: 20, 22-27, 107-113, 115-117.]

Aihealue	**Sisältö**
Riskien hallinta	Sisäisten ja ulkoisten riskien tunnistus, arviointi ja kontrollit, toimenpiteiden toteuttamisen ja tehokkuuden valvominen, riskien priorisointi ja tietoturvan arviointi. Tulosten hyödyntäminen turvallisuuskoulutuksissa. Riskien hallinnan osa-alueiden läpikäynti säännöllisesti.
Liiketoiminnan jatkuvuuden hallinta	Jatkuvuuden hallintaprosessin toteuttaminen, testaus, ylläpito ja kehittäminen, tietojen turvaaminen hätätilanteissa ja toipumisvalmiuden testaus.
Tietoturvahäiriöiden hallinta	Tietoturvatapahtumista ja -heikkouksista raportoiminen, tietoturvahäiriöiden ja parannuskohteiden hallinta, toipumissuunnitelma, Dokumentaation ajantasaisuuden ja tietojen riittävyyden varmistaminen.
Tietoturvahaavoittuvuuksilta suojautuminen	Tietoturvatiedotteiden seuraaminen, päivitysten asentamisen menettelytavat ja niiden toteutumisen valvonta.
Etätyöskentely	Etä- ja matkatyöskentelyn menettelytavat ja turvamekanismit.
Tehtävien eriyttäminen	Työtehtävien ja kehitys-, testaus- ja tuotantojärjestelmien eriyttämisen varmistaminen.
Varmuuskopiointi	Riittävän varmuuskopioinnin varmistaminen. Varmuuskopioitavien asioiden listaus, sijoitus, pääsynvalvonta ja suojaus.

Kriittiset liiketoimintajärjestelmät vaativat korkeamman tason tietoturvakäytännöt ja kontrollit. Jokaisen järjestelmän vaatiman tietoturvatason määrittäminen mahdollistaa vastaavan riskitason määrittämisen. Tavoitteena on varmistaa, että jos riski toteutuu, se ei vaaranna yrityksen kriittisinä pidettyjä tietojärjestelmiä tai liiketoiminnan jatkuvuutta.

4.9 Pääsynvalvonta

Pääsynvalvontaan (engl. access control) kuuluvat ne toimet, joilla rajoitetaan henkilöiden pääsyä yrityksen tiloihin, tietoihin ja tietojärjestelmiin. Esimerkkejä pääsynvalvonnasta ovat ovissa olevat lukot ja kirjautumistietojen vaatiminen ennen käyttöjärjestelmään pääsyä. [Hakala ym. 2006: 11; Access control 2002.]

Pääsynvalvontaan sisältyy pääsynvalvonnan toimintaperiaatteiden ja hallintatapojen määrittäminen sekä käyttöoikeuksien, käyttäjätunnusten ja kulkuoikeuksien hallinta. Pääsynvalvontaan voidaan sisällyttää myös tietojärjestelmien ja tietoliikenneverkkojen valvonta, esimerkiksi lokitietojen kerääminen sekä niissä tapahtuvien häiriöiden kirjaus. Pääsynvalvontaan kuuluvat aihealueet on lueteltu tarkemmin taulukossa 12.

Taulukko 12. Pääsynvalvonnan aihealueet. [ISO/IEC 27001:fi 2006: 38, 44-46; Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009: 65-68, 85, 88.]

Aihealue	**Sisältö**
Pääsynvalvonnan toimintaperiaatteet	Pääsynvalvonnan suunnittelu, toteutus ja valvonta sekä sisäänkirjausmenettelyt ja salasanan hallintajärjestelmät.
Pääsyoikeuksien hallinta	Pääsyoikeuksien hallintatavat.
Käyttöoikeuksien hallinta	Verkkoon, käyttöjärjestelmään, sovelluksiin ja tietoihin pääsynhallinta ja oikeuksien määräytymisperiaatteet, myös etäkäyttö.
Käyttäjätunnusten hallinta	Käyttäjätunnusten luonti, muutos ja poisto sekä niihin liittyvät ohjeistukset.
Kulkuoikeuksien hallinta	Avainten ja kulkuavainten hallinta, kulkuoikeuksien määräytymisperiaatteet sekä kulkuoikeuksien ja -tasojen listaus.
Järjestelmien valvonta	Tapahtumalokit, järjestelmien ja tietoliikenneverkon käytön tarkkailu, lokitietojen suojaus sekä pääkäyttäjä- ja operaattorilokit.
Häiriöiden kirjaus	Järjestelmissä tapahtuvien häiriöiden kirjaus ja valvonta.

Pääsynvalvontamekanismeja suunniteltaessa tulee ottaa huomioon suojeltavan tiedon tärkeys. Mitä tärkeämpää ja kriittisempää tieto on, sitä korkeamman tason pääsynvalvontamekanismit tulisi ottaa käyttöön. [Information security 2001.]

5 Tietoturva liiketoiminnassa

Tietoturvan tarkoitus yritysmaailmassa on turvata tietoja, jotka mahdollistavat yrityksen liiketoiminnan [Laaksonen ym. 2006: 17]. Turvattavia tietoja voivat olla esimerkiksi liikesalaisuudet tai asiakkaiden henkilötiedot.

Tietoturvan suunnittelu tulisi yritysmaailmassa aloittaa siitä, että se liitetään osaksi yrityksen toimintakulttuuria, sillä tietoturva koostuu pienistä teoista jokapäiväisessä työskentelyssä. Tietoturva tulisi nähdä välttämättömän pahan sijaan kilpailuetuna, joka saattaa parantaa yrityksen mahdollisuuksia tarjouskilpailuissa. Tietoturvallisuutta suunniteltaessa tulee organisaation liiketoiminnan tavoitteet ja tietoturvatavoitteet yhdistää, jotta tietoturvallisuudelle asetetut tavoitteet ovat linjassa liiketoiminnan tavoitteiden kanssa. [Laaksonen ym. 2006: 17, 117.]

Hyvän tietoturvatason ylläpitäminen vaatii suunniteltuja teknisiä ja hallinnollisia toimia. Myös niiden vaikutusten seuraaminen on tärkeää toiminnan kehittämisen kannalta. Yritysten välinen koveneva kilpailu aiheuttaa haasteita tietoturvallisuuden kehittämiselle ja toteuttamiselle, koska suurin osa yritysten ajasta kuluu operatiivisten asioiden hoitamiseen. Tämä saattaa aiheuttaa vaikeuksia riittävän henkilöstön saaminen tietoturva-asioiden hoitamiseen ja kehittämiseen. Yrityksen johdon on kuitenkin syytä varata riittävästi resursseja hyvän tietoturvatason ylläpitämiseen, sillä se on nykyisin yhä enenemässä määrin liiketoiminnan edellytys. Pahimmassa tapauksessa huono tietoturva johtaa liiketoiminnan keskeytymiseen. [Laaksonen ym. 2006: 17, 19-20.]

Valtionvarainministeri, joka vastaa valtionhallinnon tietoturvan kehittämisestä ja ylläpitämisestä, on tuottanut paljon ohjeita tietoturvallisuuden hoitamiseksi julkisessa hallinnossa VAHTI-ohjelmansa kautta [Laaksonen ym. 2006: 30]. Ohjeet ovat yleisesti saatavilla, joten myös yritykset voivat käyttää niitä hyväkseen.

Tietoturvaan liittyy paljon erilaisia lakeja, joista monet koskevat myös yrityksiä. Näitä lakeja käsitellään seuraavassa luvussa.

6 Tietoturvaan liittyvä Suomen lainsäädäntö

Suomen lainsäädännössä on paljon erilaisia lakeja, joiden tarkoituksena on taata palveluiden tietoturva ja määritellä tarvittavat tietoturvatoimenpiteet, jotka esimerkiksi takaavat yksityishenkilöiden tietosuojan. Laeissa on kiinnitetty erityisesti huomiota tunnistamistietojen ja viestinnän sisällön käsittelyyn ja niiden vaatimiin tietoturvatoimenpiteisiin. [Laaksonen ym. 2006: 80.]

Lait, jotka liittyvät tietoturvaan ovat

- perustuslaki
- laki viranomaisten toiminnan julkisuudesta (julkisuuslaki)
- henkilötietolaki (tietosuojalaki)
- laki kansainvälisistä tietoturvavelvoitteista
- laki yksityisyyden suojasta työelämässä (työelämän tietosuojalaki)
- sähköisen viestinnän tietosuojalaki (urkintalaki)
- laki tietoyhteiskunnan palvelujen tarjoamisesta
- laki sähköisestä asioinnista viranomaistoiminnassa (asiointilaki)
- laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista
- viestintämarkkinalaki.

Nämä lait esitellään pääpiirteittäin seuraavissa luvuissa.

6.1 Perustuslaki

Perustuslaki antaa pohjan laeille, joissa määritellään tietoturvavaatimuksia. Siinä lähdetään liikkeelle jokaiselle kuuluvasta yksityisyydensuojasta. Yksityisyyden suoja määritellään Suomen perustuslain (731/1999) 10 §:ssä seuraavasti:

> Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla.
>
> Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

> Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteitä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta tai kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.

Lain mukaan kirjeen, puhelun ja muun luottamuksellisen viestin suoja on loukkaamaton. Tämä tarkoittaa käytännössä sitä, ettei tietoturvaan voida puuttua tältä osin esimerkiksi valtioneuvoston tai ministeriön asetuksilla vaan asiasta päättäminen kuuluu eduskunnalle. Laissa tosin mainitaan, että joissain tilanteissa viestinnän suojan voi myös menettää. Tällaisia tapauksia ovat lähinnä rikoksiin tai rikolliseen toimintaan liittyvät tilanteet. [Suomen perustuslaki (731/1999): 10 §; Laaksonen ym. 2006: 28.]

6.2 Laki viranomaisten toiminnan julkisuudesta (julkisuuslaki)

Lakia viranomaisten toiminnan julkisuudesta (621/1999) kutsutaan julkisuuslaiksi. Sitä sovelletaan lähtökohtaisesti viranomaistoimintaan, mutta siinä on liittymäkohtia henkilötietolakiin. Laissa määriteltyä vaitiolovelvollisuutta ja hyväksikäyttökieltoa sovelletaan tietyissä tapauksissa myös sellaisiin tahoihin, jotka ovat saaneet viranomaiselta salassa pidettäviä tietoja. [Laaksonen ym. 2006: 29.]

Lain lähtökohtana on se, että kaikki asiakirjat ovat julkisia, paitsi silloin, kun laissa on säädetty peruste niiden salassapidolle. Laissa on määritelty kaikki salassa pidettävät viranomaisen asiakirjat. Tämän lisäksi laissa sanotaan, että asiakirjoissa täytyy olla merkintä salassa pitämisestä tai asiasta täytyy mainita annettaessa sellaista tietoa suullisesti. Asiakirjoihin voidaan myös tehdä merkintä tietoturvallisuusvaatimuksista, joita asiakirjaa käsiteltäessä pitää noudattaa (luokitusmerkintä). [Laki viranomaisten toiminnan julkisuudesta (621/1999).]

Salassa pidettävien asiakirjojen luokittelu on määritelty Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010). Luokittelun piiriin kuuluvat kaikki asiakirjat ja tiedot, jotka kuuluvat salassapidon piiriin tai jos niiden luovuttamista ja käyttämistä on rajoitettu jotenkin. Viranomainen voi kuitenkin itse päättää mitkä asiakirjat kuuluvat mihinkin luokitteluluokkaan, mikäli niitä ei ole laissa erikseen määritelty. Luokittelussa on neljä suojaustasoluokkaa, ja ne on määritelty sen mukaan kuinka suurta haittaa tiedon paljastuminen aiheuttaisi. Luokittelu on kerrottu tarkemmin taulukossa 13.

[Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010): 9 §; Laaksonen ym. 2006: 29.]

Taulukko 13. Salassa pidettävien asiakirjojen luokittelu. [Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010): 9 §.]

Luokka	**Selitys**
Suojaustaso I	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle.
Suojaustaso II	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle.
Suojaustaso III	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle.
Suojaustaso IV	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle.

Samankaltaista luokittelua voidaan käyttää myös yrityksissä, kun halutaan luoda tärkeää materiaalia koskevia käytäntöjä. Näiden lisäksi yritykset tarvitsevat myös luokan julkiselle tiedolle. [Laaksonen ym. 2006: 29-30.]

Julkisuuslain rikkomisesta voidaan tuomita sakkoon tai vankeuteen. Syytenimikkeet ovat tällöin salassapitorikkomus, virkasalaisuuden rikkominen tai tuottamuksellinen virkasalaisuuden rikkominen. Rangaistus riippuu teon vakavuudesta, vaihdellen sakoista enintään kahteen vuoteen vankeutta. Virkamies voidaan tuomita myös viralta pantavaksi. [Laki viranomaisten toiminnan julkisuudesta (621/1999): 35 §; Rikoslaki (39/1889): 38 luku 1 ja 2 §, 40 luku 5 §; Laaksonen ym. 2006: 31.]

6.3 Henkilötietolaki

Henkilötietolaissa (523/1999) määritellään henkilötietojen käsittelyyn liittyvät asiat, ja se sisältää myös velvoitteita tietoturvasta. Henkilötietolakia kutsutaan myös tietosuojalaiksi. Henkilötietolaki on yleislaki, joten tietosuojaan liittyviä asioita käsitellään myös muissa laeissa. Lakia sovelletaan lähes jokaisessa yrityksessä, järjestöissä, yhteisöissä ja viranomaislaitoksessa, jossa käsitellään henkilötietoja. Myös yksityishenkilöiden tekemä henkilötietojen käsittely voi joissain tapauksessa kuulua sen piiriin. Sellaiseksi tapaukseksi

ei kuitenkaan lueta yksityishenkilön yksityistarkoitusta varten pitämää henkilörekisteriä (esimerkiksi henkilökohtaista osoitekirjaa) tai henkilörekisteriä, joka sisältää vain lehdistä ja muista tiedotusvälineistä saatua tietoa. [Laaksonen ym. 2006: 31.]

Seuraavissa luvuissa käydään läpi henkilötietolain tärkeimmät kohdat pääpiirteittäin.

6.3.1 Henkilötietojen käsittelyn yleiset periaatteet

Henkilötietojen käsittelyllä tarkoitetaan ”henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä” [Henkilötietolaki (523/1999): 3 §]. Käsittelyn yleisten periaatteiden tarkoituksena on ohjata henkilörekisterin suunnittelua, toteutusta ja ylläpitämistä siten, että henkilötietolain tarkoitus toteutuu. Henkilötietolain idea voidaankin kiteyttää termiin ”hyvä tietojenkäsittelytapa”. Sillä tarkoitetaan tietojärjestelmien järjestelmällistä suunnittelua ja toteutusta, jossa huomioidaan yksityisyyden suoja lain vaatimalla tavalla. Hyvää tietojenkäsittelytapaa käyttävä henkilörekisterinpitäjä ottaa kaikessa toiminnassaan huomioon rekisteröityjen henkilöiden oikeudet ja henkilötietolain yleiset periaatteet. Yleisin periaatteisiin kuuluvat huolellisuusvelvoite, suunnitteluvelvoite, käyttötarkoitussidonnaisuusperiaate ja virheettömyysvaatimus. [Henkilötietolaki (523/1999): 5-7 ja 9 §; Laaksonen ym. 2006: 32, 38]

Huolellisuusvelvoite velvoittaa henkilötietoja käsiteltävän laillisesti ja huolellisesti sekä hyvä tietojenkäsittelytavan mukaisesti. Käsittelyssä tulee myös huomioida rekisteröityjen yksityisyyden suojaaminen. Hallintaan liittyvien prosessien, esimerkiksi käyttöoikeuksien hallinnan, tulee olla tarpeeksi korkealla laadullisella tasolla. [Henkilötietolaki (523/1999): 5 §; Laaksonen ym. 2006: 38.]

Suunnitteluvelvoite vaatii, että rekisterin käsittelyn pitää olla perusteltua rekisterinpitäjän toiminnan kannalta ja että rekisterin tietojen kerääminen ja käyttö on suunniteltua. Näiden pohjalta luodaan suunnitelma, jossa kerrotaan rekisterin tarkoitus, toimenpiteet tietoturvan hoitamisesta sekä millaisia tietoja prosessissa kerätään ja luodaan. Suunnitelmassa pitää käydä läpi, mistä siihen tulevat tiedot hankitaan ja luovutetaanko niitä ja jos niin millä perusteella. Suunnittelun pitäisi kattaa tietojen käsittely aina keräämisestä tuhoamiseen asti sekä suunnitella hallinnolliset asiat. Hallinnollisiin asioihin kuuluu esimerkiksi tieto siitä, kenellä yrityksessä on päätäntävalta rekisteriä koskevissa asioissa ja

kenellä on rekisterin käsittelyoikeus. Käytännössä jälkimmäinen tarkoittaa sitä, että tietojärjestelmässä olevan rekisterin käyttöoikeuksia voidaan määritellä monipuolisesti tai fyysiseen rekisteriin pääsyä on rajattu. Tämän suunnitelman perusteella voidaan luoda rekisteriseloste, jossa on kuvattu suunnitelman pääpiirteet. [Henkilötietolaki (523/1999): 6 §; Laaksonen ym. 2006: 36-37, 39.]

Käyttötarkoitussidonnaisuusperiaatteen tarkoituksena on, että henkilötietoja käsitellään vain suunnitteluvelvoitteessa määritellyn käsittelyn tarkoitus. Käytännössä siis rekisteriä voi käyttää vain siihen tarkoitukseen, johon se on alun perin tarkoitettu. Mikäli henkilörekisterin tarkoitus muuttuu kokonaan tai oleellisesti, tulisi suunnitella uusi rekisteri. [Henkilötietolaki (523/1999): 7 §; Laaksonen ym. 2006: 39.]

Virheettömyysvaatimus edellyttää, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja käsitellä. Henkilötietojen luottamuksellisuus, eheys ja käytettävyys tulee siis ottaa huomioon. [Henkilötietolaki (523/1999): 9 §; Laaksonen ym. 2006: 40.]

Tietyissä tilanteissa henkilötietoja saa kerätä ja tallentaa suoramainontaa, etämyyntiä tai muuta suoramarkkinointia, mielipide- tai markkinatutkimusta varten mikäli henkilö ei ole sitä kieltänyt. Tällaisia tapauksia ovat: ennakolta yksilöity ja lyhytkestoinen markkinointitoimi; rekisteriin kerätään tieto vain henkilön nimestä, iästä, sukupuolesta, äidinkielestä ja joko arvosta tai ammatista sekä yhdestä häneen liitettävästä tunnistetiedosta sekä yhteystiedoista tai rekisteriä käytetään työtehtäviin liittyvään informointiin ja se sisältää tietoja henkilön tehtävästä ja asemasta työpaikassaan. [Henkilötietolaki (523/1999): 19 §.]

6.3.2 Arkaluonteisten henkilötietojen ja henkilötunnuksen käsitteleminen

Arkaluonteisten henkilötietojen käsitteleminen on lähtökohtaisesti henkilötietolain mukaan kiellettyä. Arkaluonteiset henkilötiedot on määritelty laissa eikä mitään niistä saa käsitellä, ellei sitä ole erikseen laissa sallittu. Alla on listattu henkilötietolain sisältö arkaluonteisten henkilötietojen käsittelemisestä. [Henkilötietolaki (523/1999): 11 §; Laaksonen ym. 2006: 40.]

> Arkaluonteisina tietoina pidetään henkilötietoja, jotka kuvaavat tai on tarkoitettu kuvaamaan
>
> - rotua tai etnistä alkuperää;

- henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista;
- rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta;
- henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia;
- henkilön seksuaalista suuntautumista tai käyttäytymistä tai
- henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

Arkaluonteisia henkilötietoja voidaan kuitenkin käsitellä lain 12 § nojalla. Sellaisia tilanteita ovat esimerkiksi rekisteröidyn suostumuksella tai yrityksen järjestämä työterveydenhuolto sitä vaatiessa. Niillä henkilöillä, jotka käsittelevät arkaluonteisia henkilötietoja, on vaitiolovelvollisuus eli he eivät saa paljastaa sivullisille käsittelemiään asioita. [Henkilötietolaki (523/1999): 12 §; Laaksonen ym. 2006: 41, 43.]

Henkilötunnuksen käsittelyperusteet on kerrottu henkilötietolaissa [1999: 13 §]:

> Henkilötunnusta saa käsitellä rekisteröidyn yksiselitteisesti antamalla suostumuksella tai, jos käsittelystä säädetään laissa. Lisäksi henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää:
>
> - laissa säädetyn tehtävän suorittamiseksi;
> - rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi; tai
> - historiallista tai tieteellistä tutkimusta taikka tilastointia varten.

Käytännössä henkilötunnuksen käytön edellytys on se, että henkilö pitää pystyä tunnistamaan yksiselitteisesti. Mikäli mahdollista, on tunnistus pyrittävä toteuttamaan jollain muulla tavalla esimerkiksi käyttämällä tietyllä logiikalla luotuja käyttäjätunnuksia. Lisäksi on huomioitava, ettei henkilötunnusta ei saa merkitä turhaan esimerkiksi tulosteisiin. Tämä on hyvä ottaa huomioon myös sähköpostiviestinnässä, sillä henkilötunnusta ei saisi välittää salaamattomassa sähköpostiviestissä. [Henkilötietolaki (523/1999): 13 §; Laaksonen ym. 2006: 41.]

6.3.3 Henkilötietojen luovutus, siirto ja ulkoistaminen

Henkilötietojen luovutuksella tarkoitetaan esimerkiksi tietojen antoa yhteistyökumppanille. Henkilötietoja saa luovuttaa, mikäli henkilö ei ole luovutusta erikseen kieltänyt ja on ilmeistä, että henkilö tietää tietojen luovutuksesta. Tällöin yhteistyökumppanista tulee myös rekisterinpitäjä. [Henkilötietolaki (523/1999): 19 §; Henkilötietojen luovutus yhteistyökumppanille suoramarkkinointia varten 2004.]

Henkilötietojen siirrosta puhutaan taas silloin, kun yrityksen henkilötietorekisterin fyysinen sijainti siirtyy ulkomaille. Hyvänä esimerkkinä tästä on kansainvälinen yritys, jonka AD-hakemistopalvelu siirretään sijaitsemaan ja sitä hallinnoidaan vain yhteen niistä maista, joissa yrityksellä on liiketoimintaa. Tällöin henkilötiedot saattavat sijaita fyysisesti eri maassa. Mikäli henkilötiedot sijaitsevat EU- ja ETA-maiden ulkopuolella, tulee yrityksen ottaa huomioon lain säädökset henkilötietojen siirrosta. Käytännössä laissa sanotaan siirron olevan mahdollista, mikäli loppusijoitusmaassa taataan riittävä tietosuojan taso. Siirtotoimenpiteessä rekisterinpitäjä ei välttämättä vaihdu. [Henkilötietolaki (523/1999): 22 §; Laaksonen ym. 2006: 33-34.]

Ulkoistettaessa henkilörekisterin hallinta kolmannelle osapuolelle, on sen osapuolen velvollisuus antaa rekisterinpitäjälle asianmukaiset sitoumukset ja muutoin riittävät takeet henkilötietojen suojaamisesta ennen tietojen käsittelyyn ryhtymistä. Käytännössä osapuolet laativat sopimuksen, jossa todetaan henkilötietojen käsittelijän toimivan rekisterinpitäjän ohjeiden mukaan ja noudattavan rekisterinpitäjälle säädettyjä suojaamisvelvoitteita. Sopimukseen kannattaa ottaa mukaan myös kontrollimekanismit, jotka mahdollistavat rekisterinpitäjän tekemät tai teettämät auditoinnit. Tietoturvavelvoitteissa lopullinen vastuu on kuitenkin aina rekisterinpitäjällä. [Henkilötietolaki (523/1999): 32 §; Laaksonen ym. 2006: 46-47.]

6.3.4 Henkilötietolain vaatimukset tietoturvalle

Henkilötietolaki vaatii, että henkilörekisterin tietoihin ei saa päästä asiattomasti käsiksi vahingossa tai laittomasti. Tietojen suojaamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, suojaamisesta aiheutuvat kustannukset, henkilötietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden kannalta. Käytännössä se tarkoittaa vähintäänkin sitä, että tietojärjestelmä on suojattu salasanalla ja asiaan kuulu-

valla palomuurijärjestelmällä. Olisi myös hyvä, että jo yrityskin päästä käsiksi sen laitteistoon aiheuttaa viiveettä hälytyksen rekisterinpitäjälle. Tämä vaatisi aiemman lisäksi myös järjestelmälokien ja jonkinlaisen niitä automaattisesti tutkivan sovelluksen käytön. [Henkilötietolaki (523/1999): 32 §; Laaksonen ym. 2006: 42-43.]

Vaadittava tietoturvataso on kuitenkin ensisijaisesti kytköksissä käsiteltävien henkilötietojen laatuun. Arkaluonteisten tietojen ja henkilötunnuksen sisältävien rekistereiden tietoturvataso pitää olla korkeampi kuin muiden. Henkilötietojen käsittelyn laajuus asettaa myös vaatimuksia käyttöoikeuksien määrittämiseen ja hallitsemiseen. Lain lähtökohtana on kuitenkin se, että rekisterinpitäjä itse määrittelee riittävän tietoturvatason. Rekisterin pitäjän ei tarvitse käyttää aina uusinta teknologiaa tietoturvan takaamisesti. Järjestelmän tietoturvataso on kuitenkin hyvä päivittää säännöllisesti, koska tietoturvatekniikat kehittyvät jatkuvasti. Mikäli joltain taholta tulee vaatimus selkeästi korkeampaan tietoturvatasoon kuin mitä henkilötiedot tavallisesti edellyttäisivät, tulee sen tahon vastata tason noston aiheuttamista kustannuksista. [Laaksonen ym. 2006: 42-44.]

6.3.5 Rangaistussäännökset

Rekisterinpitäjä on henkilötietolain määräysten vastaisesta toiminnasta vahingonkorvausvelvollinen. Mikäli rekisteröidylle tai muulle henkilölle seuraa lain vastaisesta tietojen käsittelystä taloudellista tai muuta vahinkoa, on rekisterinpitäjä velvollinen korvaamaan aiheutuneet vahingot. Tietomurrosta ja henkilörekisteririkoksesta säädetään erikseen rangaistukset rikoslaissa. Vaitiolovelvollisuuden rikkominen on myös rangaistavaa ja siitä voidaan tuomita sakkoihin tai enintään kahdeksi vuodeksi vankeusrangaistukseen. [Henkilötietolaki (523/1999): 48 §; Rikoslaki (39/1889): 38 luku 1-2 ja 8-9 §; 40 luku 5 §; Laaksonen ym. 2006: 45.]

6.4 Laki kansainvälisistä tietoturvallisuusvelvoitteista

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) koskee lähinnä tilanteita, jolloin tietoaineistoa pidetään lähtökohtaisesti valtio- tai turvallisuusalaisuuksina tai tietoina, joiden paljastuminen olisi vastoin yleistä etua. Vaikka laki koskee lähinnä viranomaisia, sovelletaan sitä myös yrityksiin ja heidän työntekijöihinsä silloin, kun kyseessä on turvallisuusluokiteltu sopimus tai sitä edeltävä hankintakilpailu tai yritys on mukana

sellaisessa alihankkijana. [Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004): 1 §; Laaksonen ym. 2006: 47-48.]

6.5 Laki yksityisyyden suojasta työelämässä

Lain yksityisyyden suojasta työelämässä (759/2004) tarkoituksena on turvata työntekijöiden yksityiselämän suoja ja muita yksityisyyden suojaan liittyviä perusoikeuksia. Siitä syystä sitä kutsutaan myös työelämän tietosuojalaiksi. Lailla turvataan se, että vaikka työntekijä on työnantajan tiloissa ja käyttää työnantaja antamia työvälineitä (esimerkiksi tietokone, mobiililaite, internetyhteys), on hänellä silti oikeus yksityisyyteen ja luottamukselliseen viestintään. [Laki yksityisyyden suojasta työelämässä (759/2004): 1-2 §; Laaksonen ym. 2006: 49.]

Työsopimuslaki antaa työnjohto- ja valvontaoikeuden perusteella työnantajalle oikeuden antaa työtekijöitä koskevia sitovia ohjeita ja määräyksiä, jotka liittyvät työtehtävien hoitamiseen. Näihin ohjeisiin on hyvä liittää tietoturvatoimenpiteitä, joita työntekijöiden on syytä noudattaa työpaikalla ja myös kotona, mikäli käytössä on etäyhteys työnantajan tietojärjestelmiin. Määräyksiä annettaessa tulee ottaa huomioon, että mikäli niiden noudattaminen vaatii yhteistoimintalain mukaista käsittelyä, ei määräystä saa antaa ilman kyseistä käsittelyä. Käytännössä tilanne tulee eteen silloin, kun työntekijöitä on yli 20 ja työpaikalla otetaan käyttöön erilaisia teknisiä välineitä työntekijöiden valvontaa varten tai tehdään päätöksiä esimerkiksi internetin, tietoverkon tai kameravalvonnan käytöstä. [Laaksonen ym. 2006: 49-50.]

Laissa säädetään myös työntekijöiden henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niiden vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestien hakemisesta ja avaamisesta. [Laki yksityisyyden suojasta työelämässä (759/2004): 2 §; Laaksonen ym. 2006: 50.]

6.5.1 Valvontamenetelmät

Työnantaja voi toteuttaa teknistä valvontaa monella eri tavalla. Tekniikkavalinnan pitäisi kuitenkin olla sellainen, joka aiheuttaa vähiten uhkaa yksityisyyden suojalle ja viestin luottamuksellisuudelle. Teknisen valvonnan toteutus on syytä dokumentoida ja sitä tulee päivittää aina muutostilanteissa. [Laaksonen ym. 2006: 51.]

Valvontaa voi toteuttaa kulunvalvonnalla tai kameravalvonnalla. Kulunvalvonta on näistä lain mukaan ”lievempi” vaihtoehto, jota työnantajan pitäisi harkita näistä kahdesta vaihtoehdosta ensimmäisenä. Mikäli kulunvalvontaan halutaan liittää paikannustoiminto, tulee sille olla perustelu. Perusteluna voi olla esimerkiksi se, että työntekijän työtehtävien hoitamiseen kuuluu paljon liikkumista, esimerkiksi taksin ajaminen. [Laaksonen ym. 2006: 51-52.]

Kameravalvontaa saa käyttää vain lain määrittelemissä edellytyksissä. Edellytyksiä ovat tilassa olevien henkilöiden turvallisuuden varmistaminen, omaisuuden suojaaminen sekä tuotantoprosessin turvallisuuden ja toiminnan varmistamiseksi. Työntekijöiden henkilöstötiloissa tai henkilökohtaisella työpisteellä ei kuitenkaan saa olla kameravalvontaa. Työpisteen kameravalvonta on sallittua vain, jos työntekijän työhön liittyy välivaltauhka, turvallisuus- tai terveysriskejä, työntekijän tehtäviin kuulu merkittävän arvokkaan omaisuuden käsittelyä, valvonnalla pyritään varmistamaan työntekijän etuja ja oikeuksia tai asiasta on sovittu työnantajan ja työntekijän välillä. Kameravalvonnasta saatuja tallenteita saa käyttää vain siihen tarkoitukseen, jota varten valvonta on tehty. Tallenteita saa säilyttää vain niin pitkään, kun niitä valvonnan kannalta tarvitaan, mutta korkeintaan viisi vuotta. Laki kuitenkin mahdollistaa pidemmän säilytyksen poikkeustilanteissa. Tällaisia poikkeustilanteita ovat väärinkäytösten todistaminen irtisanomistilanteissa ja muut erityiset syyt. [Laki yksityisyyden suojasta työelämässä (759/2004): 16 §; Laaksonen ym. 2006: 52-54.]

6.5.2 Rangaistussäännökset

Mikäli laissa suojattuja oikeuksia rikotaan, voidaan rikkoja tuomita sakkoon, jollei laissa säädetä ankarampaa rangaistusta [Laki yksityisyyden suojasta työelämässä (759/2004): 24 §]. Henkilörekisteririkoksesta, tietomurrosta, salakatselusta, salakuuntelusta, viestintäsalaisuuden loukkaamisesta, salassapitorikoksesta ja virkarikoksesta säädetään rangaistukset taas rikoslaissa ja rangaistukset ovat sakoista enintään kahteen vuoteen vankeutta. [Rikoslaki (39/1889): 24 luku 5-7 §, 38 luku 1-4 ja 8-9 §, 40 luku.]

6.6 Sähköisen viestinnän tietosuojalaki

Sähköisen viestinnän tietosuojalaki (516/2004) koskee käytännössä kaikkia yrityksiä, koska ne käsittelevät työntekijöidensä tunnustamistietoja ja luottamuksellisia viestejä

viestintäverkossaan (puhelin- tai tietoverkko). Lain tarkoituksena on yksityisyydensuoja ja viestinnän luottamuksellisuus sähköisessä viestinnässä sekä edistää sen tietoturvaa ja monipuolisten palveluiden tasapainoista kehitystä. [Sähköisen viestinnän tietosuojalaki (516/2004): 1 §; Laaksonen ym. 2006: 54-55.]

Vuonna 2009 lakiin tehtiin muutos (125/2009), joka mahdollisti yhteisötilaajien (käytännössä yritysten) rikkoa viestintäsalaisuuden väärinkäytöstilanteissa, esimerkiksi yritys-salaisuuksien paljastamisen takia. Tästä syystä laki on saanut nimikseen myös urkinta-laki ja Lex Nokia. [Mikä urkintalaki? 2009.]

Laissa on määritelty paljon erilaisia termejä. Lain tulkinnan kannalta oleellisimmat ovat tunnistamistieto, paikkatieto, teleyritys ja yhteisötilaaja. Tunnistamistieto vastaa henkilötietoa, mutta se voi kohdistua henkilön lisäksi myös yritykseen. Paikkatiedolla tarkoitetaan jonkin asian maantieteellistä sijaintia, jota voidaan käyttää tarjoamaan esimerkiksi paikannuspalveluita. Lisäarvopalvelu on taas palvelu, joka käsittelee tunnistamistietoja tai paikkatietoja. Teleyritys tarjoaa viestintäverkkoon liittyviä palveluita, kuten verkko- ja viestintäpalveluita tai lisäarvopalveluita ennalta rajoittamattomalle joukolle. Näistä lisäarvopalvelu voi olla myös muun kuin teleyrityksen tarjoama. Yhteisötilaaja on taas yritys tai yhteisö, joka tilaa teleyrityksen palveluita tai muun tarjoajan lisäarvopalveluita. Yllä mainitut termit, ja niiden lisäksi muutama muu aiheeseen liittyvä termi, on määritelty tarkemmin taulukossa 14.

Taulukko 14. Sähköisen viestinnän tietosuojalakiin liittyvä termistö. [Sähköisen viestinnän tietosuojalaki (516/2004): 2 §; Laaksonen ym. 2006: 32, 55-58.]

Termi	**Määritelmä**
Käyttäjä	Luonnollinen henkilö, joka käyttää viestintäpalvelua tai lisäarvopalvelua olematta välttämättä tämän palvelun tilaaja.
Lisäarvopalvelu	Palvelu, joka perustuu tunnistamistietojen tai paikkatietojen käsittelyyn muuta tarkoitusta kuin verkkopalvelun tai viestintäpalvelun toteuttamista varten.
Paikkatieto	Tieto, joka ilmaisee liittymän tai päätelaitteen maantieteellisen sijainnin ja jota käytetään muuhun tarkoitukseen kuin verkkopalvelun tai viestintäpalvelun toteuttamiseen, esimerkiksi paikannuspalvelut.
Teleyritys	Verkkoyritys tai palveluyritys, joka harjoittaa yleistä teletoimintaa eli tarjoaa palveluja etukäteen rajoittamattomalle joukolle.
Tilaaja	Oikeushenkilö tai luonnollinen henkilö, joka on tehnyt sopimuksen viestintäpalvelun tai lisäarvopalvelun toimittamisesta.

Tunnistamistieto	Tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. Käytännössä sama kuin henkilötieto, mutta kohteena voivat olla henkilöiden lisäksi yritykset, yhdistykset ja säätiöt.
Verkkopalvelu	Teleyrityksen toteuttama palvelu, jossa viestintäverkkoa tarjotaan käytettäväksi viestien siirtoon, jakeluun tai tarjolla pitoon etukäteen rajoittamattomalle käyttäjäpiirille.
Viesti	Viestintäverkossa osapuolten välillä liikkuva tai vapaasti valikoituville vastaanottajille välitettävä sanoma, esimerkiksi puhelu, sähköpostiviesti, tekstiviesti tai puheviesti.
Viestintäpalvelu	Teleyrityksen toteuttama viestien siirto, jakelu tai tarjolla pitäminen viestintäverkossa, jota tarjotaan etukäteen rajoittamattomalle käyttäjäpiirille.
Viestintäverkko	Toisiinsa liitetyt johtimet ja laitteet muodostuvat järjestelmän, joka on tarkoitettu viestien siirtoon tai jakeluun johtimella, radioaalloilla, optisesti tai muulla sähkömagneettisella tavalla.
Yhteisötilaaja	Viestintäpalvelun tai lisäarvopalvelun tilaajana oleva yritys tai yhteisö, joka käsittelee viestintäverkossaan käyttäjien luottamuksellisia viestejä, tunnistamistietoja tai paikkatietoja, esimerkiksi yliopistot, valtion virastot, osuuskunnat ja osakeyhtiöt.
Yleinen viestintäverkko	Viestintäverkko, jota tarjotaan etukäteen rajaamattomalle käyttäjäpiirille, esimerkiksi matkaviestinverkot, kiinteät puhelinverkot, joukkoviestintäverkot ja internet.

Suljetuttuihin ja tietylle käyttäjäpiirille rajatuttuihin verkkoihin, joita ovat esimerkiksi yritysten sisäverkot, ei sovelleta sähköisen viestinnän tietosuojalakia. Niihin kuitenkin sovelletaan lain 4-5 §:iä, jotka määrittelevät sisäverkossa kulkevat viesti, tunnistamistiedot ja paikkatiedot luottamuksellisiksi. Mikäli henkilö on oikeudettomasti vastaanottanut tai saanut noita tietoja, ovat niiden sisällöt vaitiolovelvollisuuden ja hyväksikäyttökiellon alaisia. Vaikka sisäverkkoihin ei sovelleta sähköisen viestinnän tietosuojalakia, niin siihen pätevät henkilötietolaki ja laki yksityisyyden suojasta työelämässä. Sen lisäksi on huomioitava, että esimerkiksi sähköposti on aina luottamuksellista riippumatta siitä, mistä verkosta se on lähetetty. [Sähköisen viestinnän tietosuojalaki (516/2004): 3 §; Laaksonen ym. 2006: 61-62.]

Laissa käsitellään myös paikantamistietojen käsittelyä. Mikäli paikantamistiedot liittyvät viestien välittämiseen, esimerkiksi matkaviestinverkossa, niin silloin ne ovat paikantamistietojen sijaan tunnistamistietoja. Mikäli paikantamistietoja halutaan käsitellä, tulee sen olla perusteltua ja käsittelyn suunniteltua. [Sähköisen viestinnän tietosuojalaki (516/2004): 16 §; Laaksonen ym. 2006: 72-73.]

6.6.1 Oikeus käsitellä viestien tunnistamistietoja

Lakia sovelletaan lähinnä viestinnän välittäjiin, joita ovat teleyritykset ja yhteisötilaajat. Lakia ei sovelleta silloin, kun viestinnän välittäjä on itse viestinnän osapuolena, koska silloin sillä on lähtökohtaisesti laajat oikeudet käsitellä viestiä. Viestinnän osapuolet saavat käsitellä viestin sisältöä ja tunnistamistietoja ja viestinnän ulkopuolinen taho vain viestinnän osapuolten luvalla. [Sähköisen viestinnän tietosuojalaki (516/2004): 3 §; Laaksonen ym. 2006: 59, 63.]

Lain puitteissa viestinvälittäjällä on oikeus käsitellä tunnistamistietoja ainoastaan silloin, kun sillä selvitetään ja estetään väärinkäytöksiä, pyritään havaitsemaan tekninen vika tai virhe sekä palveluntarjoamista varten. Yhteisötilaajalla on oikeus käsitellä tunnistamistietoja myös silloin, kun viestit sisältävät esimerkiksi sisäistä laskutusta ja oman toiminnan teknistä kehittämistä. Joissain tilanteissa ei voi kuitenkaan olla varma, sovelletaanko lakia vai ei. Laki yksityisyydestä työelämässä asettaa tiukat ja rajalliset puitteet sille, milloin yritys voi katsoa sähköpostiviestien otsikko- ja sisältötietoja. Tämä aiheuttaa sen, että työntekijän käyttäessä esimerkiksi työsähköpostiaan viestinnässään, ei yrityksellä ole varmuutta, onko se viestinnän osapuoli vai ei. Käytännössä yritys on viestinnän osapuoli silloin, kun sähköpostit on lähetetty jostain geneerisestä osoitteesta esimerkiksi markkinointi@yritys.fi tai rekry@yritys.fi. [Sähköisen viestinnän tietosuojalaki (516/2004): 13, 13a-13k §; Laaksonen ym. 2006: 59-60.]

6.6.2 Viestien suodattaminen ja salaaminen

Laki mahdollistaa haittaohjelmia sisältävien viestien suodattamisen, mutta vain silloin, kun toimet ovat välttämättömiä palveluiden turvaamiseksi. Ilman vastaanottajan suostumusta tehtävää suodattamista saa tehdä vain silloin, kun toimenpiteisiin ryhtymättä jättäminen aiheuttaisi järjestelmän täyden toimimattomuuden. Haittaohjelmia, viruksia ja roskapostia liikkuu kuitenkin käytännössä sen verran paljon, että yhteisöjen on täytynyt aloittaa suodatustoimet jo ennen kuin se on täysin välttämätöntä. Tämä on mahdollistettu sillä, että käyttäjältä on hankittu asiaan suostumus esimerkiksi internet-yhteyden liittymäsopimuksen ehdoissa. [Sähköisen viestinnän tietosuojalaki (516/2004): 20 §; Laaksonen ym. 2006: 68-69.]

Monella yrityksellä on käytössä roskapostin suodatus, jossa mahdolliset roskapostit eristetään omaan kansioonsa sähköpostilaatikossa. Näissä suodatuksissa on se ongelma,

että välillä ”oikeita” viestejä menee vahingossa roskaposteina tähän erilliseen kansioonsa ja siitä syystä vastaanottaja ei välttämättä näe niitä silloin kun olisi tarpeen. Tällaiset tilanteet ovat hankalia, mutta lähtökohtaisesti viestin lähettäjä kantaa vastuun (mahdollisesti myös taloudelliset seuraukset) siitä meneekö viesti perille vastaanottajalle. Tästä syystä tärkeiden viestien perille meno tulisi tarkistaa jotain toista viestintä käyttäen. [Laaksonen ym. 2006: 72.]

Lain mukaan palvelun tilaajalla ja käyttäjällä on oikeus suojata viestinsä salaamalla ne, jos laissa ei toisin säädetä. Kuka tahansa saa siis käyttää haluamaansa salausteknologiaa viestiensä salaamiseen, kunhan se ei aiheuta häiriöitä verkko- ja viestintäpalveluille. [Laaksonen ym. 2006: 73.]

6.6.3 Sähköisen viestinnän tietosuojalain vaatimukset tietoturvalle

Tietoturvan näkökulmasta laki velvoittaa yhteisötilaajaa huolehtimaan käyttäjien tunnistamistietojen ja paikkatietojen käsittelyn turvasta. Laki mahdollistaa myös tietoturvaloukkauksien torjumisen laissa mainituin menetelmin ja ehdoin. Käytännössä tämä tarkoittaa roskapostien, haittaohjelmien ja muiden vastaavien ohjelmien estämisen ja poistamisen. [Sähköisen viestinnän tietosuojalaki (516/2004): 19-20 §; Laaksonen ym. 2006: 60.]

Palvelun ja käsittelyn tietoturvasta huolehtiminen tarkoittaa toimia toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi. Nämä toimet on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin. [Sähköisen viestinnän tietosuojalaki (516/2004): 19 §.]

Toiminnan turvallisuudella tarkoitetaan muun muassa, että ylläpidetään tietoturvavaatimuksien toteuttamisesta kertovaa dokumentaatiota, seurataan tietoturvatasoa säännöllisesti, varmistetaan tietoturvavaatimusten toteutuminen alihankintatilanteissa, huolehditaan laitteiden ja tiedostojen suojauksesta ja pääsynvalvonnasta, pidetään listaa järjestelmässä olevista käyttäjätunnuksista ja käyttöoikeuksista sekä valvotaan tietojärjestelmissä tapahtuvia tapahtumia [Laaksonen ym. 2006: 66.]

6.6.4 Rangaistussäännökset

Sähköisen viestinnän tietosuojalain rikkomisesta rangaistaan vain, jos teko on ollut tahallinen. Vahingossa tehdyt rikkomukset eivät siis aiheuta seuraamuksia ja vähäisetkin rikkomukset saatetaan jättää tuomitsematta. Lakia vastaan tehdyistä rikkomuksista voidaan tuomita sakkoihin. Viestintäsalaisuuden loukkaamisen, tietomurron ja vaitiolovelvollisuuden rikkomisen rangaistukset säädetään erikseen rikoslaissa ja niistä voidaan tuomita sakkoihin tai enintään kahteen vuoteen vankeutta. [Sähköisen viestinnän tietosuojalaki (516/2004): 42 §; Rikoslaki (39/1889): 38 luku 1-5 ja 8 §, 40 luku 5 §; Laaksonen ym. 2006: 75.]

6.7 Laki tietoyhteiskunnan palvelujen tarjoamisesta

Lakia tietoyhteiskunnan palvelujen tarjoamisesta (458/2002) sovelletaan silloin, kun tarjotaan etäpalveluita sähköisesti yleensä vastiketta vastaan. Käytännössä tällaisia palveluita ovat esimerkiksi internetkaupat, joissa koko osto- ja maksutapahtumaketju tapahtuu sähköisesti. Olennaista tietoyhteiskuntapalvelulle on se, että se on sähköisessä muodossa. Yhteiskuntapalvelussa myydään esimerkiksi tietokoneohjelmia, kirjoja ja elokuvia, jotka toimitetaan ostotapahtuman jälkeen sähköisessä muodossa. [Laki tietoyhteiskunnan palvelujen tarjoamisesta (458/2002): 2 §; Laaksonen ym. 2006: 77.]

6.8 Laki sähköisestä asioinnista viranomaistoiminnassa

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) määrittelee viranomaisten tarjoamien sähköisten asiointipalveluiden menettelytavat. Se tunnetaan myös nimellä asiointilaki. Lakia sovelletaan hallintoasian, tuomioistuinasian, syyteasian ja ulosottoasian sähköiseen vireillepanoon, käsittelyyn ja päätöksen tiedoksiantoon, jollei muualla laissa toisin säädetä. Tämän lisäksi lakia sovelletaan paikoitellen myös muussa viranomaistoiminnassa. [Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003): 2 §; Laaksonen ym. 2006: 78.]

Lain tarkoituksena on sujuvoittaa ja nopeuttaa sähköistä asiointia sekä parantaa sen tietoturvatasoa ja tämän lisäksi edistää sähköisten tiedonsiirtomenetelmien käyttöä. Tie-

toturva on erityisen tärkeä tilanteissa, joissa viranomaisdokumentteja välitetään sähköisesti. [Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003): 1 §; Laaksonen ym. 2006: 78.]

6.9 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (619/2009) on luotu edistämään sähköisen asioinnin turvallisuutta. Laissa määritellään vahva sähköinen tunnistaminen, sähköiset allekirjoitukset sekä niihin liittyvien palveluiden tarjoaminen niitä käyttäville palveluntarjoajille ja yleisölle. [Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (619/2009): 1 §.]

Sähköinen allekirjoitus voi yksinkertaisimmillaan olla henkilön etu- ja sukunimi sähköpostiosoitteessa tai käsin kirjoitettu allekirjoitus, joka on muutettu sähköiseen muotoon. Nämä eivät kuitenkaan ole laissa määriteltyjä vahvoja sähköisiä tunnistautumisia. Niitä ovat esimerkiksi teleyritysten mobiilivarmenteet, sähköisessä henkilökortissa oleva kansalaisvarmenne ja pankkien verkkopankkitunnukset. [Vahva sähköinen tunnistaminen, sähköinen allekirjoitus ja varmenne 2013.]

6.10 Viestintämarkkinalaki

Viestintämarkkinalakia (393/2003) sovelletaan lähinnä teleyrityksiin ja se määrittelee niiden tietoturvavelvoitteita. Laissa on myös annettu Viestintävirastolle oikeus antaa sitovia ohjeita yrityksille, joihin lakia sovelletaan. Viestintäviraston ohjeita julkaistaan heidän internetsivuillaan, ja kuka tahansa voi ottaa niitä käyttöönsä. [Viestintämarkkinalaki (393/2003): 3, 8 §; Laaksonen ym. 2006: 80.]

7 Tietoturvakartoitus

Tietoturvakartoituksen tarkoituksena oli selvittää yrityksen nykyinen tietoturvataso ja luoda lähtökohdat yrityksen tietoturvakäsikirjan päivittämiselle. Tietoturvakäsikirjan haluttiin noudattavan standardia ISO/IEC 27001 ja Kansallista turvallisuusauditointikriteeristöä KATAKRI:a soveltuvin osin.

7.1 Suojattavien kohteiden selvittäminen

Tietoturvakartoituksen tekeminen aloitettiin kartoittamalla yrityksen henkilöstöllä käytössä olevat suojattavat kohteet. Ensimmäisen kyselyn tarkoituksena oli pyrkiä selvittämään, millaisia tietoja, tietolähteitä ja välineitä henkilöstö käyttää työskennellessään.

Suojattavia kohteita kartoittavassa kyselyä luotaessa sopivien kysymysten suunnittelu aloitettiin käyttämällä apuna Tietoturvaoppaan Tietoturvakartoituksen kysymyslistaa [Tietoturvakartoituksen kysymyslista 2006]. Kysymyslistalla olevat kysymykset käsittelevät sitä, mitkä tiedot ovat arvokkaita tai erittäin arvokkaita, kuinka usein niitä käytetään, miten niitä valvotaan ja kuinka suuri menetys on, jos tiedot katoavat esimerkiksi onnettomuuden tai laitteen häviämisen seurauksena.

Näistä kysymyksistä koottiin kyselyyn seuraavat kysymykset:

- Mitä laitetta, ohjelmisto tai tietolähdettä tarvitset työssäsi?
- Kuinka usein käytät asiaa?
- Missä se sijaitsee?
- Miten olet huolehtinut edellä mainittujen suojauksesta?
- Onko se varmuuskopioitu, jos niin kuinka usein?
- Mikäli asia hajoaa tai ei ole saatavilla, niin vaikuttaako se merkittävästi työskentelyysi?

Kysymykset esitettiin taulukkomuodossa, jotta henkilöstön ei tarvitsisi vastata erikseen jokaisen työvälineen kohdalla jokaiseen kysymykseen. Täyttöä helpottaakseen taulukkoon esitäytettiin joitain tietoja, kuten tietokone, puhelin, muistitikku, intra, asiakkaiden tietoja sisältävät tiedostot ja paperit. Taulukon loppuun jätettiin kuitenkin tyhjää tilaa, jotta

vastaajat voisivat itse lisätä tärkeäksi kokemiaan asioita. Kysymysten alustuksessa pyydettiin myös suojauksen ja varmuuskopioinnin kohdalla laittamaan sarakkeeseen ”ei”, mikäli vastaaja ei ollut hoitanut asiaa ja viiva ”-” mikäli vastaaja ei kokenut sen kuuluvan työtehtäviinsä.

Näiden kysymysten lisäksi kyselyllä haluttiin erikseen kartoittaa työntekijöiden käytössä olevia paikallisia virtuaalikoneita. Koneista haluttiin tietää nimi, käyttötarkoitus, sijainti, käyttöjärjestelmä ja asennetut ohjelmat, miten se on suojattu ja varmuuskopioitu, miten sen käyttöjärjestelmäpäivityksistä on huolehdittu ja vaikuttaako sen puuttuminen merkittävästi työskentelyyn. Nämäkin kysymykset toteutettiin taulukkomuodossa ja taulukkoon oli esitäytettynä malliksi yksi rivi.

Kyselyn lopussa kysyttiin vielä avoin kysymys tietoturvasta: Miten huomioit tietoturvan päivittäisessä työssäsi? Kysymyksen yhteydessä listattiin mahdollisia käsiteltäviä asioita, kuten salasanojen pituus ja vahvuus, koneen lukitseminen ja säilytys, asiakkaista keskustelu työpaikan ulkopuolella, tiedostojen ja paperien säilytys. Kysymyksen alustuksessa kerrottiin, että sen tarkoituksena on kerätä hyviä käytänteitä ja vinkkejä.

Suojattavien kohteiden kartoituksen tulokset jäävät vain yrityksen tietoon.

7.2 Suojattavien kohteiden selvityksen laajennus

Ensimmäisen kyselyn tuloksia tutkittaessa huomattiin, että saatua tietoa pitää syventää. Toisessa kyselyssä keskityttiin siihen, missä työntekijöiden käyttämiä asiakkaita koskevia luottamuksellisia tietoja säilytetään ja kuinka kriittistä niiden häviäminen tai joutuminen vääriin käsiin aiheuttaisi yritykselle.

Kyselyssä tiedusteltiin seuraavia asioita:

- Säilytetäänkö luottamuksellisia tietoja keskitetysti?
- Missä luottamuksellisia tietoja varastoidaan?
- Mikäli projektin henkilö ei ole käytettävissä, esimerkiksi irtisanoutuminen, niin onko kaikki tarvittava luottamuksellinen tieto vielä projektin käytössä?
- Välitetäänkö asiakkaiden luottamuksellisia tietoja sähköpostitse? Ovatko ne silloin salaamattomia?

- Siirretäänkö asiakkaan luottamuksellista tietoa paikasta toiseen jollain tavalla? Miten? Ovatko ne silloin salaamattomia?
- Millainen haitta yritykselle aiheutuu, jos asiakkaan luottamuksellista tietoa häviävää? Entä jos se joutuu vääriin käsiin?
- Onko sopimuksissa sanktioita tiedon häviämisestä, vuotamisesta tai muusta samankaltaisesta tilanteesta? Millaisista tilanteista sanktioita on määritelty?

Kysely toteutettiin Surveypal-internetkyselynä ja se lähetettiin kaikille yrityksen projektipäälliköille. Kyselyn vastaukset kerättiin kolmen viikon aikana ja kaikki kahdeksan projektipäällikköä vastasivat kyselyyn. Kyselyn tulokset jäävät vain yrityksen tietoon.

7.3 Tietoturvan tason tarkempi selvitys

Kahden ensimmäisen kyselyn ulkopuolelle jäi suurin osa tietoturvaa koskevista kysymyksistä. Loput kysymykset koottiin yhdistämällä ISO/IEC 27001 -standardin ja KATAKRI: käsittelemät aihealueet ja jakamalla ne tietoturvan osa-alueihin luvussa 4 kerrotun mukaisesti. Kyselyn aihealueet on kerrottu lukujen 4.1-4.9 taulukoissa 3-12 (poisluettuna taulukko 6). Selvityksessä käytetyt kysymykset ovat liitteessä 4.

Tietoturvatason tarkempi selvitys toteutettiin kyselytutkimuksena. Kyselyä varten haastateltiin muutamia yrityksen avainhenkilöitä, joilla oli tietämystä kysymyksiä käsittelevistä asioista. Haastatteluiden tulokset jäävät vain yrityksen tietoon.

7.4 Tietoturvakartoituksen tulokset ja jatkotoimenpiteet

Tietoturvakartoituksen lopputuloksena saatiin tieto tietoturvan kartoitushetken tasosta ja lista kehitettävistä alueista. Kartoituksen tulosten arkaluontoisuuden takia tulokset jäävät kuitenkin vain kyseessä olevan yrityksen käyttöön, eikä niitä käydä sen takia tarkemmin läpi tässä dokumentissa. Kartoituksen tuloksia käytetään hyväksi tehtäessä yritykselle tietoturvan kehittämissuunnitelma ja kehitettäessä yrityksen tietoturvakäsikirjaa.

8 Yhteenveto

Työn tarkoituksena oli luoda tietoturvakartoitus, jolla voitiin määrittää yrityksen tietoturvan taso. Tutkimus toteutettiin Rongo Oy:lle, jonka antaman toimeksiannon taustalla oli halu kehittää yrityksen tietoturvakäsikirjaa. Tietoturvakäsikirjan haluttiin pohjautuvan soveltuvilta osilta ISO/IEC 27001 -standardiin ja Kansalliseen turvallisuusauditointikriteeristö KATAKRI:n. Käsikirjaa kehitettäessä oli tarkoitus hyödyntää myös Valtionhallinnon turvallisuuden johtoryhmä VAHTI:n julkaisuja. Tietoturvakartoituksen tekeminen ja käsikirjan päivittäminen olisi ollut kuitenkin liian laaja aihe insinöörityöksi, joten työssä keskityttiin vain tietoturvakartoitukseen.

Käsikirjan päivityksessä käytettävät lähdemateriaalit otettiin käyttöön myös kartoitusta tehtäessä, koska kartoituksen oli tarkoitus olla käsikirjaa tukeva teos. Lähdeaineistoon tutustuessa ensimmäiseksi ongelmaksi muodostui se, millä tietoturvan osa-alueiden jaottelulla työ haluttiin toteuttaa. ISO/IEC 27001:n ja KATAKRI:n osa-aluejaottelut olivat osaltaan samoja, mutta erosivat sen verran suuresti, että niiden yhteensovittamisen tapaa piti pohtia tarkemmin. Sen lisäksi kohde yrityksellä käytössä olevat käytännön toivat myös omat haasteensa jaottelun suunnitteluun.

Tietoturvakartoitusta varten päädyttiin myös selvittämään kaikki yritystä koskevat tietoturvaan liittyvät lainsäädännöt. Tietoturvan suunnittelussa huomioon otettavia lakeja kertyikin yllättävän paljon. Yllättävimpänä asiana nousivat esiin henkilötietolain vaatimukset henkilörekistereistä esimerkiksi se, että Windowsin käyttäjien hallintaan tarkoitettu Active Directory on henkilörekisteri ja vaatii henkilörekisteriselosteen.

Tietoturvakartoitus toteutettiin kahdella henkilöstölle lähetetyllä kyselyllä ja joidenkin avainhenkilöiden haastatteluilla. Lähteistä kyselyn kysymyksiä kerätessäni huomasin, että osa niissä mainituista asioista oli epäoleellisia yrityksen toiminnan kannalta. Lähteistä kerätyt kysymykset on siis syytä käydä mahdollisimman aikaisessa vaiheessa läpi, jotta vain yrityksen kannalta oleelliset kysymykset muokataan tietoturvakartoitukseen sopiviksi.

Kyselyiden ja haastatteluiden perusteella saadut tulokset kerättiin omiin dokumentteihinsa, jotka ovat liitteissä 2-3 ja 5. Tulosten arkaluonteisuudesta johtuen niitä ei ole julkaistu tässä dokumentissa.

Työn alussa asetin tavoitteeksi sen, että tietoturvakartoitusta varten tehdyt selvitykset voitaisiin suoraan käyttää hyödyksi tietoturvakäsikirjaa kehitettäessä. Koen onnistuneeni tässä tehtävässä hyvin, sillä työstä ja siinä mainituista muista lähteistä saa kerättyä tarpeellisen tiedon käsikirjan kirjoittamista varten. Henkilökohtaiset tavoitteeni koen myös saavuttaneeni, sillä teoriaosiota työstäessäni olen tutustunut hyvin laajalti tietoturvan eri alueisiin ja niihin liittyviin muihin materiaaleihin. Olen myös ottanut tietoturvanäkökulman huomioon yrityksen IT-järjestelmiä muokatessani ja luodessani sekä tiedottanut kollegoitani erilaisista tietoturvaan liittyvistä uutisista ja artikkeleista yrityksen sisäisiä tiedotuskanavia pitkin. Uskon, että saamaani tietoturvatietoutta ylläpitämällä kykenen huolehtimaan yrityksen tietoturvan ylläpidosta ja kehittämisestä.

Lähdeluettelo

Access control. 2002. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Access_control> Päivitetty 7.7.2013. Luettu 9.7.2013.

Campagna, Rich; Iyer, Subbu & Krishnan, Ashwin. 2011. *Mobile Device Security for Dummies.* Indiana, United States of America: Wiley Publishing Inc.

Evwaraye, Ari. 2012. *Kansallinen turvallisuusauditointikriteeristö KATAKRI - Kohti versiota III.* Verkkodokumentti. Sisäasiainministeriö. <http://www.cert.fi/attachments/cipseminaarit/cip_2012/6BsghQGlx/Evwaraye.pdf> 28. lokakuuta 2012. Luettu 1.8.2013.

Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004. 2004. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/88078_fi.pdf> 23. kesäkuuta 2004. Luettu 19.8.2013.

Hakala, Mika; Vainio, Mika & Vuorinen, Olli. 2006. *Tietoturvallisuuden käsikirja.* Porvoo: Docendo.

Henkilöstön tietoturvaohje, VAHTI 10/2006. 2006. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061127Henkil/Vahti_10_06.pdf> 27. marraskuuta 2006. Luettu 9.7.2013.

Henkilötietojen luovutus yhteistyökumppanille suoramarkkinointia varten. 2004. Verkkodokumentti. Tietosuojavaltuutetun toimisto. <http://www.tietosuoja.fi/48523.htm> Luettu 20.7.2013.

Henkilötietolaki (523/1999). 1999. Päivitetty 17.5.2011.

Higgins, Parker. *Why Two-Factor?* 2013. Verkkodokumentti. Gizmodo. <http://gizmodo.com/how-to-enable-two-factor-authentication-on-all-your-acc-510245714> 29. toukokuuta 2013. Luettu 8.7.2013.

ICT-varautumisen vaatimukset, VAHTI 2/2012. 2012. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/076_ict/20120925ICTvar/vahti_2_2012_NETTI_PDF.pdf> 25. syyskuuta 2012. Luettu 1.8.2013.

Information security. 2001. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Information_security> Päivitetty 4.3.2013. Luettu 6.3.2013.

ISO/IEC 27000-series. 2007. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/ISO/IEC_27000-series> Päivitetty 15.7.2013. Luettu 1.8.2013.

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

ISO/IEC 27001:2013. 2013. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/ISO/IEC_27001:2013> Päivitetty 26.7.2013. Luettu 21.7.2013.

Johdon tietoturvaopas, VAHTI 2/2011. 2011. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20111207Johdon/Johdon_tietoturvaopas.pdf> 7. joulukuuta 2011. Luettu 1.8.2013.

Järvinen, Petteri. 2012. *Arjen tietoturva - vinkit & ratkaisut.* Jyväskylä: Docendo.

Kansallinen turvallisuusauditointikriteeristö (KATAKRI). 2011. Verkkodokumentti. Puolustusministeriö. <http://www.defmin.fi/hallinnonala/puolustushallinnon_turvallisuustoiminta/kansallinen_turvallisuusauditointikriteeristo_(katakri)> Luettu 31.7.2013.

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II. 2009. Verkkodokumentti. Puolustusministeriö. <http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf> Päivitetty 2011. Luettu 9.7.2013.

Kohdistetut hyökkäykset, VAHTI 6/2009. 2009. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20091117Kohdis/kohdistetut_hyoekkaeykset_netti_kannet.pdf> 17. marraskuuta 2009. Luettu 19.8.2013.

Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006. 2006. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinno

n_tietoturvallisuus/20061122Kaeyttoe/vahti_9_06.pdf> 22. marraskuuta 2006. Luettu 19.8.2013.

Laakso, Matti. 2013. *Ohjelmistoturvallisuus.* Verkkodokumentti. <http://www.tietojesiturvaksi.fi/content/ohjelmistoturvallisuus> Luettu 27.8.2013.

Laaksonen, Mika; Nevasalo, Terho & Tomula, Karri. 2006. *Yrityksen tietoturvakäsikirja - Ohjeistus, toteutus ja lainsäädäntö.* Helsinki: Edita Publishing Oy.

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004). 2004. Päivitetty 1.1.2012.

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003). 2003. Päivitetty 1.12.2010.

Laki tietoyhteiskunnan palvelujen tarjoamisesta (458/2002). 2002. Päivitetty 1.1.2013.

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (619/2009). 2009. Päivitetty 1.1.2013.

Laki viranomaisten toiminnan julkisuudesta (621/1999). 1999. Päivitetty 1.5.2013.

Laki yksityisyyden suojasta työelämässä (759/2004). 2004. Päivitetty 1.6.2009.

Lokiohje, VAHTI 3/2009. 2009. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20090511Lokioh/Vahti_3_NETTI.pdf> 11. toukokuuta 2009. Luettu 1.8.2013.

McCullagh, Adrian & Caelli, William. 2000. *Non-repudiation in the digital environment.* First Monday, Volume 5, Number 8 - 7 (August). Verkkodokumentti. <http://journals.uic.edu/ojs/index.php/fm/article/view/778/687> Luettu 9.7.2013.

Mikä urkintalaki? 2009. Verkkodokumentti. Urkintalaki.fi. <http://urkintalaki.fi/mikaurkintalaki.html> Päivitetty 12.3.2009. Luettu 26.8.2013.

Multi-factor authentication. 2009. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Multi-factor_authentication> Päivitetty 3.7.2013. Luettu 8.7.2013.

Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi, VAHTI 7/2006. 2006. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060724Muutos/Vahti_7_06.pdf> 24. heinäkuuta 2006. Luettu 19.8.2013.

Nummi, Kirsi. 2011. *Tietoturvallisuuden hallinnan suunnittelu ja toteutus - Projektiopas valtionhallinnon organisaation tietoturvallisuudesta vastaavalle.* Järvenpää. Verkkodokumentti. <http://www.tietoturvatalkoot.fi/Projektiopas.pdf> Luettu 21.8.2013.

Rikoslaki (39/1889). 1891. Päivitetty 1.8.2013.

Sisäverkko-ohje, VAHTI 3/2010. 2010. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101203Sisaeve/Sisaeverkko-ohje.pdf> 3. joulukuuta 2010. Luettu 1.8.2013.

Sosiaalisen median tietoturvaohje, VAHTI 4/2010. 2010. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101222Sosiaa/Sosiaalinen_media.pdf> 22. joulukuuta 2010. Luettu 19.8.2013.

Suomen perustuslaki (731/1999). 1999. Päivitetty 1.3.2012.

Sähköisen viestinnän tietosuojalaki (516/2004). 2004. Päivitetty 1.6.2013.

Teknisen ICT-ympäristön tietoturvataso-ohje, VAHTI 3/2012. 2012. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20121122Teknis/ICT_taitto.pdf> 22. marraskuuta 2012. Luettu 1.8.2013.

Tietosuoja. 2010. Verkkodokumentti. Suomi.fi. <http://www.suomi.fi/suomifi/suomi/asioi_verkossa/tietosuoja/> 8. lokakuuta 2010. Luettu 9.7.2013.

Tietoturva. 2004. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/Tietoturva> Päivitetty 4.3.2013. Luettu 7.3.2013.

Tietoturvakartoituksen kysymyslista. 2006. Verkkodokumentti. Viestintävirasto. <http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tietoturvakartoitus_kysymyslista.pdf> 30. tammikuuta 2006. Luettu 20.2.2013.

Tietoturvakouluttajan opas, VAHTI 11/2006. 2006. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinno

n_tietoturvallisuus/20061128Tietot/Vahti_11_06.pdf> 28. marraskuuta 2006. Luettu 1.8.2013.

Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006. 2006. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060802Tietot/A_vahti_08_netti.pdf> 2. elokuuta 2006. Luettu 19.8.2013.

Tietoturvallisuus. 2013. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp> Luettu 1.8.2013.

Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005. 2005. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20050101Tietot/95673.pdf> 1. tammikuuta 2005. Luettu 16.8.2013.

Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006. 2006. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060720Tietot/Vahti_6_06.pdf> 20. heinäkuuta 2006. Luettu 19.8.2013.

Thomas, Chris. 2013 *The Advantages of Two Factor Authentication.* Verkkodokumentti. eHow. <http://www.ehow.com/list_6682961_advantages-two-factor-authentication.html> Luettu 8.7.2013.

Toimitilojen tietoturvaohje, VAHTI 2/2013. 2013. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20130530Toimit/Toimitilojen_tietoturvaohje_VAHTI_2_2013_netti.pdf> 30. toukokuuta 2013. Luettu 1.8.2013.

Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008. 2008. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20080218Taereki/Vahti2_08low.pdf> 18. helmikuuta 2008. Luettu 1.8.2013.

Vahva sähköinen tunnistaminen, sähköinen allekirjoitus ja varmenne. 2013. Verkkodokumentti. Viestintävirasto. <https://www.viestintavirasto.fi/tietoturva/sahkoinentunnistaminenjaallekirjoitus.html> 29. toukokuuta 2013. Luettu 30.7.2013.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010). 2010.

Valtion ICT-hankintojen tietoturvaohje, VAHTI 3/2011. 2011. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20111207Valtio/Valtion_ICT-hankintojen_tietoturvaohje.pdf> 7. joulukuuta 2011. Luettu 9.7.2013.

Valtionhallinnon salauskäytäntöjen tietoturvaohje, VAHTI 3/2008. 2008. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20080307Valtio/Vahti_3-2008_netti.pdf> 7. maaliskuu 2008. Luettu 19.8.2013.

Valtionhallinnon sähköpostien käsittelyohje, VAHTI 2/2005. 2005. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/94935_fi.pdf> 24. toukokuuta 2005. Luettu 19.8.2013.

Viestintämarkkinalaki (393/2003). 2003. Päivitetty 25. heinäkuuta 2007.

Voimassa olevat tietoturvaohjeet ja -määräykset. 2013. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp> Luettu 5.8.2013.

Älypuhelimien tietoturvallisuus - hyvät käytännöt, VAHTI 2/2007. 2007. Verkkodokumentti. Valtiovarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071120Aelypuh/A_vahti_2_07.pdf> 20. marraskuuta 2007. Luettu 1.8.2013.

Taulukko 1. Voimassa olevat VAHTI-ohjeistukset, jotka liittyvät yrityksen tietoturvaan. [Voimassa olevat tietoturvaohjeet ja -määräykset 2013]

Ohjeistus	**Sisältö**
Haittaohjelmilta suojautumisen yleisohje, 3/2004	Haittaohjelmat, suojattavat kohteet, haittaohjelmien torjuntaprosessi, tartunnan välttäminen, toiminnan kehittäminen ja koulutus.
Henkilöstön tietoturvaohje, VAHTI 10/2006	Asianhallinta ja tietojenkäsittely, työskentely työpaikalla, etätyö ja matkatyö sekä ongelmatilanteet.
ICT-varautumisen vaatimukset, VAHTI 2/2012	Palveluiden jatkuvuus ja riskien hallinta.
Johdon tietoturvaopas, VAHTI 2/2011	Riskienhallinta, tietoturvallisuuden johtaminen, organisointi ja suunnittelu, poikkeama- ja erityistilanteiden hallinta sekä raportointi.
Kohdistetut hyökkäykset, VAHTI 6/2009	Kohdistettujen hyökkäysten tekotavat, hyökkäyksiin varautuminen ja niiden havaitseminen sekä niiltä suojautuminen.
Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006	Käyttöoikeuksien hallinta, määrittely, hallintaympäristö, käyttäjien tunnistaminen ja pääsynvalvonta.
Lokiohje, VAHTI 3/2009	Lokien käsittelyn periaatteet, erilaiset lokityypit, vastuut lokien käsittelyssä, lokien keräys ja säilytys.
Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi, VAHTI 7/2006	Muutoksen johtaminen, ulkoistaminen, prosessien kehittäminen sekä tietoturva näissä tilanteissa, ulkoistuksen elinkaari.
Sisäverkko-ohje, VAHTI 3/2010	Sisäverkon tietoliikennemallit, tasot ja rakenne, laitteet ja riskien hallinta.
Sosiaalisen median tietoturvaohje, VAHTI 4/2010	Tietoturvariskit ja tietoturvallisuuden toteuttaminen palveluita käytettäessä sekä tarjottaessa.
Teknisen ICT-ympäristön tietoturvataso-ohje, VAHTI 3/2012	Suojattavien kohteiden määrittely ja tärkeysluokitus, tietoturvavaatimukset laitteistolle ja esimerkkejä teknisistä ratkaisuista.
Tietoturvakouluttajan opas, VAHTI 11/2006	Koulutus ja oppiminen, koulutussuunnittelu ja materiaalit, koulutustilaisuuden suunnittelu ja toteutus.
Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006	Tietoturva-arvioinnin periaatteet, arvioinnin alueet, suorittaminen, tulosten analysointi ja raportointi. Liitteissä esimerkkejä arvioinnissa käytettäviä lomakkeita.
Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005	Tietoturvapoikkeamiin varautuminen, reagointi poikkeamatilanteissa ja toipuminen niistä.
Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006	Tietoturvallisuuden sisällyttäminen hallinnon tulosohjaukseen, tietoturvariskien hallinta sekä tietoturvallisuuden arviointi, mittaaminen ja mittarit.
Toimitilojen tietoturvaohje, VAHTI 2/2013	Turvallisuusvyöhykkeet, rakenteelliset turvallisuusvaatimukset, turvallisuusvalvonta, toimeenpano ja ohjeistaminen.

Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008	Henkilöstöturvallisuus ja henkilöstöön liittyvä riskien hallinta, esimerkiksi tehtävien eriyttäminen, sijaisuudet, valtuuttaminen, ostopalvelut ja pääsyn hallinta.
Valtionhallinnon salauskäytäntöjen tietoturvaohje, VAHTI 3/2008	Salauskäytäntöjen tekniset suositukset, käyttötarpeet, käyttöönottoprosessi ja ratkaisun elinkaari.
Valtionhallinnon sähköpostien käsittelyohje, 2/2005	Suosituksia sähköpostien käsittelyohjeiksi. Liitteissä ohjeet suodatukselle ja käsittelysäännöille.
Valtion ICT-hankintojen tietoturvaohje, VAHTI 3/2011	Toimittajaan kohdistuvat tietoturvavaatimukset ICT-hankintojen osalta. Ohjeistuksessa käytetään KATAKRI:ssa määriteltyjä tietoturvatasoja.
Älypuhelimien tietoturvallisuus - hyvät käytännöt, VAHTI 2/2007	Elinkaarenhallinta, Pushmail-ratkaisut, tietoturva ja etähallinta.