Niko Weckström

INTERNET-OHJELMISTOJEN TIETOTURVA

Tietojenkäsittelyn koulutusohjelma

2014

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

INTERNET-OHJELMISTOJEN TIETOTURVA

Weckström, Niko
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
huhtikuu 2014
Ohjaaja: Nuutinen, Petri
Sivumäärä: 30
Liitteitä: 0

Asiasanat: Tietoturva, tietosuoja, selain, varmenne, käyttäjätili

Opinnäytetyössä käsitellään tietoturvaa tavallisen kuluttajan näkökulmasta. Tavoitteena oli luoda yleispätevä ohjeistus miten omaa tietoturvaa ja yksityisyyttä voidaan parantaa. Työssä käsitellään myös tietojen keruuta sekä jälkiä, joita verkkoon ja omalle työasemalle jää, kun liikutaan tietoverkoissa. Jokaisella on ja pitäisi olla oikeus valita mitä tietoja heistä tallennetaan, kenen toimesta ja miten näitä tietoja käytetään. Tietosuoja takaa ihmiselle oikeuden yksityisyyteen ja se ulottuu myös internetiin. Osataanko tästä oikeudesta pitää kiinni, riippuu käyttäjästä. Näin ollen työn tarkoituksena on myös hahmottaa sitä, mitä tietoja käyttäjästä selainliikenteen mukana kulkeutuu maailmalle. Tavalliselle kuluttajalle asia ei välttämättä ole selvä.

Työn teoreettisessa osassa tarkastellaan yleisimpiä kuluttajan käyttämiä ohjelmia, kuten selainta ja sen liitännäisiä, sähköpostia, verkkopankkia, varmennetta, sosiaalista mediaa sekä pdf-lukuohjelmaa tietoturvan näkökulmasta. Samalla tarkastellaan kohtia, joissa käyttäjästä voi paljastua tietoja. Opinnäytetyön päätarkoitus oli luoda ohjeistus tavalliselle kuluttajalle, miten omasta tietoturvasta ja samalla omasta yksityisyydestään voi huolehtia. Näin jokainen saa tiivistetyn summauksen tietoturvan perusteista.

INTERNET PROGRAMS SECURITY

Weckström, Niko
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information and Communication Technology
April 2014
Supervisor: Nuutinen, Petri
Number of pages: 30
Appendices: 0

Keywords: Information security, confidentiality, browser, certificate, user account

The purpose of this thesis is to process information security of the regular consumer point of view. The goal was to create universal guidelines how to improve personal security and privacy. The study also process data collection and traces what are left in network and workstation when surfing in network. Everyone has and should have the right to choose what information is stored about them, who is storing them and for what purpose the data is used. Confidentiality guarantees right to privacy and it also extends to the internet. Will people be able to hold on to that right depends between users. Thus the work is also intended to outline what information from browser traffic is transported to world. For the average consumer the case may not be clear.

In the theoretical section is examined the most common programs used by the consumer. Such as browser and plug-ins, e-mail, online banking, certificate, social media as well as PDF-reader in the security point of view. At the same time is examined at the points where the user may reveal information. The main purpose of the thesis was to create guidelines for the average consumer how to take care about information security and at the same time their privacy. In this way everyone gets concentrated summation of security criteria.

Sisällysluettelo

1 JOHDANTO

Opinnäytetyön aiheena oli käsitellä tietoturvaa tietoverkoissa. Työn tarkoitus on luoda summaus tavallisen kuluttajan tarvitsemista tiedoista, joiden avulla omaa tietoturvaa voidaan parantaa. Samalla tarkastellaan myös yksityisyyttä sekä syitä siihen miksi ja miten omasta yksityisyydestä tulisi huolehtia. Työssä käsitellään tietoturvaa yleisellä tasolla ja sen tarkoituksena on tarjota ohjeistus sellaisille ihmisille, joille verkon tietoturva ei ole entuudestaan tuttua. Opinnäytetyö käsittelee myös yksityisyyttä ja osittain myös tiedonkeruuta, missä mahdollisissa tilanteissa tietoa kerätään ja miksi.

Tulevaisuudessa tietoturvan ja yksityisyyden merkitys tulee entisestään korostumaan, sillä lähes kaiken voi jo nyt hoitaa verkossa. Työssäni yritän tiivistää oleellisimmat asiat, joiden avulla tavallinen kuluttaja voisi parantaa omaa tietoturvaansa sekä saada paremman kuvan siitä, miksi yksityisyydestään kannattaa huolehtia. Työssä käsitellään selaimen toimintaa, selaimen liitännäisiä sekä evästeitä, sähköpostia, verkkopankkia ja varmennetta. Tulevaisuudessa tietoa pystytään analysoimaan paremmin ja jokaisen tulisi tietää, että tiedon keruuta tapahtuu jatkuvasti selausliikenteen mukana. Miten kerättyjä tietoja voidaan tulevaisuudessa käyttää, on vielä hämärän peitossa. Mielenkiintoinen kysymys on myös; pystytäänkö kerätyistä tiedoista tunnistamaan yksittäinen käyttäjä? Tulevaisuuden kehityksen vuoksi jokaisen tulisi kiinnittää huomiota siihen, mitä itsestään verkossa kertoo. Yhteenvedossa summaan tietoturvaan vaikuttavia tekijöitä ja miten omaa tietoturvaa voidaan parantaa. Tietoturvaa parantamalla parannetaan myös omaa yksityisyyttä.

2 TIETOTURVA

Tietoturva määritellään viiden osa-alueen summaksi. Nämä osa-alueet ovat; luottamuksellisuus, käytettävyys, eheys, kiistämättömyys sekä pääsynvalvonta.

Luottamuksellisuudella tarkoitetaan sitä, että vain ne henkilöt joilla on oikeus käyttää tiettyä tietojärjestelmää pääsevät näkemään vain niitä tietoja joihin heidän käyttäjäoikeutensa riittävät. Pääsyä tietoihin voidaan rajoittaa esimerkiksi käyttäjäoikeuksien rajaamisella, salasanoilla sekä salausalgoritmeilla, mutta myös estämällä ketään ulkopuolista pääsemästä fyysisesti laitteistoon käsiksi. (Hakala, Vainio, Vuorinen, 2006, 4.) (Järvinen, 2012, 10) Luottamuksellisuudessa on otettava huomioon myös tiedon olemassa olo; halutaanko se salata vai riittääkö pelkkä rajoitettu tiedon saatavuus. Tietoliikennettä analysoimalla saadaan selville että viesti on salattu, mutta pelkästään tiedolla kuka lähetti, kenelle ja milloin, voi olla informatiivista arvoa, sillä siitä voidaan luoda hierarkia kaavio. Sen avulla voidaan paikantaa avainhenkilöt ja kohdistaa vakoilu oikeisiin kohteisiin. Luottamuksellisuus tulee siis ottaa huomioon myös tietoverkon sisällä tiedonsiirrossa, mutta myös kannettavissa laitteissa, jotka sisältävät luottamuksellista tietoa.(Cole, Krutz, Conley, Reisman, Ruebush, Gollman & Reese 2008, 7)

Käytettävyydellä tarkoitetaan sitä, että tiedot ovat silloin käytettävissä, kun niitä tarvitaan ja niiden on oltava saatavissa riittävän nopeasti. Tietojen tulee myös olla oikeassa muodossa, jotta käytettävä tietojärjestelmä osaa niitä lukea. (Hakala, Vainio, Vuorinen, 2006, 4.) Käytettävyys käsittää tietoturvan kannalta myös sen, että kolmasosapuoli ei pääse estämään oikeutettua käyttäjää pääsemästä tietojärjestelmään, tiedostoihin tai palveluun. Käytännössä tämä tarkoittaa palvelunestohyökkäykseen varautumista, johon varautuminen on vaikeaa. (Cole ym. 2008, 8)

Tietojen eheydellä varmistutaan siitä, ettei tieto ole muuttunut sillä välin kun sitä haetaan tietokannasta käsiteltäväksi tai kun tietoja viedään takaisin tietokantaan. Tieto ei saa muuttua myöskään tiedonsiirron aikana, kun lähetetään tietoa paikasta x paikkaan y. Tiedon siirrossa tietoverkoissa on riskinä mies välissä-hyökkäys [Man in

the middle attack], jossa voidaan väärentää ja kaapata osa tai kaikki lähetetyistä paketeista. Samalla hyökkäystavalla on mahdollista kiertää luottamuksellisuuden hallinta esimerkiksi muuttamalla käyttöjärjestelmän käyttämää pääsyn hallinta listaa [access control table] eli muuttamalla tai lisäämällä itselleen oikeudet järjestelmään. Tietojen eheydellä pyritään myös estämään tietojen tahaton muuttaminen. Tietojen tulee säilyä oikeina ja virheettöminä tietojenkäsittelyn ja käytönaikana. Tietoihin saa käytön aikana tulla vain sellaisia muutoksia, joita käyttäjäntunnuksilla on oikeus tehdä. Tietojen eheydestä pyritään huolehtimaan esimerkiksi erilaisilla tarkistussummilla, tiivisteillä ja yhteyksien salaamisella.(Hakala, Vainio, Vuorinen, 2006, 4.) (Järvinen, 2012, 10) (Cole ym. 2008, 7)

Luottamuksellisuus, eheys ja käytettävyys käsittelevät pääsyn hallintaa eri näkökulmista ja joiden avulla pyritään estämään ei toivottuja tapahtumia tapahtumasta. Järjestelmissä on kuitenkin aina aukkoja ja virheitä jotka mahdollistavat joko järjestelmään pääsyn hyökkääjän toimesta tai turvallisuutta voi rikkoa sallittu käyttäjä esimerkiksi puutteellisesti rajattujen käyttäjäoikeuksien vuoksi. Tämän vuoksi on määritelty sellainen tietoturva vaatimus kuin pääsynvalvonta.(Cole ym. 2008, 9) Siinä missä luottamuksellisuudella rajataan tietoihin pääsyä, pääsynvalvonnalla rajataan pääsyä tietojärjestelmän rakenteisiin. Kaikilla käyttöoikeuksilla ei ole tarvetta käyttää kaikkia järjestelmän osia. Pääsynvalvonnalla voidaan estää järjestelmien luvaton käyttö, joka voisi altistaa tietojärjestelmän haittaohjelmille sekä resurssien väärin käytölle. Rajatulla järjestelmään pääsyllä saadaan näin parannettua myös käytettävyyttä tietoturvan lisäksi. (Hakala, Vainio, Vuorinen, 2006, 5.) Pääsynvalvonnalla tunnistetaan ja todennetaan järjestelmään kirjautuva henkilö. Näistä tiedoista pidetään kirjausketjua, jonka tiedoista on mahdollista tunnistaa tietoturva rikkomuksen aiheuttanut käyttäjä.(Cole ym. 2008, 10)

Kiistämättömyydellä halutaan, että tietojärjestelmä tunnistaa ja varmistaa, että jokin tapahtuma on todella tapahtunut eikä sitä voida kiistää. Sen avulla varmistutaan esimerkiksi dokumentin alkuperästä, kuka sen on lähettänyt ja onko se mennyt perille ja kenelle se on mennyt.(Cole ym. 2008, 10) Kiistämättömyydellä varmistetaan tiedon alkuperä, mutta myös olemassa olevien tietojen luvaton käyttö.(Hakala, Vainio, Vuorinen, 2006, 5.) Tietojen kiistämättömyys voidaan toteuttaa sertifikaatein, jotka omaavat tietyn voimassaoloajan, erilaisin älykortein, jotka sisältävät käyttäjän henkilötiedot tai biometrisen tunnistuksen avulla. (Hakala, Vainio, Vuorinen, 2006, 4.) Lu-

vattomasta tiedon käytöstä on viime aikoina tullut useita tuomioita tai rikosepäilyjä. Joko yleisessä tiedossa ei ole että näin ei saa tehdä, tai sitten luullaan, että siitä ei voi jäädä kiinni. (Ruokangas, 2013) (Työntekijä katsoi luvatta... 2013) (Mika Myllylän kuolema... 2013,)

2.1 Tietosuoja ja yksityisyys

Siinä missä tietoturvalla suojataan tietojärjestelmiä ja itse tietoa, niin tietosuojassa turvaamisen kohteena ovat henkilötiedot. Henkilötietoihin kuuluvat; nimi, osoite, henkilötunnus ja syntymäaika sekä kaikki sellainen tieto, joka kuvaa ihmisen toimintaa ja ominaisuuksia. Myös tiedot selainhistoriasta sekä kaikki sellainen tieto, josta voidaan yksilöidä tietty henkilö, ovat luettavissa henkilötietojen tai tietosuojan piiriin. Tietosuojan tarkoituksena on taata ihmiselle oikeus yksityisyyteen ja estämään tietojen tarpeeton tai epäasiallinen käyttö (Järvinen, 2012, 12) (Sähköisen viestinnän tietosuojalaki, 2 Luku, 4§, Viestin, tunnistamistietojen ja paikkatietojen luottamuksellisuus) Tämä pätee kuitenkin vain Suomessa. Jokaisella maalla on omat käytäntönsä ja yksityisyys käsitteenä on vahvasti sidoksissa kulttuuriin ja yhteiskuntaan. (Järvinen, 2010, 14) Viimeisimmän löytämäni tiedon mukaan 89 maalla on oma tietosuojalakinsa. (Greenleaf, 2012, 1) Toinen lähde on kuitenkin ottanut huomioon vain 63 maan tietosuojalait. Tähän lähteeseen tutustumalla saa myös paremman kuvan eri maiden lakien eroista sekä siitä, että yksityisyyden määritelmä ei ole joka maassa sanasta sanaan samanlainen.(DLA PIPER, 2013, 5)

Henkilötiedot kiinnostavat monia tahoja ja niistä ollaan valmiita maksamaan. Yritykset haluavat nähdä yksittäisten ihmisten kulutustottumuksia, jotta voivat paremmin kohdistaa mainontaansa sekä hintojaan. Kuluttajia yritetään seurata mahdollisimman tarkkaan internetissä ja esimerkiksi tuotteen hinta voi kallistua sen mukaan millä sivuilla olet aiemmin internetissä ollut. (Varo, voit itse...2012) Rikollisia kiinnostavat tavallistenkin ihmisten tiedot, sillä niiden avulla voidaan pyrkiä saavuttamaan taloudellista hyötyä, joko myymällä ne eteenpäin, murtautumalla yksityiselle työasemalle ja vakoilemalla liikkeitäsi tai varastamalla verkossa liikkuvien identiteettejä. (Miehen epäillään vakoilleen... 2012)

Tietoturvan avulla parannetaan myös omaa yksityisyyttä ja pyritään siihen, että mitään sellaista tietoa ei vuoda vahingossa verkkoon jota sinne ei haluta. Tiedontallen-

taminen on niin halpaa, että se yksinkertaisesti on kannattavaa. Esimerkiksi Googlella on valtavat määrät dataa jo pelkästään käytettyjen hakusanojen muodossa ja esimerkiksi niistä on vuodesta 2008 ennustettu influenssan eteneminen. Jokainen on varmasti samaa mieltä että tämä on oikeanlainen tapa hyödyntää syntynyttä tietomäärää. Kuitenkin tulevaisuudessa tätä suurta tieto määrää, Big dataa eli analysoimatonta raakatietoa hyödynnetään entistä enemmän, kun sitä opitaan analysoimaan tehokkaammin ja halutulla tavalla. Kukaan ei tarkkaan pysty sanomaan mihin kaikkea tallennettua tietoa tullaan käyttämään ja kenen käsiin se lopulta päätyy. Lähivuosina tiedon kerääminen tulee lisääntymään entisestään ja jokaisen pitäisi ainakin olla tietoinen siitä mitä jälkiä verkkoon jätämme. (Paukku, 2013, Hanki dataa – hankit samalla valtaa). Jo nyt selaintietoja voidaan käyttää yksilöiviin verkkokauppa hintoihin, on kyseenalaista toimintaa pelkästään tasa-arvon näkökulmasta, yksityisyydestä puhumattakaan.

3 LAITTEISTO

Kappaleessa käsitellään laitteistoon liittyvää tietoturvaa. Mitä tulee ottaa huomioon laitteiston tilasta, jotta sitä olisi turvalista käyttää myös verkossa. Kappaleessa käsitellään myös käyttäjätilejä.

3.1 Työasema

Tietoturvan perustana on pitää oman työaseman käyttöjärjestelmä, ohjelmat, sovellukset ja verkkolaitteet ajan tasalla. Tällä tarkoitetaan sitä, että päivitetään säännöllisesti käyttöjärjestelmälle julkaistavat päivitykset ja korjaukset sekä ladataan uusimmat ohjelmisto- ja sovellusversiot sekä ladataan uusimmat virustiedot.(Allen, 2002, 39) Suuren osan päivityksistä voidaan aikatauluttaa, jolloin tietokone tarkistaa määräajoin onko uusia päivityksiä saatavilla ja lataa ne, jos näin on sallittu. Uusimpien käyttöjärjestelmäpäivitysten tai ohjelmaversioiden puuttuminen voi alentaa työaseman tietoturvaa ja näin mahdollistaa vanhan version tietoturva-aukon hyödyntämisen.(Allen, 2002, 39) Lisäksi virustentorjunta ohjelmiston tulee olla, päivitettynä, sillä ilman uusia virusten tunnistetietoja, ei työasema pysy turvallisena. Virustentorjuntaohjelma myös suorittaa reaaliaikaista tarkistusta ja estää tavallisuudesta poikkeavia toimintoja, joita ohjelmat saattavat tehdä. (Hakala, Vainio, Vuorinen, 2006, 135). Oh-

jelmia ja päivityksiä ladatessa tulee ottaa huomioon ohjelmien tunnettavuus, maine sekä latauspaikka. Kaikki lataukset tulisi tehdä vain luotettavista lähteistä esimerkiksi valmistajan omilta sivuilta ja välttää lataamista kolmansien osapuolten sivustoilta. Työaseman käyttöjärjestelmästä tulisi karsia kaikki sellaiset palvelut joita ei tarvitse. Näin tekemällä saadaan vähennettyä mahdollisten tietoturva-aukkojen määrää. Tarpeettomia ohjelmia ei myöskään tulisi asentaa, sillä ne helposti unohtuvat ja jäävät päivittämättä. Tiivistäen kielletään ensin kaikki ja otetaan vasta sen jälkeen ne toiminnot, palvelut ja ohjelmat käyttöön joita tarvitaan.(Allen, 2002, 46) Riippuen siitä kuinka henkilökohtaisia tai arkaluonteisia tietoja käsitellään, työaseman kovalevyjen salaus voi olla aiheellista. Näin voidaan ainakin estää tiedostojen käyttö, jos ne joutuvat vääriin käsiin. Toisaalta uutena riskinä on salausavaimen unohtaminen.(Järvinen, 2012, 225)

3.1.1 Käyttäjätilit

Käyttäjätilien avulla voidaan eri käyttäjille antaa eriarvoiset oikeudet käyttäjätili tyypin mukaan. Kirjautuessa kysytään käyttäjätunnusta ja salasanaa, mutta myös esimerkiksi voidaan kysyä sormenjälkeä, jos sellainen toiminto on määritelty käyttöön. (Hakala, Vainio, Vuorinen, 2006, 124) Näin voidaan parantaa tietoturvallisuutta, kun jätetään tietokoneen pääkäyttöoikeudet vain yhden tai muutaman henkilön haltuun. Käyttöoikeuksia on mahdollista muokata erittäin yksilöllisiksi kuitenkaan antamatta pääkäyttöoikeuksia.

Kotitietokoneen suojauksessa tulee ottaa huomioon myös se, että käyttäjätilin salasana on mahdollista kiertää. Se onnistuu esimerkiksi käynnistämällä tietokone USB-muistitikun avulla tai cd/dvd-levyltä ja asentamalla uusi käyttöjärjestelmä vanhan päälle. Uuden asennuksen yhteydessä luodaan uusi pääkäyttäjän tunnus ja näin päästään myös käsiksi aiemmin asennetun käyttöjärjestelmän tiedostoihin, jos levyä ei asennuksen aikana alusteta. Tähän on kuitenkin olemassa yksinkertainen ratkaisu; tietokoneen bios-asetuksista voidaan estää ulkoisesta lähteestä tapahtuva tietokoneen käynnistys. Estoasetuksen päälle laittamisen jälkeen USB-muistin tai cd/dvd-levyn avulla ei voida asentaa uutta käyttöjärjestelmää ennen kuin asetus taas muutetaan sen sallivaksi. Ongelmana on jälleen kerran salasanojen hallinta sillä, jos sitä ei ole bios-asetuksista myös määritelty, niin kuka tahansa kenellä on fyysisesti pääsy tietokoneeseen voi asetukset käydä muuttamassa halutuiksi. (Järvinen, 2012, 224)

3.2 Mobiililaite

Mobiililaitteen tietoturvaan vaikuttavat pitkälti samat asiat kuin työasemaan. Lisähuolena tosin on laitteen ja samalla tietojen häviäminen laitteen pienen koon ja mukana kulkevuuden vuoksi. Tämän vuoksi pitäisi jo etukäteen ottaa huomioon laitteen mahdollinen katoaminen. Ongelmaan on joissakin puhelimissa ratkaisuna etätyhjennys, jonka avulla tiedot voidaan pyyhkiä. Puhelin voidaan myös lukita etäyhteyden avulla joko netin kautta tai tekstiviestillä. (Järvinen, 2012, 43) Kadonnut puhelin on myös mahdollista paikantaa, edellyttäen, että siinä on vielä akkua jäljellä ja paikannusmenetelmästä riippuen yhteys internetiin. ”Paikannus voi tapahtua tukiasematietojen, wlan-verkkojen tai puhelimen GPS-sijainnin perusteella”. (Järvinen, 2012, 43) SIM-kortin suojana on PIN-koodi, ja se suojaa liittymää, mutta ei puhelinta. PIN-koodi tulisi vaihtaa tehdasasetuksen 0000 tai 1234 asetuksesta. Joissain älypuhelimissa on asetus, jossa puhelin lukitaan, jos puhelimeen on laitettu eri SIM-kortti. Saman ominaisuuden saamiseksi on myös tietoturvaohjelmia. (Järvinen, 2012, 41)

3.3 Salasana

Riittävän hyvän salasanan tulee olla tarpeeksi pitkä, sen tulee sisältää erikoismerkkejä, numeroita sekä isoja- että pieniä kirjaimia. Mikä sitten on riittävän pitkä salasana? Jokainen palvelu ei välttämättä ole niin tärkeä että sitä tarvitsisi suojata vahvalla salasanalla, vaikka se tietenkin olisi suotavaa. Jos palvelu sisältää itsestä niin paljon tietoa, että joku voisi hyvin kaapata henkilöllisyytesi ja esiintyä sinuna, niin silloin olisi hyvä suojata palvelu mahdollisimman hyvällä salasanalla. Myös luottamuksellisia tietoja sisältävissä palveluissa tulisi käyttää mahdollisimman vahvaa salasanaa. Pääsääntönä voidaan käyttää sitä, että mitä pidempi salasana sitä kauemmin sen murtaminen kestää. On myös mahdollista ettei kukaan yritä murtaa salasanaa jonka murtamiseen menisi kohtuuttoman paljon aikaa, olettaen että hyökkääjä ei tiedä mihin tietoihin edes pääsisi käsiksi. Salasanat pitäisi myös vaihtaa säännöllisin väliajoin ja jokaisessa palvelussa täytyy käyttää eri salasanaa. (Järvinen, 2012, 114)

Hyvä salasana on esimerkiksi kokonainen lause yhteen kirjoitettuna. Esimerkiksi KelloOn17.00! Jos palvelu sallii, niin ä- ja ö kirjaimet vahvistavat salasanaa. Salasana, joka on kirjoitettu eri merkein sekä tarkoittaen jotakin on helpompi muistaa. (Järvinen, 2012, 120)

4 OHJELMISTOT

Kappaleessa käsitellään yleisimpiä tavallisen kuluttajan käyttämiä ohjelmia verkossa. Erityistä huomiota kiinnitetään selaimen toimintaan ja siihen mitä jälkiä verkkoon ja omalle työasemalle voi jäädä, kun selainta käytetään.

4.1 Sähköposti

Sähköposti on nopea tapa lähettää viestejä samanaikaisesti monille vastaanottajille. Sähköpostitilit voidaan karkeasti jakaa kahteen ryhmään, POP3-palveluun ja web-pohjaiseen sähköpostiin.

Web-based email on sähköposti, johon kirjaudutaan selaimella www-sivun kautta sisään. Useimmilla on kotikäytössään juuri tämän kaltainen sähköposti. Esimerkiksi Googlen Gmail, Microsoftin Outlook.com tai Yahoon! Yahoo!Mail ovat webmail pohjaisia sähköposteja. Webmail pohjaisen sähköpostin käyttäminen vaatii internet-yhteyden, tarkoittaen sitä että edes viestien lukeminen ei onnistu yhteydettömässä tilassa. Viestit myös pysyvät palveluntarjoajan palvelimella niin kauan kunnes ne poistetaan omasta postilaatikosta. Lisäksi on huomioitava se, että viestit eivät välttämättä poistu pysyvästi, kun ne poistetaan saapuneet kansiosta, vaan ne siirtyvät sähköpostitilin roskakoriin. Vasta roskakorista poistetut viestit poistuvat pysyvästi. Tosin viestien todellinen poistaminen on puhtaasti luottamuksellinen asia; poistuvatko viestit todella palveluntarjoajan palvelimelta? Ainakaan ilmaisia web pohjaisia sähköpostipalveluja ei tulisi käyttää mihinkään luottamuksellisen tiedon lähettämiseen. (Wikipedia.org, 2013, https://en.wikipedia.org/wiki/Email) (Canavan, 2001, 115)

POP3 sähköpostipalvelu eroaa selainpohjaisesta sähköpostista siten että, käyttäjän tietokoneelle asennettu sähköpostiohjelma hakee viestit sähköpostipalvelimelta ja tallentaa ne saapuneiksi viesteiksi käyttäjän tietokoneelle asennettuun sähköposti ohjelmaan. Tämän jälkeen viestit poistetaan automaattisesti sähköpostipalvelimelta. Toisaalta asetuksista riippuen on mahdollista, että viestejä ei automaattisesti poisteta palvelimelta. Vaihtoehto POP3-protokollalle on IMAP, jonka etuna on sähköpostin käyttäminen useammalla kuin yhdellä laitteella. Tarkoittaen sitä, että viestejä säilytetään palvelimella, josta niitä voi halutessaan ladata haluamalleen päätelaitteelle ja niitä voidaan poistaa palvelimelta.
(Wikipedia.org, 2013, https://en.wikipedia.org/wiki/Email)

Sähköpostissa on useita tietoturvankannalta ongelmallisia asioita. Sähköpostiviestit eivät ole automaattisesti salattuja ja tämä aiheuttaa tietoturvariskin, sillä periaatteessa kuka tahansa voisi kaapata ja nähdä käyttäjän lähettämien viestien sisällön. Koskaan ei ole myöskään varmuutta meneekö viesti todella perille aiotulle henkilölle, ainakaan ennen kuin vastaanottajalta tulee vastaus takaisin. (Järvinen, 2012, 77) Sähköpostin liitetiedostot aiheuttavat myös tietoturvaongelman; niiden avulla voidaan lähettää haittaohjelmia, jotka seuraavat ja keräävät tietoja käyttäjästä. Nykyään yleisempi tapa levittää sähköpostin kautta haittaohjelmia on liittää sähköpostiviestiin linkki luotettavan näköiselle sivulle ja tätä kautta houkutella käyttäjä lataamaan jokin tiedosto, joka todellisuudessa on haittaohjelma. Esimerkiksi kun linkkiä on painettu, niin käyttäjä saa virheilmoituksen, että sivua ei voi näyttää oikein ja käyttäjän tulisi ladata ohjelma x, jotta sivu voidaan näyttää oikein. (Järvinen, 2012, 181)

Ongelmallisia ovat myös pitkiksi venyneet viestiketjut, sillä vastaan voi tulla tilanne, että on tarve lähettää sama viesti useammalle henkilölle ja näin vahingossa lähetetään koko viestiketju, vaikka tarkoituksena oli saada viestiketjun päällimmäinen viesti useamman henkilön tietoon. Onko oikein sitten jakaa toisesta viestinnänosapuolesta riippumatta kokoviestiketju jonkun muun kanssa, niin lain mukaan kyllä, jos viestien sisältöä ei rajoita vaitiolovelvollisuus. (Secmeter.com, 2013, http://www.secmeter.com/viestintasalaisuus.html) Todellinen ongelma kuitenkin on se, että yleensä kyseessä on inhimillinen erehdys, että koko viestiketju tulee jaetuksi. Tai ei muisteta koko viestiketjun sisältöä ja näin jaetaan vahingossa sellaista tietoa jota ei pitäisi jakaa.

Sähköpostin automaattista vastausta tulisi käyttää vain sisäiseen käyttöön, tai vastauksen tulisi lähteä vain rajatulle määrälle ihmisiä. Tämä siksi, että jos jokaiseen sähköpostiviestiin lähetetään automaattinen vastaus esimerkiksi siitä, että olen lomalla aikavälillä x-y, niin rikolliset voivat käyttää tätä tietoa hyväkseen. Automaattistenvastausten ongelma koskee ehkä enemmän yrityksiä, sillä hakkerit voisivat näin kalastaa tietoa siitä kenen tietokonetta ei lähiviikkoina käytetä ja näin yrittää rauhassa päästä tietoihin käsiksi. (Canavan, 2001, 127)

Sähköpostia ei tulisi myöskään käyttää viestien säilytyspaikkana, sillä riskinä on kaikkien tietojen menetys tai joutuminen vääriin käsiin. Parempi tapa on tallettaa tär-

keät viestit paikallisesti omalle työasemalle ja vielä salata ne, jos sen katsoo tarpeelliseksi. Näin vältytään siltä, että jos esimerkiksi palveluntarjoajalta varastetaan käyttäjätietoja ja joku pystyisi niitä hyödyntämään, niin ainakaan omasta sähköpostista ei löydy koko elämänkerran edestä tietoja. (Canavan, 2001, 117)

4.2 Selain

”WWW-selain on World Wide Webin HTML-, XHTML-, tai muilla vastaavilla kielillä toteutettujen sivujen katseluun tarkoitettu ohjelma.” (linux.fi, 2013) Selaimen avulla voidaan kommunikoida eri palvelimien välillä käyttämällä pääasiassa HTTP-protokollaa, jonka avulla www-sivuja voidaan hakea. Selaimet sisältävät myös muita protokollia esimerkiksi FTP=file transfer protocol ja HTTPS, joka on salattu versio HTTP-protokollasta. Selaimen avulla voidaan katsella www-sivuja ja niihin sisällytettyä materiaalia; videoita, kuvia, tekstiä tai muita tiedostoja. Selaimesta ja sen lisäosista riippuu, minkä tyyppistä materiaalia voidaan katsella. Eri sivuja haetaan pääasiassa URL-osoitteiden avulla, mutta sivuille voi siirtyä myös käyttämällä IP-osoitetta. Selaimella voidaan myös ottaa yhteys yksityiseen verkkoon tai tietojärjestelmän tiedostoihin ottamalla yhteys vastaavaan palvelimeen oikealla osoitteella. Suosituimpia selaimia ovat: Internet Explorer, Modzilla Firefox, Google Chrome, Opera ja Safari. (Wikipedia.org, 2013)

4.3 Selaimen ominaisuudet

Kappaleessa käsitellään selaimen eri ominaisuuksia ja toimintaa. Miten selain kerää tietoa ja minne se varastoidaan sekä mitä tietoja selain paljastaa käyttäjästä. Kappaleessa tarkastellaan myös selaimen tekniikkaa. Selaimen historiatiedot ovat luottamuksellisia tietoja. Siksi jokaisen tulisi suhtautua niihin asianmukaisella vakavuudella. (Sähköisen viestinnän tietosuojalaki, 2 Luku, 4§, Viestin, tunnistamistietojen ja paikkatietojen luottamuksellisuus). Ne paljastavat käyttäjästä parhaimmillaan todella paljon. Selailun ajankohdan, paikan, henkilökohtaiset kiinnostuksenkohteet, henkilötiedot ja salasanat, jos automaattinen täydennys on sallittu. Lisäksi, selain näyttää tallennetut salasanat selväkielisenä, sillä niitä ei ole salattu. Esimerkiksi Firefox selaimessa asetukset ja turvallisuus välilehti ja sieltä tallennetut salasanat, niin on mahdollista nähdä yksityiskohtaisesti, mihin palveluun on käytetty mitäkin salasanaa.

Selaimen välimuisti tallentaa internetistä ladattuja tiedostoja tietokoneen muistiin tai kovalevylle. Kun sama www-sivu avataan uudestaan, selain voi lukea sen ottamatta uudestaan yhteyttä palvelimeen.(Wikipedia, 2013) Erona selaimen historiaan on siis se, että historiaan tallennetaan verkkosivun osoite kun taas välimuistiin tallennetaan koko sivu, jolla on käyty. Näin ulkopuolinen kenellä on pääsy tietokoneelle, voi nähdä välimuistista millä sivuilla edellinen kävijä on käynyt. Esimerkiksi Firefox-selaimessa välimuistin sisältöä voi katsella kirjoittamalla URL-osoitekenttään: about:cache ja painamalla enter. Sen jälkeen välimuistin sisällön saa listattua List Cache Entries kohdasta. Välimuistin täyttyminen voi lisäksi hidastaa selaimen toimintaa.

Yksityisyystilassa selain ei talleta katsottuja sivuja selaimenhistoriaan tai välimuistiin ja osoiterivin muisti on poissa käytöstä. Myöskään lomakkeiden automaattinen täydennys ei ole käytössä. Uudet evästeet poistetaan automaattisesti istunnon lopettamisen jälkeen. Tulee kuitenkin muistaa, että jos merkitset sivun kirjanmerkkeihin yksityisyys tilassa, niin se jää näkyviin myös muille samaa työasemaa käyttäville. Aloitussivun muutokset ja ladatut tiedostot yksityisyystilan aikana jäävät myös muiden käyttäjien nähtäväksi. "Yksityisyystila ei vähennä operaattorin, yrityksen tietohallinnon tai www-palvelun näkemiä jälkiä." (Järvinen, 2012,77) Yksityisyys tila on tietoturvaa parantava tekijä vain paikallisesti ja siitä on hyötyä, jos työasemalla on useita käyttäjiä, mutta erillisiä käyttäjätilejä ei ole luotu.

Selaimen ottaessa yhteyttä webpalvelimeen se lähettää HTTP protokollaa käyttäen GET- pyynnön kyseiselle palvelimelle. Näin palvelin saa teknisiä tietoja, kuten sen mitä selainta käytetään ja mikä on käyttäjän valitsema kieliasetus. Näin palvelin pystyy reagoimaan pyyntöön ja esimerkiksi esittämään sivut halutulla kielellä, jos sellaiset ovat saatavilla. (Järvinen, 2010, 176) Käyttäjän kannalta tämä on hieno asia, että palvelut räätälöidään lennosta vastaamaan omia tarpeita. Tietoturvan kannalta asia on ongelmallinen aina, kun on mahdollista kerätä tietoja käyttäjästä ja jos ei ole varmuutta palvelun ylläpitäjän luotettavuudesta.

GET-pyyntö sisältää viitetiedon siitä, miltä sivulta käyttäjä on päätynyt kyseiselle sivulle, joka nyt halutaan avata. Joissain tapauksissa otsaketieto[referer] pitää sisällään myös tiedon siitä mitä artikkelia tai kohtaa www-sivuista käyttäjä katsoi. (Conti, 2008, 77). Viitetiedon avulla esimerkiksi verkkokaupasta uloskirjautuminen siirtäisi

asiakkaan sivujen tekijän haluamalle sivulle ja antaisi esimerkiksi tiedon, että olet nyt kirjautunut ulos.

Google lisää käytetyn hakutermin URL tiedon loppuun. Kun käyttäjä klikkaa www-sivulle Google-haun tuloksista, siirtyy myös tieto palvelun tarjoajan palvelimelle siitä, millä hakutermillä käyttäjä sivuille päätyi. Tämä johtuu siitä, että otsakkeen tieto sisältää osoitteen, jolta www-sivulle päädyttiin.(Conti, 2008, 76) Yksityisyyden kannalta ei ole lähtökohtaisesti miellyttävää ajatus, että ulkopuolinen taho saisi tietoonsa käytetyt hakusanat, varsinkaan, jos ne voitaisiin yhdistää tiettyyn henkilöön. Toisaalta tämän tiedon siirtyminen mahdollistaa sen, että palveluntarjoaja voi parantaa omien sivujensa metatietoja ja näin saada sivunsa näkymään niillä hakusanoilla, joita ihmiset käyttävät palvelun etsimiseen. Toisin sanoen ihmisten on helpompi löytää sitä tietoa mitä he hakutermeillään haluavat löytää.

Aina selaimen ottaessa yhteyttä internet-sivulle, se jättää jäljen sivujen ylläpitäjän palvelimelle. Näitä tietoja tallennetaan joko tekstilokeiksi tai pysyvämpään tietokantaan. Esimerkiksi yhdestä sivunnäyttöpyynnöstä jäänyt jälki lokiin oli seuraavanlainen:

86.x.x.x - - [02/Dec/2007:04:49:28 -0700] ”GET / HTTP/1.1”
200 15384 ”http://www.google.co.uk/search?hl=en&q=RUMINT”
&meta=” ”Modzilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1; .NET CLR 2.0.50727)”
(Conti, 2008, 64)

Tästä voidaan nähdä käyttäjän ip-osoite, päivämäärä ja kellonaika, jolloin sivuja haluttiin katsella. HTTP-pyyntö, mitä sivua haluttiin katsoa ja onnistuttiinko se antamaan. Tiedon siitä, miltä sivulta käyttäjä oli näille sivuille päätynyt ja koska linkki sivuille on avattu Googlen kautta, niin myös hakusanan. Lisäksi nähdään tieto siitä, mitä selainta ja käyttöjärjestelmää on käytetty. (Conti, 2008, 64) Otsakkeen mukana selain lähettää itsestään tietoja user-agent nimisessä kentässä. User-agent sisältää tiedon käytetystä selaimesta ja sen sivumoottorista, käyttöjärjestelmästä ja sen versiosta sekä käyttöjärjestelmään asennetuista lisäosista esimerkiksi .NET. (Järvinen, 2010,178) Otsakkeet voivat myös paljastaa seuraavia tietoja: prosessorin malli, ruudun koko, liitännäiset, onko äänikortti käytettävissä, paikallisen ajan ja päivämäärän, Googlen työkalupalkin version, Visual Basic Scripting version, kielivalinnan, media

soittimien versiot tai jotain muita vastaavia tietoja. (Conti, 2008, 71) Osa näistä tiedoista kerätään täysin turhaan käyttäjän näkökulmasta, eikä palvelun käyttö estyisi, jos joitain tietoja ei kerättäisi.

Selaimen otsake ja user-agent tiedot paljastavat kohteesta paljon ja mahdollisen hyökkääjän on helpompaa löytää tietoturva-aukko, kun on tiedossa mitä ohjelmia ja versioita käyttäjä käyttää. Krakkeri voisi saada otsakkeen ja user-agent tiedot esimerkiksi pystyttämällä oman palvelun, jonka avulla aina sivulla vierailija jättäisi jälkensä palvelimelle. Myöhemmin krakkeri voisi joko myydä tietoja eteenpäin tai käyttää niitä itse. Tietoturvan kannalta, erityistä huomiota pitäisi siis kiinnittää siihen minkälaisilla sivuilla liikutaan. Otsake, user-agent ja Flash Playerin tiedot sekä ip-osoite eivät silti vielä paljasta riittävästi käyttäjästä, jotta tietoja voitaisiin tehokkaasti hyödyntää ainakaan vielä.

4.3.1 Evästeet

Eväste on tekstitiedosto, jonka palvelin lähettää selaimelle. Selain tallentaa tiedon myöhempää käyttöä varten ja palauttaa tiedon automaattisesti. Istuntokohtaiset evästeet poistuvat automaattisesti, kun selain suljetaan ellei päivämäärä ole ilmoitettu. Pysyviä evästeitä voidaan tehdä antamalla evästeelle viimeinen voimassaolopäivä. Evästeen avulla tunnistetaan sivuille palaava käyttäjä ja näytetään esimerkiksi saman kaupungin säätiedot, joita viimeksi oltiin haettu. Pääasiassa evästeet ovat hyödyllisiä ja mahdollistavat esimerkiksi verkkokaupan toiminnan. Saman palvelun sisällä jokainen sivuhaku on itsenäinen tapahtuma ja niiden välillä ei olisi yhteyttä ilman evästeitä. Tietoturvaominaisuutena selain ei voi lähettää evästettä eri verkko-osoitteeseen, kuin mistä se oli saatu.(Järvinen, 2010, 165) (Conti, 2008, 73)

Evästeet eivät juurikaan muodosta tietoturvauhkaa, mutta ne voivat olla ongelmallisia yksityisyyden näkökulmasta. Mainostajat ovat kiinnostuneita yksittäisten käyttäjien tiedoista, jotta voivat kohdistaa mainontaansa paremmin. Tiettyä palvelua käytettäessä, joka voi sisältää esimerkiksi mainoksia, ladataan huomaamatta myös kolmansien osapuolten evästeitä, jotka hakevat mainoksia sivuille. "Mainostaja itse tietää, mihin palveluun kukin mainos lähetetään. Pitämällä kirjaa omista mainoksistaan ja käyttäjien evästeistä se pystyy selvittämään, missä eri palveluissa kukin käyttäjä on vieraillut. Mainostaja ei silti edelleenkään tiedä kävijästä mitään henkilökohtaista."

(Järvinen, 2010, 169). Vierailemalla verkko-osoitteessa, joka sisältää kolmansien osapuolten sisältöä, esimerkiksi mainontaa, niin teknisesti olet myös vieraillut mainostajien verkko-osoitteissa. Tätä porsaanreikää hyväksi käyttäen kolmas osapuoli voi lähettää selaimelle evästeitä ja näin seurata käyttäjää internetissä. (Conti, 2008, 75)

Sitähän ei voi tietää onko tulevaisuudessa mahdollista alkaa yhdistellä tietoja, jotta saadaan jokaisen henkilökohtaiselle selainhistorialle henkilöllisyys. Tai ainakin on mahdollista laskea todennäköisyys sille. Joka tapauksessa evästeillä voidaan melko luotettavasti yksilöidä selain ja käyttäjätili yhdistelmä.(Conti, 2008, 75)

4.4 Verkkopankki

Verkkopankin avulla voidaan huolehtia raha-asioista pankin tarjoamien internetsivujen kautta. Suurin osa suomalaisista käyttää verkkopankkia, viimeisimmän tilaston mukaan 79% suomalaisista 16-89-vuotiaista oli käyttänyt viimeisten kolmen kuukauden aikana verkkopankkia. (Tilastokeskus, 2013)

Verkkopankin käyttäminen on melko turvallista, mutta siihen liittyy pääasiassa vain muutama riski: tietojenkalastelu ja pankkitroijalaiset. Tietoja kalastellaan väärennettyjen verkkosivujen avulla. Käyttäjät voidaan houkutella väärille sivuille lähettämällä sähköpostia, jossa pyydetään vaihtamaan palvelun salasana käyttämällä sähköpostissa olevaa linkkiä, joka tietenkin vie väärennetyille sivuille. Käyttäjiä voidaan pyytää myös luettelemaan avainlukulistan tunnuksia. Huijaussivujen tunnistaminen ei välttämättä ole helppoa, mutta tarkistamalla verkko-osoitteen nimen osoitepalkista tai aina siirtymällä verkkopankinsivuille niin, että itse kirjoittaa osoitteen oikein osoitekenttään tai käyttäen kirjanmerkkiä, niin on mahdollista välttyä valesivustoilta. Lisäksi kaikki verkkopankit käyttävät ssl-salausta, jonka voi nähdä osoitekentän alusta, jonka pitäisi olla https. Jos näin ei ole, niin kyseessä todennäköisesti ei ole verkkopankkisi viralliset sivut. (Järvinen, 2012, 73) Pankkitroijalaiset ovat vakavampi uhka, ne ovat haittaohjelmia, joita tietämätön käyttäjä voi vahingossa ladata työasemalle tai joita yritetään levittää jollain muulla tavalla. Pankkitroijalaisen toimintaperiaate on siinä, että se aktivoituu, kun kirjaudutaan verkkopankkiin ja muuttaa rahasiirtojen tietoja käyttäjän huomaamatta, jolloin rahat siirtyvät väärälle tilille.(Järvinen, 2012, 64) Paras keino välttää troijalaiset on pitää käyttöjärjestelmä ja virustorjunta päivitettyinä

sekä välttää sellaisten tiedostojen lataamista, joiden sisällöstä ei ole luotettavaa tietoa.

4.5 Varmenteet

Varmenne ja sertifikaatti ovat sama asia. Sen avulla varmistutaan toisesta osapuolesta ennen salatun yhteyden muodostamista. Selain pyytää palvelimelta varmenteen. Kun palvelin on vastannut selaimen pyyntöön ja lähettänyt varmenteen tiedot, niin tämän jälkeen muodostetaan salattu yhteys ja palvelun käyttö voi alkaa. Salauksesta ei ole hyötyä, jos palveluntarjoajan luotettavuutta ei voida vahvistaa. Varmenteita myöntävät yritykset tarkastavat verkossa olevien ja varmenteita haluavien yrityksen tiedot ennen varmenteen myöntämistä. Varmenteen tiedoista käy ilmi esimerkiksi palveluntarjoajan yrityksen nimi, osoite, verkko-osoite sekä varmenteen myöntäneen yrityksen tiedot. Varmenteen aitous ja muuttumattomuus, varmenteen myöntämisen jälkeen, taataan digitaalisella allekirjoituksella, jonka selain tarkistaa. (Järvinen, 2012, 59)

Varmenteiden virheilmoituksiin tulee suhtautua vakavasti, sillä se kertoo siitä että kaikki ei ole kunnossa. Yleisin syy varmenteen virheilmoitukseen on varmenteen vanhentuminen, josta selain ilmoittaa. Useimmiten virheen syynä on se, että palvelun ylläpito on unohtanut uusia varmenteen. Vakavampi virheilmoitus olisi silloin, jos varmenteen osoite ei vastaa www-sivun osoitetta. Tässä tapauksessa on mahdollista, että huijaussivusto käyttää toisen palvelun varmennetta.(Järvinen, 2012, 62) Lisäksi on mahdollista, että varmenteen on myöntänyt taho johon selain ei luota. Tässä tapauksessa varmenteita myöntänyt yritys on voinut joutua tietomurron kohteeksi ja kun selain tai käyttöjärjestelmä on seuraavan kerran päivittänyt itsensä, niin kyseisen yrityksen myöntämät varmenteet ovat uhka selaimen näkökulmasta. (Järvinen, 2012, 63) Käyttäjän näkökulmasta hankalaa on se, että eri selaimet näyttävät varmenteen tiedot eri tavoilla.

4.6 Adobe Flash Player

Adoben Flash Player löytyy lähes jokaisesta sitä tukevasta tietokoneesta. Sitä käytetään pääasiassa internetsivuilla olevien videoiden katseluun ja Flashillä toteutettujen sovellusten suorittamiseen, esimerkiksi pelit. Adobe Flash Player ja Adobe Flash eivät ole sama asia. Adobe Flash on tarkoitettu sisällöntuottajien työkaluksi ja sen

avulla voidaan luoda ja editoida flash/shockwave tiedostoja. Tavalliselle käyttäjälle riittää Flash Player, joka on selaimen liitännäinen.

Flash Playerillä on oma muistinsa LSO, Local Shared Object, joka on verrattavissa selaimen evästeisiin. Sen avulla Flash voi tallentaa tietoja paikallisesti käyttäjän tietokoneen kovalevylle ja hakea tietoja sieltä, jos myöhemmin palataan samalle internetsivustolle. Tyypillisiä tallennettavia tietoja voivat olla esimerkiksi sivuston asetukset, kuten se mikä on äänenvoimakkuuden vakioasetus videoissa. Peleissä parhaimmat pisteet ja tallennetut pelitilanteet voivat jäädä Flashin muistiin. Flash käyttää myös väliaikaisia tiedostoja, joten kaikkea ei tallenneta pysyvästi. (Adoben www-sivut, 2013) (Järvinen, 2010, 183)

LSO:hon tallennettuja tietoja voidaan kuitenkin käyttää evästeiden ja web Storagen tapaan käyttäjien tilastolliseen seurantaan. Näin on mahdollista profiloida käyttäjiä ja se voi olla yksityisyyden kannalta huolestuttavaa. Lisäksi on mahdollista, että jos joku pääsee fyysisesti työasemallesi, niin on mahdollista nähdä Flash Playerin sisältämät tiedot, vaikka olisit poistanut kaiken selaimen historiatiedoista. Flashin sisältö pitää erikseen käydä poistamassa Flash Playerin asetuksista. Versiosta 10.1 eteenpäin Flash Player ei enää ole tallentanut tietoja paikallisesti, jos selainta on käytetty yksityisyystilassa. (Wikipedia, 2013) Flash Playerin asetuksia voidaan muuttaa joko ohjauspaneelista tai menemällä selaimella Adobe Flash Setting Manager sivulle. (Macromedian www-sivut, 2013)

WEB & DOM Storage ovat alun perin HTML5- standardissa mukana tulleet tallennustekniikat, jotka ovat pitkälti verrattavissa LSO-muistiin. Niiden avulla voidaan tallentaa huomattavasti enemmän tietoja käyttäjän työaseman kovalevylle verrattuna evästeisiin. (Microsoftin www-sivut, 2013) Erona evästeisiin on myös se, että tätä ”muistia voi käsitellä vain selaimessa paikallisesti, eikä sen sisältöä lähetetä automaattisesti takaisin palvelimelle.”(Järvinen, 2010, 183)

4.7 PDF-Lukija

Useimmissa työasemissa on asennettuna PDF-tiedostojen lukuohjelma. Pdf-lukijat ovat monimutkaisia ohjelmia ja siksi niistä voi jatkuvasti löytyä uusia tietoturvauhkia. Esimerkiksi Adoben Reader tukee JavaScriptiä, jonka avulla on mahdollista suo-

rittaa haitallista ohjelmakoodia. Haavoittuvuuksista johtuen pdf-lukijat tulisi päivittää heti uusien päivitysten ilmestyessä. (Järvinen, 2012, 185)

4.8 Java

”Java tekniikalla voidaan tehdä sovelluksia, jotka toimivat käyttöjärjestelmästä ja prosessorista riippumatta.” (Järvinen, 2012, 184) Java on tietoturvan kannalta ongelmallinen ja jos sille ei ole erityistä tarvetta, niin se kannattaa työasemalta poistaa tai jättää kokonaan asentamatta. Viime aikoina Javasta on löytynyt useita tietoturva-aukkoja ja sen käyttöä ei erityisemmin suositella.(It-viikko.fi, Noloa Oracle..., 2013) Jos Javaa kuitenkin tarvitsee, niin se tulisi päivittää heti, kun uusi päivitys on saatavilla. Useimmiten Java päivittää automaattisesti itsensä, mutta silti kannattavaa on tarkastaa versionumero säännöllisesti.(Järvinen, 2012, 184)

5 SOSIAALINEN MEDIA

Sosiaalisen median perustana on tiedon jakaminen. Oli kyseessä sitten omat henkilötiedot tai mielipiteet, niin jollekin taholle näistä tiedoista voi olla hyötyä. Sosiaalisen median ongelmana on tietosuoja. Mitä enemmän tietoa itsestäsi jaat, sitä vähemmän tietosuojaa on. Tämän vuoksi tulisi tarkkaan harkita mitä tietoja itsestään halutaan kertoa. Saadaanko tiedon luovuttamisesta suurempi hyöty kuin tiedon pitämisestä itsellä? Vaihtoehtoisesti, jos tieto on niin turhaa että sillä ei tee mitään, niin pitääkö sitä silloin jakaa? Jos vastaus on ensimmäiseen kohtaan ei ja toiseen kyllä, niin silloin tietoa voi kohtuullisen huolettomasti jakaa. Tulee kuitenkin muistaa, että useimmat sosiaalisen median palvelut ovat yhdysvaltalaisia ja sikäläisen lainsäädännön alaisia. Tästä johtuen palvelut voivat ”hyödyntää ihmisten henkilökohtaisia tietoja hyvinkin vapaasti, koska maan tietosuojalait ovat väljät.” Tietoja myydään välillisesti esimerkiksi kaupallisille tahoille, jotka haluavat ostaa rajatulle kohderyhmälle suunnattua mainontaa palvelusta. Mikään ei kuitenkaan estä palvelua myymästä tietojaan tulevaisuudessa kolmansille osapuolille. Tulee myös muistaa että tiedon tallentaminen on halvempaa kuin sen poistaminen. Tämän vuoksi esimerkiksi Facebook ei todellisuudessa poista tietojasi, jos poistat profiilisi, se vain piilottaa tietosi. Tällä hetkellä pullonkaulana on tiedon analysointi, ei sen tallentaminen. Kukaan ei tarkkaan tiedä mi-

ten sosiaalisessa mediassa jaettua tietoa tullaan käyttämään ja kenen käsiin se päätyy. (Järvinen, 2012, 294)

Sosiaalisen median riskinä on myös identiteettivarkaudet. Kaverilistoihin eksyy väistämättä vähemmän tuttuja henkilöitä, jonka takia tulisi tarkkaan käydä läpi jokaisen palvelun asetukset. Asetuksista pitäisi ainakin sen verran katsoa ketkä kaikki näkevät palveluun lähetetyt viestit sekä mitkä henkilötiedot ovat näkyvillä. Esimerkiksi kuinka perusteltua on, että Facebookissa kaverien kaverit näkevät sinun päivityksesi? Riippuen palvelun asetuksista on mahdollista selvittää todella paljon eri ihmisistä sekä heidän välisistä suhteistaan. Henkilötietojen, koulutuksen, työpaikan, perheenjäsenten sekä parhaiden kaverien selvittäminen on erittäin helppoa, jos oletusasetuksia ei ole muutettu. Kun riittävästi tietoa on saatavilla, on mahdollista, että joku voi kaapata henkilöllisyytesi ja käyttää sitä vaikka tavaroiden tilaamisen osamaksulla tai pikavippien ottamiseen. Rikolliset voivat myös tehdä osoitteenmuutoksen uhrin nimissä ja näin viivästyttää paljastumista.(Järvinen, 2012, 258) On olemassa myös toisen tyyppinen identiteettivarkaus, joka ei ole lain mukaan rikos. Toisen ihmisen nimellä voidaan esiintyä sekä käyttää hänen oikeita tietojaan että valokuvaa, jos niitä ei käytetä laittomasti. ”Laittomaksi toiminta muuttuu, mikäli sivuilla loukataan toisen kunniaa, levitetään yksityisyydensuojan piiriin kuuluvia tietoja, kiihotetaan kansanryhmää vastaan tai syyllistytään johonkin muuhun laissa kiellettyyn tekoon.” (Järvinen, 2012, 257) Tulee myös muistaa, että paras tapaa jakaa omia kokemuksiaan on vasta sen jälkeen kun tapahtuma on jo tapahtunut. Kertomalla jokaisesta liikkeestäsi reaaliaikaisesti, paljastat samalla sen, että kukaan ei ole kotona ja varkaat saavat tiedon kätevästi sosiaalisen median kautta. Esimerkiksi Facebookin Ticker ominaisuudella pystyy näkemään sellaisia päivityksiä joita muuten ei edes näkisi. Pitämällä hiirtä Ticker palkissa haluamallasi kohdalla voi nähdä sellaisen ihmisen päivityksen jota et edes tunne, kunhan vain ystäväsi on tykännyt tai kommentoinut viestiä.

Valokuvat sisältävät yllättävän paljon tietoa. Digitaalisissa kuvissa EXIF-tiedoista käy ilmi joukko kameran tietoja, kuten sarjanumero sekä valokuvaus teknisiä tietoja. EXIF-tiedoista näkyy myös kuvausajankohta sekä, jos laitteesta löytyy GPS-paikannin, niin myös maantieteelliset koordinaatit. EXIF-tiedot saattavat hävitä, jos kuva avataan kuvankäsittelyohjelmalla. Sosiaalisen median kannalta kannattaa muistaa mitä todellisuudessa tulee jakaneeksi kuvan mukana. Esimerkiksi reaaliaikaiset päivitykset ja kuvan lisäykset palveluun viestittävät varmuudella että ketään ei ole koto-

na, sillä pelkästä kuvasta näkee ajan sekä paikan missä se on otettu. Toisaalta valokuvaajat haluavat ehkä poistaa EXIF-tiedot etteivät kaikki näe heidän kuvausasetuksiaan.(Järvinen, 2010, 118)

Sosiaalisen median yhteydessä tulee myös muistaa, että netti ei unohda. Se mitä olet nyt jakanut voi myöhemmin elämässä osoittautua kiusalliseksi tai siitä voi olla suoranaista haittaa. Esimerkiksi työpaikan haku voi vaikeutua huomattavasti, jos hakijasta löytyy runsaasta epämääräistä tietoa. Toisaalta pelkän oman yksityisyyselämänsä liiallinen levittely voi olla haitallista. Vaikka tilapäivitykset olisivat kuinka harmittomia, niin saattavat ne yrityksen näkökulmasta vaikuttaa siltä, että pysyvätkö edes liikesalaisuudet salassa. Tietojensa jakamista tulee miettiä myös siltä kannalta, että tulevaisuudessa yritykset saattavat yhdistyä ja samalla todennäköisesti yhdistyy myös tietokannat. Esimerkiksi Google uusi palvelunsa keväällä 2012, jonka yhteydessä eri nimillä sekä eri käyttäjäsopimuksilla toimineet palvelut yhdistettiin yhden palvelun ja sopimuksen alle. Samalla ilmoitettiin, että Google yhdistää käyttäjien tiedot, joita oli kerätty eri palveluiden kautta. Vaikka palveluissa oli eri käyttäjäsopimukset, niin Google totesi, että heillä oli jo aiempien käyttäjäsopimuksien kautta oikeus näin tehdä. (Järvinen, 2012, 311)

6 YHTEENVETO

Perusasioina voidaan pitää seuraavia asioita; käyttöjärjestelmä ja virustentorjuntaohjelma tulee päivittää heti, kun uudet päivitykset ovat saatavilla. Lisäksi virustentorjunta ohjelmistossa on syytä säännöllisesti tarkastaa, onko käytössä uusin versio. Etenkin ilmaisissa virustentorjuntaohjelmissa uusin versio kannattaa asentaa heti kun se on saatavilla. Uusimmat versiot on syytä ladata myös kaikkiin muihinkin ohjelmiin, sillä niissä on voitu paikata tietoturva-aukkoja, eikä vanhoille ohjelmille enää tule uusia päivityksiä. Lisäksi työasemalle olisi hyvä tehdä erikseen pääkäyttäjätili ja muille käyttäjille perusoikeudet sisältävä käyttäjätili. Näin kukaan muu ei voi esimerkiksi asentaa ohjelmia ilman pääkäyttäjän salasanaa. Peruskäyttäjät eivät myöskään voi poistaa käyttöjärjestelmälle tärkeitä tiedostoja tai tehdä muutoksia työaseman toimintaan. Myös jokaisen työaseman käyttäjän yksityisyys paranee, kun jokaisella on omalla salasanalla suojattu käyttäjätili. Salasanan tulisi olla aina riittävän pitkä, sisältää isoja kirjaimia, pieniä kirjaimia, numeroita sekä erikoismerkkejä. Tämän lisäksi

käytetyt ohjelmat kuten selain ja sen lisäosat ja liitännäiset esimerkiksi Flash, sähköpostiohjelmisto, pdf-lukija, tekstinkäsittelyohjelmisto jne. tulee aina päivittää uusimpaan versioonsa. Uusin versio tulee ladata ja asentaa aina luotettavasta lähteestä esimerkiksi valmistajan sivuilta. Periaatteessa jokainen ohjelma, joka työasemalla on asennettu, tulee päivittää säännöllisesti. Työasemalla ei tule olla ainuttakaan sellaista ohjelmaa, jota ei käytetä. Käyttämättömät ohjelmat jäävät päivittämättä ja voivat heikentää työaseman tietoturvaa. Työasemaa tulisi siivota säännöllisesti ja poistaa ylimääräiset ohjelmat ja sovellukset. Javaa ei omalle työasemalle kannata asentaa missään muodossa, jos sitä ei välttämättä tarvitse. Jos Java kuitenkin on asennettuna, niin se tulee päivittää heti uusimpaan versioonsa. Uudet päivitykset kannattaa tarkistaa ja asentaa Javan virallisilta kotisivuilta.

Selaimen, kuten kaikkien muidenkin ohjelmien asetukset olisi suotavaa käydä läpi ennen niiden käyttöä. Etenkin sellaiset kohdat joissa tietoa jaetaan tai saatetaan lähettää ulkopuolisille. Esimerkiksi selainasetuksista tulee käydä läpi se kuinka paljon historia tietoja tallennetaan ja kuinka kauan niitä säilytetään. Lisäksi kun selaustietoja poistetaan, on suotavaa valita kaikki kohdat ja tyhjentää koko selaushistoria, jolloin esimerkiksi selaimen välimuistikin tyhjenee. Vaihtoehtona on myös valita, ettei selainhistoriaa tallenneta lainkaan. Näin parannetaan myös omaa yksityisyyttä niitä vastaan, joilla on pääsy työasemallesi. Selainhistoriaa poistaessa tulee myös muistaa tyhjentää Flashin LSO muisti. Tähän on saatavissa Firefox selaimeen BetterPrivacy liitännäinen, jonka avulla Flashin muisti voidaan automaattisesti tyhjentää, kun selain suljetaan (https://addons.mozilla.org/fi/firefox/addon/betterprivacy/). Yksityisyyttään voi parantaa myös siten, ettei anna selaimen tallentaa lomaketietoja tai salasanoja. Etenkin salasanojen tallentaminen selaimeen on tietoturva riski, sillä useimmissa selaimissa salasanat voi nähdä selainasetuksista, jolloin kuka tahansa kenellä on pääsy työasemalle voi ne sieltä kopioida. Turhia liitännäisiä selaimeen ei kannata asentaa, sillä ne voivat kerätä ja lähettää tietoja käyttäjästä. Lisäksi liitännäiset tulee päivittää uusimpaan versioonsa säännöllisesti. Selaimen käyttö paljastaa käyttäjästä paljon tietoja ulkopuolisille, toisin sanoen kaikille niille kenen internetsivuilla liikut. Useat sivut näyttävät mainoksia ja näitä tahoja kiinnostaa sinun mielenkiinnon kohteesi, jotta esimerkiksi mainontaa voidaan kohdistaa paremmin. Tietoja voidaan myös käyttää muuhunkin ja niitä voidaan yhdistellä, jolloin tulevaisuudessa ja jo nyt tietyllä todennäköisyydellä, on mahdollista profiloida yksittäinen käyttäjä.(Electronic Frontier Foundation, Peter Eckersley, 3) Se onko tämän kaltainen kehitys suotavaa, niin jo-

kainen voi vetää siitä omat johtopäätöksensä ja toimia sen mukaan haluaako säilyttää edes jonkin verran omaa yksityisyyttään verkossa. Disconnect liitännäisellä voidaan joitakin jäljittäjiä estää ja näin parantaa hieman omaa yksityisyyttä. (https://disconnect.me/)

Sähköpostia käytettäessä tulee muistaa, että viestit ei ole automaattisesti salattuja. Tämän vuoksi luottamuksellista tietoa ei tulisi lähettää sähköpostin välityksellä. Sähköpostia ei kannata käyttää viestien säilytyspaikkana ja viestejä poistettaessa tulee ottaa huomioon, että viestit voivat vain siirtyä sähköpostin roskakoriin, josta ne voidaan edelleen lukea. Vastausviesteissä tulee huomioida pitkät viestiketjut, ettei vahingossa lähetetä koko ketjua ulkopuolisille. Sähköpostin liitetiedostojen avulla voidaan levittää haittaohjelmia tai viestit voivat ohjata sivuille, jotka houkuttelevat käyttäjän sellaisen työasemalleen asentamaan. Tämän vuoksi tuntemattomalta lähettäjältä saadun viestin linkkejä eikä liitetiedostoja kannata avata.

Sosiaalisessa mediassa ei kannata jakaa itsestään liikaa tietoa. Mitä vähemmän tietoa itsestään jakaa sitä parempi on tietosuoja. Sosiaalisen median avulla voidaan helposti tehdä identiteettivarkauksia, joten kaikkia ei esimerkiksi tule lisätä kaverilistalle. Riskinä on myös, että epärehelliset ihmiset käyttävät hyväkseen päivitystä, jossa kerrottaan, että ollaan lomalla ulkomailla. Sosiaalinen media ei myöskään unohda ja kerran sinne laitetut kuvat voivat olla siellä ikuisesti. Esimerkiksi Facebook ei todellisuudessa poista käyttäjän tietoja, kun tili suljetaan.

Rahaliikenteessä ja verkkopankin käytössä pääsääntönä on, ettei koskaan tule antaa kellekään käyttäjätunnuksia, salasanoja tai avainlukulistoja. Näitä tietoja ei yksikään virallinen taho kysy esimerkiksi puhelimitse tai sähköpostiviestillä. Lisäksi tulee varoa väärennettyjä pankkien verkkosivuja. Väärennetyille sivuille voidaan houkutella esimerkiksi sähköpostiviestien avulla. Pankin sivuille tulee aina siirtyä kirjoittamalla itse verkkopankinosoite osoitekenttään. Verkkopankit ja verkkokaupat käyttävät sertifikaatteja, jotka todentavat palvelun luotettavuuden. Sertifikaatin puuttuminen tai -virheilmoitus on vakava tietoturva uhka eikä sellaista palvelua tule käyttää, jos virheilmoituksen syy ei ole selvä. Rahaliikenne palvelut käyttävät myös SSL-salausta, jonka käyttäjä voi tunnistaa osoitepalkista olevasta https merkinnästä.

Tietoturva muuttuu ja kehittyy jatkuvasti ja uusia tietoturvauhkia löytyy jatkuvasti lisää. Työ on kohtalaisen yleispätevä summaus perustietoturvaan liittyvistä tekijöistä. Työn tulosta voisi hyödyntää myös sellaisissa tutkimuksissa, jossa keskityttäisiin vahvemmin yksityisyyteen ja tietojen keruuseen; missä eri yhteyksissä tietoja voidaan kerätä. Myös lähteissä on paljon sellaista materiaalia, joista saattaisi olla hyötyä tämän kaltaisten tutkimusten tekoon. Maailma digitalisoituu ja kehityksen mukana on pysyttävä. Paluuta menneeseen ei ole ja ajanhermolla on pysyttävä. Satoja miljoonia käyttäjiä houkutelleet sosiaalisen median palvelut tarjoavat varmasti jotain sellaista, josta käyttäjä kokee saavansa konkreettista hyötyä. Digitalisoituminen ei ole tuonut mukanaan pelkkiä uhkia vaan myös mahdollisuuksia esimerkiksi tehokkaampaan työskentelyyn, kommunikointiin ja luonut jatkuvasti uusia palveluja, joiden hyödyt voidaan nähdä suurissa käyttäjä määrissä. Ei kukaan hukkaa aikaa palveluun, joka aiheuttaa vain tietoturvariskejä. Tulee kuitenkin muistaa, että palveluihin laitetut tiedot voivat säilyä ikuisesti. Myös tietojen käyttötarkoitus voi muuttua ja niitä voidaan hyödyntää täysin eri tarkoituksessa kuin mihin ne aluksi oli tarkoitettu. Tulevaisuudessa yksityisyyden merkitys todennäköisesti tulee muuttumaan ja tietojen keruuseen saatetaan suhtautua myönteisemmin, jos niitä kerätään ja käytetään oikein.

LÄHTEET

Adoben www-sivut. Viitattu 9.12.2013
Saatavissa: http://www.adobe.com/security/flashplayer/articles/lso/

Allen, Julia, H. 2002. CERT Verkkotietoturvan Hallinta. Helsinki: Edita Prima Oy

Canavan, John, E. 2001. Fundamentals of Network Security. Artech House INC.

Cole, E., Krutz, R, L., Conley, J, W., Reisman, B., Ruebush, M., Gollman, D., Reese, R. 2008. Network Security Fundamentals. Wiley Pathways.

Conti, Greg. 2008. Googling Security – How Much Does Google Know About You?. Pearson Education Inc.

DLA PIPER. 2013. Data Protection Laws of the World. Käsikirja. Saatavissa: http://www.dlapiper.com/data-protection-laws-of-the-world-handbook-2013/

Greenleaf, G. 2012. Global data privacy laws: 89 countries, and accelerating.

Electronic Frontier Foundation, Peter Eckersley. How Unique Is Your Web Browser?

Hakala, Mika., Vainio, Mika., Vuorinen, Olli. Tietoturvallisuuden Käsikirja. Porvoo: WS Bookwell

Helsingin Sanomat 20.6.2012. Miehen epäillään vakoilleen nuorten naisten tietokoneita haittaohjelmalla. 2012. Viitattu 24.10.2013 Saatavissa:http://www.hs.fi/kotimaa/a1305575672991

It-viikko.fi verkkosivut. Viitattu: 6.1.2014. Saatavissa:http://www.itviikko.fi/tietoturva/2013/04/24/noloa-oracle-javasta-loydettiin-taas-uusi-tietoturva-aukko/20135942/7

Järvinen, Petteri. 2012. Arjen Tietoturva. Jyväskylä: Docento Finland Oy

Järvinen, Petteri. 2010. Yksityisyys - Turvaa Digitaalinen Kotirauhasi. Jyväskylä: Docento Finland Oy

Linux.fi. 2013. viitattu: 19.11.2013. saatavissa: http://linux.fi/wiki/WWW-selaimet

Macromedian www-sivut. Viitattu: 9.12.2013. Saatavissa: http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

Microsoftin www-sivut. Viitattu: 9.12.2013. Saatavissa: http://msdn.microsoft.com/en-us/library/bg142799%28v=vs.85%29.aspx

Mika Myllylän kuolema: 90 poliisia ja virkamiestä saa syytteen urkinnasta. 2013. Uusi Suomi 10.6.2013. Viitattu 24.10.2013. Saatavissa:http://www.uusisuomi.fi/kotimaa/59842-mika-myllylan-kuolema-90-poliisia-ja-virkamiesta-saa-syytteen-urkinnasta

Paukku, Timo. 2013. Hanki dataa – hankit samalla valtaa. Helsingin Sanomat. Saatavissa: http://www.hs.fi/tiede/a1367563011999

Ruokangas, P. 2013. Poliisi: Nainen katseli 150 potilaan tietoja luvatta. Yle.fi 17.1.2013. Viitattu 24.10.2013. Saatavissa:http://yle.fi/uutiset/poliisi_nainen_katseli_150_potilaan_tietoja_luvatta/6455955

Secmeter.com. 2013. Viitattu 25.11.2013. Saatavissa: http://www.secmeter.com/viestintasalaisuus.html

Sähköisen viestinnän tietosuojalaki, 2 Luku, 4§, Viestin, tunnistamistietojen ja paikkatietojen luottamuksellisuus. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2004/20040516

Tilastokeskus. Väestön tieto- ja viestintätekniikan käyttö-tutkimus 2013. Saatavissa: http://www.stat.fi/til/sutivi/2013/sutivi_2013_2013-11-07_tie_001_fi.html

Tutkimus. Queen Mary University of London, School of Law. Legal Studies Research Paper No. 98/2012. Saatavissa: http://ssrn.com/abstract=2000034

Työntekijä katsoi luvatta 188 potilaan tietoja Keski-Suomen keskussairaalassa. 2013. Helsingin Sanomat 21.10.2013. Viitattu 24.10.2013. Saatavissa:http://www.hs.fi/kotimaa/Ty%C3%B6ntekij%C3%A4+katsoi+luvatta+188+potilaan+tietoja+Keski-Suomen+keskussairaalassa/a1382321003196

Varo, voit itse nostaa hintoja verkkokaupassa. 2012. Kauppalehti 03.07.2012. Viitattu 24.10.2013. Saatavissa: www.kauppalehti.fi/etusivu/varo,+voit+itse+nostaa+hintoja+verkkokaupassa/201207208011

Wikipedia.org. 2013. Viitattu 22.11.2013. Saatavissa:

https://en.wikipedia.org/wiki/Email

Wikipedia.org. 2013. Viitattu 28.11.2013. Saatavissa:
https://en.wikipedia.org/wiki/Adobe_Flash_Player

Wikipedia.org. 2013. Viitattu 28.11.2013 Saatavissa:
https://en.wikipedia.org/wiki/Web_storage

Wikipedia 2013. Viitattu 14.10.2013. Saatavissa:
https://fi.wikipedia.org/wiki/Tietoturva#Yleinen_tietoturvallisuus

Wikipedia.org. 2013. viitattu: 20.11.2013 saatavissa:
https://en.wikipedia.org/wiki/Web_browser

Wikipedia.org 2013. Viitattu 23.10.2013. Saatavissa:
https://fi.wikipedia.org/wiki/V%C3%A4limuisti