LAUREA - AMMATTIKORKEAKOULU

Sähköisen viestinnän tietosuoja

Virtanen, Lassi

2009 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Sähköisen viestinnän tietosuoja

Lassi Virtanen
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu 2009

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Lassi Virtanen

Sähköisen viestinnän tietosuoja

Vuosi 2009 Sivumäärä 33

Tietosuoja ja tietoturva nousevat esille uudesta näkökulmasta, kun käyttöympäristöt ja palvelut siirtyvät verkkoon. Tiedonkeruun määrä moninkertaistuu Internetin avulla. Tietosuojan ja -turvan kuherruskuukausi on nyt viimeistään ohi. Opinnäytetyössä havainnollistetaan tietosuojan tarkoitusta sekä käyttäjän omien toimien vaikutusta tietosuojaan. Työssä vastataan kysymyksiin: Mitä on tietosuoja? Mitä tietosuoja käyttäjältä vaatii?

Työssä käsitellään tietosuojaa yksittäisen käyttäjän näkökulmasta. Työ pohjautuu tietosuojasta asetettuun lainsäädäntöön: Perustuslakiin, Sähköisen viestinnän tietosuojalakiin, Henkilötietolakiin sekä Lakiin yksityisyyden suojasta työelämässä. Lainsäädäntöä havainnollistamaan on työhön kerätty määritelmiä ja tilastoja. Lisäksi työssä on käytännön osio tietosuojaa koskevista uhista sekä tavoista suojautua näiltä uhilta. Työssä käsitellään myös muutamia mediassa esille nousseita aiheita opinnäytetyön prosessin ajalta.

Tutkimuksen tavoitteena oli laaja raportti yksityisen käyttäjän tietosuojasta. Sitä käsitellään sekä lainsäädännön että käytännön tilanteiden näkökulmasta. Lisäksi tutkimuksen tuloksena syntyi käytännön ohjeistus sähköpostin, yhteisöpalveluiden sekä verkkokaupan käyttöön.

Tietosuoja ei ole vain palveluntarjoajien harteilla. Tietosuojauhat ovat päivittäisiä. Ne kohdistuvat yhä enemmän suoraan loppukäyttäjään. Tämä siirtää vastuuta järjestelmän ylläpidolta myös yksittäiselle käyttäjälle. Jotta tulevaisuuden uhkia vastaan pystytään taistelemaan, vaatii se kansainvälistä yhteistyötä sekä lisää koulutusta loppukäyttäjille.

Asiasanat: Sähköinen viestintä, Tietosuoja, Tietoturva, Sähköisen viestinnän tietosuojalaki, Henkilötietolaki, Tietoturvauhka

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Information Technology Programme

Lassi Virtanen

Privacy protection in electronic communication

Year 2009 Pages 33

Internet increases the use of new services, such as electronic commerce and e-mail, and hence, the access to all types of personal data. Information security and privacy protection are becoming more and more important. This research explains you what privacy protection means and what has to be done in order to protect privacy in electronic communication. This research answers the following questions: What is privacy protection? What does the user have to do for privacy protection?

This analysis explains what privacy protection means from the view of point of the end user. The research is based on Finnish legislation of privacy protection: the Finnish Constitution, Law of privacy protection in electronic environment, Law of personal data and Law of privacy in working life. In addition to this there are definitions and statistics to support the study. This research also analyses today's threats and how to protect oneself from them. In the media section there are articles from the period of processing of the analysis.

The purpose of this research was to create a thorough report about the user's privacy protection. It is carried out by analysing the legislation and by some real-life examples. In addition, there is a guideline for the safe use of e-mail, electronic commerce and social network services.

Privacy protection is not only something managed by service providers. Privacy protection threats have become everyday business and they concentrate more and more on end users. This shifts the responsibility from the service providers to end users. In order to respond to the future threats there is need for international co-operation and better education to the end users.

Key words: Electronic communication, Privacy protection, Information security, Law of privacy protection in electronic communication, Law of personal data, Information security threat

SISÄLLYS

1 Johdanto

Tietosuoja on jäänyt selvästi sisällöntuotannon kehityksen jalkoihin käyttöympäristön verkottuessa yhä enenevässä määrin. Kuten Web-tietoturva 2008 -seminaarissa luennoinut kansainvälisesti tunnettu tietoturvatutkija Petko D. Petkov asiaa havainnollisti: ”informaatiorikollisuus on jo tuottoisampaa kuin huumerikollisuus” (Petkov 2008). Kuinka moni tiedostaa, mihin kaikki palveluihin täytetyt tiedot menevät ja ketkä kaikki niitä tietoja pääsevät näkemään?

Opinnäytetyöni vastaa kysymyksiin ”Mitä on tietosuoja?” sekä ”Mitä tietosuoja käyttäjältä vaatii?” Käsittelen työssäni yritysten sekä järjestelmäkehityksen sijaan yksittäisen henkilön tietosuojaa sähköisessä ympäristössä tiedon tallentamisen, käytön sekä siirtämisen vaatimusten selvittämiseksi. Työni ei rajaa tietosuojaa käytettävän järjestelmän tai sisällön mukaan vaan puuttuu puhtaasti tietosuojan kannalta tiedon tallentamiseen sekä käyttöön. Vuonna 2006 Esa Suoanttila käsitteli opinnäytetyössään tietosuojaa yrityksen sekä järjestelmäkehityksen näkökulmasta.

Aiheeni on tutkimisen arvoinen ja ajankohtainen keväällä 2009. Sähköisen viestinnän tietosuojalakia uudistettiin maaliskuussa. Uudella muutoksella yhteisötilaajalle annettiin entistä laajemmat tiedonkäsittelyoikeudet. Mitä tämä kaikki tarkoittaa käyttäjän tietosuojan näkökulmasta?

Opinnäytetyössäni pyrin havainnollistamaan lukijalle tietosuojan perusteita ja heikkoja kohtia sekä opastan, miten näitä kohtia voidaan ehkäistä jo etukäteen.

2 Määritelmät

2.1 Tietosuoja

Jokaisen suomalaisen yksityisyys on lailla turvattu. Kuitenkin tietosuojakysymykset nousevat esille yhä useammin. Mitä tietosuoja käytännössä tarkoittaa? Jaettaessa yhdyssana kahtia saadaan sanat tieto ja suoja. Jokaisella yksilöllä on erilaisia yksityisiä ja yksilöllisiä tietoja. Tavallisimmin kaikilta löytyvät esimerkiksi nimi, osoite, puhelinnumero sekä sosiaaliturvatunnus. Lisäksi löytyy lukematon määrä eri palveluiden tunnuksia ja salasanoja, sähköpostiosoitteita sekä pankkitilitietoja. Suuri osa kaikista henkilöön liittyvistä asioista eivät ole salaisia, mutta tietojen yhdistely ja aiheeton kerääminen aiheuttaa uhan yksilön yksityisyydelle ja tietosuojalle.

Tietosuojalla tarkoitetaan yksilön tietojen käytön rajoittamista niin, että yksilön tietojen leviämiselle olisi mahdollisimman pieni uhka. Ongelmalliseksi tämän tekee verkottuvassa maailmassa kuitenkin se, että tietokoneen ruudulla moni tieto tuntuu muuttuvan käyttäjän silmissä abstraktiksi. Yksittäinen palvelu saa kerätä käyttöönsä tarvittavat tiedot käyttäjän yksilöimisen ja esimerkiksi laskutuksen takia. Tietojen huoleton jakaminen erilaisten palveluiden kautta asettaakin tietosuojan koetukselle. Täten on käyttäjä itse suurin uhka omalle yksityisyydelleen. (Järvinen 2002, 30-34.)

2.1.1 Ongelmat

Yksilön tietosuoja nousee esille päivittäin. Esimerkiksi maksu- tai kanta-asiakaskorttien käyttö, matkapuhelimen käyttö, julkisilla paikoilla liikkuminen tai sähköpostin käyttäminen ovat jokainen vaarantamaan tietosuojaa. Jokainen yksittäinen tiedonkeruu aiheuttaa samalla uhan tietosuojalle. Jokaisessa ei välttämättä ole riskejä, mutta digitaalisena aikakautena tietoa kerätään paljon.

Nykypäivänä suurimman uhan muodostaa kuitenkin Internet. Se on kuin suuri valvomaton basaari. Kaikki Internetissä kulkeva tieto on monien muiden nähtävillä. Kaikki, mitä Internetiin laitetaan, myös jää sinne. Aiemmin hauskalta tuntunut Internetiin laitettu kuva tai mielipidekirjoitus saattaa myöhemmässä vaiheessa olla kirjoittajaa vastaan, esimerkiksi työnhakutilanteessa. Itseään Googlesta etsimällä saattaa löytyä paljon sellaista tietoa, minkä luuli jo olleen kadonnutta. (Järvinen 2002, 30; Pfleeger 2007, 626.)

Erilaisia palveluita käytettäessä on suhtauduttava kriittisesti palvelun tarjoamaan tietosuojaan. Vaikka kaikkia omia tietoja ei löytyisikään yhdestä paikasta, on yksilön tietoja helppo koota eri palveluiden kautta. Oman yksityisyytensä voi menettää vain kerran. Tämän

vuoksi palvelun käytössä ja omien tietojen luovuttamisessa kannattaa olla ennemmin yli- kuin alivarovainen. (Järvinen 2002, 47.)

2.2 Tietoturva

Tietosuojan edellytyksenä on oikein mitoitettu tietoturva. Tietosuojasta puhuttaessa tietoturvaa voidaan harvemmin ylikorostaa. Tietoturvaa voidaan verrata oman kodin lukittuun ulko-oveen. Niin pitkään kuin ovi on kiinni ja lukossa, ovat myös kodin tavarat turvassa. Jos ovi tai ikkuna jää auki, on turvallisuus vaarassa. On kuitenkin hyvä muistaa se, että vaikka tietoturvallisuus vaarantuisi ei se automaattisesti tarkoita sitä, että jotain pahaa tapahtuisi.

Tietoturva voidaan määritellä kolmen perusperiaatteen kautta: tiedon luottamuksellisuus, eheys sekä saatavuus. Mikäli nämä asiat ovat kunnossa, voidaan puhua onnistuneesta tietoturvasta. Käsittelen seuraavissa luvuissa tarkemmin tietoturvan osia. (Järvinen 2002, 22.)

2.2.1 Luottamuksellisuus

Tiedon luottamuksellisuudella pyritään siihen, että tietoa voivat lukea ja muokata vain siihen oikeutetut henkilöt. Käytännössä tämä tarkoittaa sitä, että tiedon käyttäjät on tunnistettava ja todennettava ennen käyttöä. Lisäksi tieto on suojattava niin, että tunnistamattomat käyttäjät eivät sitä voi käsitellä. (Järvinen 2002, 22.)

2.2.2 Eheys

Tiedon eheys tarkoittaa sitä, että tieto pysyy muuttumattomana viestiketjun alusta loppuun. Eheyttä voi vaarantaa esimerkiksi kovalevyn hajoaminen, tiedon muuttuminen siirrettäessä tai viruksen tekemät muutokset tallennettuun tietoon. (Järvinen 2002, 22-23.)

Eheys voidaan varmistaa esimerkiksi erilaisilla tarkistussummilla, tiedon salaamisella, lokitiedostojen seurannalla, erilaisilla tiedonsiirtoprotokollilla tai virustentorjuntaohjelmistoilla. (Järvinen 2002, 22-23.)

2.2.3 Saatavuus

Tiedon saatavuudella pyritään siihen, että tieto on saatavilla silloin kun tietoa halutaan käyttää. Verkossa tarjottavissa palveluissa tämä tarkoittaa yleensä ympäri vuorokauden tarjolla olevaa tietoa. Työelämässä tarjottavissa palveluissa tämä tarkoittaa yleisesti sitä, että tieto on käytettävissä työaikana. (Järvinen 2002, 24.)

Uhkia tiedon saatavuudelle aiheuttaa esimerkiksi palvelunestohyökkäys järjestelmää vastaan, alimitoitettu järjestelmä, verkkoyhteyksien tai sähkön katkeaminen tai yhteensopimattomat järjestelmät ja mediat. (Järvinen 2002, 24.)

2.2.4 Muut osa-alueet

Muita tärkeitä osa-alueita tietoturvassa ovat tunnistaminen ja todentaminen, pääsynvalvonta sekä kiistämättömyys.

Perinteisen tavan mukaan käyttäjä tunnistetaan käyttäjätunnuksen avulla ja todennetaan siihen liitetyn henkilökohtaisen salasanan avulla. Todennettava kohde voi käyttäjän lisäksi olla myös laite, verkosta löytyvä tieto tai kokonainen verkkopalvelu. Tunnistamisen riskejä on useita. Tunnistamme esimerkiksi sähköpostin lähettäjän usein vain lähettäjän osoitteen perusteella. Lähettäjän osoite on kuitenkin erittäin helppo väärentää. Tunnistamme verkkopalvelun osoitteen tai sivulta löytyvän tutun logon perusteella. Myös nämä ovat erittäin helppoja väärentää. Molemmissa tapauksissa ainoa keino luotettavaan todentamiseen on digitaalinen allekirjoitus tai varmenne. Todentaminen voidaan hoitaa kolmella eri tavalla: yksilöllisten ominaisuuksien perusteella, esineen, esimerkiksi avaimen perusteella, tai yksilöllisen tiedon, esimerkiksi salasanan perusteella. (Järvinen 2002, 24-27.)

Todentamisen jälkeen tulee palvelussa huolehtia pääsynvalvonnasta. Pääsynvalvonnalla varmistetaan se, että vain tietoon oikeutetut todennetut käyttäjät pääsevät tietoa käyttämään. Pääsynvalvontaan liittyy olennaisena osana myös seuranta, jolla pyritään ongelmatapauksissa todentamaan tietoa käyttäneet tahot. (Järvinen 2002, 27.)

Viimeisenä kohtana tietoturvassa on mainittava teon kiistämättömyys. Tätä tarvitaan erityisesti sähköisessä kaupankäynnissä, jossa on kiistatta pystyttävä todistamaan tilauksen tekeminen, vastaanottaminen sekä lähettäminen. (Järvinen 2002, 27-28.)

2.2.5 Ongelmat

Mikä tietoturvan toteuttamisesta tekee niin vaikean, vaikka sen määritteleminen on niin yksinkertaista? Yksittäisen käyttäjän kohdalla suurin ongelma lienee siinä, että mukavuuden ja tietoturvan suhde on vakio. Mikäli salasana on pidempi ja monimutkaisempi on se vaikeampi muistaa. Toisaalta se on samalla turvallisempi. Mikäli verkon yli tapahtuvaa liikennettä halutaan seurata ja suodattaa, hidastaa se liikennettä ja tekee käytöstä monimutkaisempaa ja kalliimpaa. Toisaalta tällöin tietoturva paranee, sillä haittaohjelmat ja ulkopuoliset käyttäjät eivät pääse palveluun käsiksi. (Järvinen 2002, 43-44.)

Vaikka järjestelmät olisivat täydellisesti suojattuja voi yksittäinen käyttäjä vaarantaa tietoturvan esimerkiksi liian heikolla salasanallaan. Nykyään myös social engineering ja phishing hyökkäävät suoraan käyttäjään, jolloin käyttäjästä itsestään tulee huonon tietoturvakoulutuksen tai -ymmärryksen puitteissa järjestelmän suurin tietoturvauhka. (Järvinen 2002, 44.)

Viimeisenä lienee tarvittavaa mainita, että ainoa täysin tietoturvallinen ratkaisu on jättää laite kauppaan ja palvelu käyttämättä. Muuten on altistuttava sille mahdollisuudelle, että tietoturvauhka on olemassa. (Järvinen 2002, 44.)

3 Tilastot

Tilastokeskuksen mukaan 83 prosenttia 16-74-vuotiaista suomalaisista käyttää Internetiä. Alle 40-vuotiaista Internetiä käyttää lähes kaikki. Yli 60-vuotiaista Internetiä käyttää kuitenkin vain noin 40 prosenttia väestöstä. Internetin käyttö on kuitenkin kasvanut suhteellisesti eniten juuri yli 60-vuotiaiden joukossa. Seuraavaksi tarkastellaan tarkemmin mihin ja missä Internetiä käytettiin vuonna 2008. (Tilastokeskus 2008 a.)

3.1 Internetin käyttötarkoitukset

Noin 90 prosenttia suomalaisista käyttää sähköpostia. Alle 30-vuotiaista sähköpostia käyttää 95 prosenttia väestöstä. Seuraavaksi suurimpana Internetin käyttötarkoituksena on tiedonhaku tavaroista ja palveluista. Tätä on tehnyt 88 prosenttia suomalaisista. Kuitenkin vain 33 prosenttia on tehnyt ostoksia verkkokaupasta. Verkkokaupasta ostaminen on kuitenkin noussut tasaisesti vuoden 2004 vertailuajasta, jolloin verkkokaupassa oli asioinut vain 20 prosenttia väestöstä. (Tilastokeskus 2008 a.)

Vuodesta 2004 vuoteen 2008 suurimman nousun käyttäjämäärissä on kuitenkin tehnyt pankkiasiointi. Vuonna 2004 pankissa asioi Internetin kautta 50 prosenttia väestöstä. Vuonna 2008 jo 72 prosenttia koko väestöstä käytti verkkopankkia. Muina tärkeinä nousijoina voidaan mainita blogien lukeminen, joka on noussut vuoden 2006 15 prosentista vuoden 2008 38 prosenttiin. Lisäksi matka- ja majoituspalveluita selailee jo 70 prosenttia väestöstä. (Tilastokeskus 2008 a.)

Voidaan siis todeta, että Internetin käyttötarkoitus on laajentunut pelkästä tiedonhankinnasta, myös erilaisten palveluiden ja tavaroiden tilaamiseen sekä päivittäisasioiden, kuten pankkiasioiden hoitamiseen. Lisäksi blogien lukijoiden kasvu kertoo siitä, että käyttäjät etsivät nykyään enemmän suoraan tietoa ja kokemuksia palveluista muilta käyttäjiltä. Näiden syiden takia onkin tietosuojasta huolehtiminen yhä tärkeämpää.

3.2 Internetin käyttöpaikat

Suurin osa (n. 75 prosenttia) käyttää Internetiä kotona. Toiseksi yleisin käyttöpaikka on työpaikka, jossa Internetiä käyttää noin 45 prosenttia väestöstä. Seuraavaksi suurimpina käyttöpaikkoina ovat tilaston mukaan ”Jonkun muun luona” 30 prosentin osuudellaan sekä oppilaitos vajaan 20 prosentin osuudellaan. (Tilastokeskus 2008 b.)

Kirjasto, langaton julkinen yhteys, Internet-kahvila, julkisen tilan tarjoama yhteys sekä yhdistyksen ja yhteisön tarjoamat käyttöpaikat ovat kaikki alle 10 prosentin osuudellaan joukon viimeisinä. Juuri nämä ovat tulevaisuudessa niitä käyttöpaikkoja, joiden käyttö tulee kasvamaan monipuolisempien mobiililaitteiden ansiosta ja joissa tietosuojakysymykset nousevat esille. (Tilastokeskus 2008 b.)

3.3 Tietosuojatapaukset

Rikoslain 38 luku määrittelee rangaistukset tieto- ja viestintärikoksista. Suomessa näistä rikoksista tuomittuja on vuosittain edelleen vähän. Luku on jopa laskemaan päin, sillä vuonna 2005 oikeudessa tuomittiin 39 vastaajaa eri rangaistuksiin, kun vuonna 2007 luku oli vain 24. Tuomiot ovat olleet ehdottoman vankeuden ja päiväsakkojen väliltä. Käytännössä tapauksia on niin vähän, ettei tuomion keskiarvoa ole oleellista määrittää. (Tilastokeskus 2009.)

Useimmin vuonna 2007 tuomiot ovat tulleet 38:9§:n henkilörekisteririkoksesta (12 tuomiota). Lisäksi seitsemän tuomioita on annettu 38:3§1 viestintäsalaisuuden loukkauksesta, kaksi 38:5§1 tietoliikenteen häirinnästä, yksi 38:7a§1 tietojärjestelmän häirinnästä, yksi 38:8§1-2 tietomurrosta sekä yksi 38:8§3 tietomurron yrityksestä. (Tilastokeskus 2009.)

Tilastot eivät kerro tapauksista, jotka eivät ole saapuneet viranomaisten tietoon asti. Kuten Petteri Järvinen kolumnissaan toteaa: ”On mahdollista, että varsinkin pk-yrityksissä lakia on rikottu puhtaasta tietämättömyydestä” (Järvinen 2009). Näitä tapauksia lähes varmasti on, mutta tuskin kukaan osaa kertoa tarkkaa lukua.

4 Ajantasainen lainsäädäntö

Tietosuojaa sekä yksityisyyden suojaa on säädeltävä. Sähköisen tietosuojan sekä yksityisyyden suojan säätelyn perustan luo laki. Euroopan alueella sähköistä tietosuojaa koskevia lakeja on myös pyritty yhtenäistämään EY:n direktiivien avulla.

Suomen lainsäädännössä sähköisen viestinnän tietosuojaa sekä yksityiselämän suojaa säädetään neljän eri lain avulla: Perustuslaki, Sähköisen viestinnän tietosuojalaki, Henkilötietolaki

sekä Laki yksityisyyden suojasta työelämässä. Tässä luvussa käydään läpi nämä neljä lakia niiltä osin, kun on yksityisen sähköisen asioinnin kannalta tarpeellista.

4.1 Suomen perustuslaki (1999/731)

Suomen perustuslakiin on kirjattu jokaisen yksityiselämä, kotirauha sekä kunnia turvatuksi. Lisäksi laissa on mainittu, että ”Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton”. (10 § 1-2mom.)

4.2 Sähköisen viestinnän tietosuojalaki (2004/516)

Sähköisen viestinnän tietosuojalaki on tullut voimaan 1.9.2004. Lailla korvattiin aikaisempi 22.4.1999 voimaan tullut laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta. Lisäksi lailla korvattiin aikaisempi asetus Viestintäviraston maksuista 2002/1126. Sähköisen viestinnän tietosuojalain perustana käytetään EY:n direktiiviä: Sähköisen viestinnän tietosuojadirektiivi 2002/58/EY. (44 §.)

Sähköisen viestinnän tietosuojalaki luo perustan sähköisen viestinnän tietosuojaan: ”Lain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisen sähköisen viestinnän palvelujen tasapainoista kehittymistä” (1 §).

Lakia sovelletaan Internetissä tarjottaviin palveluihin. Lakia ei sovelleta rajattuihin verkkoihin, joita ei ole liitetty Internetiin. Lakia ei myöskään sovelleta verkossa välitettävään viestiin, jossa yksittäisessä tapauksessa viestiä ei voida yhdistää tunnistetietojen avulla vastaanottajaan. Lakia ei myöskään sovelleta viranomaiskäyttöön tarkoitetuissa verkoissa. (3 §.)

4.2.1 Yksityisyyden ja luottamuksellisuuden suoja

Viesti ja sen tunnistamis- sekä paikkatiedot ovat luottamuksellisia. Tämä koskee myös ”verkkosivujen selaamisesta kertyviä tunnistamistietoja” (4 §). Myös ”yleisesti vastaanotettavaksi” (4 §) tarkoitetun viestin tunnistamistiedot ovat luottamuksellisia. (4 §.)

Käyttäjällä on oikeus omien tunnistamistietojensa suojaamiseen ”haluamallaan tavalla” (6 §), mikäli muussa laissa ei toisin ole säädetty. Tämän suojauksen purkavan tai kiertävän järjestelmän tai laitteen valmistus, myynti, käyttö sekä hallussapito on kielletty, mikäli järjestelmää käytetään ensisijaisesti ”oikeudettomaan purkamiseen” (6 §). Verkkopalvelun käyttöä kuvaavien tietojen, cookien tallentaminen on sallittua, mikäli palveluntarjoaja kertoo etukäteen mihin tietoja käytetään. Mikäli tietoja käytetään palvelun toteuttamiseen eikä lisäpalveluun on niiden käyttö sallittua myös ilman käyttäjän erillistä hyväksyntää. Käyttö on kuitenkin

sallittua vain palvelun vaatimassa laajuudessa, eikä yksityisyyden suojaa saa rajoittaa tarpeettomasti. (6 §; 7 §.)

4.2.2 Viestin, ja tunnistamis- ja paikkatietojen käsittely

Viestiä ja sen tunnistamistietoja saa käsitellä vain ”käsittelyn tarkoituksen vaatimassa laajuudessa” (8 §). Tunnistamistietoja saa käsitellä ”verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun toteuttamiseksi ja käyttämiseksi sekä näiden tietoturvasta huolehtimiseksi” (9 §). Viestin lähettäjä tai vastaanottaja voi käsitellä tietoja rajauksitta. (8 §; 9 §.)

Teleyritys, palveluntarjoaja tai yhteisötilaaja voi käyttää tunnistamistietoja markkinoinnissa, mikäli siihen on saatu tilaajalta lupa. Lisäksi tunnistamistietoja voidaan käyttää palvelun teknistä kehittämistä varten tai väärinkäytöstapauksissa. Tunnistamistietojen käsittelijän on ilmoitettava tilaajalle mitä tunnistamistietoja käytetään ja kuinka pitkään niiden käsittely kestää. Tunnistamistietojen käsittelijä on velvoitettu säilyttämään viranomaistarpeita varten 12 kuukauden ajan tunnistamistiedot puheluista, Internet-yhteyspalvelusta, sähköpostista sekä Internet-puheluista. Säilytysvelvollisuus ei koske viestin sisältöä eikä verkkosivujen selaamisesta saatavia tunnistetietoja. (10 §; 11 §; 12 §; 13 §; 14 §; 14a §.)

Teleyritys voi käsitellä paikkatietoja lisäpalvelun tarjoamiseksi, mikäli tilaaja ei ole sitä erikseen kieltänyt. Tilaajalla pitää olla helppo ja ilmainen tapa kieltää paikkatietojensa käyttö. Tilaajalle on myös kerrottava paikkatietojen tarkkuus, käsittelyn tarkoitus sekä se voidaanko tietoja luovuttaa kolmannelle osapuolelle. Paikkatietoihin perustuvaan lisäpalveluun on aina pyydettävä erillinen suostumus tilaajalta. Suostuminen pitää olla mahdollista peruuttaa helposti ja ilman maksua. (17 §; 18 §.)

4.2.3 Viestinnän tietoturva

Palveluntarjoajalla on velvollisuus huolehtia tarjoamansa palvelun tietoturvasta. Tämä kattaa toiminnan turvallisuudesta, tietoliikenneturvallisuudesta, laitteisto- ja ohjelmistoturvallisuudesta sekä tietoaineistoturvallisuudesta huolehtimisen. Palveluntarjoajat vastaavat myös palvelun toteuttamisessa olevan mahdollisen kolmannen osapuolen tietoturvasta. (19 §.)

Palveluntarjoajan on oikeus puuttua tietoturvan varmistamiseksi sähköiseen viestintään kolmella eri tavalla: Estämällä viestien välittäminen, poistamalla viesteistä haitallinen sisältö sekä toteuttamalla näihin verrattavissa olevat tekniset toimenpiteet. Näihin toimenpiteisiin saa kuitenkin ryhtyä vain, jos ne ovat välttämättömiä tietoturvan kannalta. ”Toimenpiteet on toteutettava huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen” (20 §). Toimenpiteet on lopetettava heti, kun niille ei ole enää tarvetta. (20 §.)

Palveluntarjoajan on ilmoitettava Viestintävirastolle tietämistään tietoturvaloukkauksista, uhista sekä toimenpiteistä, joilla nämä voidaan estää. 21 §:n mukaan tietoturvaloukkauksen tai uhan jälkeen on palveluntarjoajan ”tiedotettava tarkoituksenmukaisella tavalla toteuttamistaan toimista ja niiden mahdollisista vaikutuksista palvelun käyttöön”. (21 §.)

4.2.4 Ohjaus ja valvonta

Sähköisen viestinnän tietosuojalain ohjausta, kehittämistä ja toteutumista valvoo liikenne- ja viestintämisteriö sekä tietosuojavaltuutettu. Näillä tahoilla on oikeus saada tapauksen kannalta tarpeellisia viestinnän tunnistamis- ja paikkatietoja, jos on syytä epäillä rikoslaissa määriteltyjä tietosuojarikkomuksia. (30 §; 33 §.)

Hätäkeskus, meripelastuskeskus, meripelastuslohkokeskus sekä poliisi ovat oikeutettuja saamaan hätäilmoituksen tekijän tai kohteen tunnistamis- ja paikkatietoja. (35 §.)

Tämän lain noudattamatta jättämisestä ”on tuomittava sähköisen viestinnän tietosuojarikkomuksesta sakkoon, jollei teosta muualla laissa säädetä ankarampaa rangaistusta. Rangaistusta ei tuomita, mikäli rikkomus on vähäinen” (42 §).

4.2.5 Tulevat muutokset

Maaliskuussa 2009 hyväksyttiin sähköisen viestinnän tietosuojalakiin paljon kiistelty muutos yhteisötilaajan oikeuksiin. Muutos astuu voimaan 1.6.2009. Muutoksella yhteisötilaajalle annettiin entistä laajemmat oikeudet tiedon käsittelemiseen. Tiedon käsittely on kuitenkin rajattu väärinkäytöstapauksiin sekä väärinkäytöstapausten ehkäisyyn. Yksittäiselle käyttäjälle tämä ei mielestäni tuo heikennystä nykyiseen tietosuojaan ja turvaan, korkeitaan parannusta, sillä lakiin on päivitetty pykälä tietoturvan toteuttamisesta. (Hallituksen esitys 48/2008.)

4.3 Henkilötietolaki (1999/523)

Uusi henkilötietolaki on tullut voimaan 1.6.1999. Lailla kumottiin aikaisempi henkilörekisterilaki 1987/471. (50 §.)

Henkilötietolain ”tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista” (1 §). Lakia sovelletaan henkilötietojen käsittelyyn Suomen alueella. Laki ei koske henkilökohtaisiin tarkoituksiin tehtävää eikä ulkomailla tehtävää henkilötietojen käsittelyä. (4 §.)

4.3.1 Henkilötietojen käsittely

Rekisterinpitäjä on velvoitettu huolellisuuteen ja hyvään tietojenkäsittelytapaan henkilötietojen käsittelyssä. Lisäksi on huolehdittava, ettei rekisteröidyn yksityistiedot vaarannu, eikä yksityisyyden suojan oikeuksia rajoiteta tarpeettomasti. (5 §.)

”Henkilötietojen käsittelyn tulee olla asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta. Henkilötietojen käsittelyn tarkoitukset sekä se, mistä henkilötiedot säännönmukaisesti hankitaan ja mihin niitä säännönmukaisesti luovutetaan, on määriteltävä ennen henkilötietojen keräämistä tai muodostamista henkilörekisteriksi” (6 §).

Henkilötietojen käsittely perustuu rekisteröidyn hyväksyntään käsitellä tietoja. Lisäksi henkilötietoja voidaan kerätä rekisteriin mm. asiakassuhteen, työsuhteen tai muusta laista johtuvan velvoitteen takia. Lain 8 §:n mukaan tietoja rekisteristä saa luovuttaa ”vain, jos henkilötiedon luovuttaminen kuuluu tavanomaisena osana kysymyksessä olevan toiminnan harjoittamiseen edellyttäen, että tarkoitus, johon tiedot luovutetaan, ei ole yhteensopimaton henkilötietojen käsittelyn tarkoituksen kanssa ja että rekisteröidyn voidaan olettaa tietävän henkilötietojen tällaisesta luovuttamisesta”. (8 §.)

Käsiteltävien henkilötietojen tulee olla käsittelyn kannalta tarpeellisia ja rekisterinpitäjän tulee pitää huoli siitä, että tiedot ovat rekisterissä oikein. Henkilörekisterissä käsiteltävistä tiedoista tulee olla rekisteriseloste jokaisen saatavilla. (9 §.)

4.3.2 Arkaluonteiset tiedot

Arkaluontoisten tietojen käsittely ilman asianomaisen lupaa on kielletty. Arkaluontoisina tietoina pidetään muun muassa etnistä alkuperää, yhteiskunnallista vakaumusta, rikollista tekoa tai siitä saatua rangaistusta, terveydentilaa, seksuaalista suuntautumista sekä henkilön sosiaalihuollon tarvetta. Näitä tietoja saa käsitellä, mikäli henkilö on antanut siihen suostumuksen tai henkilö on itse saattanut asian julkiseksi. Laissa on lisäksi määritelty pykälässä 12 muutamia muita poikkeuksia arkaluontoisten tietojen käsittelyyn. (11 §; 12 §.)

Henkilötunnusta saa käsitellä rekisteröidyn suostumuksella, lain vaatimuksesta tai mikäli rekisteröidyn yksiselitteinen yksilöiminen on tärkeää. ”Rekisterinpitäjän on huolehdittava siitä, että henkilötunnusta ei merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin” (13 §). Mikäli henkilötunnus rekisteristä löytyy, on sen käsittelyssä oltava erityisen huolellinen ja tarkka. (13 §.)

4.3.3 Rekisteröidyn oikeudet

”Rekisterinpitäjän on henkilötietoja kerätessään huolehdittava siitä, että rekisteröity voi saada tiedon rekisterinpitäjästä ja tarvittaessa tämän edustajasta, henkilötietojen käsittelyn tarkoituksesta sekä siitä, mihin tietoja säännönmukaisesti luovutetaan, samoin kuin ne tiedot, jotka ovat tarpeen rekisteröidyn oikeuksien käyttämiseksi asianomaisessa henkilötietojen käsittelyssä” (24 §).

Jokaisella on oikeus saada tietää, mitä tietoja hänestä on rekisteriin talletettu. Lisäksi jokaisella on oikeus pyytää tietojensa korjaamista tai poistamista rekisteristä. Tietojen poisto onnistuu markkinointirekistereistä sekä henkilömatrikkeleista ja sukututkimusta varten kerätyistä rekistereistä. Tietojen korjausta tai poistoa on pyydettävä aina kirjallisesti, johon rekisterinpitäjän on kieltäytyessään vastattava myös kirjallisesti. (26 §; 29 §; 30 §.)

4.3.4 Ohjaus ja valvonta

Henkilötietojen käsittelyä ohjaa ja valvoo tietosuojavaltuutettu, tietosuojalautakunta sekä muut tietosuojaviranomaiset. Tietosuojaviranomaiset toimivat yhdessä muiden Euroopan Unionin jäsenvaltioiden tietosuojaviranomaisten kanssa. Tietosuojalautakunta voi kieltää määräysten vastaisen henkilötietojen käsittelyn tai määrätä rekisteritoiminnan lopetettavaksi. (38 §; 44 §.)

Rekisterinpitäjä on velvoitettu korvaamaan rekisteröidylle tai muulle henkilölle lainvastaisesta rekisteristä aiheutuneet taloudelliset tai muut vahingot. Tahallisesta tai huolimattomasta toiminnasta vaarantaa yksityisyyttä tai yksityisen oikeuksia voidaan tuomita sakkorangaistukseen. (47 §; 48 §.)

4.4 Laki yksityisyyden suojasta työelämässä (2004/759)

Laki yksityisyyden suojasta työelämässä on tullut voimaan 1.10.2004. Lailla kumottiin aikaisempi laki yksityisyyden suojasta työelämässä 477/2001. Lain tarkoituksena on turvata yksityisyyden suojaa sekä sitä turvaavia perusoikeuksia työelämässä. (1 §; 25 §; 26 §.)

4.4.1 Henkilötietojen käsittely

Työnantaja saa käsitellä vain tehtävän kannalta tarpeellisia henkilötietoja. Tiedot voivat 3 §:n mukaan liittyä ”työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työtehtävien erityisluonteesta”. (3 §.)

Työnantaja voi kerätä henkilötietoja muualta kuin työntekijältä itseltään, mutta tällöin työntekijältä on saatava suostumus tietojen keräämiseen. Suostumus ei ole tarpeellista viranomaisilta tai henkilöluottotiedoista saaduista tiedoista. Mikäli työntekijän luotettavuuden selvittämiseksi etsitään tietoa muualta kuin työntekijältä itseltään, on työntekijälle ilmoitettava tiedoista ennen niiden käyttöä työntekijää koskevassa päätöksenteossa. (4 §.)

Työntekijän terveystietoja saavat käsitellä vain niiden pohjalta päätöksiä tai toimeenpanoja tekevät henkilöt. Työnantajalla on oikeus saada työntekijän luottotietoja, mikäli työntekijän tehtävät edellyttävät erityistä luotettavuutta. Lisäksi työtehtävien pitää olla käytännössä myös sellaisia, joissa pääsee käsiksi esimerkiksi omaisuuteen, käyttöoikeustietoihin tai työtehtävässä on ”merkittäviä taloudellisia sitoumuksia” (5 a §). Henkilötietojen hankinnan kustannukset maksaa työnantaja. (5 §; 5 a §.)

4.4.2 Sähköpostin käsittely

Työnantajan on huolehdittava työntekijän sähköpostin käytön perusedellytykset: sähköpostin edelleenlähettäminen, lomavastaaja sekä mahdollisuus ohjata työntekijän viestit hänen poissa ollessaan työnantajan hyväksymälle toiselle henkilölle. (18 §.)

Näiden toimenpiteiden jälkeen työnantajalla on oikeus hakea viestin tunnistetietoja selvittääkseen, onko työntekijä vastaanottanut työnantajalle kuuluvia viestejä työntekijän poissa ollessa. Tämä on mahdollista vain, mikäli se on yritystoiminnan kannalta välttämätöntä; asiantilaa ei saada muuten selville; työtehtävästä johtuen on ilmeistä, että työntekijä on vastaanottanut työnantajalle kuuluvia viestejä; työntekijä on tilapäisesti estynyt työtehtäviensä suorittamisesta tai työntekijältä ei voida kohtuullisessa ajassa saada suostumusta. Näissäkin tapauksissa tunnistetietojen käsittely on sallittu vain työnantajalle välttämättömissä viesteissä. (19 §.)

Mikäli viestin tunnistetietojen perusteella on selvää, että viesti on työnantajalle kuuluva ja se on työtehtävien kannalta välttämätön, eikä lähettäjältä tai vastaanottajalta saada selvyyttä viestin sisällöstä, saa työnantaja avata viestin. (20 §.)

Mikäli viestin tunnistetietoja tai itse viestiä avataan, on siitä tehtävä työntekijälle allekirjoitettu kirjallinen selvitys, josta käy ilmi miksi tietoja on käsitelty, kuka tietoja on käsitellyt sekä koska tietoja on käsitelty. Lisäksi viestin avaamisen yhteydessä selvitykseen on kirjattava kenelle tieto avatusta viestistä on annettu. Selvitys on toimitettava ilman aiheetonta viivästystä työntekijälle. (19 §; 20 §.)

4.4.3 Yhteistoimintamenettely

Työntekijöihin kohdistuvasta teknisestä valvonnasta on sovittava yhdessä työntekijöiden kanssa yhteistoimintamenettelyn kautta. Yhteistoimintamenettelyn jälkeen työnantajan on määriteltävä valvonnan tarkoitus ja menetelmät sekä 21 §:n mukaan ”tiedotettava työntekijöille valvonnan tarkoituksesta, käyttöönotosta ja siinä käytettävistä menetelmistä sekä sähköpostin ja tietoverkon käytöstä”. (21 §.)

4.5 Ongelmakohdat

Tietosuojan kannalta lainsäädännöstä voidaan nostaa esille kaksi ongelmakohtaa: Lainsäädännön maantieteelliset rajat sekä lainsäädännön tulkittavuus. Tarkastelen molempia seuraavaksi vielä hieman tarkemmin.

4.5.1 Lain maantieteellinen rajoittuneisuus

Suomen lainsäädännöllä turvataan tietosuoja vain Suomen alueella toimivilla palveluilla. Suurin osa yleisessä viestintäverkossa, Internetissä, tarjottavista palveluista sijaitsee kuitenkin fyysisesti Suomen rajojen ulkopuolella. Näihin palveluihin lakia ei voida soveltaa. Lisäksi ulkomailla sijaitsevaa palvelua joudutaan käyttämään yleisen viestintäverkon kautta usean eri maan kautta. Tällöin palvelua käytettäessä joudutaan miettimään myös jokaisen kauttakulkumaan lainsäädäntöä. Tämä nostaa esille tietosuojan kannalta oleellisen kohdan: käsiteltävän tiedon on oltava mahdollisimman lähellä käyttäjää. Tätä ongelmaa on pyritty ratkaisemaan EU:n sisällä yhtenäistämällä lainsäädäntöä.

4.5.2 Lain tulkittavuus

Toisen ongelman muodostaa lainsäädännön tulkittavuus. Uusia verkkopalveluita kehitetään nopeasti. Nykyisellä tavallaan lainsäädäntö ei pysy kehityksen mukana. Kun lainsäädäntöä pyritään kehittämään nykypäivän tasolle, tulee säädäntöön helposti hyväksyttyä sellaisia kohtia ja termejä, joita pystytään tulkitsemaan eri lailla.

Otetaan esimerkkinä paljon keskustelua herättänyt Sähköisen viestinnän tietosuojalaissa käytetty termi yhteisötilaaja. Se on määritelty koskemaan yritystä tai yhteisöä, mutta tarkempaa rajausta yhteisölle ei ole tehty. Termi on kuitenkin erittäin ratkaisevassa osassa tunnistamistietojen käsittelyn osalta. Hallituksen esitys 48/2008 sähköisen viestinnän tietosuojalain uudistamisesta koski yhteisötilaajan oikeuksien laajentamista. Perustuslakivaliokunnan puheenjohtaja Kimmo Sasi puuttui eduskunnan täysistunnossa 13/2009 yhteisötilaajan termiin kysymällä ”Kertokaa minulle yksikin taloyhtiö, joka on yhteisötilaaja” (PTK 13/2009 vp). Kuitenkin Kielitoimiston sanakirja sanoo, että yhteisön voi käytännössä muodostaa vaikka kaksi ihmistä. (2004/516, 2 §; PTK 13/2009 vp.)

Olisiko tässä nyt uskottava Kotimaisten kielten tutkimuskeskusta vai Perustuslakivaliokunnan puheenjohtajaa ja kansanedustajaa? Miten lakia voidaan soveltaa ja tulkita, mikäli ei edes tiedetä ketä se koskee?

5 Tietoturvauhat ja niihin varautuminen

Edellä on käsitelty tietosuojaa ja sen vaatimaa tietoturvaa yleisellä tasolla. Lisäksi on käsitelty lainsäädäntöä. Ne eivät kuitenkaan kerro sitä, mitkä ovat tällä hetkellä todellisia uhkia yksityisyydelle ja tietoturvalle. Asiaa lähestytään tässä kappaleessa eri tahojen tietoturvaraporttien kautta. Samalla katsotaan, miten Suomi on suunnitellut varautuvansa uhkia vastaan tulevaisuudessa.

5.1 CERT-FI

CERT-FI:n käsittelemien tapausten määrä vuonna 2008 oli yli 3500. Vuonna 2007 tapauksia oli yli 2600 ja vuonna 2006 alle 1500. Vuoden 2008 suurimpina uhkina pidettiin laajoja Internetin infrastruktuuria koskevia haavoittuvuuksia, haitallisen sisällön levittämistä sekä www-palvelimien sisällön muokkausta palvelinohjelmistojen haavoittuvuuksien kautta. (CERT-FI 2008, 1-8.)

Raportissaan CERT-FI nostaa esille myös sähköisen viestinnän luottamuksellisuuden. Erityistä huolta on herättänyt se, että Ruotsin puolustusvoimien signaalitiedustelu on saanut luvan tarkkailla kiinteässä verkossa kulkevaa tietoliikennettä vuoden 2009 alusta alkaen. Tämä koskee suomalaisia, sillä suurin osa suomalaisten ulkomaan Internet-liikenteestä kulkee Ruotsin kautta. Juuri tämänlaiset ulkomaiset säädökset uhkaavat suomalaisten tietosuojaa ulkomaisia verkkopalveluita käytettäessä. (CERT-FI 2008, 3.)

Tulevaisuuden uhista raportissa mainitaan etähallittavien ja päivitettävien haittaohjelmien levittäminen tietokoneisiin. Haittaohjelmien kehittyessä yhä monikäyttöisemmiksi nousevat ne myös suuremmaksi uhaksi tietosuojan ja tietoturvan kannalta. CERT-FI:n mukaan haittaohjelmien erilaiset levitystavat tulevat edelleen kehittymään. Lisäksi murretuilla WWW-sivuilla sekä roskapostilla tulee olemaan edelleen merkittävä rooli uhkien joukossa. (CERT-FI 2008, 8.)

5.2 F-Secure

Suomalaisen tietoturvayhtiö F-Securen mukaan vuoden 2008 ensimmäisen puoliskon suurena ongelmana olivat Internetin kautta leviävät haittaohjelmat, sekä niiden määrän kasvun kiih-

tyminen. Vanhoista haittaohjelmista tehtiin uusia variaatioita. Lisäksi raportissa mainitaan, että haittaohjelmia käytettiin kohdennettuihin hyökkäyksiin. Näissä tapauksissa haittaohjelmat levitettiin sähköpostin välityksellä. Niiltä tapauksilta suojautuminen vaatii teknisen suojautumisen lisäksi käyttäjältä tietoa ja valppautta sekä yritykseltä vahvaa tietoturvakulttuuria. (F-Secure 2008.)

Muiksi uhiksi raportissa mainittiin muun muassa kolmannen osapuolen sovellukset kuten Adoben Flash sekä mobiililaitteisiin kohdistuvat tietoturvauhat. Hyvänä kehityksenä pidettiin Internet-selainten kehitystä, sillä niiden uudet päivitetyt versiot aiheuttavat vaikeuksia verkon kautta leviäville haittaohjelmille. (F-Secure 2008.)

5.3 Symantec

Kansainvälisen tietoturvayhtiö Symantecin mukaan vuonna 2008 tietoturvauhissa näkyivät monimutkaisemmat ja hienostuneemmat hyökkäykset. Avoimista suorista hyökkäyksistä on siirrytty epäsuoriin hyökkäyksiin HTTP- ja P2P-kanavien kautta. Näillä hyökkääjät pyrkivät välttelemään kiinnijäämistään pidempään. Uhissa painottui tarkoitus hyötyä loppukäyttäjistä taloudellisesti. Tästä syystä hyökkääjät ovat jatkaneet erilaisten verkkohuijausten kehittämistä. (Symantec 2009, 11-12.)

Toiset rikollisryhmät ovat hävinneet. Toiset isommat organisaatiot ovat pystyneet jatkamaan toimintaansa. Nämä valeyritykset ja niiden tulevat kilpailijat tulevat todennäköisesti olemaan tulevaisuuden tietoturvauhkien takana. Hyökkääjien ja hyökkäystapojen kehittyessä nousee yhä suurempi tarve kansainväliselle yhteistyölle valtioiden, yritysten sekä muiden organisaatioiden välille. (Symantec 2009, 11-12.)

5.4 Kansallinen tietoturvastrategia

Liikenne- ja viestintäministeriö julkaisi joulukuussa 2008 periaatepäätöksen kansallisesta tietoturvastrategiasta teemalla ”Turvallinen arki tietoyhteiskunnassa - Ei tuurilla vaan taidolla” (Liikenne- ja viestintäministeriö 2008, 1). Strategialla pyritään siihen, että ”kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen sekä tieto- ja viestintäverkoissa että niihin liittyvissä palveluissa” (Liikenne- ja viestintäministeriö 2008, 1). Strategian tavoitteena on, että vuonna 2015 Suomi on tietoturvan edelläkävijämaa. (Liikenne- ja viestintäministeriö 2008, 1.)

Tietoturvastrategian kolme painopistettä ovat: Perustaidot arjen tietoyhteiskunnassa, Tietoihin liittyvien riskien hallinta ja toimintavarmuus sekä Kilpailukyky ja kansainvälinen verkostoyhteistyö. Katsotaan alla hieman tarkemmin mitä toimenpiteitä eri painopisteissä on. (Liikenne- ja Viestintäministeriö 2008, 1.)

5.4.1 Perustaidot arjen tietoyhteiskunnassa

Tietoturva on palveluiden tuottajien lisäksi myös käyttäjien toimista kiinni. Ensimmäisessä painopisteessä pyritään lisäämään käyttäjien tietoa ja osaamista. Näitä pyritään vahvistamaan kolmella eri tavalla: kehittämällä kansallista tietoturva-hanketta, seuraamalla tietoisuuden tasoa ja kehittämällä tietoturvaosaamista sekä laatimalla aktiivinen ja ennakoiva viestintäsuunnitelma. (Liikenne- ja viestintäministeriö 2008, 1-2.)

Palveluntarjoajan tulisi varmistaa tarjoamansa palvelun turvallisuus sekä käyttämiensä tietojen luottamuksellisuus. Strategiassa huomautetaan, ettei palveluntarjoaja voi ulkoistaa vastuutaan. Tämä tarkoittaa sitä, että tietoturvanäkökohdat tulee ottaa huomioon myös järjestelmähankinnoissa ja sopimusprosesseissa. Turvallisen sähköisen palvelun pohja on kiteytetty strategiassa neljään kohtaan: lisätään tietoturvavaatimukset osaksi tarjouspyyntöjä, edistetään tietoturvaratkaisujen käyttöä, selvitetään mahdollisuutta kehittää turvallisille palveluille myönnettävää sertifikaattia sekä lisätään sertifioitujen tietoturva-ammattilaisten määrää. (Liikenne- ja viestintäministeriö 2008, 1-2.)

5.4.2 Tietoihin liittyvien riskien hallinta ja toimintavarmuus

Toisessa painopisteessä keskitytään palvelun toimintavarmuuteen sekä palvelun käytön riskien hallintaan. Strategiassa linjataan, että palvelun käytön tulee olla turvallista ja luottamuksellista. Lisäksi käyttäjille on taattava riittävä viranomaistuki, mikäli tietoturvaa on loukattu. Palveluiden ulkoistustilanteessa tulee varmistaa palvelun tietoturva koko palveluketjun osalta. Tästä kantaa vastuun aina palvelun tarjoaja, ei ulkoistuskumppani. (Liikenne- ja viestintäministeriö 2008, 2.)

Palveluiden tietoturvan ohella myös palvelun toiminta ja yritysten toiminnan jatkuvuus on varmistettava. Strategiassa on mainittu, että ”kriittisen infrastruktuurin toimivuus ja tieto- ja viestintäjärjestelmien sekä viestintäpalveluiden turvallisuus tulee varmistaa kaikissa tilanteissa - normaalioloista poikkeusoloihin asti” (Liikenne- ja viestintäministeriö 2008, 2). Kriittisen infrastruktuurin ulkopuolisissa palveluissa ja yrityksissä pyritään tukemaan erilaisten riskienhallintamallien käyttöä ja koulutusta. Lisäksi selvitetään erilaisia varautumismalleja verkkojen ja verkostojen hallintaan. (Liikenne- ja viestintäministeriö 2008, 2-3.)

5.4.3 Kilpailukyky ja kansainvälinen verkostoyhteistyö

Viimeisessä painopisteessä keskitytään kansainvälisyyteen. Yritysten kansainvälistä toimintaa EU-alueella pyritään helpottamaan yhtenäisten EU-direktiivien kautta. Yhtenäiset säädökset eri valtioiden kanssa mahdollistavat yritysten helpomman liikkumisen. Yritysten kilpailukykyi-

syys on turvattava myös tietosuojan kannalta. Näillä toimilla pyritään turvaamaan yritysten toimintaa Suomessa sekä suomalaisten yritysten toiminta ulkomailla. Lisäksi pyritään lisäämään Suomen houkuttelevuutta ulkomaisten yritysten sijoittautumiskohteena. (Liikenne- ja viestintäministeriö 2008, 3.)

Tietoturvauhat eivät ole vain Suomen ongelma. Suomi on osa globaalia tietoverkkotaloutta. Suurin osa tietoturvauhkista tuleekin maamme rajojen ulkopuolelta. Tämän takia Suomen on lisättävä kansainvälistä yhteistyötä uhkien torjumisessa. Jotta Suomi voi toimia kansainvälisesti on sen pystyttävä priorisoimaan kansainvälistä toimintaa ja keskittyä tietoturvan kannalta olennaisiin kohteisiin. Tähän strategiassa pyritään puuttumaan selvittämällä mahdollisuutta perustaa suomeen kansallinen tietoturvallisuus-viranomainen. (Liikenne- ja viestintäministeriö 2008, 3-4.)

6 Tietosuoja käytännössä

Lauseella ”Internet on ehkä suurin uhka yksityisyydelle” alkaa tietosuoja Internetissä -kappale kirjassa Security in Computing. Olemme ehkä havainneet lukiessamme tätä työtä saman asian. Mitä nämä uhat käytännössä ovat ja miten niihin voi varautua? Parhaiten pääsemme liikkeelle luomalla kuvitteellisen mallin tavallisesta päivästä. (Pfleeger 2007, 626.)

6.1 Esimerkkitapaus

Aloitamme päivämme kotona lukemalla omalta koneeltamme henkilökohtaisen sähköpostimme. Tämän jälkeen katsomme Internetistä julkisen liikenteen kulkuyhteyden työpaikalle. Töissä avaamme työkoneen, kirjaudumme yrityksen verkkoon ja aloitamme työt käyttämällä yrityksen tarjoamia laitteita ja palveluita. Töissä tauolla kirjaudumme yhteisöpalveluun ja lähetämme muutamia viestejä ystävillemme. Samalla saatamme lähettää muutaman yksityisen sähköpostin selaimen sähköpostiliittymän kautta. Kotona illalla saatamme vielä kirjautua verkkokauppaan tilataksemme lempikirjailijamme uutuusteoksen näppärästi postitse kotiin.

Kaikkea tätä tehdessä eivät tietosuojakysymykset välttämättä nouse esille. Miten tietosuoja voi muka vaarantua, kun kukaan muu ei ole seuraamassa tekemisiäni? Käydään esimerkkitapausta lävitse yksittäisten tapahtumien kautta.

6.2 Sähköpostin käyttö

Jotta sähköpostin luomat tietoturvauhat havainnollistuvat on hyvä hieman selventää, miten sähköposti toimii. Sähköpostilla on aina lähettäjä ja vastaanottaja. Koska sähköpostin lähettäjä ja vastaanottaja eivät välttämättä aina ole samaan aikaan paikalla, tarvitaan lähettäjälle

ja vastaanottajalle palvelun tarjoajan toteuttamat sähköpostilaatikot. Lisäksi tarvitaan vähintään yksi reititin lähettäjän ja vastaanottajan palvelun tarjoajien väliin, jotta sähköposti voidaan toimittaa. Näin jokaisen sähköpostin liikuttamiseen tarvitaan vähintään viisi eri tahoa. Jokainen näistä tahoista luo oman tietosuojariskin. (Pfleeger 2007, 635.)

Esimerkissä käytettiin sekä yksityistä, että yrityksen sähköpostia. Alla on mainittu yksittäisiä tekijöitä, joita on hyvä ottaa huomioon sähköpostin kanssa:

- Työsähköposti on tarkoitettu työkäyttöön. Henkilökohtaiseen viestintään tulee käyttää yksityistä sähköpostia (Valtiovarainministeriö 2006.)
- Internetin kautta ei ole luvallista välittää salassa pidettävää tietoa ilman asianmukaista salaamista (Valtiovarainministeriö 2006.)
- Käytä asianmukaista roskaposti- sekä virussuodatinta (Symantec 2009, 94.)
- Älä avaa liitteitä, ellet odota kyseistä liitettä tai tiedä sen tarkoitusta (Symantec 2009, 94.)
- Vältä sähköpostitse tulleiden tuntemattomien linkkien avaamista (Symantec 2009, 94.)

6.3 Sosiaaliset yhteisöpalvelut

Nykyään suureksi uhaksi tietosuojalle on Internetissä noussut yhteisöpalvelut. Näissä käyttäjät vaihtavat kuulumisiaan, kokemuksiaan sekä kuvia keskenään. Henkilöllisyysvarkauksissa juuri näiden palveluiden kautta saadut tiedot aiheuttavat suuren uhan.

Alla mainitut yksittäiset kohdat auttavat suojautumaan yhteisöpalveluiden uhkia vastaan:

- Käytä eri palveluissa eri tunnuksia sekä riittävän hyvää salasanaa (Pfleeger 2007,628.)
- Älä kerro henkilötietojasi turhaan, äläkä kirjoita niitä nettisivuille tai keskustelupalstoille (Järvinen 2002, 189.)
- Henkilötunnus ei ole valtionsalaisuus, mutta kerro se vain hyvät perustelut esittäneelle taholle (Järvinen 2002, 189.)
- Internetillä on norsun muisti. Harkitse ennen kuin kirjoitat tai lähetät viestin. (Järvinen 2002, 30.)

6.4 Verkkokauppa

Verkkokaupassa asiointi helpottaa monien elämää. Tuotteiden vertailu ominaisuuksien, hinnan ja käyttökokemuksien perusteella on helppoa. Kaupasta toiseen pääsee yhdellä painalluksella, ja maksu onnistuu helposti maksukortilla tai verkkopankkitunnuksilla. Mikä siinä muka voisi mennä pieleen?

Verkkokaupassa asioidessa on hyvä muistaa muutamia perusasioita tietosuojan ja onnistuneen kaupan edellytyksenä.

- Varmista kenen kanssa asioit. Huolehdi että löydät sivuilta kauppiaan yhteystiedot (TIEKE 2001.)
- Tarkista, että luottamuksellisten tietojen lähetys tapahtuu salattua yhteyttä käyttäen (TIEKE 2001.)
- Älä anna koskaan maksukorttisi tunnuslukua verkossa asioidessasi tai sähköpostitse (Viestintävirasto 2009.)
- Harkitse, mikäli tarjous on liian hyvä ollakseen totta (TIEKE 2001.)

Internetissä asioidessa on hyvä käyttää omaa harkintakykyään. On tiedostettava se, että kaikki eivät ole Internetissä liikkeellä rehellisin mielin. Mikäli joku kuulostaa liian hyvältä ollakseen totta, se myös todennäköisesti on. Internet palveluineen on kuitenkin tehty helpottamaan elämäämme. Älä jätä mahdollisuutta hyödyntämättä. Harkitse ja käytä järkeäsi. Muista, että Internetiin kerran laitettu tieto myös jää sinne.

7 Tietosuoja mediassa

Voidaan sanoa, että vuonna 2008 tietosuoja ja tietoturva käsitteinä nousivat uutiskynnyksen yli. Tapauksia on noussut esille käyttäjien kasvaneen tietotason ansiosta. Suurimpina syinä kuitenkin tähän ovat varmasti olleet tietosuojavaltuutettu Reijo Aarnio sekä Electronic Frontier Finland ry, jotka ovat useasti ottaneet kantaa tietosuojaa koskeviin kysymyksiin.

Tässä luvussa käsitellään edellä mainittujen tahojen lisäksi muutamia vuosina 2008 sekä 2009 mediassa esille nousseita tapauksia yksittäisten artikkeleiden kautta. Näistä saadaan kuvaa Internetin tuomista uhista, mutta toisaalta nähdään myös median tavat käsitellä erilaisia tietosuoja- ja tietoturvakysymyksiä.

7.1 Tietosuojavaltuutettu

Tietosuojavaltuutettuna Suomessa on toiminut marraskuusta 1997 lähtien Reijo Aarnio. Tietosuojavaltuutetun tehtävät on määritelty kahdessa eri laissa: henkilötietolaissa sekä laissa tietosuojalautakunnasta ja tietosuojavaltuutetusta. Tietosuojavaltuutetulla on seitsemän eri tehtävää: ohjaus ja neuvonta, ottaa kantaa tietosuojatapauksissa, ohjata käytännesääntöjen laadinnassa, valvoa ja tehdä tarkastuksia, antaa lausuntoja viranomaisille, tiedottaa sekä toimia kansainvälisessä yhteistyössä. (Tietosuojavaltuutetun toimisto 2009 a; Tietosuojavaltuutetun toimisto 2009 b.)

7.2 Electronic Frontier Finland ry

Electronic Frontier Finland on kansalaisten sähköisiä oikeuksia puolustava rekisteröity yhdistys. Yhdistyksen tavoitteena on herättää keskustelua ja pyrkiä vaikuttamaan lainsäädäntöhankkeisiin sananvapaudesta ja tekijänoikeuksista. Yhdistyksen periaatteita ovat yksityisyyden kunnioittaminen, roskapostin kieltäminen sekä avoimen ohjelmistokehityksen tukeminen. Yhdistys toimii yhteistyössä ulkomaisten järjestöjen kanssa joilla on samanlaiset tavoitteet ja arvot. (Electronic Frontier Finland ry 2009 a.)

Vuosina 2008 sekä 2009 yhdistys on näkynyt erityisesti mediassa sähköisen äänestyksen sekä Lex Nokiana tunnetun sähköisen viestinnän tietosuojalain uudistuksen vastustajana. (Electronic Frontier Finland ry 2009 b.)

7.3 Netti paljastaa elämäsi

Taloussanomien syyskuussa 2008 ilmestyneessä artikkelissa käsitellään yksilön tekojen vaikutuksia omaan tietosuojaansa. Artikkelissa korostetaan kuinka Internetistä tietoja etsimällä ja tietoja yhdistelemällä voi selvitä henkilön lähes koko elämä. Artikkeliin haastateltu tietosuojavaltuutettu Aarnio pitää ongelmaa erittäin suurena. Aarnio korostaa, että tietosuoja ei tarkoita automaationa tietojen suojaamista vaan sitä, että yksilöllä on oikeus omiin tietoihinsa. Artikkelissa Aarnio korostaa, että yksilö voi itse vaikuttaa omien tietojensa leviämiseen. Tietosuojaviranomaiset ovat auttamassa tietosuojaa koskevissa riitatapauksissa. Kuitenkin, jotta riitatapauksiin asti ei jouduttaisi, kehottaa Aarnio kriittisyyteen omien tietojensa antamisen kanssa. (Kokko 2008.)

Hyvänä esimerkkinä artikkelissa nostetaan suuren suosion saavuttanut Facebook. Käyttäjät kirjoittavat palveluun itsestään kaikenlaista ja yhtäkkiä huomaavat joutuneensa identiteettivarkauden uhriksi. Palveluntarjoaja ei ota tästä vastuuta, sillä käyttäjä on itse tiedot palveluun kirjoittanut. Artikkelissa korostetaan kuinka identiteettivarkaudet ovat maailmalla suuri ongelma. Aarnio toivoo, että varkauksien varalle saataisiin luotua järjestelmä ihmisten oikeusturvan parantamiseksi ennen kuin ongelma räjähtää käsiin. (Kokko 2008.)

Artikkeli toimii hyvänä esimerkkinä tietosuojavaltuutettu Aarnion toimenkuvasta. Asiaa lähestytään helposti ymmärrettävästi ja selkeästi. Artikkelissa kerrotaan tietosuojan nykytilasta ja nykytilaan ehdotetaan selvää parannusta. Näillä yksittäisillä ehdotuksilla saadaan median kautta myös tavalliset käyttäjät pohtimaan omaa tietosuojaansa.

7.4 Poliisista, päivää

Poliisiylijohtaja Mikko Paatero tarkasteli intimiteettisuojan asemaa poliisilehden blogissaan 2.10.2008. Kirjoituksessa käsiteltiin Kauhajoen syyskuisen ammuskelun tapahtumia. Kirjoituksessaan Paatero oli sitä mieltä, että tietosuojan olisi annettava tilaa yleiselle turvallisuudelle. Paatero kuitenkin tarkentaa, ettei tavoitteena olisi poliisivaltio. (Paatero 2008.)

Kirjoitus jättää avatun tietosuojan käsittelyn hieman vajaaksi. Tietosuojan keventämistä ehdotettiin, mutta todellista linjaa ei kuitenkaan mainittu. Kirjoituksesta jää avoimeksi se, mitä tietoja tulisi turvallisuuden nimissä kertoa ja kenelle niitä tietoja tulisi antaa.

7.5 Tietovarkauksia tehty satoja

Taloussanomat uutisoi elokuussa 2008 julkaistussa artikkelissaan Suomessa esiintyneistä tietovarkauksista. Artikkelin mukaan elokuuhun mennessä vuonna 2008 suomalaisilta oli varastettu tietoja yli kolmesataa kertaa. Varkaudet on tehty verkon kautta levinneiden haittaohjelmien avulla, jotka ovat keränneet käyttäjiltä henkilökohtaisia tietoja. Maailmalla tapausten lukumäärä lasketaan sadoissa tuhansissa. Artikkelissa kerrotaan, että jopa lyhytaikaisen haittaohjelmatartunnan aikana työasemalla olevat salaisuudet on ehditty siirtää suomalaisten viranomaisten ulottuviin. Nykyaikaiset haittaohjelmat ovat vaikeasti havaittavia ja ne ovat oppineet kaappaamaan jopa salattuja verkkopankki-istuntoja. (Sokala 2008.)

Artikkelissa puututaan nykypäivän arkiseen tietoturvaongelmaan. Kuten kappaleessa viisi mainitut tietoturvayhtiöt toteavat, ovat haittaohjelmat nykypäivän ja tulevaisuuden yksi suurimmista uhista. Näiden uhkien selättäminen vaatii myös palvelun käyttäjän osaamisen ja tietoisuuden kasvua.

7.6 Tietosuoja on luottamuksen varassa

Viimeisenä artikkelina on hyvä tutkia Petteri Järvisen maaliskuussa 2009 Talouselämässä julkaistua kolumnia tietosuojasta. Järvinen aloittaa kolumnin kritisoimalla median uutisointia sähköisen viestinnän tietosuojalain muutoksesta. Järvisen mukaan tiedotusvälineet suhtautuivat asiaan epäammattimaisesti. ”Tasapuolisen käsittelyn sijaan ne pelottelivat urkinnalla ja Nokian painostuksella, josta ainoaksi todisteeksi jäi lopulta yksittäinen, lauantaina keskiyöllä kirjoitettu sähköpostiviesti” (Järvinen 2009). Järvisen mukaan lain hyväksymisen jälkeen on kuitenkin ryhdyttävä töihin tietoturvan parantamiseksi lain edellytysten mukaan. Asiaa ei helpota se, että monilla työpaikoilla luottamus tietosuojaan ei ole kovin korkealla. Järvisen mukaan ”Yllättävän moni uskoi, että oma työnantaja rikkoo lakia ja lukee salaa sähköposteja”. (Järvinen 2009.)

Järvinen korostaa kolumnissaan, että uusi laki sallii vain sähköpostin tunnistetietojen käsittelyn. Hän kuitenkin paljastaa, että sähköpostiliikenteen tai palomuurilokien seuranta on helppoa. Lisäksi siitä ei jää juurikaan jälkiä. Järvinen sanoo, että tätä tosiasiaa ei uusi laki muuta. Lopuksi Järvinen siirtää vastuun yrityksille. Sisäinen luottamus on saatava tietojärjestelmien ohella kuntoon. (Järvinen 2009.)

Kolumnissaan Järvinen kiteyttää hyvin sen koko mediaryöpyn, minkä sähköisen viestinnän tietosuojalaki on saanut aikaiseksi. Korjataan väärät huhut ja kerrotaan miten asiassa tulee edetä. Kolumni saa varmasti lakimuutokseen ennen kielteisesti suhtautuneen pohtimaan asemaansa uudestaan. Ehkä tästä muutoksesta saadaan lisävoimaa yritysten tietoturva- ja tietosuojakulttuurin nykyaikaistamiseen sekä tätä kautta yksilön tietosuojan parantumiseen?

8 Yhteenveto

Työssäni käsittelin tietosuojaa kolmesta eri näkökulmasta: käsitteenä, lainsäädännön kannalta sekä käytännössä. Käsitteenä tietosuojalle ja tietoturvalle on annettu selvät periaatteet. Periaatteessa tämän ei siis tulisi olla vaikea asia. Lainsäädännössä tietosuojan ja tietoturvan periaatteita on pyritty jäsentämään ja toisaalta lainsäädännön kautta pyritään turvaamaan jokaisen oikeus yksityisyyteen.

Kuitenkin voimme huomata, että tietoturvauhat ovat päivittäisiä. Internet on nostanut tietosuojamme aivan uuteen vaaraan. Tietosuojaamme uhkaa verkossa erilaiset haittaohjelmat sekä eri tahojen verkontiedustelut. Toki tietosuojakysymykset nousevat päivittäin esille erilaisten asiakasrekistereiden ja vaikkapa matkapuhelimen tai sähköpostin käytön kautta. Internet ei ole siis ainoa uhka tietosuojallemme.

Internetin kautta tuleviin tietosuojauhkiin on kuitenkin käytännössä helppoa varautua. Valtio- ja organisaatiotasolla kansainvälisen yhteistyön kautta pystymme vastaamaan niihin haasteisiin, joita erilaiset uhat meille asettavat. Yksittäisen käyttäjän tasolla on mahdollista vaikuttaa omaan tietoturvaansa ja -suojaansa. Pitämällä laitteistonsa päivitettynä ja harkintakyvyn mukana päätöksissä voidaan suojautua suurimmalta osalta hyökkäyksistä ja uhista.

Kuten mediasta voimme havaita ovat tietosuojakysymykset nousseet uutiskynnyksen yli. Tämä on erittäin hyvä asia, sillä käyttäjien tulee havahtua, jotta erilaisiin tietosuojaa vaarantaviin tilanteisiin osattaisiin varautua. Vaikka tietosuoja tällä hetkellä olisikin monessa tilanteessa luottamuksen ja hyvän onnen varassa, ei sen tarvitsisi olla sitä enää tulevaisuudessa.

Tietosuojan kannalta olisi olennaista, että liikenne- ja viestintäministeriön julkaisema tietoturvastrategia nousee tulevaisuudessa tarpeeksi esille. Se, että Suomi olisi vuonna 2015 tieto-

turvan edelläkävijämaa, vaatii vielä paljon työtä. Oikeaan suuntaan ollaan joka tapauksessa menossa. Se ei kuitenkaan poista sitä asiaa, että myös tulevaisuudessa yksityisyytemme sekä tietosuojamme ovat vaarassa päivittäin.

Työni tavoitteena minulla oli tutustua tietosuojaan kattavasti useammasta eri näkökulmasta. Mielestäni onnistuin tässä hyvin sillä käsittelin tietosuojaa käsitteenä, lainsäädännön sekä käytännön kautta. Työ muodostaa selvän kokonaisuuden tietosuojaa koskevista asioista.

Kokonaisuudessaan opinnäytetyöprosessiin meni noin vuosi. En pidä sitä liian pitkänä aikana. Vuoden aikana aiheeni on muotoutunut sellaiseksi kuin se on nyt. Olen tutustunut laajalti aiheeseen sekä seurannut aiheen nykytilaa ja kehitystä. Lopputuloksena olen mielestäni saanut aikaan hyvän kokonaisuuden sähköisen viestinnän tietosuojasta.

Termistö

CERT-FI:n tehtävänä Suomessa on ”tietoturvaloukkausten ennaltaehkäisy, havainnointi ratkaisu sekä tietoturvauhkista tiedottaminen” (CERT-FI 2009 a).

Digitaalinen allekirjoitus on allekirjoitus, joka on sähköisessä muodossa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä. (Viestintävirasto 2007.)

Henkilörekisteri on käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuva henkilötietoja sisältävä tietojoukko, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla tai joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta. (1999/523, 3 §.)

Henkilötieto on kaikenlaista luonnollista henkilöä tai hänen ominaisuuksiaan tai elinolosuhteitaan kuvaava merkintä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. (1999/523, 3 §.)

HTTP on Internet-selaimien ja -palvelimien käyttämä protokolla tiedostojen, kuten tekstin ja kivien siirtämiseen. (Wendell 2008, 609.)

P2P on vertaisverkko. (Valtiovarainministeriö 2008.)

Paikkatieto on tietoa, joka ilmaisee liittymän tai päätelaitteen maantieteellisen sijainnin ja jota käytetään muuhun tarkoitukseen kuin verkkopalvelun tai viestintäpalvelun toteuttamiseen. (2004/516, 2 §.)

Palvelunestohyökkäyksen tarkoituksena on estää kohdejärjestelmän toiminta siinä tehtävässä mihin se on tarkoitettu. (CERT-FI 2007.)

Phishing on taloudellisesti hyödynnettävän tiedon, kuten verkkopankkitunnusten, luottokorttinumeroiden tai henkilötietojen laitonta hankkimista. (CERT-FI 2005.)

Protokolla on säännöstö, joka määrittelee datayhteydelle käytettävät yhteydenpitotavat, koodin sekä siirto-, ohjaus- ja toipumismenettelyt. (Valtiovarainministeriö 2008.)

Rekisterinpitäjä on yksi tai useampi henkilö, yhteisö, laitos tai säätiö, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty. (1999/523, 3 §.)

Rekisteröity on henkilö, jota henkilötieto koskee. (1999/523, 3 §.)

Social Engineering on käyttäjän manipulointia ja sosiaalista tiedustelua. (Valtiovarainministeriö 2008.)

Tunnistamistieto on tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. (2004/516, 2 §.)

Varmennetta käytetään Internetin sivustoilla ikään kuin henkilöllisyystodistuksena. Varmenne kertoo, että verkkosivusto oikeasti on sen niminen, joka väittää olevansa. (CERT-FI 2009 b.)

Viestintäverkko on toisiinsa liitetyistä johtimista ja laitteista muodostuva järjestelmä, joka on tarkoitettu viestien siirtoon tai jakeluun johtimella, radioaalloilla, optisesti tai muulla sähkömagneettisella tavalla. (2004/516, 2 §.)

Yhteisö on esimerkiksi elämänmuodon, taloudellisen tai aatteellisten päämäärien perusteella kokonaisuuden muodostava ihmisryhmä tai yhteenliittymä. (Grönros 2006, 645.)

Yhteisötilaaja on viestintäpalvelun tai lisäarvopalvelun tilaajana oleva yritys tai yhteisö, joka käsittelee viestintäverkossaan käyttäjien luottamuksellisia viestejä, tunnistamistietoja tai paikkatietoja. (2004/516, 2 §.)

Yleinen viestintäverkko on viestintäverkko, jota tarjotaan etukäteen rajaamattomalle käyttäjäpiirille. (2004/516, 2 §.)

Lähteet

Kirjalliset ja julkaistut lähteet:

Grönros, E. 2006. Kielitoimiston sanakirja 3. osa. Jyväskylä: Gummerus kirjapaino Oy.

Hallituksen esitys eduskunnalle sähköisen viestinnän tietosuojalain ja eräiden siihen liittyvien lakien muuttamisesta. 48/2008. Hallituksen esitys.

Henkilötietolaki. 22.4. 1999/523.

Järvinen, P. 2002. Tietoturva § Yksityisyys. Jyväskylä: Docendo Finland Oy.

Laki yksityisyyden suojasta työelämässä. 13.8. 2004/759.

Liikenne- ja viestintäministeriö. 1.12. 2008. Valtioneuvoston periaatepäätös kansallisesta tietoturvastrategiasta.

Pfleeger, C. & Pfleeger, S. 2007. Security in Computing. Fourth Edition. Boston: Pearson Education Inc.

Suomen perustuslaki. 11.6. 1999/731.

Sähköisen viestinnän tietosuojalaki. 16.6. 2004/516.

Wendell, O. 2008. CCENT/CCNA ICND1 Official Exam Certification Guide. 2. Painos. Indianapolis: Cisco Press

Artikkelit:

Järvinen, P. Tietosuoja on luottamuksen varassa. Talouselämä 20.3.2009. Viitattu 21.4.2009. http://www.talouselama.fi/kolumni/article257323.ece

Kokko, O. Varo, netti paljastaa elämäsi. Taloussanomat 4.9.2008. Viitattu 21.4.2009. http://www.taloussanomat.fi/tyo-ja-koulutus/2008/09/04/varo-netti-paljastaa-elamasi/200822890/139

Paatero, M. Poliisista, päivää. Poliisilehti 2.10.2008. Viitattu 21.4.2009. http://www.poliisilehti.fi/intermin/hankkeet/blogi/home.nsf/Pages/8FE996984DA50EF1C22574D60034149B

Sokala, H. Tietosuojavarkauksia tehty satoja. Taloussanomat 7.8.2008. Viitattu 21.4.2009. http://www.taloussanomat.fi/tietotekniikka/2008/08/07/tietovarkauksia-tehty-satoja/200820394/133

Opinnäytetyöt:

Suoanttila E. 2006. Tietosuoja organisaation tietojen käsittelyssä ja järjestelmäkehityksessä. Laurea-ammattikorkeakoulu. Laurea Leppävaara. Espoo

Sähköiset lähteet:

CERT-FI. 2005. Suojautuminen phishing-hyökkäyksiltä. Viitattu 17.4.2009. http://cert.fi/ohjeet/2005/ohje-2005-01.html

CERT-FI. 2007. Hyväksikäyttö. Viitattu 17.4.2009.
http://cert.fi/haavoittuvuudet/hyvaksikaytto.html

CERT-FI. 2008. Vuosikatsaus. Viitattu 20.4.2009.
http://www.cert.fi/attachments/tietoturvakatsaukset/5DRJBj1uS/CERT-FI_vuosikatsaus_2008.pdf

CERT-FI. 2009 a. Etusivu. Viitattu 20.4.2009. http://cert.fi

CERT-FI. 2009 b. Tietoturvariski MD5 -algoritmia käyttävissä varmenteissa. Viitattu 17.4.2009.
http://cert.fi/tietoturvanyt/2009/01/ttn200901021055.html

Eduskunnan täysistunto. 2009. PTK 13/2009 vp. Viitattu 20.4.2009.
http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/ptk_13_2009_ke_p_1.shtml

Electronic Frontier Finland ry. 2009 a. Viitattu 21.4.2009. http://www.effi.org

Electronic Frontier Finland ry. 2009 b. Uutisia. Viitattu 21.4.2009.
http://www.effi.org/uutiset/

F-Secure. 2008. Tietoturvakatsaus tammi-kesäkuu 2008. Viitattu 20.4.2009.
http://www.f-secure.fi/2008/1/index.html

Symantec. 2009. Global Internet Security Threat Report. Viitattu 20.4.2009.
http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

TIEKE. 2001. Ostoksilla verkkokaupassa. Viitattu 27.4.2009.
http://www.tieke.fi/mp/db/file_library/x/IMG/12421/file/Ostoksillaverkkokaupassa-opas.pdf

Tietosuojavaltuutetun toimisto. 2009 a. Organisaatio. Viitattu 21.4.2009.
http://www.tietosuoja.fi/1669.htm

Tietosuojavaltuutetun toimisto. 2009 b. Tehtävät. Viitattu 21.4.2009.
http://www.tietosuoja.fi/1552.htm

Tilastokeskus. 2008 a. Internetin käyttäjiä enemmän kuin vuosi sitten. Viitattu 20.4.2009.
http://tilastokeskus.fi/til/sutivi/2008/sutivi_2008_2008-08-25_tie_001.html

Tilastokeskus. 2008 b. Internetin käyttöpaikat keväällä 2008, prosenttia 16-74 -vuotiaista. Viitattu 20.4.2009.
http://tilastokeskus.fi/til/sutivi/2008/sutivi_2008_2008-08-25_kuv_011.html

Tilastokeskus. 2009. Syytetyt, tuomitut ja keskimääräiset rangaistukset alueittain ja rikoksittain, käräjäoikeudet ja hovioikeudet ensimmäisenä oikeusasteena 2005-2007. Viitattu 20.4.2009.
http://pxweb2.stat.fi/Dialog/varval.asp?ma=020_syyttr_tau_101_fi&ti=Syytetyt%2C+tuomitut+ja+keskim%E4%E4r%E4iset+rangaistukset+alueittain+ja+rikoksittain%2C++k%E4r%E4j%E4oikeudet+ja+hovioikeudet+ensimm%E4isen%E4+oikeusasteena+2005%2D2007&path=../Database/StatFin/oik/syyttr/&lang=3&multilang=fi

Valtiovarainministeriö. 2006. Henkilöstön tietoturvaohje. Viitattu 20.4.2009.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061127Henkil/Vahti_10_06.pdf

Valtiovarainministeriö. 2008. Valtionhallinnon tietoturvasanasto. Viitattu 17.4.2009. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/Vahti_8_NETTI%2b_KANNET.pdf

Viestintävirasto. 2007. Lyhenteet ja määritelmät. Viitattu 17.4.2009. http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/yhenteetjamaaritelmat.html

Viestintävirasto. 2009. Tietoturvaopas - Verkkokaupat. Viitattu 28.4.2009. http://www.tietoturvaopas.fi/internetinpalvelut/verkkokaupat.html

Muut julkaisemattomat lähteet:

Petkov P. 2008. Web-tietoturva -seminaari 2008. Helsinki: 31.5.2008