HAAGA-HELIA
ammattikorkeakoulu

Peruskäyttäjän tietoturva verkkopalveluissa

Juha Tuukkanen

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2015

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

16.4.2015

Tekijä(t)
Juha Tuukkanen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Peruskäyttäjän tietoturva verkkopalveluissa

Sivu- ja liitesivumäärä
38 + 1

Opinnäytetyön aiheena oli tutkia peruskäyttäjän tietoturvaa käyttäjätunnistusta hyödyntävissä verkkopalveluissa. Verkkopalveluiden määrä sekä monimuotoisuus kasvavat jatkuvasti ja käyttäjätunnistuksen tietoturvaratkaisut vaihtelevat runsaasti eri palveluiden välillä. Peruskäyttäjän tietoturvallisuutta uhkaavat verkossa monet tekijät. Riippuen verkkopalvelun luonteesta, tietoturvalla voi olla suora suhde käyttäjän yksityisyyteen. Verkkopalveluun annetut tiedot saattavat päätyä julkisiksi verkossa esim. tietovuodon yhteydessä. Tämä vaarantaa peruskäyttäjän tietoturvan myös muissa verkkopalveluissa, mutta tapahtuneen vahingon hahmottaminen on yleensä uhriksi joutuneelle vaikeaa.

Työssä tarkastellaan miten peruskäyttäjä voi hahmottaa tarvitsemansa tietoturvan tason ja siihen liittyvät epäkohdat käyttämässään verkkopalvelussa, sekä millaisia ovat hyvät käyttäjävarmennuskäytännöt käytännössä peruskäyttäjän ja verkkopalvelun toteuttajan näkökulmista.

Työssä tutkitaan ja vertaillaan käyttäjänäkökulmasta kolmea kansallisesti suosittua verkkopalvelua liittyen niiden ratkaisuihin käyttäjän tunnistuksessa ja tietoturvassa. Palvelujen tarkastelu tehdään siitä näkökulmasta mitä ulkopuoliselle käyttäjälle niistä on havaittavissa.

Työssä tarkastellaan käyttäjän tietoturvan lainsäädännöllistä näkökulmaa, pyritään kuvaamaan mitä verkkopalvelulta vaaditaan käyttäjiensä tietojen asialliseen turvaamiseen, koostetaan tietoturvaohjeistus verkkopalveluiden peruskäyttäjälle, sekä hahmotellaan mihin elementteihin voisi perustua verkkopalveluiden yleinen tietoturvakriteeristö.

Asiasanat
Tietoturva, verkkopalvelut, sähköinen tunnistaminen, kyberturvallisuus

Abstract

Authors
Juha Tuukkanen

Degree programme
Degree programme in Information Technology

The title of thesis
User security in web services

Number of report pages and attachment pages
38 + 1

The subject of the thesis is to examine the information security principles of the basic web user in services that utilize user authentication. The amount and diversity of web services are growing constantly and the methods of user authentication principles vary. The online information security of the basic web user faces many threats. Depending on the nature of the online service, information security can be directly related to the privacy of the user. This thesis examines how the basic web user can comprehend the needed security level and possible security shortcomings in a web service. The thesis also examines from the web developer's perspective the methods which make up adequate and good user authentication and security practices in web services.

This thesis includes a theory section and an empirical section. The theoretical background information was gathered to explain the main topics and concepts related to the subject of online security practices. The empirical part of the thesis was executed by conducting a review of the user authentication methods of three popular Finnish online services. The online services were reviewed based on the information visible to the basic user.

The objective of the thesis was also to examine the legislative aspects of information security and to describe what is required from an online service to adequately secure user information. This thesis also compiles a set of instructions for the basic user in regards to personal online security.

Key words
Information security, online services, user authentication, cybersecurity

Sisällys

1 Johdanto

Opinnäytetyöni käsittelee peruskäyttäjän tietoturvaa verkkopalveluissa.

Verkkopalveluiden määrä ja monimuotoisuus kasvaa jatkuvasti. Palveluiden tietoturva-, sekä käyttäjätunnistusratkaisuja on monenlaisia. Joissain palveluissa käyttäjän tietojen turvaaminen voi olla toissijaista, joissain äärimmäisen tärkeää. Peruskäyttäjän hahmotus omasta tietoturvastaan, sekä verkkokäyttäytymisensä suhteesta siihen, voi usein olla pinnallista ja hataralla pohjalla.

Käyttäjätunnistusratkaisujen valinnassa palveluntarjoajalle merkitsevät monet tekijät taloudellisista realiteeteista käytettävyyteen. Keskimääräistä monimutkaisemmat käyttäjän varmistusratkaisut ovat toteutukseltaan ja ylläpidoltaan kalliimpia ja saattavat myös nostaa palvelun käyttökynnyksen liian korkeaksi. Usein käyttäjät eivät osaa vaatia palvelulta asianmukaisia tietoturvakäytäntöjä, vaan pikemminkin haluavat palvelun olevan mahdollisimman helppokäyttöinen.

Viime vuosina yksi tietoturvaa uhkaava trendi on ollut laajat käyttäjätunnusten vuodot verkkosivustoilta. Yksikin huonon tietoturvatason omaava sivusto voi vaarantaa käyttäjiensä tietoturvan kaikissa verkkopalveluissa. Peruskäyttäjä ei välttämättä ymmärrä mikä merkitys vuodolla on jos itse on tietovuodossa uhrin roolissa. Viestinnästä esim. käyttäjätunnusten vuototapauksissa vastaa viestintäviraston kyberturvallisuuskeskus. Omaehtoista viestintää vuodon kohteeksi joutuneen palvelun osalta rajoittaa usein häpeäkokemus vuodon kohteeksi joutumisesta. Julkisuuteen tulleet tapaukset ovat paljastuneet yleensä siinä vaiheessa kun käyttäjätunnukset on jo julkisessa jaossa. Saattaa olla myös tapauksia, sivustoja, joissa tietomurto on tapahtunut, mutta tätä ei ole tuotu julkisuuteen tai edes havaittu.

Työllä ei ole toimeksiantajaa. Aihe kiinnostaa itseäni koska käyttäjätunnistusta edellyttävien verkkopalveluiden tietoturvatasoille ei ole yleistä kriteeristöä, varsinkaan niin että peruskäyttäjä voisi arvioida omalta kohdaltaan mikä on käyttämänsä verkkopalvelun tietoturvan taso. Usein käyttäjän tietoturvallisuuden heikoin lenkki on käyttäjä itse, mutta palveluita suunnitellessa on myös mahdollista minimoida käyttäjän mahdollisuudet aiheuttaa itselleen haittaa. Verkkopalveluiden lisääntyessä myös monet henkilökohtaiseen tietoturvallisuuteen liittyvät näkökulmat ovat käyttäjille epäselviä. Näen epäkohtia verkkopalveluiden olemassa olevissa tietoturvakäytänteissä, sekä tiedotuksessa esim. liittyen tietomurtoihin. Pyrin työssä selventämään hyviä tietoturvakäytänteitä peruskäyttäjän, sekä palveluiden suunnittelun näkökulmista.

1.1 Tavoitteet, tutkimusongelma ja rajaus

Opinnäytetyö pyrkii vastaamaan kysymyksiin: ”Mikä on nykyisen lainsäädännön suhde peruskäyttäjän tietoturvaan ja sen takaamiseen verkkopalveluissa?”, ”Miten peruskäyttäjä voi arvioida käyttämänsä verkkopalvelun tietoturvan tason ja luotettavuuden?”, ”Mitkä ovat verkkopalveluiden käyttäjätunnistuksen metodien ja yleisen tietoturvan heikkoudet sekä vahvuudet?”. ”Miten peruskäyttäjä voi parantaa henkilökohtaista tietoturvaansa eri verkkosivustoja käyttäessään?”, ”Mitkä ovat yleisimpiä peruskäyttäjän tietoturvan vaarantavia tekijöitä?”, sekä ”Millainen voisi olla peruskäyttäjille suunnattujen verkkopalveluiden tietoturvatason kriteeristö?”.

Tämän työn tarkastelun ulkopuolelle rajataan pankki-, mobiili-, sekä sirukorttivarmennuksia käyttävät palvelut. Näiden osalta tietoturvataso on oleellisesti korkeampi suhteessa käyttäjätunnuksella ja salasanalla käyttäjävarmistusta suorittaviin palveluihin, vaikkakin pankki- yms. palveluihin liittyen käyttäjien tietoturvaa koetellaan jatkuvasti.

Työssä ei tarkastella erityisesti yritysten tietoturvaratkaisuja, vaan työ keskittyy tarkastelemaan peruskäyttäjän henkilökohtaista tietoturvaa, vaikka se onkin usein sidoksissa myös käyttäjän työnantajan tietoturvallisuuteen.

Tämän opinnäytetyön tulokset voivat olla hyödyllisiä sekä peruskäyttäjälle että verkkopalveluja ja etenkin niiden tietoturvaratkaisuja suunnittelevalle taholle. Työ tarjoaa tietopaketin hyvistä käytänteistä verkkopalvelujen ja yksityisen käyttäjän tietoturvallisuuteen liittyen.

1.2 Työn rakenne

Opinnäytetyö jakautuu kahdeksaan lukuun. Luvuissa 2 – 4 muodostetaan teoreettinen viitekehys aiheesta. Teoriatausta keskittyy tietoturvan perusteiden määrittelyyn ja käyttäjävarmennuskäytänteisiin. Luvussa 5 esitellään esimerkkeinä kolmen eri verkkosivuston käyttäjävarmennusratkaisut. Luku 6 käsittelee peruskäyttäjän mahdollisuuksia arvioida käyttämänsä verkkopalvelun tietoturvaratkaisuja, sekä sisältää peruskäyttäjän ohjeiston hyvän tietoturvan takaamiseksi. Luvussa 7 pohditaan hypoteettisesti millainen voisi olla verkkopalvelujen tietoturvakriteeristö ja millaiset hyvät tietoturvaratkaisut siinä tulisi huomioida. Luku 8 sisältää yhteenvedon ja johtopäätökset aiheesta, sekä arvioidaan omaa työskentelyä ja oppimista opinnäytetyöprosessin aikana.

2 Tietoturva

Tietoturvalla tarkoitetaan tietojen, tietokoneiden ja tietoliikenteen suojaamista erilaisia uhkia vastaan. Uhkia aiheuttavat esimerkiksi laiteviat, ohjelmiston virheet ja tietovälineiden turmeltuminen, mutta myös ilkivalta ja rikollisuus. (Korpela, 2005:10)

Tässä luvussa käsitellään tietoturvan määritelmää, sekä kerrotaan lainsäädännöstä verkkopalveluihin liittyen.

2.1 Tietoturvan määritelmä

Tietoturvallisuuden klassinen määritelmä koostuu kolmesta osatekijästä

- luottamuksellisuus
- käytettävyys
- eheys.

Luottamuksellisuus tarkoittaa tietojärjestelmän tietojen olemista vain niihin oikeutettujen henkilöiden käytettävissä. Luottamuksellisuutta ylläpidetään suojaamalla tietojärjestelmät käyttäjätunnuksin ja salasanoin. Arkaluontoisia tai erityisen arvokkaita tietoja voidaan suojata salaamalla ne salakirjoitusmenetelmin. (Hakala, Vainio & Vuorinen 2006: 4)

Käytettävyydellä tarkoitetaan sitä, että tiedot ovat tietojärjestelmässä saatavissa oikeassa muodossa ja riittävän nopeasti. Käytettävyyttä ylläpidetään pitämällä huolta siitä, että tieto- ja tietoliikennejärjestelmien laitteet ovat tarpeeksi tehokkaita, sekä että käytettävät ohjelmistot soveltuvat järjestelmään tallennettujen tietojen käsittelyyn mahdollisimman hyvin. (Hakala, Vainio & Vuorinen 2006: 4)

Eheydellä tarkoitetaan laajasti ymmärrettynä sitä, että tiedot pitävät paikkansa eivätkä ne sisällä tahallisia tai tahattomia virheitä. Eheyden varmistamiseen pyritään pääasiassa ohjelmistoteknisillä ratkaisuilla, ohjelmoimalla järjestelmiin syöttörajoitteita ja tarkistuksia, sekä tallennus- ja tiedonsiirto-operaatioihin tiivisteitä tai varmistussummia. Laitteistotasolla pyritään virheiden estoon käyttämällä esim. virheenkorjaavia muisteja tai väyliä. Tietoliikenneratkaisuissa voidaan käyttää virheen tunnistus- ja korjausmekanismeilla varustettuja protokollia ja laitteita. (Hakala, Vainio & Vuorinen 2006: 4-5)

Tietoturvallisuuden klassinen määritelmä sisältää olennaiset osat joista on huolehdittava ennen muita tietoturvallisuuden osatekijöitä. Klassista määritelmää voidaan pitää riittämättömänä, koska se ei ota huomioon riittävästi tiedon tuottajan tai omistajan identiteettiä, eikä se huomioi laitteistojen tai tieto- ja tietoliikennejärjestelmän arvoa.

Klassisen määritelmän lisäksi tietoturvallisuus kokonaisuutena voidaan jakaa kahdeksaan pienempään eri osa-alueeseen, jotka ovat:

- hallinnollinen turvallisuus
- fyysinen turvallisuus
- henkilöstöturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- laitteistoturvallisuus
- tietoliikenneturvallisuus
- käyttöturvallisuus.

(Hakala, Vainio & Vuorinen 2006: 10)

Hallinnollisella turvallisuudella varmistetaan tietoturvan johtamista ja kehittämistä. Fyysiseen turvallisuuteen kuuluu rakennusten tilojen ja niihin sijoitettujen laitteiden suojaaminen fyysisiltä uhkilta. Henkilöstöturvallisuudella tarkoitetaan niitä toimia, joilla varmistetaan tietojärjestelmän käyttäjien toimintakyky, sekä rajataan heidän mahdollisuuksiaan käyttää tietoja ja tietojärjestelmiä. Ohjelmistoturvallisuuteen kuuluu ohjelmistoihin liittyvät seikat, mm. ohjelmistojen yhteensopivuudet, päivitys ja testaus. Tietoaineistoturvallisuuteen kuuluu tietojen varmistamiseen, säilyttämiseen, palauttamiseen ja tuhoamiseen liittyvät toimet. Laitteistoturvallisuus käsittää tietokoneiden ja muiden järjestelmään kytkettyjen laitteiden tarkoituksenmukaisen mitoituksen, toiminnan testauksen, huollon järjestämisen sekä varautumisen laitteiden kulumiseen ja vanhentumiseen. Tietoliikenneturvallisuudessa pyritään huolehtimaan tiedonsiirtoratkaisujen, kuten lähi- ja laajaverkkoyhteyksien sekä muiden viestijärjestelmien turvallisuudesta. Käyttöturvallisuus käsittää päivittäisten toimintojen ja rutiinien turvaamisen, ja se sisältää kaikki manuaalisen ja automaattisen tietojenkäsittelyn suojatoimenpiteet, kuten salasanojen hallinnoinnin ja järjestelmien valvonnan. (Hakala, Vainio & Vuorinen 2006: 10-12)

Tietoturvallisuuden kanssa kulkee rinnakkain käsite tietosuoja, joka on vakiintunut nimitys henkilötietojen suojalle. Tietosuojalla tarkoitetaan yksityistä ihmistä koskevia tietoja, esimerkiksi ihmisen nimeä, puhelinnumeroa, perhesuhteita, lempiruokaa, tulojen määrää ja terveystietoja. Tietosuoja pyrkii takaamaan henkilölle oikeuden yksityisyyteen, sekä estämään henkilön tietojen tarpeettoman tai epäasiallisen käytön. Osa henkilötiedoista on erittäin arkaluonteisia, osa sellaisia joita joudumme kertomaan usein. Tietosuojan käsitteen tilalla käytetään välillä suunnilleen samaa tarkoittavaa käsitettä yksityisyys. Tietojärjestelmissä ja verkkopalveluissa tietosuojan tarkoituksena on ohjata rekisterinpitäjiä asianmukaiseen henkilötietojen käsittelytapaan ja turvata tiedon kohteen yksityisyyttä, etuja ja oikeuksia. (Korpela, 2005)

2.2 Mitä Suomen lainsäädäntö peruskäyttäjän tietoturvasta verkkopalveluissa

Kuka tahansa kansalainen voi perustaa verkkosivuston yksinkertaisella tilausmenettelyllä verkossa. Mikäli halutaan rekisteröidä uniikki verkko-osoite, rekisteröijää pyydetään ilmoittamaan nimensä sekä muut yhteystiedot. Tämän jälkeen perustaja saa haltuunsa osoitteen ja verkkosivuston tilan, jonne hän voi esimerkiksi asentaa valmiin sisällönhallintatyökalun jolla esimerkiksi verkkofoorumin tai verkkokaupan ylläpitäminen onnistuu. Missään kohtaa ei käyttäjä verkkosivuston perustamisprosessissa joudu tekemisiin lainsäädännön kanssa, joka sanelisi pelisäännöt siitä miten esimerkiksi henkilörekisteriä ylläpidetään ja miten sen turvallisuus taataan. Yksityisten verkkosivustojen ylläpidon suhteen lainsäädäntöön liittyvät asiat ovat useimmiten korkeintaan muodollisuus, liittyen rekisteriselosteen ylläpitoon.

Verkkopalveluiden tietoturvallisuuden määrittely lainsäädännön osalta lähtee tilanteesta jossa sivusto käsittelee tai luetteloi käyttäjiä ja heidän tietojaan. Peruskäyttäjän kannalta olennaista on, että Suomen lakia sovelletaan henkilötietojen käsittelyyn, jossa rekisterinpitäjän toimipaikka on Suomen alueella tai muutoin Suomen oikeudenkäytön piirissä.

Verkkopalvelun ylläpitäjään soveltuu laissa mainitusti ”Rekisterinpitäjän tulee käsitellä henkilötietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa sekä toimia muutoinkin niin, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta.”

Laissa mainitaan että ”henkilötietoja saa käsitellä ainoastaan rekisteröidyn yksiselitteisesti antamalla suostumuksella.” Tämä varmistetaan verkkopalvelun käyttösopimuksella.

Verkkopalvelun ylläpitäjän velvollisuudesta rekisterinpitäjänä mainitaan laissa:
”Rekisterinpitäjän on laadittava henkilörekisteristä rekisteriseloste, josta ilmenee:
1) rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot;
2) henkilötietojen käsittelyn tarkoitus;
3) kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä;
4) mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö tietoja Euroopan unionin tai Euroopan talousalueen ulkopuolelle; sekä
5) kuvaus rekisterin suojauksen periaatteista.
Rekisterinpitäjän on pidettävä rekisteriseloste jokaisen saatavilla.”
Em. lainaus tarkoittaa siis julkisesti ylläpidettävää selostetta siitä, mitä tietoja verkkosivustolla käyttäjistä tallennetaan, mihin niitä luovutetaan, sekä miten tietoja suojataan.

Tietomurrosta lainsäädännössä mainitaan:
”Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.”
Lainsäädäntöön tietomurrosta liittyy oleellisesti verkkopalvelun ylläpitäjän velvollisuudet, tunnistetietojen luovuttamiseen viranomaiselle, rikoksen selvitystä varten pyydettäessä. Tietomurron osalta myös yritys on rangaistava.”

Viestintäsalaisuuden loukkaukseksi lainsäädännössä käsitetään
” Joka oikeudettomasti
1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka
2) hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta, on tuomittava viestintäsalaisuuden loukkauksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Yritys on rangaistava.”

Viimeisen 20 vuoden aikana tietoverkkoihin ja tietoyhteiskunnan muihin osa-alueisiin liittyen lainsäädäntöön on tehtyä lukuisia lisäyksiä. Lainsäädäntö on muuttumassa. Eri lait ja säännökset on kerätty yhden Tietoyhteiskuntakaari-lain alle. Hallitus hyväksyi tietoyhteiskuntakaaren sisällön 6. marraskuuta 2014, ja se tulee pääosin voimaan 1. tammikuuta 2015. (Liikenne- ja viestintäministeriö 2014)

Tietoyhteiskuntakaareen on koottu seuraavat lait

- Viestintämarkkinalaki
- Sähköisen viestinnän tietosuojalaki
- Verkkotunnuslaki
- Laki radiotaajuuksista ja telelaitteista
- Laki lapsipornografian levittämisen estotoimista
- Laki televisio- ja radiotoiminnasta
- Laki eräiden suojauksen purkujärjestelmien kieltämisestä
- Laki eräiden radiotaajuuksien huutokaupoista.

”Tietoyhteiskuntakaariesitys sisältää 360 pykälää. Nyt voimassa olevista säädöksistä on poistetty päällekkäisyydet ja sääntelyä on selkeytetty.” (Liikenne- ja viestintäministeriö 2014)

Yksi verkkopalveluihinkin liittyvä, lainsäädännöllinen ongelma on, ettei yksityiselle henkilölle toisena henkilönä esiintymistä, eli identiteettivarkautta, ole kriminalisoitu. Julkiselle viranomaiselle, esimerkiksi poliisille toisena henkilönä esiintyminen on kriminalisoitu. Sekä reaali- että virtuaalimaailmassa toiselle henkilölle voi valehdella olevansa joku muu ilman että väitteestä suoraan seuraisi mitään. Identiteettivarkauksiin liittyvät ongelmat ovat lainsäätäjien tiedossa. Oikeusministeriön työryhmä on toukokuussa 2014 saanut valmiiksi mietinnön EU:n tietoverkkorikosdirektiivin edellyttämistä lainsäädännön muutoksista. Samassa yhteydessä identiteettivarkaus kriminalisoitaisiin itsenäisenä rikoksena.

2.3 Tietoturvaan liittyvä lainsäädäntö Euroopassa

Tietoverkkorikoksiin liittyvä kansainvälinen lainsäädäntö on ollut intensiivisen kehittämisen kohteena. Keskeisimpänä kansainvälisenä kohteena voidaan pitää Euroopan neuvoston piirissä laadittua tietoverkkorikossopimusta, joka on esikuvana tietoverkkorikosdirektiiville. Tietoverkkorikollisuuden maailmanlaajuisen ja korostetusti rajat ylittävän luonteen vuoksi tavoitteena on että mahdollisimman moni valtio myös Euroopan neuvoston ulkopuolelta liittyisi tietoverkkorikosdirektiiviin. Kaikki EU:n jäsenvaltiotkaan eivät ole siihen vielä liittyneet, joten tämän direktiivin voidaan olettaa tukevan myös kyseisten valtioiden liittymistä yleissopimukseen. (Oikeusministeriö 2014)

Euroopan unionissa on valmisteltavana yleinen tietosuoja-asetus. Sen tavoitteena on mm. tietosuojan globaalin ulottuvuuden huomioiminen sekä tietosuojasääntöjen täytäntöönpanon valvonnan tehostaminen. Asetuksen tarkoituksena on patistaa rekisterinpitäjiä ja yrityksiä tarkistamaan tietosuojakäytäntönsä lainmukaisuuden. Yritysten tulisi myös varmistaa tietoturvatasonsa riittävyys ja varautua ongelmatilanteisiin. Tietosuoja-asetuksella pyritään ohjaamaan yhteisöjä ja yrityksiä ottamaan tietosuoja-asiansa huomioon kokonaisvaltaisesti toimintansa suunnittelussa. Ehdotettu tietosuoja-asetus koskisi henkilötietojen käsittelyä riippumatta siitä, onko rekisterinpitäjä yksityisen vai julkisen sektorin toimija. Velvoitteensa laiminlyöville rekisterinpitäjille voidaan langettaa merkittäviä rangaistusmaksuja. Asetuksen tullessa voimaan, tulee myös Suomessa arvioitavaksi uudelleen kansallinen erityislainsäädäntö, koska se ei voi olla ristiriidassa asetuksen kanssa. Mm. Google, Amazon, Facebook, sekä muut globaalit toimijat joutuvat huomioimaan toimintansa osalta eurooppalaisen sääntelyn. Asetus kohdistuu oleellisin osin suuriin toimijoihin, ja sen tavoitteena on luoda riittävä pelote, jotta kansalaisen yksityisyyttä turvaava lainsäädäntö otetaan vakavasti. Kun asetus hyväksytään lopullisesti, suomalaisilla organisaatioilla on kaksi vuotta aikaa sopeuttaa toimintansa EU:n tietosuoja-asetuksen vaatimusten mukaiseksi. (Andreasson, Koivisto, Ylipartanen 2014)

2.4 Viranomaisten suhtautuminen käytännössä

Tietotekniikan ja tietoverkkojen käytön lisääntyessä on myös niiden hyödyntäminen laittomassa toiminnassa lisääntynyt. Suuntaus jatkuu tasaisesti eri palvelujen siirtyessä jatkuvasti enenevässä määrin Internetiin ja mobiiliverkkoihin. Valtioiden rajat eivät enää ole rajoittavana tekijänä verkkorikollisuudessa. Tietotekniikkarikoksen käsite on arkipäiväistynyt. Rikoksen tekeminen tietotekniikkaa hyödyntämällä ei välttämättä vaadi minkäänlaisia erityistaitoja. Itse rikokset ovat usein normaaleja petoksia, kavalluksia, sekä muunlaisia omaisuuteen kohdistuvia rikoksia. Verkkorikollisuudessa yleisin motiivi on taloudellisen hyödyn saaminen. (Keskusrikospoliisi 2014b)

”Tietotekniikkarikoksilla tarkoitetaan sekä
1) tietotekniikkaan ja tietoverkkoihin kohdistuvia rikoksia että
2) tietotekniikkaa ja tietoverkkoja hyväksi käyttäen tehtyjä rikoksia.
Tietotekniikkaan ja tietoverkkoihin kohdistuvia rikoksia ovat esimerkiksi tietomurrot, haittaohjelmien avulla tehdyt tietojen kaappaukset ja erilaiset verkkohyökkäykset. Tietotekniikkaa ja tietoverkkoja hyväksi käyttäviä rikoksia voivat olla lähes mitkä tahansa rikokset, joiden tekemisessä on käytetty tietotekniikkaa eri tavoin hyväksi.” (Keskusrikospoliisi 2014b)

Tietoliikennerikokset sekä muutoin tietoliikenneyhteyksiä hyödyntäen tehdyt rikokset ovat rikollisuusympäristön uusin ja vakavin uhka. Tietotekniikka- ja tietoverkkorikollisuuden on arvioitu yleistyvän Suomessa lähivuosina. (Muttilainen, Huotari 2014)

Esimerkiksi ulkomailta käsin suoritettavissa huijauksissa poliisin mahdollisuudet auttaa peruskäyttäjää ovat valitettavan vähäiset. Juttujen onnistunut selvittäminen ja menetettyjen rahojen takaisin saaminen on hankalaa, koska Suomen poliisilla ei ole toimivaltuuksia Suomen valtion rajojen ulkopuolella. Poliisi voi ainoastaan pyytää virka-apua kyseessä olevan maan poliisivoimilta. Tämä tie on usein hidas eikä kaikissa maissa tuota toivottua lopputulosta. (Keskusrikospoliisi 2014a)

Tietotekniikkarikoksen tunnusmerkistö täyttyy, kun loukataan tietojenkäsittelyrauhaa. Tietojenkäsittelyrauha on verrannollinen kotirauhan käsitteeseen. Laki suojaa tietojenkäsittelyrauhaa eli tiedon käytettävyyttä, eheyttä ja luottamuksellisuutta. Tietotekniikkarikosten määrittely tulee rikoslaista. Kun ilman lupaa käyttää toisen henkilön käyttäjätunnusta ja salasanaa tai muutoin ylittää saamansa käyttäjäoikeudet, syyllistyy tietomurtoon. Esimerkiksi tietomurron yrityksen tunnusmerkistö täyttyy viattomalta tuntuvaa porttiskannausta suoritettaessa. Tietomurtorikoksessa ei tarvitse onnistuneesti murtaa mitään, vaan rikos

tapahtuu, kun ylitetään omat oikeudet tai käytetään luvatta toisen oikeuksia. Rikoslaki säätää tietomurrosta rangaistukseksi sakkoa tai enintään yhden vuoden vankeutta. Jos tekijä pääsee luvatta tunkeutumaan toisen henkilön tietokoneelle, tekoa katsotaan useimmiten muuna rikoksena kuin tietomurtona. Rikoksen määrittely tulee siitä mitä tekijä toisen koneessa luvatta tekee. Nämä rikokset ovat yleensä asianomistajarikoksia, joka tarkoittaa että poliisi voi aloittaa tutkinnan vasta, mikäli asianomistaja tekee rikosilmoituksen ja vaatii tekijälle rangaistusta. Tietokoneen ja tietoverkkojen peruskäyttäjän tärkein sääntö on se, että jos jokin on kiellettyä verkon ulkopuolella, on se kiellettyä myös verkossa. (Keskusrikospoliisi 2014c)

Vaikka salasanan varastaminen ja toisen käyttäjän verkkopalvelutilin luvaton käyttö katsotaan useimmiten rikolliseksi tietomurroksi, viranomaisten käytännön ohje tällaiseen tapaukseen liittyen on useimmiten salasanojen vaihtaminen käyttäjän käyttämiin palveluihin. Viranomaisten tulee opastaa tietomurron kohteeksi joutunutta tekemään rikosilmoituksen, mikäli henkilö kokee että on joutunut laittoman toiminnan uhriksi. Useimmiten nämä rikosilmoitukset eivät kuitenkaan johda tutkintaan, ellei kyseessä ole käyttäjälle aiheutunut merkittävä taloudellinen haitta, tai muu tietomurrosta välillisesti aiheutunut merkittävämpi rikos. Silti tietosuojan loukkaus, missä murtautuja on päässyt käsiksi käyttäjän yksityisiin tietoihin, dokumentteihin tai esimerkiksi kuvagalleriaan, sekä mahdollisesti jakanut näitä tietoja julkisessa verkossa, voi aiheuttaa murron kohteeksi joutuneelle suuriakin henkisiä kärsimyksiä tai mainehaittaa. Usein verkkopalveluiden sijainti toisessa maassa vaikeuttaa poliisin selvitystyötä tietotekniikkarikosten osalta oleellisesti.

Jos ajatellaan reaalitilannetta esimerkiksi massatietovuotojen kautta, missä kymmeniä tuhansia käyttäjätunnuksia ja salasanoja julkiseksi vuodettaessa myös tietomurtojen määrä voi olla tuhansia. Tällaisen tietomurtomäärän edessä, mikäli jokainen murron kohteeksi joutunut tekisi asiasta rikosilmoituksen, poliisi on resursseissaan melko voimaton. Näin ollen voitaisiin sanoa että tietomurtojen osalta lain toteutuminen yksityishenkilön osalta on verrannollinen vaikkapa liikenteessä punaisia valoja päin kävelemiseen. Teko on laissa säädetty rikoksena, mutta tosiasiassa viranomaisilla ei ole resursseja valvontaan.

3 Peruskäyttäjän kohtaamat uhkat verkossa

Moni peruskäyttäjä ajattelee virheellisesti tietokoneensa sisällön olevan merkityksetöntä ulkopuolisille, tai ettei kukaan halua murtautua käyttäjän laitteeseen. Kun koneen kovalevy meneekin sekaisin, huomataan että siellä oli yhtä ja toista korvaamatonta. Tietokone voi jumittua siten että korjaamiseen tarvitaan kallista asiantuntijatyötä. Tietokonevirus saattaa levittää yksityisen päiväkirjan ympäri maailmaa ihmisten naureskeltavaksi. Rikolliset yrittävät kaapata suuren määrän kotitietokoneita hyökkäystensä ja hyväksikäyttönsä välineeksi, ja kun siinä onnistutaan, joutuu kotikäyttäjä ikävään välikäteen.(Korpela, 2005: 10)

Useimmiten peruskäyttäjän tietoturvaa verkossa koetellaan sattumanvaraisesti, perustuen esimerkiksi käyttäjän päätelaitteen puutteisiin tietoturvassa, esimerkiksi porttiskannauksen kautta. Voi kuitenkin myös olla tilanteita jossa käyttäjä valikoituu kohteeksi hyökkäykselle. Syitä kohteeksi valikoitumiseen voi olla lukuisia:

- Henkilö on merkittävässä roolissa työnantajaansa nähden ja hänellä on laajat oikeudet työnantajansa tietoihin, joihin halutaan päästä käsiksi
- Henkilön työllistävällä yrityksellä on kehitteillä vaikkapa jokin uusi tuote ja kilpaileva taho haluaa henkilön kautta päästä käsiksi työnantajan tietoihin tai tietojärjestelmiin
- Kohdehenkilöllä voi olla katkera kiista vaikkapa sukulaisen kanssa ja hänellä on tietoja joihin toinen osapuoli haluaa päästä käsiksi
- Kohdehenkilö voi olla suututtanut jonkun joka tuntee hakkerin
- Kohdehenkilön luottokelpoisuus on hyvä joka tekee henkilöstä taloudellisesti kiinnostavan kohteen
- Kohdehenkilön työnantajan toimintaa halutaan häiritä jotain tiettyä asiaa ajavien yksilöiden toimesta
- Kohdehenkilöllä tai hänen työnantajallaan voi olla hallussaan toista yritystä koskevia tietoja jotka kolmas osapuoli haluaa osakseen
- Kohdehenkilö yrittää pitää jotain salassa vaikkapa asianajajalta katkerassa avioerotilanteessa
- Kohdehenkilön tai hänen työnantajansa toimiin liittyy poliittisia näkemyksiä, joiden vastapuoli haluaa ajaa omaa asiaansa selvittämällä tai julkistamalla salaisia tietoja

(Thomas 2005: 11)

Tietoturva on monille vaikeasti ymmärrettävä, hahmoton ja joskus pelottavakin asia. Siten se usein jää vaille riittävää huomiota. Peruskäyttäjistä etenkin nuorten, on helppo oppia käyttämään tietokoneita kokeilemalla ja seuraamalla toisten esimerkkiä. Tietoturvaa ei yleensä kuitenkaan opita tällä tavoin. Tietoturva voidaan kokea ylimääräiseksi ongelmak-

si, joka häiritsee varsinaista tietokoneen käyttöä. Tietoturvan merkitys ymmärretään usein liian myöhään, esimerkiksi kun yksityinen valokuvagalleria vuotaa verkkoon tai lähes valmis tutkielma häviää. (Korpela, 2005: 14)

3.1 Yleisimmät peruskäyttäjää verkossa uhkaavat tekijät

Rikolliset kehittävät koko ajan uusia keinoja, joilla he pyrkivät huijaamaan sekä yrityksiä että yksityisiä henkilöitä. Sähköposti ja Internet ovat antaneet mahdollisuuden tavoittaa suuriakin ihmismääriä helposti ja lähes ilman kustannuksia. Suurimittaisten huijausyritysten takana on usein kansainvälinen järjestäytynyt rikollisuus, mutta joukossa on myös rikollista yksityisyritteliäisyyttä. (Keskusrikospoliisi 2014a)

3.1.1 Kiristyshaittaohjelmat

Kiristyshaittaohjelmat ovat olleet viime vuosina näkyvä ilmiö peruskäyttäjien keskuudessa. Kiristyshaittaohjelma kaappaa käyttäjän tietokoneen haltuunsa ja vaatii käyttäjältä maksua, jolla koneen lukitus avataan ja sen tiedostot pelastetaan. Maksun suorittaminen ei kuitenkaan kannata, koska se ei useimmiten korjaa tilannetta. Kiristyshaittaohjelma voi viestinnässä käyttäjälle naamioitua olevansa poliisiviranomaisen toimintaa, siten että se liittyy laittomaan materiaaliin jota käyttäjän koneesta väitetään löytyneen. Maksun suorittaminen ilmaistaan tällöin olevan sakko. (Andreasson, Koivisto, Ylipartanen 2014)

3.1.2 Huijaukset

Rikolliset kehittävät jatkuvasti erilaisia keinoja yritysten ja yksityisten henkilöiden huijaamiseen. Huijauksissa sähköpostitse lähetetään perinteisesti ns. nigerialaiskirjeitä, joissa yritetään huijata rahaa erilaisilla peitetarinoilla. Tarinoissa voidaan vedota joko ihmisten auttamishaluun tai haluun saada helppoa rahaa, välillä molempiin yhtä aikaa. Ilmoitukset huomattavista lotto- tai arpajaisvoitoista ovat myös tavallisia, vaikka viestin vastaanottaja ei olisi mihinkään arpajaisiin osallistunut. Myös valheelliset nettirakkaat ovat onnistuneet kalastamaan isojakin summia hyväuskoisilta kumppaneiltaan verkon välityksellä. (Keskusrikospoliisi 2014a)

Internetin eri kauppapaikoilla tapahtuu huijauksia jonkin verran, samoin esimerkiksi sijoitusten ja lomaosakkeiden kaupassa. Epärehellisyyttä on syytä epäillä mikäli myyjä painostaa tekemään kaupat nopeasti, tai jos myyjätahosta ei löydy kunnollisia taustatietoja. Kaikkiin huijausmuotoihin pätee sama vanha sääntö: jos jokin tuntuu liian hyvältä ollakseen totta, se ei yleensä olekaan totta. (Keskusrikospoliisi 2014a)

3.1.3 Tietojen kalastelu

Tietojen kalastelulla tarkoitetaan käyttäjälle suunnattua valheellista viestintää, jossa käyttäjä ohjataan esimerkiksi aidolta näyttävän sähköpostiviestin kautta aidolta näyttävälle pankkisivustolle, jonne käyttäjää pyydetään syöttämään pankkitunnuksensa. Tosiasiassa nämä tunnukset eivät rekisteröidy pankin palveluun, vaan ne otetaan rikollisten toimesta talteen ja niitä käytetään välittömästi oikealla pankkisivustolla rahan siirtämiseen rikollisten tilille. Yhtä lailla tietojen kalastelijoiden kohteena voi olla käyttäjän salasanat tai luottokorttitiedot. Suomessa tietojen kalastelua on mm. tehty verohallinnon, poliisiviranomaisen, pankkien ja tullin nimissä.

Tietojen kalasteluyrityksen tunnistaa helpoiten selaimen osoiteriviltä, koska kalasteluun käytetyt sivustot sijaitsevat usein palvelimilla, joiden verkkotunnus eroaa selkeästi pankin omista palvelimista. Tietojen kalastelusivustot eivät myöskään välttämättä käytä salattua verkkoyhteyttä. Salatun yhteyden tunnistaa selaimen osoiterivillä olevasta lukitusta lukkoikonista. Tietojen kalastelua tehdään roskapostituksen metodilla, eli lähettämällä viesti mahdollisimman monen vastaanottajan sähköpostiin, olettaen että pieni osa vastaanottajista reagoi halutulla tavalla. Roskapostittajan identiteetti on kuitenkin usein mahdoton selvittää. (Andreasson, Koivisto, Ylipartanen 2014)

3.1.4 Verkon aktiivilaitteiden haavoittuvuudet

Verkon aktiivilaitteella tarkoitetaan yleisesti tietoliikenneverkkoa käyttävää laitetta. Tällaisia ovat tietokoneiden lisäksi mm. laajakaistamodeemit, verkkokovalevyt, ja verkkotulostimet. Verkon aktiivilaitteen haavoittuvuuden ansiosta hyökkääjän on mahdollista päästä käsiksi kohteen lähiverkkoon ja siellä sijaitseviin laitteisiin ja tietoihin. Peruskäyttäjän tulee pitää huolta että ohjelmistojen lisäksi, käyttämiensä verkkolaitteiden osalta päivitykset ovat kunnossa. (Andreasson, Koivisto, Ylipartanen 2014)

3.1.5 Käyttäjien yksilöiminen ja seuranta

Perinteisesti verkkopalvelut seuraavat ja yksilöivät käyttäjiään evästeiden avulla. Evästeellä tarkoitetaan sitä tietoa, jonka palveluntarjoajan palvelin lähettää käyttäjän selaimelle. Palvelin pyytää selainta tallentamaan evästeen käyttäjän päätelaitteelle, jotta palvelin voi mahdollisesti myöhemmin pyytää tietoa takaisin. Evästeen ansiosta palvelimella voidaan seurata mitä sivuja käyttäjä avaa, missä järjestyksessä, ja kuinka usein käyttäjä ottaa yhteyttä palveluun. Käyttäjät voivat itse poistaa evästeitä tai estää niiden käytön selaimensa asetuksilla. (Andreasson, Koivisto, Ylipartanen 2014)

3.1.6 Palvelunestohyökkäykset

Palvelunestohyökkäyksissä tai hajautetuissa palvelunestohyökkäyksissä hyökkääjä kuormittaa hyökkäyksen kohteena olevaa sivustoa tai palvelua suurella liikennemäärällä, joka voi väliaikaisesti tukkia tietoliikenneyhteyden tai kaataa palvelimen. Hyökkäyksen tekijät sekä heidän motiivinsa jäävät useimmissa tapauksissa tuntemattomiksi, koska haitallinen liikenne näyttää tulevan lukuisista eri osoitteista. Palvelunestohyökkäykset koskettavat peruskäyttäjää vain välillisesti siten, että esimerkiksi tietyllä hetkellä tärkeä palvelu poistetaan saatavilta. Tällainen hetki voi liittyä johonkin kriisiin ja palvelu voi olla esimerkiksi uutis- tai viranomaisen tiedotussivusto. (Andreasson, Koivisto, Ylipartanen 2014)

3.1.7 Massatietovuodot

Yksi peruskäyttäjän tietoturvaa Internetissä uhkaava tekijä on viime vuosina ollut verkkosivustojen käyttäjätietojen massavuodot julkisuuteen. Näissä vuodoissa yksittäinen krakkeri tai krakkeriryhmä murtautuu verkkosivustolle niin, että se saa käsiinsä verkkosivuston käyttäjätietokannan. Monissa tapauksissa tällainen käyttäjätietokanta on murron jälkeen julkaistu avoimesti tietoverkossa. Tällaisessa tietomurrossa kyse on aina äärimmäisen vakavasta tapahtumasta, koska se voi kerralla uhata satojen tuhansien käyttäjien tietoturvaa myös toisaalla verkossa, kuin vain murretussa palvelussa. Pahimmassa tapauksessa vuonna 2010 arviolta 127 000 suomalaisen Älypää-pelisivuston käyttäjän salasana, tunnus ja sähköpostiosoite vuotivat nettiin.

Käyttäjätietojen massavuotojen jälkitoimenpiteissä on useita haasteita. Yleensä välittömästi massavuodon tapahduttua jokin virallinen tai epävirallinen taho julkaisee palvelun jossa käyttäjä voi tarkistaa ovatko hänen tietonsa julkisessa jaossa. Käyttäjä identifioi itsensä antamalla esimerkiksi sähköpostiosoitteensa, jonka perusteella palvelu hakee vuodetun tietokannan puhdistetusta versiosta vastaavuutta. Palvelu josta käyttäjätiedot on vuodettu, lähettää käyttäjiensä sähköpostiosoitteisiin tiedon tapahtuneesta ja kehottaa käyttäjiä vaihtamaan salasanansa sivustolle sekä palveluun. Yleensä murrettu sivusto laittaa myös kirjautumissivunsa yhteyteen tiedon tapahtuneesta, tai muuttaa automaattisesti käyttäjiensä salasanat sivustolleen.

Käyttäjätietojen massavuodoilla on kuitenkin kauaskantoisempia seurauksia kuin vain välittömästi itse vuodon jälkeen. Vuosina 2009-2014 yhteensä ainakin 13 verkkosivustoa Suomessa on kokenut käyttäjätietokantansa varastamisen krakkerien toimesta, sekä sen tapahtuneen vuodon Internetiin. Peruskäyttäjä ei kuitenkaan voi tarkistaa mistään onko hänen tietojaan vuodettu verkkoon, ja jos on, mitä tietoja. Samanaikaisesti kaikki nämä

käyttäjätietokannat ovat jaossa, koostetusti esimerkiksi TOR-verkossa kenen tahansa, esimerkiksi verkkorikollisen ladattavana.

Peruskäyttäjän tietoturvallisuuden perusongelmakohdat, kuten saman tai samankaltaisten salasanojen käyttö, aiheuttaa sen että myös pitkän ajan päästä krakkeri voi halutessaan murrettuja käyttäjätietoja hyväksikäyttämällä tehdä tietomurtoja. Käyttäjätietolistoista on hyötyä krakkereille, mikäli kohteeksi valitun henkilön yksityisiä tietoja osataan soveltaa.

Viimeisen seitsemän vuoden aikana tapahtuneet käyttäjätietojen massavuodot suomalaisissa palveluissa ovat:

- ”78k passlist” 2007 – tuntematon lähde (50 000 käyttäjätunnusta / salasanaa / sähköpostiosoitetta. Lisäksi 20 000 tunnusta / sähköpostia joissa salasana salatussa formaatissa)
- Älypää 2010 (127 000 nimeä / käyttäjätunnusta / salasanaa / sähköpostiosoitetta)
- Helistin 2011 (73 000 käyttäjätunnusta / salasanaa / sähköpostiosoitetta)
- Netcar 2011 (12 000 käyttäjätunnusta / salasanaa / sähköpostiosoitetta)
- SETA 2011 (16 000 käyttäjätunnusta / salasanaa / sähköpostiosoitetta. Lisäksi 4 000 tunnusta / sähköpostia joissa salasana salatussa formaatissa)
- Hetudump 2011 (16 000 henkilötunnusta / henkilötietoa / sähköpostiosoitetta)
- Napsu 2011 (16 000 käyttäjätunnusta / salasanaa / sähköpostiosoitetta)
- Lautapeli (500 käyttäjätunnusta / salasanaa / sähköpostiosoitetta)
- Koiratuote 2011 (25 000 nimeä / sähköpostiosoitetta, 3000 henkilötietoa)
- Hotmail 2011 (6300 salasanaa / sähköpostiosoitetta)
- Overdrive 2012 (24 000 käyttäjätunnusta / salasanaa / sähköpostiosoitetta)

Jos päällekkäisyyksiä ei oteta huomioon, yllä olevat tietovuodot koskevat yli 360 000 suomalaista käyttäjätunnusta tai käyttäjää.

Ulkomaalaisia palveluja joissa läsnä suomalaisia käyttäjiä:

- Yahoo 2012 (450 000 käyttäjätunnusta / salasanaa / sähköpostiosoitetta)
- Adobe 2013 (150 miljoonaa salattua salasanaa / sähköpostiosoitetta, yli 270 000 suomalaista salattua salasanaa / sähköpostiosoitetta)
- Gmail 2014 (4 900 000 vuodettua salasanaa / sähköpostiosoitetta, suomalaisten lukumäärä tuntematon)

Yhteensä edellä mainitut suomalaiset ja ulkomaalaiset tietovuodot koskevat n. 600 000 – 800 000 suomalista Internetin käyttäjää. Syystä tai toisesta, yllä olevia listoja tietomurron

ja käyttäjätunnusten massavuodon kohteeksi joutuneista sivustoista ei löydy koostettuna Internetistä. Verkon peruskäyttäjällä ei myöskään ole mahdollisuutta tarkistaa onko hänen tietojaan jossain vaiheessa vuodettu, ja jos on niin mitä tietoja. Luonnollisesti laajan tietovuotorekisterin ylläpitämisessä olisi omat haasteensa, sen ollessa lähtökohtaisesti laiton rekisteri, koska tiedot on hankittu laittomin keinoin, sekä myös koska se itsessään voisi joutua väärinkäytösten kohteeksi. Missään yllämainituista käyttäjätunnusten tietovuototapauksista verkkopalvelun ylläpitäjät eivät ole joutuneet varsinaisesti lailliseen vastuuseen siitä, miten käyttäjien tietoja on säilytetty, vaikka salasanojen säilytyksen selvätekstisessä muodossa voidaan todeta olevan merkittävä laiminlyönti palvelun ylläpidon taholta, vaan tapausten osalta laillisia toimia on kohdistettu ainoastaan murtautujatahojen selvitykseen.

Koska laajan tietomurron tapahtuminen on verkkosivustolle ylläpitäjänsä osalta yleensä häpeällinen tapahtuma, varsinkin mikäli se johtuu jonkinlaisesta tietoturvan laiminlyönnistä, on vaikea sanoa kuinka paljon tapahtuu tietomurtoja joissa verkkosivuston käyttäjäkanta on varastettu, muttei sitä jaeta julkisesti, eikä murron kohteeksi joutunut verkkosivusto tiedota tapahtuneesta, tai pahimmassa tapauksessa edes huomaa tapahtunutta.

4 Käyttäjävarmennuskäytännöt verkkopalveluissa

Verkkopalvelussa käyttäjän todentamisessa pyritään varmistumaan käyttäjän henkilöllisyydestä. Joskus tilanne voi olla myös päinvastainen sikäli, että verkkopalvelun pitää todentaa käyttäjälle olevansa se, joksi käyttäjä sitä kuvittelee.

Verkkopalveluun kirjautumisessa on kaksi vaihetta. Ensin tunnistetaan nimen, käyttäjätunnuksen, tai asiakasnumeron perusteella, kuka käyttäjä on kyseessä. Tämän jälkeen todennetaan että käyttäjä todellisuudessa on se joka hän väittää olevansa. Verkkopalvelussa todennus suoritetaan yleensä salasanalla. Tässä luvussa käsitellään verkkopalveluiden käyttäjävarmennuskäytäntöjä ja niiden toteutustapoja.

4.1 Varmennustyypit

Tunnistautuminen voidaan jakaa kolmeen tasoon:

- Heikko tunnistautuminen
- Vahva tunnistautuminen
- Sähköinen allekirjoitus

Heikossa tunnistautumisessa yleisin menetelmä on tunnus-salasanapari. Tällöin käyttäjällä voi olla käytössään useita sähköisiä identiteettejä. Käyttäjän todellista henkilöllisyyttä ei heikossa tunnistautumisessa varmisteta. Vahvassa tunnistautumisessa käyttäjä yhdistetään todelliseen henkilöllisyyteen, esimerkiksi pankkien Tupas-tunnistuksella. Sähköinen allekirjoitus on menetelmä joka varmentaa allekirjoittajan henkilöllisyyden ja viestin sisällön. Jos viestin sisältöä muutetaan, ei sähköinen allekirjoitus enää täsmää. (KRYSP 2010)

4.1.1 Salasanavarmennus

Verkkopalveluissa ja tietojärjestelmissä ylipäätään yleisin todennustapa on salasana. Kyseessä on tällöin salaisuus, jonka palvelu ja käyttäjä jakavat keskenään. Käyttäjä identifioidaan ensin käyttäjätunnuksen tai nimen perusteella, ja sitten todennetaan oikeaksi perustuen salasanaan. Salasanaa verrataan palvelun rekisteriin, ja mikäli se vastaa käyttäjän kohdalla tallennettua tietoa, pääsy palveluun avautuu. Toisin kuin vaikkapa kotiavaimen tai pankkikortin kadotessa, salasana voi paljastua ulkopuoliselle ilman että käyttäjä huomaa näin tapahtuneen. Salasana ei itsessään takaa mitään, koska kyse on immateriaalisesta tiedosta jota voi monistaa ja jakaa loputtomasti. Salasanaan liittyy myös unohdusvaara, sekä sitä voidaan yrittää murtaa erilaisia tekniikoita käyttämällä. Verkkopalveluissa salasanavarmistusta käytetään paljon, koska se on helppo ja halpa toteuttaa. (Järvinen 2003)

4.1.2 Mobiilivarmenne

Termillä ”mobiili” viitataan matkapuhelimiin, tabletteihin ja kannettaviin tietokoneisiin, kun niitä käytetään kiinteiden työpisteiden ulkopuolella. Mobiilivarmenteella käyttäjä voi todistaa oman henkilöllisyytensä, sekä suorittaa eri palveluissa allekirjoituksen. Mobiilivarmenne on turvallinen tunnistamisratkaisu sähköisissä palveluissa ja se on yksi Suomessa linjatuista vahvan tunnistamisen konsepteista. Mobiilivarmenne toimii kaikissa suomalaisissa liittymissä, ja se vaatii käyttöönottoa operaattorilta. (Korpela 2005)

4.1.3 Pankkivarmennus ja TUPAS

Verkkopankissa asiakkaan tunnistamiseen käytetään kahta tai kolmea eri koodia, jotka asiakkaan on kirjoitettava kirjautumisensa yhteydessä. Pankit jakavat asiakkailleen yleensä asiakasnumeron, mahdollisen tunnusluvun, sekä listan kertakäyttötunnuksista. Tällöin käyttäjän todennus perustuu sekä fyysiseen esineeseen(lista) että tietoon (seuraava tai satunnainen käyttämätön numero). Lisäksi voidaan käyttää jonkinlaista varmistustunnusta. Tunnuksilla asiakas voi hoitaa asiansa verkkopankissa tai maksuautomaateissa. Verkkopankissa asioitaessa kaikki tietoliikenne selaimen ja pankin palvelimen välillä on vahvasti salakirjoitettua.

Pankkivarmennuspalveluun liittyy oleellisesti TUPAS-palvelu, joka on Finanssialan Keskusliiton määrittelemä metodi tunnistaa verkkopalvelujen käyttäjiä pankkien verkkopalvelutunnuksilla. TUPAS-tunnistus toimii niin, että kun käyttäjä kirjautuu palveluntarjoajan verkkopalveluun, käyttäjän istunto tallennetaan ja käyttäjä ohjataan oman pankin tunnistautumissivulle. Kun käyttäjä syöttää pankin toimittamat käyttäjätunnuksensa pankin sivuille, pankki lähettää palveluntarjoajalle tiedot siitä kuka kirjautunut henkilö on. Tupastunnistus täyttää lain määritelmän asiakkaan vahvasta sähköisestä tunnistamisesta. (Korpela 2005)

4.1.4 Tunnistautuminen sähköisellä henkilökortilla

Tunnistusta edellyttävään asiointiin on Suomessa erikseen kehitetty sähköinen henkilökortti. Tämä tunnistautumistapa on maksullinen ja vaatii erityisen kortinlukulaitteen, sekä siihen liittyvän ohjelmiston käyttäjän koneessa. Kortin suosio on jäänyt melko pieneksi, eikä sen käyttömahdollisuudet palveluissa ole suuret. Olennaisinta sähköisessä henkilökortissa on sen sisältämä kansalaisvarmenne, joka on tietokoneen luettavassa muodossa oleva, vahvistettu todistus henkilöllisyydestä. (Korpela 2005)

4.1.5 Verkkotunnistaminen ja maksaminen – Vetuma-palvelu

Kansalaisen tunnistus- ja maksamispalvelu Vetuman avulla henkilö voi tunnistautua ja maksaa sähköisesti niissä asiointipalveluissa, joihin palvelu on liitetty. Vetuma-palvelu mahdollistaa tunnistamisen sähköisellä henkilökortilla olevalla kansalaisvarmenteella, mobiilioperaattoreiden myöntämillä varmenteilla, sekä pankkien tupas-tunnuksilla. Vetuma-palvelu mahdollistaa osaltaan kuntien ja valtionhallinnon organisaatioiden palveluprosessien uudistamisen. (Verkkotunnistaminen ja -maksaminen Vetuma)

4.1.6 Biometrinen tunnistus

Biometrinen tunnistus perustuu ihmisen ulkonäköön, ääneen tai olemukseen. Eri varmennuskäytännöistä biometrinen tunnistus on vaikein toteuttaa. Biometrisillä tekniikoilla koodataan ihmisen ominaisuuksia tietokoneen ymmärtämään muotoon. Henkilön ääni, kasvonpiirteet, silmän iiris, tai sormenjälki voidaan digitoida. Biometristä tunnistusta suoritettaessa kohteena olevaa näytettä verrataan mitattuihin arvoihin. Vain hyvin harvoilla henkilöillä on samanlaiset biometriset tunnisteet, joten biometrisellä tekniikalla ihminen voidaan tunnistaa lähes varmasti. Biometrisia tunnisteita ei voi unohtaa kotiin ja biometristen tunnistuslaitteiden huijaaminen on hankalaa. Turvallisesti toteutettuna biometristen tunnisteiden käyttö henkilön tunnistamisessa nopeuttaa tunnistamista sekä parantaa tunnistamisen laatua. (Tietosuojavaltuutetun toimisto 2010)

4.2 Hyvät käyttäjävarmennuskäytännöt verkkopalveluissa

Metodeja käyttäjän tunnistamiseen verkkopalvelussa on lukuisia. Palvelu voi käyttää yhtä tai useampaa metodia käyttäjän varmentamiseen. Hyvä käyttäjävarmennuskäytäntö takaa aukottomasti riittävän turvallisuusasteen suhteessa palvelussa tarvittavaan tietoturvan tasoon, tai toimii portaittain tarvittavan tietoturvatason kasvaessa. Hyvä varmennuskäytäntö on ensisijaisesti palvelun tietoturvatasoa vastaava ja toissijaisesti palvelun käyttäjälle mahdollisimman mutkaton käyttää.

Hyvää käyttäjävarmennuskäytäntöä ei sanele tasonsa puolesta suoraan koskemansa palvelun taloudelliset resurssit, vaan käytännön tietoturvatarve. Hyvä varmennuskäytäntö eliminoi automaattisesti mahdolliset käyttäjistä johtuvat puutteet sen käytössä, eli pitää huolen että sitä itseään käytetään asianmukaisesti, esimerkiksi pakottamalla käyttäjää antamaan riittävän monimutkaisen salasanan. Hyvän käyttäjävarmennuskäytännön data ei ole hyödyllistä varkaalle, vaikka se kokonaisuudessaan joutuisi vääriin käsiin. Hyvä käyttäjävarmennuskäytäntö toimii aina suhteessa ympäristöönsä, mutta kuitenkin itsenäi-

sesti niin ettei petä, vaikka käyttöympäristössä, esimerkiksi fyysisissä laitteissa olisi puutteita.

4.3 Sopimus palvelun ja käyttäjän välillä

Usein internetpalveluita voidaan käyttää ilman sopimuksia, mutta monissa tapauksissa viestintä palvelun ja käyttäjän välillä alkaa rekisteröitymisen yhteydessä käsiteltävästä internetpalvelusopimuksesta. Käyttäjän on hyväksyttävä palvelun käyttöehdot tai sopimus jotta pääsee käyttämään palvelua. Käyttäjällä ei ole mahdollisuutta neuvotella sopimuksesta vaan sen hyväksymättä jättäminen johtaa palvelun käytön eväämiseen. Usein mitä laajempi ja suositumpi palvelu on, sitä monitahoisemmat ovat myös käyttöehdot, ja sitä suurempi mahdollisuus palvelun ylläpitäjällä on muotoilla käyttöehdoista omia tarkoitusperiään palvelevat. Palvelun ylläpitäjällä on myös mahdollisuus muuttaa palvelun käyttöehtoja palvelun suosion kasvaessa, silläkin riskillä että käyttöehtoja muutettaessa käyttäjälle epäedullisemmaksi, menetetään pieni osa käyttäjäkunnasta mutta saavutetaan esimerkiksi suurempi kaupallinen hyöty.

Sopimuksista on hyvä tarkastaa, onko siinä käsitelty seuraavia asioita:
1. Mitä tietoja kerätään (asiakastiedot ja muut tiedot)
2. Tietoon liittyvät oikeudet
3. Sovellettava lainsäädäntö
4. Mihin tieto on tallennettu
5. Tietojen käyttötarkoitus (mihin ja miten tietoja hyödynnetään)
6. Tietojen luovuttaminen ja jakaminen kolmansille osapuolille
7. Markkinointi
8. Tietojen julkisuus/yksityisyys ja miten tietoa suojataan
9. Tietojen säilytysaika
10. Mitä tiedoille tapahtuu, kun sopimus päättyy.
(Viestintävirasto 2014a)

4.4 Esiintyminen väärillä henkilötiedoilla

Käyttäjä voi internetpalveluun rekisteröityessään ilmoittaa valheelliset tiedot itsestään, mikäli haluaa esiintyä palvelussa anonyyminä niin, ettei todellinen henkilöllisyys ole tunnistettavissa. Tämä on mahdollista, mikäli palvelu käyttää heikkoa tunnistusta. Käyttäjän tulee huomioida että tällöinkin palvelun ylläpidon on mahdollista tunnistaa IP-osoitteen perusteella käyttäjän lokaatio, sekä mahdollisesti yhdistää käyttäjä samasta päätelaitteesta käytettyihin muihin tunnuksiin samassa tai muissa palveluissa. IP-osoitteensa käyttäjä voi halutessaan salata käyttämällä proxy-palvelua, esimerkiksi Tor-verkkoa.

Koska varsinaisesti toisena henkilönä esiintymistä, eli identiteettivarkauttakaan ei ole toistaiseksi kriminalisoitu, ei keksittyjen väärien tietojen käyttämisessä verkkopalveluissa ole laillista estettä, kunhan ei ole kyse tunnistautumisesta viranomaiselle. Väärien tietojen käyttämisessä tulee erotella kuvitteellisten henkilötietojen käyttäminen sekä esiintyminen tahallisesti toisena laillisena henkilönä. Tahallisesti toisena henkilönä esiintyminen verkossa ei toistaiseksi ole laitonta, mutta lakia rikotaan, mikäli toiseksi henkilöksi tekeytymällä tehdään toimenpiteitä jotka esimerkiksi täyttävät petoksen tunnusmerkistön. Vaikka henkilö ei tekisi verkossa mitään laitonta, voi väärällä nimellä esiintymisestä koitua vaikeuksia. Mikäli henkilö esimerkiksi kommentoi vahvistavasti toisella tilillä viestejä jotka on kirjoittanut alun perin oikealla nimellään, voi tämän paljastuessa henkilö kokea maineensa ja uskottavuutensa menetyksen vaikkapa nettiyhteisössä.

Nyt valmisteilla olevan, identiteettivarkauden kriminalisointiin tähtäävään lainsäädännön tullessa voimaan, on arvioitavissa, ettei tällöinkään rangaistavaksi katsota toimintaa missä verkossa käytettävä väärä identiteetti on keksitty, eikä se ole assosioitavissa kehenkään tiettyyn henkilöön. Rangaistavuuden ulkopuolelle jäänevät myös tapaukset joissa käytettäviä henkilötietoja on yhdistelty eri henkilöiltä, esimerkiksi käytettäessä yhden henkilön nimeä ja toisen henkilön kuvaa. Se onko toisen henkilön tiedoilla esiintyminen internetpalvelussa kiellettyä, riippuu käyttäjän ja palvelun välisestä käyttösopimuksesta. Mikäli käyttäjä esiintyy palvelussa väärillä tiedoilla, samalla kun palvelun käyttöehdot tämän kieltävät, voi käyttäjä paljastuessaan menettää tunnuksensa palveluun sekä saada porttikiellon.

4.5 Reagointi epäselvissä tunnistustapahtumissa

Yksi näkökulma käyttäjän tietoturvaan verkkopalvelussa on se, miten palvelu suhtautuu tilanteeseen missä käyttäjän tunnistus on epäselvää, tai käyttäjä on kadottanut tunnistustietonsa, eli tunnuksensa tai salasanansa.

Monissa palveluissa käytössä on kirjautumishistoria jossa käyttäjä voi tarkastella IP-osoitteiden perusteella viimeisimpiä kirjautumislokaatioita. Tämä toki edellyttää että käyttäjä osaa tulkita kirjautumislokaatiolistaa siten että erottaa siitä mahdollisen asiattoman käytön. Usein esimerkiksi verkkoyhteyden tarjoajan osalta se kaupunki, joksi käyttäjän alkuperä IP-osoitteen perusteella tunnistetaan, on toinen kuin missä käyttäjä sijaitsee, ja tämä voi aiheuttaa sekaannusta. Verkkopalveluita käytetään nykyään myös useista eri päätelaitteista samanaikaisesti, joten käyttäjän kirjautumislokaatioita voi olla useita. Jotkut palvelut, kuten Microsoftin sähköposti / verkkotallennuspalvelut, käyttävät kirjautumislokaation seurannassa aktiivista suhdetta itse kirjautumiseen niin, että käyttäjältä kysytään varmistuskysymyksiä tunnuksen ja salasanan lisäksi mikäli hän kirjautuu palveluun ennes-

tään tuntemattomasta osoitteesta. Useissa suosituissa palveluissa tällainen mekanismi on mahdollista asettaa erikseen päälle, myös antamalla palvelulle tiedoksi vain tietyt luotetut kirjautumislokaatiot, esimerkiksi IP-osoitteiden kautta.

Käyttäjätunnuksen ja salasanan palautusmekanismia voidaan käyttää hyväksi vaikkapa krakkerin toimesta, mikäli se on toteutettu esimerkiksi yksinkertaisella turvakysymyksellä. Harva käyttäjä muistaa käyttämiensä palveluiden osalta minkä turvakysymyksen on valinnut, varsinkin jos ei ole käyttänyt palautuspalvelua lähiaikoina tai koskaan. Jos turvakysymyksenä on esimerkiksi ”Lempihahmosi”, voi krakkeri saada vastauksen kysymykseen vaikkapa seuraamalla henkilön tykkäyksiä muissa verkkopalveluissa, tai saada vastauksen turvakysymykseen suoraan käyttäjältä jonkin verkkopalvelun keskustelussa. Käyttäjätunnuksen tai salasanan palauttamisessa yleisesti käytetty turvakysymys tulisi siis aina tuplavarmentaa muita yksityisiä tietoja kysymällä, tai esimerkiksi mobiilivarmistuksella.

Käyttäjän tunnistus voi olla myös epäselvää esimerkiksi tilanteessa missä käyttäjä on syöttänyt salasanansa ja tunnuksensa useaan kertaan palveluun kirjautumisen yhteydessä väärin. Usein kyse on aidosti käyttäjän unohtamasta salasanasta, mutta kyse voi myös olla mahdollisen krakkerin yrittämästä sanakirjahyökkäyksestä missä salasanaa yritetään arvata, joko hienostuneesti soveltamalla käyttäjän henkilökohtaisia tietoja yhdistäen sanoja sekä numerosarjoja, tai laajemmalla metodilla käyttäen esimerkiksi sanakirjatietokantaa kaikista mahdollisista sanoista ja arvaamalla näitä yksitellen. Käyttäjätunnuksen ja salasanan arvaamisen epäkohtaan on helppo varautua. Kirjautumisyritykset voidaan rajoittaa esimerkiksi kymmeneen kappaleeseen kymmenessä minuutissa, jolloin salasanojen arvaaminen ei ole tehokasta. Toinen varautumiskeino joka vain harvoissa verkkopalveluissa on käytössä, on tilanteesta jossa salasanaa on yritetty arvata tietty määrä kertoja, käyttäjälle tiedottaminen esimerkiksi kirjautumisen yhteydessä. Tiliinsä kohdistuvien salasanan arvausyritysten tiedostamisesta voi olla käyttäjälle hyötyä, jotta hän voi esimerkiksi vaihtaa salasanansa palvelussa monimutkaisempaan, tai ottaa käyttöön mobiilivarmennuksen.

Koska nykyään on melko yleistä että palveluja käytetään niin, että niihin on kirjauduttu samanaikaisesti useista eri päätelaitteista, ei varsinaisen rinnakkaiskäytön osalta tarvitse käyttäjää lähtökohtaisesti tiedottaa. Poikkeuksen voi muodostaa tilanteet missä käyttäjä on kirjautunut esimerkiksi kahdesta eri lokaatiosta jotka IP-tunnistetietojen perusteella sijaitsevat kaukana toisistaan.

Yleisesti palvelun reagointi epäselvissä tunnistustapahtumissa voisi olla tiedotusmuotoista, mutta niin että käyttäjälle näytettävä tieto on suodatettu ymmärrettävään muotoon.

Käyttäjän osalta turhaa huolenaihetta voi aiheuttaa esimerkiksi pelkkiä tunnistamattomia kirjautumisessa käytettyjä IP-osoitteita sisältävä lista, mutta listan tietoihin usein käytettyjen osoitteiden lisääminen, sekä esimerkiksi paikkatiedon liittäminen tekee tiedosta käyttäjälle helpommin tulkittavaa.

4.6 Käyttäjävarmennuksen suhde palvelun käyttökynnykseen

Tietoturvallisuuden ja palvelun käytettävyyden suhde on aina ongelmallinen. Tietoturvallisuuden lisääminen luo aina käyttäjän toiminnalle lisähaasteita ja esteitä, siinä missä käytettävyyden tavoite on ylimääräisten esteiden ja haasteiden poistaminen palvelun käyttäjältä. Tietoturvan tasoa verkkopalvelussa ei pidä määrittää mahdollisimman suureksi, vaan riittävän suureksi. Tietoturvaratkaisuja lisättäessä yleensä palvelun kustannukset nousevat ja käyttömukavuus heikkenee. Jossakin vaiheessa ylitetään raja, missä tietoturvan lisäämisestä saatava lisäturva ei enää vastaa sen saavuttamisen hintaa.

Käyttäjävarmennuksen oikea suhde palvelun käyttökynnykseen riippuu aina käytetyistä varmennustekniikoista, sekä siitä millaista tietoturvatasoa palvelulta odotetaan. Lähtökohtaisesti voidaan kuitenkin sanoa, ettei asianmukaisesta tietoturvatasosta pidä koskaan tinkiä käyttökynnyksen laskemiseksi. Oikeanlaisen suhteen saavuttaminen tietoturvatason ja riittävän käytettävyyden välille on aina haasteellista, ja siihen liittyvään suunnitteluun tulee verkkopalvelussa kiinnittää erityistä huomiota.

Suunnittelussa tulee käyttää tasapainoisesti asiantuntemusta sekä käytettävyydestä että tietoturvasta. Olemassa olevan palvelun osalta voidaan testata käyttäjän toimintaa suhteessa palvelun tietoturvallisuustoimintoihin, esimerkiksi normaalin käytettävyystutkimuksen kautta, minkä tuloksien perusteella voidaan palvelua kehittää edelleen.

5 Esimerkkejä palveluntarjoajien käyttäjävarmennuskäytännöistä

Tässä luvussa tarkastelun kohteeksi on otettu kolmen, Suomessa kansallisesti suositun, verkkopalvelutarjoajan käyttäjävarmennuskäytännöt. Tarkastelun kohteeksi on palveluissa otettu joitain tietoturvaan liittyviä toimintoja, jotka näkyvät vertailumatriisissa (liite). Tarkastelu ei ole kattava tietoturvaselvitys, vaan pyrkii havainnoimaan mitä perusasioita tietoturvaan liittyen käyttäjä voi palvelusta päätellä. Tarkastelussa selaimina toimi normaalin tarkastelun osalta Mozilla Firefox 34.0, sekä ulkomaanyhteyksien testaamiseen Tor Browser 4.0.1.

5.1 Tarkastelutapa ja -kriteerit

Kohdassa 5.1 verkkopalveluiden käyttäjävarmennuskäytäntöjä tarkasteltiin seuraavassa toimintajärjestyksessä:

1. Verkkopalveluun rekisteröityminen – käyttöehdot ja palvelun yleinen vaikutelma
2. Verkkopalvelun käyttö – sisäänkirjautuminen, käyttäjälle näkyvät tietoturvaominaisuudet sekä tietoturvallisuuteen liittyvät toiminnallisuudet
3. Poikkeustilanteet - palvelun käyttö ulkomaisesta osoitteesta samanaikaisesti paikallisen kirjautumisen kanssa, ongelmat sisäänkirjautumisessa
4. Verkkopalvelun toiminta tilanteessa jossa käyttäjä on unohtanut salasanansa - turvakysymyksen toteutus ja salasanan palautus

Vertailumatriisissa, joka on liitteenä, kuvataan tarkastelukriteerit toiminnan tasolla, sekä huomiot kohdittain jokaisen palvelun osalta. Tarkastelun kohteeksi valitut toiminnot liittyvät verkkosivuston tietoturvan peruselementteihin.

Kunnollisen salasanan ollessa merkityksellinen elementti tietoturvassa, eri kohdissa on tarkasteltu salasanan syntaksin älykästä suodatuspakotusta, eli sitä ettei salasanaksi hyväksytä liian lyhyttä, kirjoitusasultaan helposti arvattavaa tai jo käytössä ollutta salasanaa. Lisäksi salasanan syötössä tarkastellaan estoja jotka tulevat voimaan salasanan liiallisesta väärinsyötöstä. Kun käyttäjä rekisteröityy palveluun, tulisi hänen hahmottaa selkeästi mitä palvelun profiiliinsa syöttämiä tietoja hänestä välittömästi julkaistaan, sekä rajata pois julkaistavia tietoja. IP-kirjautumislokaatioiden rekisteröiminen ja esittäminen käyttäjille antaa mahdollisuuden tarkastella kirjautumislokia ja havainnoida mahdolliset luvattomat käyttötapaukset. Mikäli käyttäjä kirjautuu lyhyellä aikavälillä kahdesta fyysisesti etäisestä paikasta, järjestelmän tulisi tiedottaa tästä käyttäjää ja varmistaa että toiminta on ollut tarkoituksenmukaista. Ylipäätään käyttäjälle tulisi antaa vaihtoehtoja tietoturvaratkaisujen suhteen niin, että minimivaihtoehdossakin toteutuu palvelun luonteeseen nähden asialliset tietoturvakäytännöt.

5.2 Tarkasteltavat palvelut

5.2.1 Suomi24-verkkoportaalin sähköpostipalvelut

Palvelun omistaja on Aller Media Oy, sen kotimaa on Suomi, ja pääasiallinen tarkoitus on tarjota käyttäjälle sähköposti- sekä verkkoyhteisöpalveluita. Palvelun sijoitus Suomessa käytetyimpien verkkopalvelujen listalla on 16 (sijoitus marraskuussa 2014, lähde:alexa.com). Verkko-osoite josta palvelun käyttö aloitettiin: http://www.suomi24.fi/

Palvelun tietoturvan taso voidaan arvioida riittäväksi, sisältäen joitain oleellisia puutteita. Salasanojen pakottaminen monimutkaiseksi on toteutettu hyvin, vaikkakaan salasanaa tarkisteta esimerkiksi käyttäjätunnukseen verraten. Palveluun ei tarvitse syöttää henkilötietoja. Palvelu luo käyttäjälle julkisen profiilin kuitenkaan ilmoittamatta siitä selkeästi. Käyttöehdot on esitetty selkeästi. Salasanan säilötysmuodosta salaamattomana ei ole viitteitä. Salasanan palautusmekaniikka on keskitasoa, saman salasanan käyttö toistuvasti onnistuu. Käyttäjätietojen hallinta ja yksityisyysasetukset ovat hyvällä tasolla. Käyttäjä voi selkeästi valita mitä tietoja haluaa julkiseksi, kunhan hahmottaa mitä julkinen tässä tapauksessa on. Järjestelmä ei tue kaksivaiheista varmistusta. Palvelu ei käytä IP-tietojen indikointia käyttäjälle missään palvelun toiminnan osiossa. Käyttäjä ei voi tarkastella viimeisiä toimintoja eikä kirjautumisosoitteita. Palvelussa ei ole rajoituksia tai tiedotusta samanaikaisen kirjautumisen, muuttuneen kirjautumislokaation, tai kirjautumispaikkojen sijainnin suhteen. Palvelun kirjautumisessa väärän salasanan syöttömahdollisuus on rajaton. Käyttäjän mahdollisuus tehdä oikea arvio palvelun tietoturvan tasosta on riittävä.

Peruskäyttäjälle näkyviä puutteita palvelun tietoturvassa olivat IP-tietojen poissaolo, salasanan syöttömahdollisuuden rajattomuus, salasanan syntaksin älykäs suodatus, käyttäjätietojen julkaisupaikan hahmottomuus, saman salasanan uusiokäyttö, samanaikaisen käytön mahdollisuus sekä järjestelmän välittämättömyys kirjautumislokaatiosta.

5.2.2 Huuto.net -verkkopalvelu

Palvelun omistaja on Sanoma Media Finland Oy, sen kotipaikka on Suomi, ja pääasiallinen tarkoitus on tarjota käyttäjälle huutokaupanomaista verkkopalvelua. Palvelun sijoitus Suomessa käytetyimpien verkkopalvelujen listalla on 27 (sijoitus marraskuussa 2014, lähde:alexa.com). Verkko-osoite josta palvelun käyttö aloitettiin: http://www.huuto.net/
Palvelun tietoturvan taso voidaan arvioida varsin hyväksi. Salasanan pakotus tulee olla vähintään kahdeksan merkkiä pitkä. Järjestelmässä on älykäs tarkistus niin, ettei salasana voi olla käyttäjätunnus. Rekisteröinti palveluun vaatii varmistuksen sähköpostiosoitteesta. Käyttöehdot jaoteltu selkeästi ja niiden muoto on selkeä. Salasanan säilötysmuodosta

salaamattomana ei ole viitteitä. Ei kaksivaiheista varmistusta, vain tunnistautuminen tunnuksella ja salasanalla. Käyttäjällä on mahdollisuus plus-palveluun, jossa varmistetaan henkilötiedot pankki- tai mobiilivarmenteella. Plus-palvelua käyttäville annetaan lisätoimintoja ja käyttöoikeuksia. Käyttäjä voi valita haluaako hän palvelussa asioida kaikkien käyttäjien, vai vaan tunnistettujen käyttäjien kanssa. Salasanan vaihto toimii tilaamalla sähköpostiin linkki vaihtamiseen. Vaihtamispyynnön viestissä selviää asianmukaisesti IP-osoite josta pyyntö tehty, sekä aikatieto. Viimeisiä toimintoja tai kirjautumislokaatioita ei mahdollista tarkistella. Käyttäjätietojen esitystapa selkeä, muttei indikointia siitä, missä vaiheessa muiden käyttäjien kanssa asioidessa mitäkin tietoja näytetään toiselle. Palvelussa ei ole rajoituksia tai tiedotusta samanaikaisen kirjautumisen, muuttuneen kirjautumislokaation, tai kirjautumispaikkojen sijainnin suhteen. Palvelun kirjautumisessa väärän salasanan syöttömahdollisuus on rajaton. Käyttäjän mahdollisuus tehdä oikea arvio palvelun tietoturvan tasosta on hyvä. Portaittainen tunnistusvahvuus on hyvä lähtökohta tälle palvelulle käyttötarkoituksensa puolesta.

Peruskäyttäjälle näkyviä puutteita palvelun tietoturvassa olivat monimutkaisen salasanan pakottamattomuus, IP-tietojen näyttämisen puute itse palvelussa, salasanan syöttömahdollisuuden rajattomuus, saman salasanan uusiokäyttö, samanaikaisen käytön mahdollisuus sekä järjestelmän välittämättömyys kirjautumislokaatioista.

5.2.3 Dropbox -pilvipalvelu

Palvelun omistaja on Dropbox, Inc., sen kotipaikka on San Francisco, Yhdysvallat, ja pääasiallinen tarkoitus on tarjota käyttäjälle verkkotallennuspalveluita eri päätelaitteille. Palvelun sijoitus Suomessa käytetyimpien verkkopalvelujen listalla on 121 (sijoitus marraskuussa 2014, lähde:alexa.com). Verkko-osoite josta palvelun käyttö aloitettiin: https://www.dropbox.com/

Palvelun tietoturvan taso voitaisiin yleisesti arvioida hyväksi. Salasanasääntönä on vain kuuden merkin pituusvaatimus. Ei älykästä suodatusta syntaksin osalta. Palvelun käyttöönotto on nopeaa, ei varmistuksia rekisteröinnissä. Englanninkieliset käyttöehdot on jaoteltu selkeästi. Suomalaisen käyttäjän huomioitava että käyttöehtoihin pätee Californian osavaltion lainsäädäntö. Palvelussa mahdollisuus kaksivaiheiseen varmennukseen, jossa uudella laitteella palveluun kirjauduttaessa salasanan lisäksi tarvitaan puhelimeen lähetetty koodi. Käyttäjän tiedot ja materiaali yksityistä kunnes julkaistaan. Salasanan palautus toimii tilaamalla vaihtolinkki kirjautumissähköpostiin. Käyttäjällä mahdollisuus tarkastella viimeisiä kirjautumislokaatioita sijainnin ja IP-osoitteen perusteella, päätelaitteen yhteystyyppiä, sekä liittyvää aikatietoa. Palvelussa ei ole rajoituksia tai tiedotusta samanaikaisen

kirjautumisen, muuttuneen kirjautumislokaation, tai kirjautumispaikkojen sijainnin suhteen. Väärä salasana on mahdollista syöttää 11 kertaa jonka jälkeen aikajakso jolloin kirjautuminen ei mahdollista. Käyttäjän mahdollisuus tehdä oikea arvio palvelun tietoturvan tasosta on hyvä.

Peruskäyttäjälle näkyviä puutteita palvelun tietoturvassa oli mahdollisuus liian yksinkertaiseen salasanaan, IP-tietojen näyttämisen puute viestinnässä, saman salasanan uusiokäyttö, samanaikaisen käytön mahdollisuus sekä järjestelmän välittämättömyys kirjautumislokaatioista, joskin tähän auttaa kirjautumistietojen näyttäminen. Palvelun luonne on myös sellainen että sitä käytetään useilta päätelaitteilta samanaikaisesti.

5.3 Vertailumatriisi ja johtopäätökset

Edellä käsitellyt kolme sivustoa valittiin satunnaisesti Suomessa suosituimpien verkkopalveluiden listalta, huomioiden että niiden käytössä olennaista on käyttäjän kirjautuminen järjestelmään. Dropbox.com löytyy Suomessa suosituimpien palveluiden vasta sijalta 121 mutta sen käyttö on jatkuvassa kasvussa.

Vertailumatriisissa käytetty ilmaisu tietoturvavaikutelmasta on tarkastelijan subjektiivinen kokemus ja perustuu lukuisiin asioihin, sisältäen mm. tietoturvatoiminnallisuuksien esitystavan, palvelun käyttöliittymän ja viestinnän uskottavuuden, sekä palvelun toiminnan virheettömyyden.

Jokaisessa palvelussa oli puutteita käyttäjävarmennuskäytäntöjensä osalta. Puutteet on todennäköisesti ylläpidon tiedossa ja joko niiden korjaamista ei pidetä palvelun tietoturvatasolle olennaisena, tai kun kyseessä on suositut isot palvelut, korjaavien muutosten tekeminen on kallista ja työlästä. Kaikille palveluille yhteisiä puutteita olivat saman salasanan uusiokäyttö sekä samanaikaisen käytön mahdollisuus sekä järjestelmän välittämättömyys kirjautumislokaatioista. Näitä puutteita ei ole esimerkiksi Microsoftin tai Googlen verkkopalveluissa.

Jos tarkasteltujen palveluiden tietoturvaratkaisuista yhdistäisi parhaat puolet, saavutettaisiin varsin hyvän tietoturvatason omaava järjestelmä, joka kuvataan 7. luvussa.

6 Peruskäyttäjän mahdollisuudet arvioida verkkopalvelun tietoturvan taso

Aloittaessaan verkkopalvelun käytön, käyttäjä tekee tietoisesti tai tiedostamattomasti oletuksia palvelun tietoturvasta perustuen siihen tietämykseen ja kokemukseen mikä hänellä on , sekä parhaimmassa tapauksessa reagoi vastaavasti. Jos verkkopalvelu vaikuttaa epäluotettavalta, sen käyttö on syytä lopettaa, eikä sille kannata luovuttaa tietojaan. Peruskäyttäjä ei lähtökohtaisesti näe verkkopalvelun tietoturvaratkaisujen toteutustapoja, vaan voi lähinnä havainnoida ainoastaan palvelun puutteet tietoturvassa. Esimerkiksi salasanan säilytystä salatussa muodossa käyttäjä ei voi päätellä mistään, mutta salasanan säilytyksen selvätekstisessä muodossa käyttäjä voi havaita yrittäessään palauttaa sen.

Käyttäjäystävällisin tapa tietoturvaratkaisujen toteuttamiseen on läpinäkyvästi siten, että käyttäjälle tarjotaan mahdollisuus kaiken sen tiedon käyttämiseen minkä palvelussa generoi. Lisäksi käyttäjille tarjottu tieto tulisi tulkita valmiiksi niin, että siitä on käyttäjälle hyötyä. Esimerkiksi palvelun käyttäjätilin osalta IP-osoitteen näyttö on hyödyllisintä niin, että se tehdään kaikissa toiminnoissa ja tulkitaan käyttäjälle tiedoksi fyysisestä lokaatiosta.

Verkkopalvelun tietoturvallisuuteen suomalaiselle käyttäjälle vaikuttaa olennaisesti se, sijaitseeko palvelu Suomessa vai ulkomailla. Suomalaisen palvelun osalta mahdollisten rikostapausten selvittely on oleellisesti suoraviivaisempaa kuin ulkomaalaisten palveluiden osalta.

6.1 Käyttäjätietojen tallennus ja säilytys

Käyttäjätiedot on mahdollista varastaa kaikkialta, missä niitä säilytetään. Verkkopalvelun ylläpitäjän tulee kuitenkin aina tehdä parhaansa suojatakseen palvelunsa käyttäjätiedot potentiaalisilta hyökkääjiltä. Yksittäinen käyttäjä on usein heikoin lenkki, mutta käyttäjätietoja säilyttäviin palvelimiin ja palveluihin murtaudutaan jatkuvasti. Sen lisäksi, onko tunnistetietoja mahdollista varastaa, on olennaista, onko niistä varastettaessa mitään hyötyä varkaalle. Esimerkiksi sormenjälkitunnistuksessa tunnistetieto on vain digitaalista dataa, millä ei ilman sormea pysty huijaamaan sormenjäljen lukemiseen suunniteltua laitetta. Verkkopalvelun tulee säilyttää osa käyttäjätiedoista, kuten salasana ja muut arkaluontoiset tiedot, jollakin standardilla salausalgoritmilla kryptatussa muodossa. Kryptauksen lisäksi salasanan tallennuksessa tulee käyttää yksilökohtaisesti ns. kryptografista suolaa, jolloin salasanoja ei saada purettua selkokieliseksi, mahdollisen varkaan taholta, vaikka hän saisikin selville kryptauksen salausavaimen. Verkkopalvelun ylläpitäjän tulee huolehtia fyysisten palvelimien turvallisuudesta, sekä tietojen säilyvyyden että turvallisen säilytyksen osalta.

6.2 Miten käyttäjä voi itse vaikuttaa tietoturvaansa

Voidaan olettaa että peruskäyttäjä ei tiedä tietoturvaan liittyviä määritelmiä, eikä lähtökohtaisesti osaa hahmottaa kaikkia niitä uhkia joita hän voi potentiaalisesti käyttämissään verkkopalveluissa kohdata. Peruskäyttäjä ei myöskään välttämättä hahmota mihin omistamaansa tietoon tai tietojärjestelmään esimerkiksi ulkopuolisella verkkorikollisella voi olla kiinnostusta. Usein peruskäyttäjän kiinnostus tietoturvallisuuteen syntyy vasta siinä vaiheessa kun jonkinlainen ongelmatilanne on edessä tai takana. Verkkopalveluiden oletetaan olevan lähtökohtaisesti turvallisia ja henkilökohtaiset toimenpiteet tai velvoitteet hyvän tietoturvan ylläpitämiseksi hämärtyvät siinä missä vastuu tietoturvallisuudesta koetaan olevan palvelun ylläpitäjällä.

Tietojen turvaaminen liittyy pitkälti siihen mitkä ovat peruskäyttäjän arkiset toimintatavat ja rutiinit. Tietoturvaa ei pitäisi joutua jatkuvasti erikseen ajattelemaan, jolloin se voi muodostua ahdistavaksi ja rasittavaksi. Peruskäyttäjän kannattaa keskittyä hyvien menettelytapojen omaksumiseen, jotka ovat läsnä päivittäisissä tai viikoittaisissa rutiineissa. (Korpela 2005)

Mikäli peruskäyttäjän tietoturvaa tai -suojaa loukataan, käyttäjä on usein yksin ongelmansa kanssa. Esimerkiksi sähköpostipalvelun tilin luvatonta käyttöä epäillessään käyttäjän tulee tehdä asiasta rikosilmoitus. Poliisin toimivaltuudet voivat kuitenkin loppua siihen että palvelu sijaitsee ulkomailla, eikä virka-apupyyntö tuota tulosta. Voidaan myös nähdä, ettei henkilölle ole aiheutunut niin merkittävää haittaa että asiaa tulisi tutkia.

Peruskäyttäjän tulisi siis ymmärtää että vastuu tietoturvallisuuden toteutumisesta omalla kohdallaan on pääasiassa hänellä itsellään, pääpainon ollessa ennakoivassa toiminnassa. Henkilön tulee ymmärtää myös että hänen henkilökohtainen tietoturvansa voi vaikuttaa ystävien ja läheisten, sekä mahdollisesti myös työnantajan tietoturvan ja tietosuojan toteutumiseen. Verkkopalveluita käytettäessä tulisi miettiä mitä palveluissa tekee, miten ja kenen kanssa.

Peruskäyttäjän tietoturvasta julkaistaan ohjeistoja verkkolehdissä ja muilla runsaita käyttäjämääriä saavuttavilla sivustoilla. Myös eri verkkopalvelujen tarjoajat, esimerkiksi pankit, antavat käyttäjilleen ohjeistuksia hyvään tietoturvaan. Seuraavassa käyttäjälle kohdistettu, koostettu ohjeistus jolla peruskäyttäjän tietoturva pysyy hyvällä tasolla.

6.3 Ohjeistus peruskäyttäjän hyvään tietoturvaan

Huolehdi tietokoneen käyttöjärjestelmän ja perusohjelmien päivityksestä. Erittäin tärkeää päivittäminen on Windows-käyttöjärjestelmän osalta. Päivitykset suoritetaan verkon välityksellä joko päivitettävän ohjelman kautta automaattisesti tai poistamalla ja lataamalla ohjelman uusi versio.

Ota käyttöön tietokoneessa palomuuri joka valvoo koneelta lähtevää ja siihen saapuvaa tietoliikennettä. Säädä palomuuriohjelman asetukset sellaiseksi että se ei ilmoita jatkuvasti syntyneistä yhteyksistä. Jos palomuuriohjelma kysyy jonkin ohjelman osalta sallitaanko sen Internet-yhteyden käyttö, varmista että kyseessä on ohjelma joka on tarkoituksenmukaisesti asennettu koneeseen.

Asenna koneeseesi virustorjuntaohjelmisto ja huolehdi sen ajantasaisuudesta. Vaikka useimmat virustorjuntaohjelmat päivittävät itseään automaattisesti, on hyvä välillä tarkistaa että uusimmat päivitykset on ladattu.

Varmuuskopioi koneen sinulle tärkeät tiedot säännöllisti. Arvioi tietokoneen tietosisällön arvo itsellesi ja mitoita varmuuskopioinnin laajuus ja aikataulut tämän mukaisesti. Nykypäivänä automaattinen varmuuskopiointi pilvipalveluun on käyttäjälle vaivattomin ja turvallisin ratkaisu.

Määrittele salasanat monimutkaisiksi. Salasana ei saa olla yksittäinen sana, vaan siinä tulee olla satunnaisuutta joka tekee siitä monimutkaisen. Käytä muistisääntöjä monimutkaisten salasanojen muistamiseksi. Käytä eri salasanoja eri palveluissa. Salasanojen hallintaan löytyy apuohjelmia, jotka muistavat eri palveluiden salasanat ja auttavat myös muodostamaan niitä.

Suhtaudu varauksella kaikkeen verkossa vastaantulevaan. Älä toimi hätäisesti vaan harkitse tarkoin ennen kuin sitoudut ostoksiin tai teet muita sopimuksia verkossa. Käytä maalaisjärkeä ja sovella verkkokäyttäytymiseesi tarvittaessa reaalimaailman pelisääntöjä. Käytä lähdekritiikkiä, oli kyse sitten sähköpostista, verkkopalvelusta tai ohjelmasta.

Luovuta tietojasi eteenpäin vain jos tiedät mihin niitä käytetään, tämä koskien etenkin henkilötietoja. Mieti tarkkaan millaisia tietoja jaat sosiaalisessa mediassa, esimerkiksi siltä kannalta voiko potentiaalinen rikollinen käyttää hyväkseen tietoa siitä missä liikut. Suhtaudu äärimmäisellä varauksella kyselyihin joissa pyydetään kirjautumistietoja palveluihin tai luottokorttitietoja.

Laadi omalla kohdallasi tietoturvakäyttäytymiseen liittyvät pelisäännöt ja noudata niitä. Päivitä aika ajoin tietouttasi tietoturvaan liittyen. Jos tietokonettasi käyttää vaikkapa muut perheenjäsenet, myös heitä tulee opastaa asianmukaiseen tietoturvakäyttäytymiseen.

Huolehdi asianmukaisesti laitteiden ja verkkoyhteyksien turvallisuudesta ja toimivuudesta. Noudata laitteiden mukana tulevia ohjeita ja säilytä laiteiden ostokuitit, verkkopalvelusopimukset, ohjelmistojen levykkeet, sekä ohjeet paikassa josta löydät ne helposti.

Jos kohtaat ongelmia tai vaikkapa loukkauksia tietoturvasi osalta, harkitse tarvittavia toimenpiteitä rauhallisesti. Hae ohjeita ja neuvoja asiantuntevista lähteistä. Tarvittaessa ota yhteys poliisiin rikosilmoituksen muodossa jos koet että kohdallasi on tapahtunut rikos.

7 Verkkopalvelun tietoturvakriteeristö ja hyvät tietoturvaratkaisut

Verkkopalveluiden määrä ja monimuotoisuus kasvaa jatkuvasti. Palveluiden tietoturva-, sekä käyttäjätunnistusratkaisuja on monenlaisia. Joissain palveluissa käyttäjän tietojen turvaaminen voi olla toissijaista, joissain äärimmäisen tärkeää. Esimerkiksi pankkipalvelujen osalta käyttäjällä on oletus siitä että palvelun tietoturvallisuus on erittäin korkealla tasolla ja käyttäjä voi olla varma siitä että hänen asiointinsa on turvallista ja ongelmatonta.

Verkkopalveluja suunnitellessa lähtökohtana pitäisi olla aukottomat yleisesti hyväksytyt tietoturvaratkaisut. Todellisuudessa verkkopalveluita voi kuitenkin perustaa kuka tahansa ja perustamisen budjetti voi vaihdella lähes mitättömästä, esimerkiksi pienen piirin foorumista, kattavaan, esimerkiksi maailmanlaajuisesti suosittuun sähköpostipalveluun. Tämän vuoksi on selvää että myös tietoturvaratkaisut verkkopalveluissa voivat vaihdella laajalla skaalalla, eikä tähän lainalaisuuteen ole lähitulevaisuudessa muutosta nähtävissä. Valitettava tosiasia on siis että verkkopalveluiden tietoturvan määrittelee perustajansa asiantuntijuuden lisäksi sen toteutukseen allokoitavien resurssien määrä.

Koska peruskäyttäjälle verkkopalvelun tietoturvaratkaisujen toteutusaste ei useimmiten ole selkeästi havaittavissa, tilannetta voisi helpottaa portaittainen kriteeristö, jolla verkkopalvelut merkitsisivät oman palvelunsa tietoturvaratkaisujen tilan. Tällainen kriteeristö ja ne asiat joita se ottaa huomioon, tulisi luonnollisesti olla helposti peruskäyttäjälle helposti omaksuttavissa, siinä vaiheessa kun käyttäjä tekee valintaa palvelun käytöstä. Kriteeristön avulla ja yksinkertaisesta merkinnästä havainnoimalla peruskäyttäjä voisi tehdä johtopäätökset siitä haluaako hän palvelua käyttää, sekä mitä hän voi odottaa verkkopalvelun tietoturvaratkaisuilta.

Koska palveluiden määrä ja vaihtuvuus Internetissä on valtava, kriteeristöä ei olisi järkevää toteuttaa sertifikaattiperiaatteella. Kyseessä voisi sen sijaan olla jonkinlainen palvelulupaus käyttäjälle käytetystä tietoturvaratkaisusta. Nykytilanteessa, jossa verkkopalvelujen tietoturvaratkaisujen osalta ei ole valvontaa tai säännöstöä, verkkopalvelujen tietoturvaratkaisujen pettämisen seurauksena suurimmat kärsijät ovat sen käyttäjät. Tilanteessa jossa verkkopalvelujen määrän ja monimuotoisuuden kasvu on jatkuvaa, palvelulupauksella tietoturvatasosta voitaisiin mahdollisesti luoda kannustavaa ilmapiiriä hyvien tietoturvakäytänteiden luomiseen. Kriteeristön pääasiallinen merkitys pitkällä tähtäimellä olisi siis ennaltaehkäisevä niin, että palveluja suunnitellessa otettaisiin huomioon hyvät ja asianmukaiset tietoturvaratkaisut.

Verkkopalveluiden tietoturvakriteeristö tulisi todellisuudessa olla alan tietoturva-asiantuntijatahojen suunnittelema ja määrittelemä, yhteistyössä merkittävien verkkopalveluja tarjoavien ja koordinoivien tahojen kanssa, huomioiden palvelujen nykytilan ja kehityksen tulevaisuudessa. Tässä työssä voidaan kuitenkin tarkastella millaisia ovat hyvän verkkopalvelun tietoturvatoiminnallisuudet, joiden perusteella verkkopalveluiden tietoturvakriteeristö voitaisiin muodostaa.

7.1 Verkkopalvelun hyvät tietoturvakäytännöt

Hyvän verkkopalvelun tietoturvakäytännöt lähtee liikkeelle rekisteröimisprosessista. Kun käyttäjä alkaa syöttämään tietojaan, tulee yhteyden palvelimen ja käyttäjän välillä olla suojattu. Käyttäjältä ei tule pyytää rekisteröinnissä kuin ne tiedot jotka ovat palvelun kannalta oleellisia. Käyttäjälle näytettävät käyttöehdot tulee olla selkeästi laaditut ja mahdollisesti osioitu ymmärrettävästi. Koska harva jaksaa pitkiin käyttöehtoihin perehtyä, olisi hyvä jos käyttöehdoista näytettäisiin käyttäjälle tiivistelmä.

Rekisteriseloste tulee olla asianmukainen ja päivitetty palvelun nykytilaa vastaavaksi. Käyttäjän antamiin tietoihin tulee soveltaa tarkistuksia, etenkin salasanan osalta. Salasanalta tulee vaatia riittävä pituus sekä numeroiden tai erikoismerkkien käyttöä. Syntaksin pakotuksen lisäksi on hyvä ohjeistaa käyttäjää miten turvallinen salasana generoidaan. Sähköpostiosoitteen oikeellisuus on syytä varmentaa vahvistusviestillä. Käyttäjän kirjautuessa palveluun tulee ilmaista selkeästi jos käyttäjästä julkaistaan jotain tietoja avoimesti verkossa automaattisesti rekisteröitymisen yhteydessä.

Käyttäjälle tulee tarjota suhteessa palvelun tietoturvavaatimuksiin vaihtoehtoisia kirjautumisen varmennustapoja, esimerkiksi mobiililaitteella tai pankkitunnuksilla. Hyvä käytäntö on porrastaa käyttäjän tunnistustaso sen mukaan mitä hän palvelussa tekee, sekä informoida käyttäjän tunnistuksesta muita käyttäjiä. Palveluun kirjautumisessa tulee olla varmistuksia, niin ettei salasanaa voida yrittää arvata murtoa yrittävän toimesta loputtomasti. On hyvä antaa käyttäjälle järkevä määrä mahdollisuuksia salasanansa arvaamiseen, esimerkiksi 10 kappaletta, ja sen jälkeen asettaa ajallinen tauko seuraavaan yritykseen. Käyttäjille on hyvä viestiä tapahtumasta missä hänen salasanaansa on yritetty arvata ja järjestelmä on lukkiutunut.

IP-osoitetiedot on jokaisessa verkkopalvelussa ylläpitäjän käytettävissä. Osoitetiedot on hyvä tarjota myös käyttäjälle hänen oman tilinsä osalta. IP-osoitetiedot voidaan näyttää sisäänkirjautuneelle käyttäjälle viimeisten kirjautumisten osalta, sekä esimerkiksi salasanan uusimispyyntöjen osalta. IP-osoite ei itsessään kerro peruskäyttäjälle paljoa, vaan sitä

se vaatii tulkintaa. On hyvä jos tämä tulkinta voidaan tehdä automaattisesti käyttäjän puolesta, muuttamalla IP-osoite paikkatiedoksi, sekä vertaamalla sitä esimerkiksi kirjautumisten osalta käyttäjän aikaisempiin osoitteisiin ja ilmoittamalla poikkeavuuksista. Oikeanlaisella IP-osoitetietojen läpinäkyvällä hyödyntämisellä saavutetaan paljon käyttäjän oman tietoturvatulkinnan osalta, eikä sille löydy korvaajaa muista metodeista. IP-osoitetietojen osalta voidaan, suhteessa palvelun luonteeseen, tehdä rajoituksia, esimerkiksi niin että päällekkäistä kirjautumista kahdesta eri lokaatiosta sallita. Kahta kirjautumislokaatiota voidaan verrata keskenään ja tehdä päätelmä niiden etäisyydestä, sekä siitä onko toisessa lokaatiossa kyseessä käyttäjää vakoileva taho. Jotkut palvelut, kuten pilvitallennuspalvelut on suunniteltu nimenomaisesti useasta päätelaitteesta samanaikaisesti käytettäväksi, ja siten niiden osalta ei voi tehdä rajoituksia, vaan käyttäjän nähtävissä tulee olla kirjautumislokaatiot. Varmistuksia kirjautumiseen IP-osoitetietojen perusteella voidaan tehdä myös niin, että verrataan viimeistä kirjautumispaikkaa tai IP-osoitetta nykyiseen. Mikäli näiden etäisyys on suuri, suoritetaan kirjautumiseen liittyen lisävarmennustoimenpiteitä.

Käyttäjän tiedot tulee tallentaa palvelimelle asianmukaisesti. Salasana tulee kryptata vahvasti ja yksilöllisesti. Palvelun luonteesta riippuen myös muita tietoja voidaan salata. Palvelun palvelimien osalta tulee laskelmoida salattujen tietojen käsittelyn taakka.

Salasanan ja käyttäjätunnuksen palautuksen toteutus käyttäjälle sähköpostilla, esimerkiksi unohtamistapauksessa, on palvelun tietoturvan oleellinen ja usein vähälle huomiolle jäävä osa-alue. Tulee huomioida että verkkopalveluissa paljon käytetty turvakysymys-metodi sisältää merkittävän riskin tietojen kalastelun osalta. Itse salasanan palautusprosessi ei saa antaa sitä yrittävälle ylimääräisiä tietoja käyttäjästä. Turvakysymys tulee sitoa muuhun varmennustietoon, eikä yhteen käyttäjään liittyvään kysymykseen vastaamisen taakse saa asettaa järjestelmään pääsyä. Kaikki salasanan palautustapahtumaan liittyvät tiedot, kuten IP-osoite josta pyyntö on tehty sekä aikatieto tulee ilmaista käyttäjälle viestinnässä esimerkiksi sähköpostilla. Käyttäjälle tulee viestittää salasanan palautustapahtumasta sitä ennen ja sen jälkeen. Kun käyttäjä muuttaa salasanansa, järjestelmän ei tule sallia aikaisemmin käytettyjä salasanoja tai välttämättä edes variaatioita niistä.

Verkkopalvelua käyttäessään ja sinne materiaalia ladatessaan sekä tuottaessaan, käyttäjälle tulee näyttää mikä on materiaalin julkisuusaste. Palvelun luonteen ja sen sääntöjen puitteissa käyttäjälle tulee antaa mahdollisuus valita kaikkien tietojensa ja materiaalin osalta, näytetäänkö niitä julkisesti. Käyttäjätiedot tulee olla helposti käyttäjän löydettävissä ja muokattavissa, mielellään samasta paikasta palvelussa.

Yleisesti palvelun tietoturvaominaisuuksista tulisi tehdä käyttäjälle mahdollisimman läpinäkyviä. On parempi että käyttäjän nähtävissä on hänen halutessaan pitkälti kaikki tiedot mitkä järjestelmään kirjautuvat käyttäjien toiminnan osalta muutenkin. Tietoturvaominaisuuksista tulee viestiä käyttäjää oikeanlaisella kielellä konkreettisesti, tulkita automaattisesti tapahtumia ja tietojoukkoja, sekä esittää näiden tulkinnat käyttäjälle.

8 Yhteenveto ja johtopäätökset

Nykypäivän informaatioyhteiskunnassa verkkopalveluiden määrä ja monimuotoisuus kasvaa jatkuvasti. Sosiaalisen median ja digitaalisten palveluiden merkitys etenkin nuorelle ikäpolvelle kasvaa. Samalla ikuinen totuus käyttäjän tai palvelun maineen hauraudesta on läsnä. Fyysisestä omaisuudesta huolehtimisen rinnalle on noussut huoli sähköisen identiteetin ja immateriaalisen omaisuuden turvaamisesta. Verkkopalveluissa säilötään yksityistä materiaalia ja käyttäjätietojen joutuminen vääriin käsiin voi tuntua käyttäjästä samalta kuin vaikkapa kotiavainten menetys. Silti tietoturva voi olla monelle mystinen ja hahmoton käsite. Verkkopalveluiden tietoturva-, sekä käyttäjävarmennusratkaisut ovat uskottavan palvelun kannalta ensisijaisen tärkeitä ja ne tulisi suunnitella huolellisesti vaadittua tietoturvatasoa vastaavaksi.

Kansallinen lainsäädäntö verkkopalvelujen ja kansalaisen tietoturvaan liittyen kulkee jälkijunassa. Lainsäädäntö keskittyy säännöstön luomiseen suurille, esimerkiksi verkkoyhteyksiä tai televisiopalveluita tarjoaville operaattoreille, niiden toimintaan liittyen. Verkkopalvelujen perustamiseen, sekä siihen millainen on tietoturvallinen verkkopalvelu, ei Suomen lainsäädännössä varsinaisesti oteta kantaa. On kuitenkin positiivista huomata että tietoverkkorikoksiin ja tietosuojan merkitykseen liittyviä direktiivejä ja asetuksia valmistellaan Euroopan unionissa. Valmistuessaan ja hyväksyttyinä nämä direktiivit antavat hyviä ohjeita paremmalle kansalliselle lainsäädännölle myös Suomessa.

Hyvän tietoturvan keskiössä on käyttäjä, joka valitsee mitä palveluita käyttää ja miten. Mikäli käyttäjä ei välitä omasta tietoturvastaan, mikään tietoturvaratkaisu ei sitä myöskään korvaa. Peruskäyttäjän tietoturva muodostuu aukottomasta kokonaisuudesta toimintatapoja. Käyttäjän tietoturvaohjeistoja julkaistaan aika ajoin eri tahoilla. Perusohjeistus pysyy yleisesti samana. Luku kuusi sisältää kuvauksen peruskäyttäjän hyvistä tietoturvakäytännöistä. 7. luvussa käsiteltiin millaisia konkreettisia toiminnallisuuksia verkkopalvelun käyttäjävarmennusratkaisuja suunnitellessa tulisi huomioida.

Verkkopalveluiden hyvät tietoturvaratkaisut ottavat huomioon erilaiset käyttäjät, vaihtelevine tietoturvakäsityksineen, ja opastavat tai edellyttävät hyviä tietoturvakäytänteitä. Käyttäjävarmennuskäytänteitä on olemassa laaja valikoima. Yleisimmin verkkopalveluissa käytössä olevassa käyttäjävarmennuksessa tunnuksen ja salasanan kautta, on useita heikkouksia jotka eivät ole muuttuneet vuosikymmeniin. Tulevaisuudessa voidaan nähdä käyttäjävarmennustekniikoiden siirtymistä entistä enemmän automaattiseksi, esimerkiksi biometriseen tunnistukseen pohjautuvaksi.

8.1 Oma työskentely ja oppiminen

Omaa työskentelyni opinnäytetyön teossa olisi voinut olla ajankäytöllisesti harkitumpaa. Vaikka lähdeaineistoon tutustuminen jakautui alkuperäisen aikataulun mukaisesti, loppukädessä itse työ syntyi melko lyhyessä ajassa, parin viikon intensiivisen työstämisen tuloksena. Aiheen käsittelyssä olisin voinut keskittyä tarkemmin vain joko käyttäjän tai palvelun suunnittelun näkökulmaan. Työn laajuutta olisi voinut rajoittaa hyvissä ajoin tutkimusongelmakysymyksiä vähentämällä.

Työn aihevalinta muodostui kiinnostuksestani tietoturvaa kohtaan. Vaikka aihe onkin tullut vuosien saatossa tutuksi, osa käyttäjävarmennukäytäntöihin liittyvästä tiedosta ja suuri osa lainsäädännöllisestä tiedosta tuli uutena. Koen että työntekoprosessin aikana perustermistö aiheeseen liittyen täsmentyi itselleni. Työn tavoitteena oli tarjota kattava paketti tietoa liittyen peruskäyttäjän tietoturvaan verkkopalveluissa. Arvioisin että työ antaa peruskäyttäjälle riittävät ohjeet hyvään tietoturvaan liittyen, sekä tarjoaa verkkopalvelun tietokäyttäjävarmennusratkaisuja suunnittelevalle käytännössä mallin hyvästä käyttäjävarmennustoteutuksesta. Arvioisin että työ vastaa tutkimusongelmakysymyksiin riittävästi tai hyvin.

Lähteet

Andreasson, Ari., Koivisto, Juha., Ylipartanen, Arto. 2014. Tietosuojavastaavan käsikirja 2. Tietosanoma.

Hakala, Mika., Vainio, Mika., Vuorinen, Olli. 2006. Tietoturvallisuuden käsikirja. Dodenco.

Julkishallinnon yhteinen verkkotunnistamisen ja -maksamisen palvelu, (Vetuma). Luettu 5.12.2014. Luettavissa: http://www.suomi.fi/suomifi/tyohuone/yhteiset_palvelut/verkkotunnistaminen_ja_maksaminen_vetuma

Järvinen, Petteri. 2003. Salausmenetelmät. Docendo.

Keskusrikospoliisi 2014a. Huijauksen monet muodot. Luettu 2.12.2014. Luettavissa: www.poliisi.fi/krp/nettihuijaus

Keskusrikospoliisi 2014b. Tietotekniikkarikollisuus. Luettu 2.12.2014. Luettavissa: http://www.poliisi.fi/poliisi/krp/home.nsf/pages/63B3FC75928EFB7EC2256C8B0043A41E?opendocument

Keskusrikospoliisi 2014c. Tietotekniikkarikosten tunnusmerkistöjä. Luettu 3.12.2014. Luettavissa: http://www.poliisi.fi/poliisi/krp/home.nsf/pages/C2315A82BE4616A1C225783E0056EDE0

Korpela, Jukka. 2005. Turvallisesti netissä. Docendo.

KRYSP, Sähköisen asiointipalvelun työpöytäratkaisu, Vaatimusmäärittely, 2010. Luettu 5.12.2014. Luettavissa: http://www.paikkatietopalvelu.fi/Raportit/Vaatimusmaarittely_v2.00.pdf

Laakso, Matti. Verkkopalvelun tarjoaja – kunnioitatko käyttäjän yksityisyyttä? Saatavissa: http://julkaisumyynti.turkuamk.fi/filemanager/productfiled/1230file1Upload.pdf#page=29

Liikenne- ja viestintäministeriö 2014. Tietoyhteiskuntakaari. Luettu 4.12.2014. Luettavissa: http://www.lvm.fi/web/hanke/tietoyhteiskuntakaari

Muttilainen, Vesa., Huotari, Vesa 2014. Poliisin toimintaympäristö - Poliisiammattikorkeakoulun katsaus 2014. Luettu 2.12.2014. Luettavissa

http://www.poliisiammattikorkeakoulu.fi/poliisi/poliisioppilaitos/home.nsf/files/7F5D1EBE712AABF6C2257D3A0029EA8A/$file/Raportteja_112_web.pdf

Oikeusministeriö 2014. Tietoverkkorikosdirektiivin täytäntöönpano. Luettu 3.12.2014. Luettavissa:
http://oikeusministerio.fi/fi/index/julkaisut/julkaisuarkisto/1398348937425/Files/OMML_27_2014_mietinto_104_sKoRJATTU.pdf

Tietosuojavaltuutetun toimisto. 2010. Biometrinen tunnistus, mikä se on? Luettu 5.12.2014. Luettavissa:
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqPiEON/Biometrinen_tunnistus_mika_se_on.pdf

Thomas, Tom. 2005. Verkkojen tietoturva. Edita publishing Oy / IT Press.

Viestintävirasto 2014a. Mitä tulikaan sovittua? Luettu 28.11.2014. Luettavissa:
https://www.viestintavirasto.fi/attachments/cert/certtiedostot/Sopimukset_ja_yksityisyyden_suoja_20141028.pdf

Liitteet

	HTTPS	Turvallisen salasanan pakottaminen	Rekisteröinnin prosessi ja kirjautuminen	Käyttöehtojen laajuus ja esitystapa	Salasanan säilytys salatussa muodossa	Kaksivaiheinen varmennus ja yksityisyysasetukset	Salasanan palautusmetodit - turvakysymyksen toteutus	Käyttäjän mahdollisuus tarkastella viimeisiä toimintoja tai kirjautumis-paikkoja	Käyttäjän mahdollisuudet hahmottaa mitä tietoja hänestä näytetään muille	Uuteen kirjautumis-paikkaan liittyvä varmennus	Tietoturva-ja käyttöominaisuuksien esitys käyttäjälle	Sisään-kirjautumiseen liittyvät varmistukset
Suomi24 - verkko-sivuston sähköposti-palvelu	Käytössä rekisteröinnistä lähtien	6-20 merkkiä, vähintään yksi kirjain ja yksi numero. Ei hyväksytä merkkejä å, ä tai ö. Ei älykästä suodatusta, ts. "terotesti1" kelpaa.	Captcha -varmistus, ei pakkoa syöttää henkilötietoja. Perustiedot vaadittu, ei vahvaa henkilötunnistusta. Vaihtoehtoisen sähköpostin vahvistus suoritettava erikseen. Rekisteröinti luo käyttäjälle automaattisesti julkisen profiilin. Kirjautuminen käyttäjätunnuksella.	16 kohtaa. Laajuus n. 6 sivua. Esitystapa ja käytetty kieli selkeää. Palvelun tarjoajalla mahdollisuus muuttaa käyttöehtoja vapaasti ilmoituksella.	Ei viitteitä ettei salasanaa säilytettäisi salatussa muodossa.	Ei muita varmennekeinoja kuin tunnus / salasana. Yksityisyysasetukset hyvät. Käyttäjätunnuksen poistaminen selkeää. Mahdollisuus valita kuka pääsee katsomaan käyttäjätietoja "kaikki / kaverit / ei kukaan".	Salasanan palautus vain rekisteröitymisen yhteydessä annettuun osoitteeseen syöttämällä käyttäjätunnus. Palautuksen metodina uudistuslinkin tilaus ja uuden salasanan asettaminen linkin päässä. Ei IP-osoitetietoa palauttajasta. Aikaisemman salasanan asettaminen onnistui uudelleen. Sähköpostiviestillä ilmoitus salasanan uudistamisesta.	Ei toimintoa järjestelmässä.	Käyttäjätiedot listattuna muutettavissa. Jokaisen tiedon osalta mahdollisuus valita sen "näyttäminen profiilissa", eli julkisesti. Lähtökohtaisesti profiili on julkinen ja mm. oikea nimi näytetään.	Ei rajoituksia kirjautumispaikkoihin tai päällekkäisyyksiin liittyen. Palvelun käyttö onnistui samaan aikaan sekä suomalaisesti IP-osoitteesta että toisesta osoitteesta jonka fyysinen lokaatio oli n. 8000 km päässä.	Palvelussa on käytössä 90 päivän aktiivisuusaika. Käyttäjän tiedot poistetaan 90 päivän epäaktiivisuuden jälkeen. IP-tietoja ei hyödynnetä käyttäjälle näkyvästi missään toiminnoissa. Tietoturvaominaisuudet ja vaikutelma riittävä, näyttötapa ja viesteintä niiden osalta melko selkeää.	Ei varmistusta muuttuneeseen lokaatioon liittyen. Virheellisen salasanan syöttömahdollisuudessa ei rajoitusta?
Huuto.net –verkko-palvelu	Käytössä rekisteröinnistä lähtien	Ohjeistuksena salasanan oltava vähintään 8 merkkiä. Älykäs suodatus jossa tarkistuksen jälkeen "salasana ei voi olla sama kuin käyttäjätunnus". Kuitenkin "terotesti1" kelpaa.	Käyttätietojen syöttämisen jälkeen sähköpostiin lähetetty vahvistusviesti rekisteröitymisestä. Vaatii käyttäjältä 24 tunnin sisällä viestin linkkiin reagoimista rekisteröimisen jatkamiseksi. Ei henkilötietojen syöttöpakkoa.	Käyttöehtojen laajuus n. 5 sivua. Jaottelu ja kieli selkeää. Rekisteriseloste asianmukainen.	Ei viitteitä ettei salasanaa säilytettäisi salatussa muodossa.	Ei muuta kirjautumismetodia kuin tunnus / salasana. Mahdollisuus maksulliseen plus-palveluun jossa varmennetaan käyttäjän henkilötiedot, jonka jälkeen käyttäjälle uusia toimintoja palvelun sisällä.	Salasanan palautus syöttämällä käyttäjätunnus, jonka jälkeen sähköpostiosoitteeseen lähetään ohjeet salasanan vaihtoon. Ohjeessa salasanan vaihdon tilaajan IP-osoitetieto sekä kellonaika. Aikaisemman salasanan asettaminen onnistui uudelleen.	Ei toimintoa järjestelmässä.	Käyttäjätiedot listattuna muutettavissa. Ei mitään indikaattoreita yksityisistä / julkisista tiedoista. Ei mahdollista tarkastella omaa profiilia. Sen ilmaisu, mitä tietoja toisille käyttäjille minkäkin toiminnan osalta itsestä näytetään, ei selkeää.	Ei rajoituksia kirjautumispaikkoihin tai päällekkäisyyksiin liittyen. Palvelun käyttö onnistui samaan aikaan sekä suomalaisesti IP-osoitteesta että toisesta osoitteesta jonka fyysinen lokaatio oli n. 8000 km päässä.	Palvelun Tietoturvaominaisuuksista palvelun luonteeseen liittyen muiden käyttäjien tunnistautumisen indikointi on selkeää. Käyttäjä voi valita tunnistautuuko palveluun, sekä voi halutessaan käyttää palvelua vain henkilötiedoilla varmistettujen toisten käyttäjien kanssa. Tietoturvavaikutelma hyvä.	Palvelun täysversion käyttö TOR-verkon läpi ei onnistunut, vaan palvelusta piti käyttää mobiiliversiota. Virheviesti joka käyttäjälle TOR-verkosta kirjautuessa ilmaistaan oli "virheellinen tunnus tai salasana". Todellisuudessa käytön eston syy on jokin muu varmistustoimenpide joka käyttäjälle ei näy. Virheellisen salasanan syöttömahdollisuudessa ei rajoitusta?
Dropbox –pilvipalvelu	Käytössä aina.	Suositus hyvän salasanan mudostamistekniikasta. Salasanan oltava 6 merkkiä pitkä, ei muita sääntöjä. Ei älykästä suodastusta, ts. "terote" kelpaa.	Rekisteröinti yksinkertainen. Nimen, sähköpostiosoitteen ja salasanan syötön jälkeen palvelun aloitus. Kirjautuminen sähköpostiosoitteella.	Käyttöehdot englanniksi. Laajuus n. 10 sivua, jaoteltu viiteen alaosioon. Käytetty kieli suureksi osaksi selkeää. Käyttöehtoihin pätee Californian osavaltion lainsäädäntö. Palvelun tarjoaja päivittää käyttöehtoja "aika ajoin". Mikäli käyttöehdoissa muutetaan käyttäjien oikeuksia, ilmoitus tehdään sähköpostitse.	Ei viitteitä ettei salasanaa säilytettäisi salatussa muodossa.	Kaksivaiheinen varmennus mahdollinen, jossa uudella laitteella palveluun kirjauduttaessa salasanan lisäksi tarvitaan puhelimeen lähetetty koodi. Yksityisyysasetukset hyvät. Mitkään käyttäjän tiedot ei ole julkisia ellei erikseen jotain sisältöä julkaista ja linkata verkkoon.	Salasanan palautus rekisteröitymisen yhteydessä annettuun osoitteeseen syöttämällä osoite. Virheellisen osoitteen syöttämisestä virheilmoitus, oikean sähköpostiosoitteen syöttäminen tuottaa ilmoituksen salasanan palautusviestin lähetyksestä. Sähköpostiin linkki salasanan vaihtamisosoitteeseen. Aikaisemman salasanan asettaminen onnistui uudelleen. Ei sähköposti-ilmoitusta salasanan vaihdosta.	Toteutettu niin että näytetään listalla jokaisesta eri kirjautumisesta selaimen malli, kirjautumismaa, kirjautumisaika, sekä IP-osoite mistä kirjauduttu.	Käyttäjätiedot osioittain muutettavissa. Käyttäjälle selkeää ettei hänestä näytetä tietoja oletuksena verkkoon. Sisällön jakaminen linkkien muodostamisen kautta toimivaa. Mikään sisältö ei ole julkisena jaossa ellei sille generoida linkkiä.	Ei rajoituksia kirjautumispaikkoihin tai päällekkäisyyksiin liittyen. Palvelun käyttö onnistui samaan aikaan sekä suomalaisesti IP-osoitteesta että toisesta osoitteesta jonka fyysinen lokaatio oli n. 8000 km päässä.	IP-tietoja ei hyödynnetä sähköpostiviestinnässä. Tietoturvaominaisuudet asianmukaiset, näyttötapa ja viestintä selkeää. Yleinen tietoturvavaikutelma hyvä.	Ei varmistusta muuttuneeseen lokaatioon liittyen. Virheellinen salasana mahdollista syöttää 11 kertaa jonka jälkeen muutaman minuutin ajallinen käyttökatkos jona aikana kirjautuminen ei mahdollista.