Tampereen ammattikorkeakoulun ja Oulun yliopiston opiskelijoiden tietoisuus Web-järjestelmien uhista ja haavoittuvuuksista

Oulun yliopisto
Tietojenkäsittely tieteiden laitos
Pro gradu-tutkielma
Jari Oiva
13.12.2013

Tiivistelmä

Web-järjestelmät ovat yleistyneet nykyään monissa organisaatioissa nopeaa tahtia. Organisaatiossa hyödynnetään Internet protokollaa ja tietoarkkitehtuuria. Myös pilvipalvelujen käyttö on yleistynyt nopeasti. Tämä tuottaa vaikeuksia tietoturvassa ja yksityisyydessä. Kaikki tieto, joka kulkee verkon välityksellä saattaa olla alttiina monille uhille. Hyökkääjät pyrkivät käyttämään hyväkseen haavoittuvuuksia, joista moni viittaa koodi-injektioon. Normaalisti hyökkääjien motiivina on hyötyä taloudellisesti saada toisesta tietoa tai tehdä vain kiusaa. Useasti hyökkäyksien kohteeksi joutuvat yritykset, mikä vaikuttaa suoraan yritysten asiakkaisiin.

Tässä tutkielmassa perehdyttiin web-järjestelmien tietoturvaongelmiin. Tutkimuskysymyksenä oli, mitä haavoittuvuuksia on web-järjestelmissä, mikä web-järjestelmiä mahdollisesti uhkaa ja millainen tietämys korkeakouluopiskelijoilla on kyseisistä asioista. Tutkimuksessa otettiin esille kymmenen Viestintäviraston julkaisemaa tietomurtotapausta web-järjestelmiin/tietoverkkoon. Tutkimusta varten haastateltiin opiskelijoita Oulun yliopistolta ja Tampereen ammattikorkeakoululta.

Tutkimuksen kohteena oli Tampereen ammattikorkeakoulun ja Oulun yliopiston opiskelijoita, joista pääosa oli toisen vuoden opiskelijoita. Tutkimuksessa perehdyttiin web-järjestelmien tietoturvaan ja yksityisyyteen, minkälainen näkemys korkeakouluopiskelijoilla on web-järjestelmien tietoturvasta, yksityisyydestä ja tutkittiin niihin kohdistuneita uhkia ja haavoittuvuuksista. Työssä tutkittiin myös miten kahden korkeakoulun opiskelijoiden näkemykset uhista ja haavoittuvuuksia poikkesivat toisistaan. Tutkimus suoritettiin haastattelujen avulla.

Korkeakouluopiskelijoilta kysyttiin yleisiä kysymyksiä tietoturvasta, yksityisyydestä ja tietoutta niiden uhista ja haavoittuvuuksista. Tutkimuksen perusteella voitiin päätellä, että opiskelijat osasivat hyvin määritellä tietoturvan ja yksityisyyden. Opiskelijat osasivat myös erotella uhat ja haavoittuvuudet, mutta yksityiskohtaisessa tietämyksessä web-järjestelmiin kohdistuvista haavoittuvuuksista oli puutteita. Opiskelijat eivät myöskään osanneet määritellä, mitä uhkia liittyy Internet protokollaan. Vastauksissa eroavaisuuksia ei suuremmin ilmennyt koulujen välillä. Oppilaat ovat hakeneet tiedot kyseisistä asioista pääsääntöisesti työpaikan tai harrastuksien parista. Kokeneemmilla opiskelijoilla oli parempi tietämys haavoittuvuuksista, kuin uusilla opiskelijoilla.

Avainsanat: web-järjestelmä, tietoturva, yksityisyys, uhka, haavoittuvuus

Esipuhe

Tutkimusaiheeni valikoitui siten, että olen kiinnostunut tietoturvasta viestiliikenteen kannalta, miten voidaan kommunikoida verkon välityksellä mahdollisimman turvallisesti ja minkälaista tietoutta alalle pyrkivillä on. Kohderyhmäksi valikoitui nykyinen kouluni (Oulun yliopiston) opiskelijat ja entinen kouluni (Tampereen ammattikorkeakoulun) opiskelijat, joiden tietoturvallisuustietoisuutta pyrittiin selvittämään uhkien ja haavoittuvuuksien osalta. Erityiskiitokset tästä menee Tampereen ammattikorkeakouluun, miten hyvällä asenteella sieltä lähdettiin tähän tutkielmaan mukaan.

Oulu 13.12.2013

Lyhenteet

APT	Advanced persistent threat
ATK	Automaattinen tietojenkäsittely
CSRF	Cross-Site Request Forgery
DNS	Domain Name System
DOM	Document Object Model
DoS	Denial of Service
EU	Euroopan Union
GIF	Graphic Interchange Forma
GPS	Global Positioning System
HTML	Hypertext Markup Language
HTML5	Hypertext Markup Language5
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure-as-a-Service
IBM	International Business Machines
ICT	Information and communications technology
IRC	Internet Relay Chat
IP	Internet protocol
IPA	Information-technology Promotion Agency
IT	information technology
ITL	The Information Technology Laboratory
JPG	Joint Photographic Experts Group
MDE	Model-Driven engineering
MSL	Maximum segment lifetime
MSS	Maximum segment size
MSS	Maximum segment size

MTU	Maximum segment lifetime
Nato	The North Atlantic Treaty Organization
NFC	Near field Communication
NIST	The National Institute of Standards and Technology
NT	New technology
OMIS	organization memory information system
OS	Operating system
OSI	Open Systems Interconnection
PaaS	Platform-as-a-Service
PC	Personal computer
PEP	Packetized Ensemble Protocol
PGP	Pretty Good Privacy
PK	Pieni ja keskisuuri yritys
PKI	Public Key Infrastructure
QoS	Quality of Service
QUI	Graphical User Interface
RDBMS	Relation Database Management System
SaaS	Software-as-a-Service
SATAN	the Administrator Tool for Analyzing Networks
SSL	Secure Sockets Layer
SMTP	Simple Mail Transfer Protocol
SOA	Service-oriented applications
SuPo	Suojelupoliisi
SQL	Structured Query Language
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
WWW	World Wide Web

XSS Cross-Site Scripting

Sisältö

1. Johdanto

Internet-selainten pahin tietoturvauhka ei ole enää puskurien ylivuotohaavoittuvuudet, vaan tilalle on tullut uudenlainen ohjelmointivirhe, jota kutsutaan XSS (Cross-Site Scripting)-haavoittuvuudeksi. XSS-haavoittuvuus toimii web-palvelimien sovellusten välityksellä. joka ottaa vastaan ulkoisesta lähteestä dataa. Tällaista dataa voivat lähettää normaalit käyttäjät WWW-järjestelmän välityksellä. Tällöin muutos tavallisista käyttäjistä sisällöntuottajiksi on tuonut haavoittuvuuksiin uuden ulottuvuuden. (Hämäläinen, 2007.) Tässä tutkimuksessa syvennytään tarkastelemaan web- järjestelmien erilaisia uhkia ja haavoittuvuuksia. Tutkimuskohteeksi tähän valikoitu Tampereen ammattikorkeakoulun ja Oulun yliopiston tietojenkäsittelyn oppilaita, joilta kysyttiin uhista ja haavoittuvuuksista. Koska normaaleista käyttäjistä muodostuu web-järjestelmien kehittäjiä, tällä tutkimuksella pyritään selvittämään, minkälainen tietous tietojenkäsittelyn opiskelijoilla on tietoturvasta.

1.1 Tutkimusongelma ja tutkimuskysymys

Tutkielman tarkoituksena oli selvittää Tampereen ammattikorkeakoulun ja Oulun yliopistonopiskelijoiden tietoisuutta web-järjestelmien haavoittuvuuksista, samalla myös selvittää mitä eroavaisuuksia löytyy oppilaiden näkökulmissa. Tutkimuksen taustaa selvitettiin tieteellisten artikkeleiden ja kirjallisuuden pohjalta. Materiaalia etsittiin Internetistä ja muista aikaisemmista tutkielmista. Työssä tutkittiin, minkälaisia tapauksia liittyy web-järjestelmien tietoturvaan, miksi tietoturva on nykypäivänä tärkeä huomioida ja kuinka hyvin Tampereen ammattikorkeakoulun ja Oulun yliopiston opiskelijat tiedostavat asian. Tutkimuksen toisena aiheena oli tehdä tapauskohtaista tutkimusta tietoturvasta ja yksityisyydestä hyökkäyksistä/uhista. Tähän on hyödynnetty viestintäviraston julkaisemia raportteja. Ensimmäisenä tutkimuksen aiheena tarkasteltiin yleisesti web-järjestelmiä (Tolvanen, 2007.) niihin liittyviä kehityssuuntia ja tietoliikennettä web- järjestelmien välillä. Tutkimuksessa otettiin myös esille yritysten näkökulma web-järjestelmissä, koska yritykset joutuvat monesti tietomurron kohteeksi (Porvari, 2012). Viimeisenä kirjallisuus katsauksessa tutkittiin tietoturvaa/yksityisyyttä, niihin kohdistuvia uhkia ja hyökkäyksiä. Näiden aineistojen pohjalta voitiin tehdä vertailua, minkälainen tietous Tampereen ammattikorkeakoulun ja Oulun yliopiston opiskelijoilla on web-järjestelmien haavoittuvuuksista.

Seuraavassa on määritelty tutkimuskysymykset:

1. Mitä web-järjestelmien haavoittuvuudet ja uhat merkitsevät?
2. Mikä on opiskelijoiden tietoisuus web-järjestelmien haavoittuvuuksista ja uhista, Tampereen ammattikorkeakoulussa ja Oulun yliopistossa?
3. Miten opiskelijoiden tietoisuus eroaa toisistaan?
4. Miten opiskelijoiden tietoisuus eroaa kirjallisuudesta esitetyistä teorioista?

1.2 Tutkimuksen toteutus

Tutkimus suoritettiin laadullisena tutkimuksena. Tutkimuksessa pyrittiin selvittämään korkeakouluopiskelijoiden tietoisuutta tietoturvasta ja haavoittuvuuksista ja mikä käsitys opiskelijoilla oli niihin kohdistuvista uhista. Tutkimuksen pohjana hyödynnettiin Viestintäviraston raportteja viime vuosilta, jotta voitiin hahmottaa käsitys, miksi tieto-

turva on nykypäivänä niin tärkeää ja minkälainen tietous on mahdollisilla tulevilla työntekijöillä, jotka saattavat joutua olemaan tekemisissä web- järjestelmien haavoittuvuuksien kanssa. Tutkimuksen kohderyhmäksi valikoitui Tampereen ammattikorkeakoulu ja Oulun yliopisto, jotta voitiin samalla myös selvittää, onko kahden korkeakoulun opiskelijoiden välillä näkemyseroja web- järjestelmien haavoittuvuuksista. Kummastakin korkeakoulusta valittiin kymmenen oppilasta ja heiltä kysyttiin yleisiä kysymyksiä koskien tietoturvaa/yksityisyyttä ja niihin liittyvää tietoisuutta uhista/haavoittuvuuksista. Haastateltavat olivat vähintään toisen vuosikurssin opiskelijoita, joten tutkimukseen osallistuneilla saattoi olla jonkinlainen näkemys ennestään tietoturvasta. Tukena tässä tutkimuksessa käytettiin myös valmiiksi tutkittuja tapauksia web- järjestelmistä ja niiden haavoittuvuuksista, joiden pohjalta voitiin tehdä havaintoja korkeakouluopiskelijoiden tietoisuudesta web- järjestelmiin kohdistuvista uhista/haavoittuvuuksista

Tutkimuksen rakenne

Tutkimuksen rakenne muodostui seitsemästä luvusta siten, että luvussa kaksi esiteltiin web-järjestelmiä yleisesti, luvussa kolme tietoturvaa ja luvussa neljä tutkimusmenetelmiä. Varsinaisessa tutkimuksessa, jota esitellään luvussa viisi, perehdytään web-järjestelmien tietoturvaan ja niihin kohdistuviin uhkiin/haavoittuvuuksiin. Tutkimusta varten haastateltiin kahden eri organisaation opiskelijoita, jotta saatiin eri näkökulmia korkeakouluopiskelijoiden tietoisuudesta tietoturvasta ja niihin kohdistuvista haavoittuvuuksista joka vaarantaa normaalikäyttäjän yksityisyyden. Lopuksi, luvuissa kuusi ja seitsemän, vertaillaan kirjallisen materiaalin ja haastattelujen tuottamia tuloksia keskenään. Tässä keskitytään web- järjestelmistä havaittuihin uhkiin ja haavoittuvuuksiin.

2. Web-järjestelmät

Tässä esitellään yleisesti web-järjestelmiä ja niiden kehittämistä. Lisäksi tuodaan esille internet protokolla, arkkitehtuuria ja pilvilaskentaa.

2.1 Yleistä web-järjestelmistä

Web-järjestelmä luodaan WWW (World Wide Web)-pohjalle, joka voi olla mikä tahansa verkossa tapahtuva toiminta (Tolvanen, 2007). Pressman (2005) on kuvannut web-sovelluksien ominaisuuksia yhdellätoista attribuutilla. Verkosta riippuvuus (network intensiveness): asiakkaat voivat kommunikoida verkon välityksellä ja verkko palvelee myös organisaatiota (esim. Intranet). Samanaikaisuus (concurrency)**:** useat web-sovelluksen käyttäjät voivat olla verkossa samanaikaisesti, mutta toimintatavat poikkeavat toisistaan. Ennustamaton kuormitus (unpredictalbe load): käyttäjä määrät eroavat suuresti toisistaan eri päivinä, esimerkiksi, jos tiistaina on 300 käyttäjää, keskiviikkona saattaa olla 3000 käyttäjää. Suorituskyky (performance): verkossa tiedonlataamisajat eivät saa olla kovin pitkiä, jotta käyttäjille jää positiivinen käyttökokemus. Palveluaste, saatavuus (availability): vaikka 100% eheyttä ei saavutetakaan sovelluksessa, käyttäjät vaativat palvelua ”24/7/365”. Tietoa käyttäjälle (data driven): sovelluksen ensisijainen tarkoitus on tarjota hypermedia-palveluja käyttäjälle (tekstiä, grafiikkaa, ääntä ja videoita). Sisällöntärkeys (content sensitive): sisällön laatu ja esitystapa ovat ensisijaisen tärkeitä laatutekijöitä sovelluksessa. Jatkuva evoluutio (continuous evolution): web-sovellukset kehittyvät jatkuvasti. Välittömyys (immediacy): web-sovelluksen kehittäminen muutamasta päivästä viikkoihin. Tietoturva, varmuus (security): web-sovelluksissa pitää olla toimiva tietoturva, jotta käyttäjä kokee turvalliseksi käyttää sovelluksen palveluja. Esteettisyys (aesthetics): teknisen suunnittelun lisäksi sovelluksen ulkoasuun pitää panostaa myös, jotta sovellusta olisi mieluisa käyttää. (Pressman, 2005. s.502 - 503.) Toisinkuin tavalliset sovellukset, niin web-sovellukset kehittyvät kokoajan lisää. Web-järjestelmien tietoturvan testaamiseen pitää panostaa todella paljon, koska ilman tätä ohjelmiston tulevaisuus saattaa vaarantua. (Oulun seudun ammattikorkeakoulu, s.d.)

WWW kehitettiin 1990-luvun alkuvaiheessa ja yritykset ottivat kyseisen järjestelmän todellisuudessa käyttöönsä vasta 2000-luvun vaihteessa. Yritykset ovat nykyään alkaneet ottamaan yhä suurempaa roolia web-järjestelmien kehittämisessä. Näitä järjestelmiä voidaan kutsua myös verkkopalveluiksi. Verkkopalvelut voidaan nykyään jakaa seitsemään eri kategoriaan: Esitetyyppiset verkkopalvelut tuotekatalogityyppiset verkkopalvelut, yhteisölliset verkkopalvelut, asiakirjojen jakeluun painottuneet verkkopalvelut, uutispalvelut, henkilökohtaiset sivustot ja portaalit. (Tolvanen, 2007.)

WWW-järjestelmän loi Tim Berners-Lee, jonka tarkoituksena oli pyrkiä saamaan aikaiseksi maailman laajuinen verkko. WWW on web-järjestelmä, jolla voidaan saada yhteys kaikkialle, missä on vastaanottava päätelaite, esimerkiksi yhteys voidaan muodostaa Suomesta Yhdysvaltoihin. Nykypäivänä tietokoneen lisäksi päätelaitteena voidaan käyttää myös älypuhelimia. WWW-järjestelmän pohjalle voidaan rakentaa web-sivustoja, jonka prototyypin Berners-Lee kehitti jo 1980-1990-luvun vaihteessa. Hänelle tärkeää oli saada tavalliset käyttäjät mukaan käyttämään nettiä tietojen levittämiseen ja ottamaan huomioon kulttuurilliset vaikutukset. Berners-Lee vielä huomautti, että tiedon

saanti netin kautta on joka ihmisen oikeus ja web-sivuille pääsy pitää olla ilmainen. (Mitchell, s.d.; Ghosh, 2013.)

Web-järjestelmiä voidaan tuottaa monilla eri kielellä, joita voivat olla esimerkiksi HTML (Hypertext Markup Language) (Ek & Hellstadius, 1998.) ja kehittyneempi HTML5 (Korpela, 2011.) Berners-Lee kehitti vuonna 1991 HTTP (Hypertext Transfer Protocol) protokollan, joka mahdollisti nopeamman tiedon siirron verkonvälityksellä. HTML-kieli on joukko, symboleja, joista muodostuu Internet-sivu. HTML-kieltä tukevat suosituimmat web-selaimet (esimerkiksi Microsoftin Internet Explorer ja Netscape Navigator).(Rouse, 2005.) HTML5, joka on kehittyneempi kieli kuin HTML, kehitettiin parantamaan HTML-kielen puutteita. HTML5-kielen kehittäminen on vielä keskeneräistä, mutta sen katsotaan saavuttavansa lopullisen muotonsa vuonna 2020. Kyseisen kielen salaisuus perustuu sen monipuolisuuteen, joka tarjoaa jokaiselle käyttäjälle jotakin. HTML5-kieli on tuonut uusia ulottuvuuksia verkkosivujen rakentamiseen joita ovat muun muassa: piirtoalusta (vuorovaikutteisia piirtotoimintoja), videoiden esitys suorana selaimessa, paikkatiedot (mahdollistaa palvelujen tuottamisen käyttäjän sijainnin mukaan), selaimen muisti (tarjoaa paljon parempia tiedontallennusmahdollisuuksia kuin evästeet), lomakkeisiin uusia piirteitä, sovellusmuisti (voidaan ohjata selain lataamaan suoraan tiedostot offline-käyttöön), rakenteiset elementit (voidaan esimerkiksi paremmin merkata navigointialue) ja merkitysten kuvailu keinot (mikrotiedot ja mikromuodot). HTML5 on hieman kiistanalainen nimitys ja osa kehittäjistä on luopunut kokonaan sen nimityksestä. HTML5-kielen sovellustoimintaa käsitellään normaalisti JavaScript-kielellä, mutta myös Java-kieltä voidaan käyttää. HTML5-kieli on ollut vasta vähänaikaa olemassa, jonka seurauksena selaimet eivät välttämättä vielä ymmärrä kaikkia merkkejä, HTML5:en merkinnät poikkeavat merkittävästä edeltäjänsä (HTML) merkinnöistä. Vaikka HTML ja HTML5:en merkinnät poikkeavat toisistaan paljon, niin sitä ei kannata kuitenkaan säikähtää vaan HTML5 merkinnät ovat yksinkertaisia ja helppo oppia. Kun ollaan siirtymässä HTML5-sivujen tekemiseen, mitään merkittävää ei tarvitse tehdä, vaan HTML ja HTML5-kielet tukevat toisiaan, selaimet myös ymmärtävät tämän. HTML5:ssa on monia uusia piirteitä, jotka helpottavat hakukoneiden sivujen etsintää, mutta hakukoneet eivät vielä pysty ottamaan HTML5:en uusia rakenteellisia uudistuksia huomioon. (Korpela, 2011 s. 11 - 21.)

Web-järjestelmien kehittyminen on mahdollistanut myös sosiaalisen median. Sosiaalinen media voidaan määritellä laajasti, jolloin siihen voidaan lukea muun muassa Wikipedia, Facebook, Twitter Yahoo ja Youtube. Sosiaalinen media terminä käytettiin ensimmäisen kerran jo vuonna 1950-luvulla. Yritykset hyödyntävät Web 2.0 liiketoimintamallia sosiaalisessa mediassa. Web 2.0 toimii WWW-järjestelmän kautta. Kyseinen järjestelmä on edistänyt sosiaalista mediaa, viemällä sen normaaleille web-sivustoille. Sosiaalinen media on tuonut ihmiset nykypäivänä paremmin sähköisen viestinnän pariin ja päätelaitevalikoima on myös lisääntynyt, esimerkiksi älypuhelimiin. Sosiaalisen median kautta voidaan helposti pitää yhteyttä ystäviin, perheen jäseniin, yrityksiin, yritysten asiakkaisiin tai koulussa voi olla organisoitua yhteyden pitoa, esimerkiksi IRC:n (Internet Relay Chat) välityksellä. IRC:n on kehittänyt Jarkko Oikarinen Oulun yliopistolla. (Oinas-Kukkonen, 2013 s. 1 - 40; MacManus & Porter, 2005.)

2.2 Transmission Control Protocol/Internet protocol (TCP/IP)

TCP/IP (Transmission Control Protocol/Internet protocol) on viestiä lähettävä järjestelmä, jonka avulla yksityinen käyttäjä voi lähettää Internetin kautta viestejä toiselle käyttäjälle, TCP/IP-järjestelmää käyttää esimerkiksi Intranet. TCP/IP on kaksi kerroksinen ohjelma, korkeampi taso on Transmission Control Protocol, joka hallinnoi ja kokoaa viestipaketteja pienempiin osiin ja lähettää ne kokonaisina vastaanottajalle Inter-

netin välityksellä. Internet protocol on alempikerroksen protokolla, joka käsittelee osoitteita, jotta viesti saapuu oikeaan osoitteeseen. Internet protokolla toimii yleisesti palvelimen välityksellä eli viesti lähetetään käyttäjältä käyttäjälle (point to point), esimerkiksi yritys lähettää asiakkaalleen viestin. Monet tuntevat yleensä vain korkeamman tason sovelluksen, jonka apuna käytetään muun muassa HTTP-järjestelmää viestien lähettämiseen. Koko protokolla tapahtuu siis Internetin välityksellä, mutta koko tapahtuma toimii WWW-järjestelmällä. Protokollaan yhteyden saamiseen ei tarvita kuin vain PC (personal computer) ja puhelinmodeemi. TCP/IP- protokolla jaetaan viiteen eri kerrokseen, joita ovat: 1. Fyysinen kerros, tämä ylläpitää fyysisiä linkkejä verkkoon joita ovat esimerkiksi kytkimet ja reitittimet. 2. Linkkikerros, tämä kerros mahdollistaa luotettavan tietojen siirron fyysisen kerroksen avulla, lisäksi linkkikerros mahdollistaa virheiden havaitsemisen tiedonsiirrossa. 3. Verkkokerros, tämä mahdollistaa verkostoitumisen, että tieto löytää oikean osoitteen ja löytää paikasta toiseen. 4. Kuljetuskerros, tämä kerros sijaitsee yläpuolella, päätehtävänä on käsitellä tiedot ja tiedonsiirron. 5. Sovelluskerros, tämä kerros määrittelee kuinka eri käyttäjien pitäisi käyttää verkkoa. (Rouse, 2008; Naker, 2006.)

IP-osoitteella, joka on tärkeä osa Internet protokollaa, lähetetään viesti toiseen paikaan (vastaanottajalle). IP-osoitetta voidaan verrata Postin toimintaan, henkilö vie kirjeen postiin, jonka kautta se toimitetaan lajittelukeskukseen, lajittelukeskus toimittaa sen lähimmälle lajittelukeskukselle (oman paikkakunnan), josta se toimitetaan perille. Lajittelukeskus toimii tässä tapauksessa reitittimenä, joka ohjaa viestin kulkua ja postiosoite toimittaa IP-osoitetta. Postitoimistossa postivirkailija tarkastaa lähimmän lajittelukeskuksen, kuten tietoliikenteessä, kukin dataa välittävä olio on kiinnostunut vain oman tasonsa protokollasta. IP- osoite kerrotaan muodossa n.n.n.n, missä kunkin IP-osoitekentän 8-bitin kuvaama kokonaisluku. Esimerkiksi 115.132.104.200 on yksi IP-osoite, sama ilmoitettuna bitteinä on 01110011 10000100 01101000 11001000. Bitti on binääriluku, joka voidaan laskea kaksijärjestelmällä tai päinvastoin, IP- osoite ilmoitetaan kymmenjärjestelmällä, mutta se joudutaan laskemaan myös bitteinä, koska tieto ilmoitetaan bitteinä tiedonsiirrossa ja tiedonkoossa. (Kaario, 2002 s. 53 - 55; Mitchell s.d.)

TCP/IP yhteyden viat voidaan jakaa kahteen ryhmään, yhteyden muodostamisen estäviin vikoihin ja yhteyttä hidastaviin vikoihin. Yhteyttä estävät viat ovat yleensä perus virheitä joita voivat olla: Väärä IP-osoite tai väärät turvallisuusasetukset. Nämä virheet voivat kaataa koko järjestelmän. Yhteyttä hidastavat viat voivat olla yhteyden kuormituksessa, huonossa reititysprotokollassa tai sovelluksissa. TCP/IP-yhteydessä on valvottava kunkin protokollan lähettämä datan määrää, parhaassa tapauksessa kukin protokolla käyttää omaa maksimikokoaan. Maksimikoon määritykset tehdään NT:ssä (new technology), joka tehdään TCP/IP-protokollapinoon rekisterin välityksellä. Tärkeimmät määritykset ovat Maximum transmission unit (MTU) ja TCP:n maximum segment size (MSS). TCP ei saisi lähettää suurempia segmenttejä, joita IP pystyy kerralla käsittelemään. TCP:n maximum segment lifetime (MSL) vaikuttavat myös osaltaan nopeuteen, se määrittelee kuinka kauan enintään etäjärjestelmän lähettämä segmentti risteilee verkossa ennen saapumistaan päämääräänsä eli vastaanottavaan järjestelmään. (Hakala & Vainio, 2002 s. 262 - 263.)

2.3 Web 2.0 tukevat arkkitehtuuria

Chang ja Gray ovat tutkineet, miten web 2.0 voisi tulla käyttöön arkielämässä. Tutkimuksen mukaan ihmiset ovat tänä päivinä Internet riippuvaisia, jonka johdosta web 2.0 voitaisiin hyödyntää myös opetusmielessä (kampus-elämässä). Tämän kaltainen opetustapahtuma voisi olla vaihtoehtona face-to-face tapaamisille. Tässä muodossa opettamisessa on se hyöty, että voidaan seurata ihmisten käyttäytymistä interaktiivisessa tapahtumassa. Kaikki muutkin palvelut toimisivat myös web 2.0 välityksellä, joita ovat esimerkiksi opinto-ohjaus, terveyspalvelut ja paikallisia julkisenliikenteen palveluja. Tämän palvelun välityksellä myös opiskeluajan seuranta toimisi kätevästi ja voidaan tehdä arvioita, kuinka pitkään opetustapahtuma kestää. Verkon välityksellä opettajat voisivat myös helposti tarjota vaihtoehtoisia koulutehtäviä. Huonona puolena tässä on, kommunikoinnin selkeys. tulevatko kaikki asiat selkeästi esille Internetin välityksellä. Tutkimuksessa mainittiin, että edellä mainitut asiat ovat seurausta Internetin-riippuvuudesta, haluammeko elää tällaista elämää. Käytännössä kaikki arkiset asiat tapahtuisivat kokonaan Internetin kautta. (Chang & Gray, 2013.)

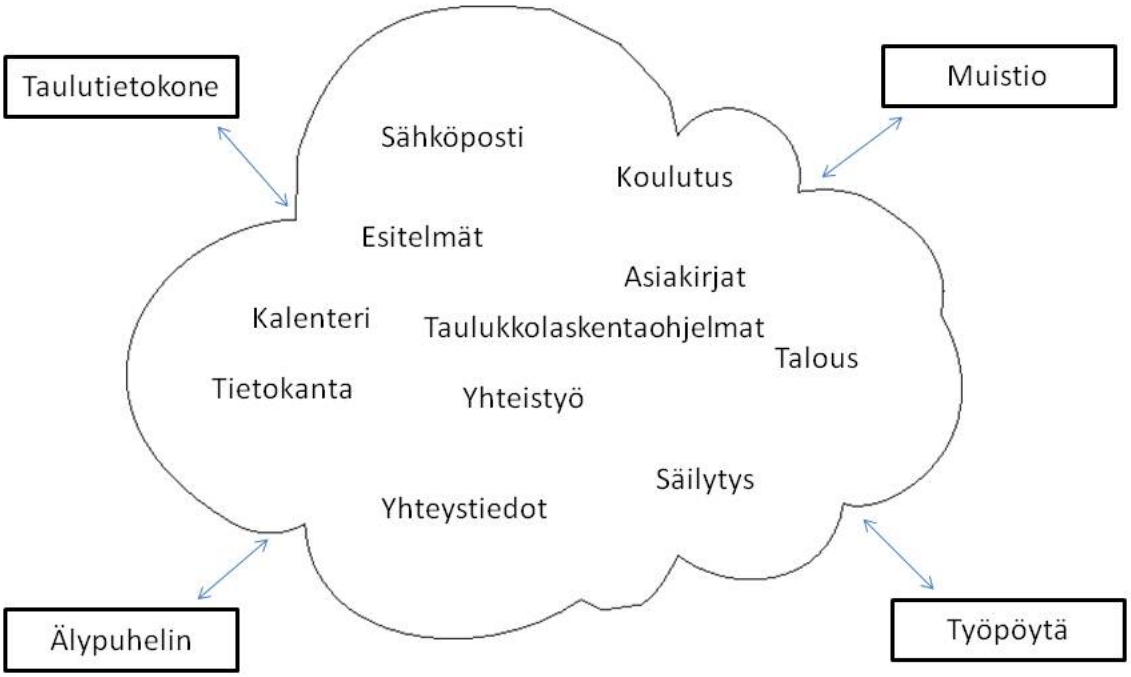
2.3.1 SOA (service-oriented application)

Integraatioarkkitehtuuri määrittelee ja kuvaa tavan liittää toisiinsa ohjelmistoja. Tätä tukee myös palveluorientoitunut arkkitehtuuri (SOA). SOA teknologia ei aina välttämättä kuitenkaan vaadi integraatioarkkitehtuurin käyttöä. SOA teknologiaa tarvitaan normaalisti vasta silloin, kun on tarve koordinoida monimutkaisempia palveluja. SOA:n avulla on tarkoituksena löytää eri ohjelmistojen välille yhteys, jotta ne kommunikoisivat keskenään. Palveluorientoituneen arkkitehtuurin tarkoituksena on siis, että se tekee kaikki palvelupyynnöt ohjelmistoille käyttäjän puolesta. SOA arkkitehtuurityylin hyviä puolia on, että se tekee sovellusten välisen kommunikoinnin mahdollisimman löysin sidoksin. (Ruohonen, 2013.)

2.3.2 Pilvilaskenta

Asiantuntijat ovat kehittäneet pilvilaskennalle määritelmän, mutta yksiselitteistä määritelmää on miltei mahdoton sanoa. Pilvilaskenta voidaan määritellä virtuaalisesti toisiinsa kytkettyinä tietokoneina, pilvipalvelun määrittelyyn kuuluu siis pilven skaalattavuus ja käytön mukaan tapahtuva laskutus, joka on helppo näyttää toteen pilvipalvelun kuormittavuudessa. Pilvipalvelun muita määritelmiä ovat sen verkkokeskeisyys, globaalisuus ja tietojenkäsittelyresurssien ulkoistus. Pilvipalvelulla tarkoitetaan Internetin välityksellä tapahtuvaa palvelua, joista voidaan yksinkertaisesti laskuttaa käytön mukaan asiakkaita. Pilvilaskenta jaetaan kolmeen pääryhmään: SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service) ja IaaS (Infrastructure-as-a-Service). SaaS on pilvilaskennassa sovelluskerros, joka on loppukäyttäjille näkyvin kerros. Tämä on rajapinta pilven ja erilaisten päätelaitteiden yhdistelmänä. Ostamisen sijaan vuokrataan palvelu ja joissakin tapauksissa palvelu voi olla myös täysin ilmainen (Google Gmail). Tyypillisiä palvelun kattavia alueita ovat laitteisto, ohjelmisto ja ylläpito. PaaS on sovellusalusta, jonka tehtävänä on antaa sovelluskehittäjälle verkkopalvelu toimittajan alustalle. Tunnetuimpia sovellusalustalla toimivia ohjelmistoympäristöjä ovat Google App Engine, Force.com ja Windows Azure. Sovellusalustan etuja ovat nopea skaalaus ja kuorman tasaus. IaaS on infrastruktuuri, jonka palveluihin kuuluu laitteistot ja ohjelmistot (esimerkiksi käyttöjärjestelmän virtuaalisointiin liittyvä teknologia). Tässä vaihtoehdossa palveluntarjoajan tehtävänä on pitää pääkeskus toimintakunnossa ja antaa palvelun liittyvä asentaminen asiakkaan vastuulle. Selkeästi tunnetuin palvelun tarjoaja on Amazon. Palvelun ostajalla on mahdollisuus valita muun muassa ohjelmointikieli, käyttöjärjes-

telmä ja tietokanta käyttämäänsä palvelininstanssiin. Asentamisen lisäksi myös kapasiteetin hallinta, joka tapahtuu palvelininstansseja käynnistämällä ja sammuttamalla on asiakkaan vastuulla. Infrastruktuuri jaetaan tarkemmin laskennallisiin resursseihin tietovarastoon ja viestinvälitykseen. (Kommeri, 2011.)



Kuva 1. Pilvilaskenta-malli. (Synergy, s.d.)

Kuva 1 esittää, kuinka pilvilaskenta toimii, pilvipalvelut tarjoavat eri palveluja useille eri alustoille, joita ovat esimerkiksi sähköposti, tietokanta ja kalenteri. Palvelut ovat pilven ulkopuolella ja alustat kuuluvat myös pilven ulkopuolelle, mutta palvelujen ja alustojen välinen liikenne on molemminpuolista.

Synergy (Yhdysvaltalainen IT-yritys) tarjoaa pilvipalveluja ja on määritellyt ne kolmeen toteutusmalliin. Tyypillisimpiä pilvipalvelujen toteutusmalleja ovat: Yksityiset pilvet, julkiset pilvet ja hybridi. Yksityiset pilvet ovat tyypillisesti tarkoitettu yrityksen sisäisiin ekosysteemeihin. Datakeskukset voidaan virtualisoida ja luoda tehokkaampia palvelimia. Sovellukset voidaan helposti asentaa virtuaaliseksi ja käyttää sitä helposti esimerkiksi Intranetissä. Yksityiset pilvet luottavat yrityksessä koulutettuun IT-ammattilaisiin, jotka osaavat hyödyntää tätä pilven toteutusmallia. Julkista pilveä ohjastetaan kolmannen osapuolen datakeskuksen välityksellä. Lähtökohtana on se, että datakeskuksia rakennetaan organisaation ulkopuolelle. Tämän toteutusmallin periaate on se, että datakeskus voi olla yhteydessä useisiin organisaatioihin. Tätä mallia pääkäyttäjä voi helposti hyödyntää suoraan asiakkaaseen. Kolmas toteutusmalli on hybridi, jota käytetään yhdistetysti yksityistä ja julkista pilveä. Esimerkiksi organisaatio voi tuottaa palvelua yksityisellä pilvellä, mutta voidaan hyödyntää myös julkista pilveä varmuuskopiointiin ja palautus tarkoituksiin. (Synergy, s.d.)

Pilvipalveluissa on sen yksinkertaisuutensa vuoksi havaittu väärinkäytöksiä ja rikollisia tarkoitusperiä. Verkkorikolliset käyttävät bottiarmeijoita eli verkkoon kytketään koneiden välityksellä haittaohjelmia. Espanjassa vuonna 2010 poliisit pidättivät Mariposa-nimisen bottiverkon. Maribosalla oli 13 miljoonaa haittaohjelmaa. Haittaohjelmat mahdollistavat koneiden käyttämisen käyttäjän huomaamatta. Niiden tarkoituksena on saada käyttäjät käyttämään WWW-palveluja yhtäaikaisesti ja ylikuormittamaan palvelinta,

jolloin yritys ei enää kykene vastaamaan enää asiakkaiden kysymyksiin. Motiiveiksi on kerrottu kiristys, kiusanteko ja kilpailijoiden toiminnan häiritseminen. Pilvipalvelumallissa tarjoavat tähän ongelmaan kahdenlaista ratkaisua, ensimmäisenä on resurssien skaalautuvuus. Hyvänä puolena tässä on, ettei massiivinen hyökkäys laita kohdetta alas. Huonona puolena on se, ettei kapasiteetin nostaminen oli ilmaista, vaan se on todella kallista. Toisena hyvänä puolena on se, ettei resursseihin massiivinen hyökkäys ole ilmaista vaan se saattaa tulla hyökkääjälle hyvin kalliiksi. Toinen tapa suojautua ongelmaan on rajojen skaalautuvuuden asettaminen etukäteen. Vaikka käyttäjälle kapasiteettia on näennäisesti käytössä loputtomasti, sitä on silti käytössä vain tarpeen mukaan. Hajautetun palveluhyökkäyksen estäminen on kallista, jos halutaan vaaditulle tasolle. Kapasiteetin nostaminen on kallista ja huono ratkaisumalli. Sen sijaan hyökkäykset tulisi tunnistaa ja osallistuvilta koneilta tuleva liikenne ja palvelupyynnöt tulisi myös tunnistaa. (Salo, 2010 s. 109.)

3. Tietoturva

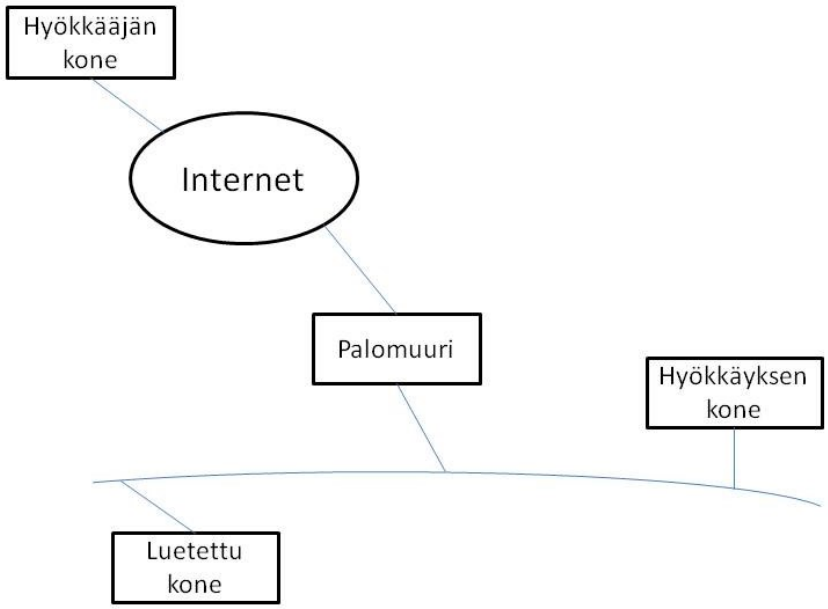
Pozzobon on tutkinut tietomurtojen historiaa. Ensimmäinen virallinen tietomurto on tapahtunut vuonna 1980. Hakkerointi nimityksen tietomurroille keksi Massachusetts Institute of Technology 1960- luvulla. Vuonna 1983 luotiin avoimeen lähdekoodiin pohjautuvat vim-järjestelmä (voidaan hyödyntää tietoturvan haavoittuvuuksissa). Vuonna 1988 Computer Emergency Response Team aloitti järjestelmällisen raportoinnin tietoturva-uhista ja haitoista. Vuonna 1995 Computer Incident Advisory Committee raportoi ensimmäisestä TCP/IP- hyökkäyksestä. Vuosina 1984 - 1986 Dorothy Denning ja Peter Neumann kehittivät ensimmäisen järjestelmän jolla voidaan havaita tietomurtoja ja ehkäistä niitä. Tämä järjestelmä oli lähinnä prototyyppi, jota kehitettiin myöhemmin. 1990- luvulla tietomurtojen yleistyttyä, erilaiset organisaatiot joutuivat kehittelemään omia tietoturvaratkaisuja, miten voidaan torjua tietomurtoja. (Pozzobon, 2013.) Demchenko, Gommans, Laat & Oudenaarde tekemässä tutkielmassa on esitetty erilaisille uhkakuville omat merkitykset. Tietoturvauhkien osana on haavoittuvuus, hyödyntäminen (exploit) uhka ja hyökkäys, joille voidaan pyrkiä kehittämään tietoturvamalli. Haavoittuvuus: tällä tarkoitetaan tutkimuksen mukaan järjestelmän heikkoutta ja tietoturva-aukkoja. Hyökkääjä pyrkii rikkomaan tietoturvapolitiikkaa. Hyödyntäminen: hyökkääjän tarkoituksena on hyödyntää ohjelmiston haavoittuvuuksia. Uhka: uhalla on tarkoitus tehdä tietomurto järjestelmään, kunhan siihen tulee mahdollisuus. Hyökkäys: tarkoitetaan järjestelmään koituvaa uhkaa, jonka tarkoituksena tuottaa ikävyyksiä järjestelmille. (Demchenko, Gommans, Laat & Oudenaarde, 2005.)

Tietoturvaa tarvitaan tärkeiden ja luottamuksellisten tietojen käsittelyssä. Monille tietoturva tuo ensimmäisenä mieleen varmuuskopioinnin tai hakkerit. Molemmat termit liittyvät tietoturvaan, mutta ovat vain pieni osa sitä. Tietosuoja, jota myös yksityisyyden suojaksi sanotaan (privacy) on käsitteenä tullut jälkeenpäin. Käsite on tullut esille, kun on huomattu, kuinka helposti tietoja voidaan kerätä tietotekniikan yleistyttyä. Tietoturva koostuu kolmesta eri osa-alueesta: tiedon luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability), joista tulee helppo muisti sääntö CIA. Luottamuksellisuudella (C) tarkoitetaan sitä, ettei kukaan ulkopuolinen pääse lukemaan tietoja, joita ei hänelle ole tarkoitettu, vaan tietoon pääsee käsiksi vain ne joilla on oikeus tietoon. Eheys (I) tarkoittaa, ettei mikään ulkopuolinen taho pääse tai pysty muuttamaan tietoja. Tällä tarkoitetaan sitä, ettei ulkopuolinen pääse tietoja poistamaan tai tekemään asiattomia muutoksia. Virukset voivat esimerkiksi rikkoa ohjelma- tai dokumenttitiedostoja. Saatavuudella (A) tarkoitetaan, että verkkoyhteys toimii jouhevasti ja tietojärjestelmien toiminta on turvattu. (Järvinen, 2002 s. 21 – 24.)

Tietokonevirukset ovat yleisimpiä tietoturvaan kohdistuneita uhkia. Vuoden 1995 suurimpana uhkana on ollut Internet- verkko ja sen käyttöönotto. ATK-henkilöstön huomio kohdistuu lähinnä käyttöjärjestelmiin, ohjelmistoihin ja tietoverkon suojaukseen. Erityisesti on noussut huoli TCP/IP – protokollaperheen turvallisuudesta. Huoli on aiheellinen, vaikka asiantuntijapiireissä on pitkään tiedetty, ettei TCP/IP:en turvallisuuteen voida ihan täysin luottaa, mutta vasta viime aikoina siihen on löytynyt näyttöä. Unix- käyttöjärjestelmän turvallisuutta on myös viime aikoina kritisoitu ja osin ihan aiheesta, mutta Unix ei turvallisuusominaisuuksiltaan ole kuitenkaan muita käyttöjärjestelmiä huonompi (esim. Novell-, Windows NT- ja OS/2) vaan Unixissa on pikemminkin kehittyneemmät turvallisuusominaisuudet. Unix–käyttöjärjestelmä on ollut jo vuosien ajan käytössä yliopistoympäristöissä ja sen lähdekoodi on ollut tuhansien ihmisten saatavilla.

Tämä on mahdollistanut sen, että Unixin turvallisuusominaisuuksiin on voinut tutustua paremmin kuin muihin käyttöjärjestelmiin. (Nikander, Peltonen & Viljainen, 1996 s. 11 - 14.)

Tietoturvaan liittyviä asioita on lisäksi sähköpostien väärennys, esimerkiksi SMTP-protokollassa (TCP- pohjainen protokolla) kulkeva sähköpostiviesti kulkee selkokielisenä. Käytännössä tämän SMTP-protokollan lisäksi tarvitsee tuntea RFC822-otsake-kenttien formaatti. Näiden perusteella voidaan määritellä viestin sisältö otsake-kentillä. Muita tietoturvaan kohdistuvia uhkia on verkon sanakuuntelu, jos hyökkääjällä on fyysinen pääsy tietoliikennemediaan (esim. Ethernet- kaapeliin), nimipalvelun käänteisrelaation hyödyntämiseen (tavallisen nimipalvelun avulla muunnetaan domain- nimi vastaavaksi IP- osoitteeksi) ja verkkomyrsky, jossa järjestelmään tulee niin paljon liikennettä, että järjestelmän prosessointikapasiteetti menee suurelta osalta verkkoliikenteen käsittelyyn. ((Nikander, Peltonen & Viljainen, 1996 s. 91-95.)



Kuva 2. Tilanne hyökkäyksestä. (Nikander, Peltonen & Viljainen, 1996.)

Kuva 2 esittää perinteistä sekvenssihyökkäystä. Hyökkääjä pyrkii hyökkäämään palomuurin läpi lähettämällä luotetun koneen nimissä väärennettyjä tietoja palomuurin läpi hyökkäyksen kohteelle.

Sekvenssihyökkäyksellä tarkoitetaan sitä, että hyökkääjä lähettää paketteja luotetun koneen kautta palomuurin läpi, ja pyrkii lisäksi arvaamaan minkä alkusekvenssi numeron kohde antaa seuraavaksi TCP-yhteydelle. Jos hyökkääjä tuntee riittävästi käyttämästään protokollasta, hän voi kohtuullisella todennäköisyydellä arvata myös ensimmäistä pakettia seuraavien TCP-pakettien sekvenssinumerot. Hyökkäys tapahtuu hyödyntäen Internet Protokollan pakettien kulkua, Kuvassa 2, hyökkäyksen liikenne on esitetty konkreettisesti. (Nikander, Peltonen & Viljainen, 1996 s. 90 - 91.)

Ennen suojaamisen tarkempia yksityiskohtia pitää suunnitella verkon rakenne: Mihin segmentteihin tai aliverkkoihin mitäkin palveluja sijoitetaan, millaisia kaapelointijärjestelmiä ja aktiivilaitteita käytetään sekä mitä laajaverkkoliittymiä hankitaan. Järjestelmän toiminnan kannalta on tärkeää, että mahdollisimman vähän pullonkauloja syntyy, eikä verkkoon tunkeutuminen ole helppoa. Liikenteelliset pullonkaulat on pyritty ehkäisemään liittämällä palvelimet ja tehotyöasemat suoraan kytkimeen. Laitteet kan-

nattaa ryhmitellä kytkimiin etupäässä sen perusteella, mitä organisaation toimintaprosessia ne edustavat. Lisää turvallisuutta saadaan aikaan määrittelemällä useampia sisäverkkoja kuhunkin kytkimeen. Molemmilla sisäverkoilla on omat nimipalvelunsa, jotka vastaavat vain sisäverkkoihin tulleisiin kyselyihin. Niiden nimiä tai IP-osoitteita ei kerrota muille. Kaikki julkiset Internetiin liittyvät palvelut on sijoitettu pakettisuodattimena toimivana reitittimeen omana segmenttinä. Tähän liitetyt koneet voivat joutua hyökkäyksen uhreiksi, mutta niiden tilapäinen toimettomuus ei haittaa organisaation toimintaa. Ensimmäinen SMTP-postipalvelin sijoitetaan tähän heikosti suojattuun segmenttiin. Sen tehtävänä on ottaa vastaan sähköpostia ja lähettää edelleen sisäiseen palvelimeen. Sisäinen sähköposti toimii Intranet- palvelimen kautta. Sähköpostinpalvelimen lisäksi tähän etuvarustukseen sijoitetaan erillinen julkinen DNS (domain name system)-palvelin, jonka tehtävän on huolehtia ainoastaan etuvarustukseen laitteiden DNS- nimistä. SMTP-postipalvelimen konfigurointiin on kiinnitettävä huomiota, useammissa tapauksissa palvelun tukkimat hyökkäykset ovat kohdistettuja postipalvelimiin. Organisaation postipalvelinta ei saisi reitittää muiden organisaatioiden palvelimien kanssa. Jos ei reititystä estetä, joudutaan aika suurella todennäköisyydellä hyökkäyksen uhriksi. Tyypillinen hyökkäys on, että lähetetään sähköpostia suoraan telnet-istunnosta uhrina toimivan organisaation postipalvelimeen. Hyökkäyksen takia uhrille alkaa tulvimaan virheellisiä sähköposteja, jotka palvelimet tallentavat kiintolevylle. Viestejä saattaa olla kymmeniätuhansia, joka tukkii palvelimen, viestien mukana tulleiden liitetiedostojen avulla. Palomuureilla ja reitittimien pakettisuodattimilla voidaan estää sisäverkkoon tapahtuvat yhteyden avaukset. (Hakala, Vainio & Vuorinen, 2006 s. 185 – 187.)

Suomessa on määritetty tietosuolaki, miten henkilökohtaisia viestejä pitää ja saa käsitellä. Valtaosa sähköisen viestinnän tietosuojalaista kohdistuu viestien välittäjin. Teleyritykset ja yhteisötilat välittävät henkilökohtaisia viestejä. Yhteisötilaa käyttävät pääsääntöisesti yritysten työntekijät. Tätä tarkoitusta varten yhteisötilaa hallinnoi järjestelmä, jossa käsitellään käyttäjiin liittyviä tietoja palvelimin ja päätelaittein. Yhteisötilaan kertyy käyttäjistä luottamuksellisia tietoja, myös sähköpostiviestien kautta. Teleyrityksille kertyy samankaltaisia tietoja kuin yhteisötilassa. Viestien luottamuksellisuuden turvaamiseksi on säädetty laki, joka koskee myös yksityisten keskinäisiä suhteita. Käyttäjien tunnistaminen yhteisötilaan ja teleyrityksiin pitää tapahtua luottamuksellisesti, eikä tietoja saa levittää ulkopuolisille, esimerkiksi verkkopankkiin tunnistautumisessa on otettu edellä mainitut asiat huomioon. Sähköisen tiedon tunnistamistiedoilla tarkoitetaan tilaajaan tai käyttäjään yhdistettävissä olevia tietoja, jota viestintäverkoissa käsitellään viestien siirtämiseksi. Tyypillisissä tunnistamistiedoissa käy ilmi, kuka puhuu puhelimessa kenenkin kanssa, ketkä lähettelevät toisilleen sähköposti- tai tekstiviestejä tai millä Internet- sivustolla kukin surffaa. Sähköisen viestinnän tietosuojalaki on luonnolliseen henkilöön yhdistettävien tietojen osalta erityislaki suhteessa henkilötietolakiin. Sähköisen viestinnän tietosuojalain yleinen ohjaus ja kehittämisen valvonta kuuluu liikenne- ja viestintävirastolle. Sähköisen viestinnän tietosuojalain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuus ja yksityisyys. (Helepuro, Perttula & Ristola, 2004 s. 13 – 20 & s. 251.)

Yritykset laativat tietojärjestelmänsä tietoturvan parantamisen avuksi tietoturvastrategian. Ennen tietoturvastrategiaa pitää kuitenkin laatia tietoturvapolitiikka. Tietoturvapolitiikka on johdon hyväksymä tietoturvasuunnitelma, joka on koko organisaation tietoturvan perustuskivi. Tietoturvapolitiikka voi olla vain muutaman sivun tiivistelmä, josta käy ilmi asiakkaille, työntekijöille ja sijoittajille, mitkä ovat yrityksen arvot. Tietoturvapolitiikka ei ole kovin yksityiskohtainen vaan siitä voi käydä ilmi esimerkiksi virustorjunnat tai salasanapolitiikka, nämä taas kertovat yksityiskohtaisemmin toimintaohjeet. Tietoturvapolitiikka laaditaan kirjalliseen muotoon, joka voi kestää 5 vuotta (keskipitkä) tai 10 vuotta (pitkä). Hyvä tietoturvapolitiikka sisältää seuraavat osa-alueet:

Organisaation oman tietoturvallisuuden määritteleminen, johdon ilmaisu ja tuki tietoturvan tavoitteiden saavuttamiseksi, rakenteet, jolla tietoturvallisuuteen pyritään ja erityisesti riskien kartoitus, yhteenveto tietoturvakäytännöistä, yhteenveto lainsäädännöstä, yhteenveto turvallisuusajattelun edistämisestä ja turvallisuuskoulutuksen järjestämisestä, kuvaus liiketoiminnan jatkuvuuden hallinnasta, määritelmät tietoturvallisuuden vastuualueista käytännöt ja seuraukset turvallisuuspolitiikan rikkomisesta ja luettelo politiikan tarkentavista tietoturvaohjeista. Tietoturvapolitiikka pitää kirjoittaa ymmärrettävään muotoon, jotta muutkin kuin siitä vastaavat ymmärtäisivät sen. Ennen tietoturvapolitiikkaa pitää tehdä riskikartoitus miksi suunnitelma on hyvä olla. Organisaatiolla pitää olla myös jatkuvuussuunnitelma, jos käykin niin, että tietoliikenteessä ilmenee häiriöitä, onko varasuunnitelmaa? Tietoturvapolitiikan jälkeen voidaan laatia tietoturvastrategia, josta pitää käydä ilmi seuraavat asiat: uuden virustorjunnan valinta ja asennus, salasanapolitiikan luominen, salatun sähköpostin luominen, salatun sähköpostin käyttöön otto, henkilöstön tietoturvakoulutuksen käynnistäminen ja palvelinohjelmien päivitysten varmistaminen. Viimeisenä pitää laatia toimintaohjeet, jossa käy ilmi edellä mainitut asiat ja tietoturva säilyy riittävän kovalla tasolla. (Tikkunen, 2012.) Whitman ja Mattord ehdottavat tietoturvastrategian lisäksi tietoturvan suunnittelemista. Tietoturvan suunnittelussa on tärkeää ottaa huomioon, että kaikki organisaation sisäiset asiat liittyvät toisiinsa, kun ollaan suunnittelemassa tietoturvaa. Organisaation sisäisiin ryhmiin kuuluu henkilökunta, organisaation johto, sidosryhmät ja muut ulkoiset yritykseen sidoksissa olevat tekijät. Tietoturvan suunnittelussa pitää ottaa huomioon eri ympäristöt joita ovat: fyysinen ympäristö, poliittinen ja oikeudellinen ympäristö, kilpailu ympäristö ja tekninen ympäristö. Tietoturvan suunnittelulla on tarkoituksena hakea turvallista kommunikointia organisaation jäsenten kesken, sekä turvallista kommunikointia johtoon. Tietoturvan suunnittelussa johdon on tutkittava nykyaikaisen organisaation toimintaa, koska ilman tätä tietoturvan suunnittelu saattaa olla uhattuna, päämääränä onnistunut tietoturva. (Whitman & Mattord, 2008 s. 26.)

Porvari tehnyt väitöskirjan tietoturvallisuuden merkityksestä liiketoiminnalle ja millaisia tietoriskejä voi olla osana liiketoimintaa. Tietoturvallisuuden taso ei enää vastaa nykypäivänä liiketoiminnan vaatimuksia. Tietoyhteiskunnassa tiedon merkitys yhteiskunnassa ja sen eri osatekijöissä kuten, liike-elämä, hallinto, terveydenhuolto, tutkimuksen ja näiden eri toimintojen strategisena voimavarana on tullut yhä merkittävämmäksi. Yrityksen johto asettaa tietoturvallisuudelle tavoitteita ja vaatimuksia. Niihin voivat vaikuttaa omistajat, asiakkaat, sopimuskumppanit, käyttäjät ja yhteiskunta lakien asetusten ja viranomaismääräysten muodossa. Tietoturvallisuus on nykypäivänä yhä merkittävämmässä roolissa yksityishenkiöille, sillä esimerkiksi lääkemääräykset siirretään verkossa. Myös verkkokaupan ja sähköisen asioinnin tulee olla luotettava. Tietoriskit voivat olla joko liikeriskejä tai vahinkoriskejä. Tietotekniikka kehittyy koko ajan, eikä uusien tietojärjestelmien riskejä oteta aina tarpeeksi huomioon. Vakuutusyhtiöissä riskit on ryhmitelty eri osa-alueisiin, omaisuusriskeihin, keskeytysriskeihin, henkilöriskeihin, rikosriskeihin, vastuu- ja sopimusriskeihin sekä virheisiin, erehdyksiin, osaamattomuuteen ja laatuongelmiin. Omaisuusriski: yritykset ovat investoineet suuria summia tietotekniikkaan. Tekniikka kehittyy kokoajan ja tietotaitoa ei ole mahdollisuus saada muualta (eli jos tuotekehitys ei ole ajan tasalla), voidaan kilpailijalle menettää markkina-asema useammaksi vuodeksi. Tuote kehityksen menettäminen kilpailijalla on riski. Esimerkiksi jos yrityksen tietoja tuhoutuu tapaturmaisesti tulipalon seurauksena, tietoja ei ole muualta saatavilla. Keskeytysriski: yrityksen tietopalvelun ja tietoverkkojen keskeytyminen syynä voi olla edellä mainitut asiat tai esimerkiksi sähkökatkokset. Keskeytysriskit ovat yleensä paljon suurempia kuin omaisuusriskit. Henkilöriskit: osaava henkilö on äärimmäisen tärkeä voimavara yritykselle, henkilön poissaolo saattaa olla vahingollista liiketoiminnalle ja voi myös viivästyttää hankkeita. Rikosriski: rikosris-

kejä ovat varkaudet, ilkivallat, tietotekniikan hyväksikäyttäminen tehdyistä petoksista, kavalluksista ja vastaavanlaisista laittomista teoista. Riskejä aiheutuu myös tietoverkon vakoilusta ja tietomurroista. Tietoverkkoihin liittyvät uhat ovat jokapäiväisiä. Vastuu- ja sopimusriskit: yrityksen vastuuriskeillä tarkoitetaan mahdollisia korvauksia sovittujen asioiden rikkomisesta. Jos tietojenkäsittely kohdistetaan vain omaan yritykseen, vastuuriski on pieni, mutta jos ne kohdistetaan asiakkaisiin, riskit kasvavat. Virheet, erehdykset, muut inhimilliset tekijät ja laatuongelmat: ohjelmistoissa on virheitä ja tietoturva-aukkoja. Nämä koskevat ennen kaikkea päivittämättömiä käyttöjärjestelmiä. Tietopalveluissa käyttäjille voi sattua virheitä ja niistä voi koitua ylimääräisiä kustannuksia. Väitöskirjassa on otettu myös esille tietopalveluiden ulkoistamista ulkomaille. Yrityksen aikomus laajentaa ulkomaille on aina riski. Ensiksi pitää päättää, mihin maahan laajennetaan ja millainen siellä on kilpailuympäristö. (Porvari, 2012.)

Toval, Nicolás, Moros ja Garcia määrittelevät, minkä takia nykypäivänä pitää olla huolestunut oman organisaation tietojärjestelmän tietoturvallisuudesta. Tutkimuksessa todetaan, että tietojärjestelmissä tarvitaan skaalautuva infrastruktuuria, jonka tarkoituksena on ennalta ehkäistä tietoturvaan kohdistuneita hyökkäyksiä. Internet on nykypäivänä suuri tietovarasto, jonne hyökkääjän on hyvä iskeä. Tietojärjestelmä on yhteydessä Internetiin, jonka johdosta tietojärjestelmä on alttiina esimerkiksi viruksille ja madoille, joiden tehtävänä on vaarantaa tietoturva. Tietojärjestelmät käsittelevät yrityksen henkilöstö- ja taloustietoja, mistä johtuen skaalautuvan tietoturvan merkitys korostuu, jotta hyökkäyksiltä voitaisiin välttyä. (Toval, Nicolás, Moros & Garcia, 2002.) Monet vanhat sovellukset viedään nykyään uuden tekniikan pariin, kuten esimerkiksi SOA. Tämä on omalta osaltaan lisäämään myös tietoturva riskejä. Nykyajan IT-teollisuudessa pitää pystyä varautumaan näihin seikkoihin. Berger, Sohr ja Koschke ehdottavat tietoturvan parantamiseksi staattista analysaattoria, jonka tehtävänä on hakea haavoittuvuuksia (esim. Crosssite scripting ja SQL-injektio). Tämä järjestelmä on lähinnä tarkoitettu yrityksen liiketoiminnan tietoturvaan ja niiden suojaamiseksi. Staattinen analysaattori toimii hyvin myös mobiilisovelluksissa eli myös langatonta tietoliikennettä voidaan tarkkailla. Ennen staattista analysaattoria käytettiin koodi analysaattoria, jonka vikoja tällä pyritään paikkaamaan. Staattisen analysaattorin kehittämiseksi on jouduttu tekemään kattavaa tietoturvauhkien analysoimista. Staattisen analysaattoria varten joudutaan tekemään riskien mallinnus ja tietoturva strategia, miten uhkiin puututaan. Riskien mallinnus suoritetaan tarkistamalla sovelluksen arkkitehtuuri, josta pitää käydä ilmi tietoturvapuutteet. (Berger, Sohr & Koschke, 2013.) Stoneburner, Hayden ja Feringa kertovat, että The Information Technology Laboratory (ITL) ja the National Institute of Standards and Technology (NIST) edistävät Yhdysvaltojen teknologiaa ja taloutta. ITL kehittää testaustietoja ja vertailumenetelmiä, joilla voidaan vaikuttaa myös tietoturvaan. ITL:än toimenkuvaan kuuluu kehittää teknistä, fyysistä, hallinnollisia ja hallintaa koskevia standardeja ja suuntaviivaisia kustannustehokasta, jolla voidaan parantaa tietoturvaa ja yksityisyyttä, arkaluonteisia luokittelemattomia tietoja Federal- tietojärjestelmissä (Yhdysvalloissa käytössä olevia tietojärjestelmiä, joiden tarkoituksena on edistää yhdysvaltalaisten taloutta tarjoamalla heille teknistä johtajuutta, eli tarkoituksena on pyrkiä hyödyntämään tietotekniikkaa talousasioissa). ITL on julkaissut 800 raporttia tutkimuksia, ohjautuvista tavoitteiden hankkimisesta tietoturvaan. Tämän koko hankkeen tarkoituksena on edistää IT-turvallisuutta ja luetella järjestelmän suojauksia. Hankkeessa käydään läpi tietojärjestelmän elinkaari, joka tulee raportoida. Raporttien avulla voidaan nähdä yksinkertaisesti tietoturvapuutteet ja niitä voidaan vahvistaa. Raportit pitää olla lyhyitä ja ytimekkäitä, jotta eri organisaatioissa voidaan helposti puuttua tietoturvaan ja yksityisyyttä koskeviin asioihin. Tutkimuksen asiakirjojen julkaisemisesta vastaa NIST, jota tulee käyttää kaikki, jotka ovat kiinnostuneita tietojärjestelmän tietoturvallisuudesta ja oman organisaation tietoturvasta. Raportissa tulee mainita myös

tukijärjestelmät ja tärkeimmät sovellukset. On odotettavissa, että näitä yleisimpiä periaatteita, mitä tässä on mainittu, käytetään teknologian eri aloilla ja voidaan lopullisen asiakirjojen pohjalta kehittää yksityiskohtaisempia ohjeita. (Stoneburner, Hayden & Feringa, 2004.)

3.1 Tulevaisuuden näkymiä tietoturvasta

Suojelupoliisi (SuPo) on julkaissut vuoden 2012 vuosikertomuksen, jossa käy ilmi Suomea, sekä maailmaa uhkaavat tietoturvallisuus tekijät. SuPo on Suomen turvallisuus viranomainen, jonka konkreettisena tehtävänä on vastata Suomen valtion- ja yhteiskuntajärjestyksestä. Vuosikertomuksesta käy ilmi, että Suomeen kohdistuneet urkinnat eivät ole vähentyneet, mutta eri EU- maiden julkisuuteen tulleiden tapausten johdosta, laittomiin urkintoihin kiinnitetään yhä tarkempaa huomiota. Turvallisuus tulee muuttumaan tulevaisuudessa. Maailma on vuonna 2030 hyvin erilainen paikka asua kuin tänä päivänä. Venäjän presidentti vuotuisessa linjapuheessaan joulukuussa 2012 kertoi maailman siirtyvän muutosten aikaan. Kansainvälinen kilpailu luonnonvaroista, energiasta ja teknologiasta kiihtyy, joka aiheuttaa jännitteitä eri maiden välille. Yhdysvalloissa julkaistiin raportti vuonna 2012, jossa arvioidaan vuoteen 2030 mennessä vallitseva kehityssuunta. Yksilöiden merkitys voimistuu huomattavasti seuraavan 15 – 20 vuoden aikana. Taloudellisen kasvun- ja globaalin keskiluokan nousu ja koulutus lisääntyy. Terrorismintorjuntaa on lisätty Suomessa. Henkilöiden lukumäärä on kasvanut kolmenumeroisiksi numeroiksi. Ulkomaisten tiedustelijoiden määrä Suomessa kasvoi hieman vuoden 2012 aikana. Ulkomaisten urkkijoiden keskeisimpiin päämääriin kuuluvat politiikan ennakoiminen ja päätöksen tekoon vaikuttaminen. Päähuomio 2000- luvulla on siirtynyt Suomen sisäpolitiikasta kansainvälisiin suhteisiin. Pääkohtana ovat Suomen turvallisuus- ja EU- politiikka sekä erityisesti Suomen Nato- politiikka. Sotilaallisen tiedustelun avulla vieraat valtiot pyrkivät selvittämään Suomen sotilaallista valmiutta ja yhteiskunnan kriisinsietokykyä. (Suojelupoliisi, 2012.)

Viestintävirasto on julkaissut myös oman raporttinsa vuodelta 2012. Viestintäviraston tehtävänä on tuottaa varmaa ja vaivatonta viestintää Suomessa. Viestintäviraston mukaan matkaviestiverkon liittymien määrä ylitti yhdeksän miljoonan liittymän rajan. Samaan aikaan kiinteän puhelinliittymien määrä laski alle yhteen miljoonaan ja laajakaistaliittymien määrä pysyi 1,6 miljoonassa. Matkapuhelimien palveluhinnat pysyivät samana, mutta sen sijaan tiedonsiirtopalvelujen hinnat laskivat. Teleyritykset raportoivat viestintävirastolle 40 tietoturvauhasta ja tietoonsa saamiaan tietoturvauhkia, jotka ylittivät uutiskynnyksen. Vuoden aikana merkittävimmät tietoturvauhkaukset olivat teleoperaattorin toimintoihin tehty murto, teleoperaattorin nimipalvelimiin kohdistunut tietomurto sekä operaattorin hallintaverkostossa paljastunut haittaohjelmatorjunta. Merkittäviä olivat myös palveluestohyökkäysten kohdistuminen useisiin mediataloihin sekä tapaukset, joissa DNS palvelimia käytettiin hyökkäystehon vahvistukseen. Viestintäviraston toimialueeseen kuuluu myös vahvistaa kansallista tietoturvaa. Viestintävirasto on osallistunut kansallisen kyberturvallisuusstrategian valmisteluun, joka julkaistiin Tammikuussa 2013. FI- verkkotunnusten tietojärjestelmien käytettävyys säilyi erittäin korkealla tasolla. Vuoden aikana verkkotunnusten asiointijärjestelmää kehitettiin ottamalla käyttöön open data–rajapinta, jonka kautta verkkotunnusrekisterin julkisia tietoja (myönnetyt tunnukset, haltijat, tunnusten voimassaolo) voidaan saattaa järjestelmään rekisteröityjen tahojen käyttöön. Vuoden 2012 aikana myönnettiin noin 52 000 uutta FI-verkkotunnusta. Vuoden lopussa FI- verkkotunnuksia oli voimassa noin 300 000. (Viestintävirasto, 2012.)

Alalfi, Cordy ja Dean ovat tehneet selvityksen, kuinka hyvin sovelluksien tietoturvan testaus toimii malliperusteisella tekniikalla (Model-Driven engineering (MDE)). Malli

kehitettiin, koska ohjelmistot ovat nykypäivänä yhä monimutkaisempia ja niihin pitää myös tietoturvan tasolla varautua. Menetelmän tarkoituksena on testata sovellusten haavoittuvuuksia, kuten esimerkiksi SQL- injektioita ja cross-site scripting- haavoittuvuutta. Tämän mallin tarkoituksena on testata web- sovelluksia haavoittuvuuksien varalta. Toisena asiana on otettu huomioon kulun valvonta eli tarkkaillaan verkkoliikennettä, jotta vältyttäisiin tietoturva- hyökkäyksiltä. MDE- malli tarkistaa myös lähdekoodin muutokset, onko siellä uhkatekijöitä. (Alalfi, Cordy & Dean, 2012.) Hodován ja Kiss ovat tutkineet kuinka web- kielet, kuten esimerkiksi Javascript ja PHP tulevat sivustojen ylläpitäjille lisäämään tietoturva kustannuksia, koska ne ovat suosittuja ja hyökkääjät osaavat hyödyntää näiden kielten suosiota. Yleisimmin käytetyt ohjelmointikielet lisäävät tietoturvallisuuden huolenaihetta, vuoden 2005 puolenvälin jälkeen on raportoitu lisää haavoittuvuuksia juuri suosituille ohjelmointikielille. Koodit toimivat suosittujen selainten välityksellä (esim. Applen Safari tai Google Chrome) ja näihin haavoittuvuuksiin hyökkääjä iskee, myös mobiiliselaimen tietoturvallisuus on nykypäivänä uhattuna. Webkit on suosituin selainmoottori, joita käyttävät myös Applen Safari tai Google Chrome, joihin hyökkääjän on helppo iskeä. Vuoden 2012 aikana Webkitin markkinaosuus kaikista selaimista oli 38%. Webkit aloitti toimintansa yli kymmenen vuotta sitten ja sitä kehitetään kokoajan, mutta siitä huolimatta Webkitin selainmoottoreista löytyi virheitä, joita hyökkääjä voi hyödyntää. (Hodován & Kiss, 2012.)

3.2 Uhat

TCP/IP-verkon suurimmat uhkakuvat ovat sen avoimuus ja joustavuus. Kuka tahansa voi liittyä verkkoon ja tehdä siellä mitä tahansa. IP-maailmassa hyökkäyksien todentaminen voi olla haasteellista, koska siellä voidaan esiintyä toisena henkilönä. Verkkoon tunkeutuminen ja yhteyksien kaappaamista voidaan hankaloittaa hyvällä tietoturvapolitiikalla, kuitenkaan käytössä ei ole järjestelmää mihin ei voida tunkeutua. Kiusanteko ja uteliaisuus ovat useiden amatöörien tietomurtojen takana. Suurimmaksi osaksi kiusaa tehdään siten, että etsitään protokollasta jokin reikä, isketään sinne ja tehdään palvelin toimintakyvyttömäksi. (Kaario, 2002.)

Tähän on otettu esille muutamia yleisiä hyökkäysmenetelmiä: fyysinen hyökkäys kohdistetaan suoraan laitteeseen tai sen tukilaitteisiin, kuten esimerkiksi sähkönjakeluun. Järjestelmän tietojen tunnistamisesta hyökkääjä saa haltuunsa tai arvaa järjestelmään vaadittavat tunnukset. Tunnukset voidaan saada haltuun verkkoliikennettä kuuntelemalla, keskusteluryhmien kautta ja tunnusten haltioilta. Troijan hevoset ovat viattoman näköisiä objekteja, käyttäjä houkutellaan käsittelemään objektia, jotta ohjelmakoodi tulee suoritettua. Monet nykyiset sähköpostien mukana tulevat liitetiedot sisältävät Troijan hevosen. Itsenäiset agentit ovat verkkomatoja, jotka toimivat ilman hyökkääjän tai hyökkäyksen kohteena olevan järjestelmän apua. Itsenäiset agentit hyökkäävät yleensä Windows- käyttöjärjestelmiin. (Koskinen, Kervinen, Lehtonen, Vatiainen & Viitanen, 2004.)

Garfinkel ja Spafford ovat kirjoittaneet Javasta, ettei sitä tarkoitettu turvalliseen ohjelmointiin. Java suunniteltiin alun perin suljetuksi ohjelmointikieleksi ja se myös rajoitti jonkin verran kohteen ohjelmointia. Kun alun perin Javalla alettiin tuottaa web- sivuja, se herätti heti huolta käyttäjissä. Internetin käyttäjät voivat helposti klikata jonkin sivun auki. Ohjelmoijan on pitänyt miettiä tarkkaan tietoturva-asetuksia, kun Javalla tehdään sivuja. Turvallisen ohjelmointikielen etuja on se, että se suojaa monilta tavanomaisilta tietoturvauhilta, mutta jos lähtee pelkästään valitsemaan turvallista kieltä, lopputuloksena on sitten muita mahdollisia vikoja. Java työllistää ohjelmoijia eritavoilla, siinä on paljon uhkia, mutta myös mahdollisuuksia. Kuten aikaisemmin mainittiin, Javaa ei ole tarkoitettu turvalliseksi kieleksi. Java on suosittu kieli, kun tehdään web-sovelluksia.

Javan turvallisuuspolitiikkaa vaikeuttaa se, että Java on suunniteltu kahteen eri käyttötarkoitukseen, yleiseen tietokoneen ohjelmointiin (esim. sähköposteihin ja nettiselaimiin) ja verkossa olevin sovelluksin ohjelmointiin (esimerkiksi verkossa suoritettavat animaatiot ja reaaliaikainen chattailu). Garfinkelin ja Spaffordin mukaan epävarmoissa tilanteissa kannattaa jättää ajamatta kokonaan Java- sovellus, se vähentää tietoturva- uhkaa. (Garfinkel & Spafford, 1997 s. 42 – 47.)

Rubin, Geer ja Ranum vuoden 1997 kirjassaan ovat määritelleet tietoturvan uhat ja seuraukset neljään osaan: eheys, luottamuksellisuus, palvelunesto ja todennus (authentication) Eheyteen liittyvät uhat tarkoittavat muutosta käyttäjien tietoihin, Troijan hevosen saamista selaimeen, muutosta muistiin ja muutosviestin kauttakulkuliikenteeseen. Suojautumiskeinona tähän on salauksen tarkistaminen. Tietoturvan luottamuksellisuuden uhilla tarkoitetaan verkon salakuuntelua, palvelimentietojen varkauksia ja asiakastietojen varastamista. Luottamuksellisuuden rikkoutuminen aiheuttaa tietojen katoamista ja yksityisyyden häviämistä. Luottamuksellisuuden uhilta voidaan suojautua salaamalla verkon valtakirjat. Palveluneston uhilla tarkoitetaan käyttäjien tekemiä viestiketjujen häviämistä, tehdään koneelle turhia pyyntöjä, tarkoituksena on saada levy tai muisti täyteen ja eristetään DNS- yhteyden toiminta hyökkäyksillä. Palveluneston seurauksilla tarkoitetaan häirintää, kiusa ja käyttäjien työskentelyn vaikeuttamista. Tätä hyökkäystä vastaan on hankala puolustautua. Todennus uhilla tarkoitetaan laillisten käyttäjien tietojen väärin käyttöä. Todennusuhat aiheuttavat sen, että käyttäjä saadaan uskomaan, että virheelliset tiedot ovat voimassa. Tätä vastaan voidaan suojautua salaamalla omassa käytössä oleva järjestelmä. (Rubin, Geer & Ranum, 1997 s.13.)

IPA (Information-technology Promotion Agency) on tehnyt listauksen vuoden 2012 kymmenestä yleisimmästä tietoturva uhasta:

1. **APT (Advanced persistent threat)-hyökkäykset:** Tämä on troijalainen virus, jonka tarkoituksena on salaa ujuttautua käyttäjien tietokoneiden tietoihin. Troijalainen iskee yleisimmin web-pohjaisten ohjelmistojen kautta tai sähköpostien välityksellä. APT-hyökkäyksien tarkoitus on vakoilla käyttäjän tietokonetta.

2. **Arvaamaton tuho (Unpredictable Disasters):** tuhoaa IT-järjestelmiä. Tuottaa taloudellista tappiota, laitevikoja, ohjelmisto vikoja tai aiheuttaa muuta ikävyyksiä käyttäjille. Iskee normaalisti yrityksiin ja organisaatioihin, tarkoituksena tuottaa tappioita kohteelle.

3. **Haktivismi (Hactivist) hyökkäykset:** vuonna 2010 haktivismilla tehtiin kyberhyökkäys, tarkoituksena oli saada organisaatioilta/yrityksiltä taloustietoja. Normaalisti hyökkääjän tarkoituksena on saada huomiota tai muutosta johonkin asiaan. Hyökkääjä iskee WWW-sovelluksen välityksellä.

4. **Peitehyökkäykset asiakasohjelmistoihin (Attacks Targeting Unpatched client software):** tämä on virus, joka iskee ohjelmistojen aukkoihin, lähinnä Javan ja Adobe Readerin- kautta. Peitehyökkäys voi iskeä myös käyttöjärjestelmiin, käytännössä Windowsiin. Viruksen voi myös saada avaamalla tuntematomia sähköposteja. Hyökkäyksen tarkoituksena on vakoilla käyttäjän PC:en sisäistä järjestelmää.

5. **Hyökkäyksen web- sivustoille (Website Attacks):** web-sivuille hyökkäys tehdään web- sovelluksen, Middleware- ohjelmistojen tai käyttöjärjestelmien välityksellä. Suurimmaksi osaksi hyökkäys suoritetaan web- sovelluksen- kautta. Hyökkääjä käyttää apunaan koodi- injektioita (hyökkäykset toteutetaan suu-

rimmaksi osaksi kuitenkin SQL-injektiolla). Hyökkäyksen tarkoituksena on tehdä kohteelle kiusaa.

6. **Hyökkäykset älypuhelimiin ja taulutietokoneisiin (Attack Targeting Smartphone and Tables):** hyökkääjät iskevät samalla lailla kuin tavallisiin tietokoneisiin (PC) eli web-sivujen välityksellä. Hyökkääjän tarkoituksena on kaapata kohteelta, henkilökohtaisia tietoja, osoitekirja, valokuvia ja elokuvia. Viruksen voi huomata siitä esimerkiksi, että päätelaite (älypuhelin) saattaa sammua yllättäen

7. **Vaara digitaalisissa todistuksissa (Danger in Digital Certificates**): todistukset käyttävät PKI (public key infrastructure)- teknologiaa, jota ovat käyttäneet web- operaattorit tai ohjelmistojen kehittäjät. Hyökkääjät iskevät, joko verkon välityksellä tai Windows XP:en ja uusimpien versioiden- välityksellä. Hyökkääjien tarkoituksena on vakoilla kohdetta.

8. **Sisäiset uhat (Internal Threats):** sisäiset uhat ovat organisaatioiden ja yritysten sisäisiä. Suurin riskitekijä on henkilökunta. Esimerkiksi henkilökunnan entinen henkilökunnanjäsen saattaa tuhota yrityksen tärkeitä tietoja. Myös henkilökunta saattaa ottaa omaan haltuun yrityksen salassa pidettäviä tietoja. Tarkoituksena tässä hyökkäyksessä on kiusanteko tai uteliaisuus.

9. **Uudelleen käytetään samoja tilitietoja (Reuse of the Same Credential):** monet verkkopalvelut tarjoajat verkkopankkeja ja tarjoavat maksupalveluja. Hyökkääjä iskee asiakkaiden tilitietoihin, joita voidaan käyttää hyväksi. Esimerkiksi salasanaa ei ole asetettu tai salasanaa ei ole hoidettu kunnolla. Tarkoituksena on huijata verkkopankkia. Huijaajan motiivina on raha ja käyttää uudelleen vanhoja tilitietoja.

10. **Yksityisyyden invaasio (Privacy Invasion):** käyttäjä määrittelee nykyisen paikkatietonsa ja selainhistoriansa. Tässä hyödynnetään eri palvelimien käyttäjien tietoja. Hyökkääjä iskee älypuhelimen tai selaimen avulla. Esimerkiksi tämän avulla voidaan seurata käyttäjän liikkeitä. Hyökkääjän tarkoituksena on vakoilla kohdetta ja kohteen liikkeitä. Liikkeiden vakoilu onnistuu älypuhelimia hyödyksi käyttäen.

(IPA, 2012.)

3.3 Haavoittuvuuksia

Vuonna 2013 kymmenen yleisintä haavoittuvuutta olivat:

1. **Injektio (injection):** injektiolla tarkoitetaan sitä, että hyökkääjän tarkoituksena on päästä murtautumaan kohteen koneelle web-sovellusten välityksellä. Käytännössä hyökkäys tapahtuu niin, että hyökkääjä pyrkii lähettämään omaa dataa kohteen koneelle, jotta hyökkääjä saisi kohteen yksityisiä tietoja selville. Tämä mahdollistaa sen, että hyökkääjä voi saada selville kohteen henkilökohtaisia tietoja esimerkiksi SQL- pyynnöillä. Kohteena voivat olla sekä yksityishenkilöt, että organisaatiot

2. **Epävarma todennus ja järjestelmän hallinta (broken authentication and session management):** järjestelmän salasanat ja käyttäjätunnukset ovat vaarassa joutua ulkopuolisen hallintaan. Salasanoissa ei le käytetty salaustekniikkaa.

3. **Cross-site Scripting:** järjestelmä ei varmista, että käyttäjälle on oikeus kirjautua sisälle järjestelmään. Tämä mahdollistaa sen, että kuka tahansa voi lähettää dataa järjestelmään

4. **Tietoturvaloukkauksille alttiit lähdekoodit (insecure direct object references):** internet-sivustoilla olevat linkit saattavat vaarantaa tietokoneen tietoturva.

5. **Väärät tietoturva-asetukset (security misconfiguration):** web-sovelluksen tietoturva on puutteellinen.

6. **Arkaluonteisten tietojen altistuminen (sensitive data exposure):** arkaluonteisten tietojen päätyminen ulkopuolisten tietoon, esimerkiksi: salasanat, luottokorinnumerot ja potilastiedot. Näitä tietoja olisi hyvä suojella erityisesti

7. **Web-sovelluksen puutteellinen tietoturvataso (missing function level access control):** Hyökkääjä pääsee käsiksi web-sovellukseen URL (Uniform Resource Locator)-asetuksiin (normaalisti hyökkääjä on oikeutettu käyttämään järjestelmää).

8. **Cross-site request forgery (CSRF):** hyökkääjä lataa omalle koneelle kohteen tietoja, hyödyntäen Internet-selaimia. Tämä tapahtuu siten, että hyökkääjä luo HTTP-pyyntöjä kohteen koneelle.

9. **Heikkojen tiedostojen hyödyntäminen sovellukseen hyökkäämisessä (using components with vulnerabilities):** hyökkääjä tunnistaa tietoturvalle alttiita tiedostoja kohteen sovelluksessa. Tämän jälkeen hyökkääjä suorittaa iskun siihen tiedostoon.

10. **Vahvistamaton tiedonsiirto (unvalidated redirects and forwards):** hyökkääjä huijaa järjestelmää, jonne pääsee käsiksi. Tämän jälkeen hyökkääjä kykenee muuttamaan HTML-koodia.

(OWASP, 2013)

Käytännön haavoittuvuus on ohjelmoijalle sattunut tavallinen virhe, joista yleisimmät ovat puskurit, joihin luettavan datan kokoa ei millään tavalla tarkasteta. Tavallisten käyttäjien kannattaa ottaa huomioon myös salasanojen arvaukset. Tutkimusten mukaan n. 25 – 30% salasanoista on helppo arvata. Helpoimmat salasanat ovat nimiä tai luonnollisen kielen sanoja, jonkin verran esiintyy myös takaperin kirjoitettuja sanoja. Hyökkääjät pyrkivät selvittämään ensin käyttäjätunnukset ja vähän kehittyneimmissä tapauksissa, saamaan luettelon koneen tunnuksista ja kryptatut salasanat. (Nikander, Peltonen & Viljainen, 1996 s. 184- 185.)

TCP/IP kohdistuneet hyökkäykset kohdistetaan niiden aukkoihin, joita ei ole ennen havaittu. Yleisimpiä aukkoja ovat: Denial of Servise (DoS –hyökkäykset), SYN Flood, Ping of Death, UDP Echo, Smurf ja Teardrop. DoS-hyökkäys eli palvelunestohyökkäyksissä tarkoituksena on estää jonkin palvelun tai palvelimen normaali toiminta. Tässä ei siis ole kyse tietomurrosta vaan kiusanteosta. DoS-hyökkäyksen naamiointi keinona on tehdä hyökkäys hajautetusti eli tehdään eri puolelle Internettiä moninkertaisia hyökkäyksiä, tämän takia tätä hyökkäystä vastaan on vaikea puolustautua. SYN-tulvan idea on yksinkertainen. Lähetetään jollekin TCP- palvelimelle useita pyyntöjä, mutta jätetään vastaamatta niihin, jolloin on paljon avoimia yhteyksiä ja resurssit loppuvat kesken,

tämän takia uusien yhteyksien luominen on mahdotonta. Ping of Death- hyökkäyksellä tarkoituksena on lähettää Ping- ohjelmalla IP – paketteja, joissa on määritetty datan maksimimäärä (64 kilotavua), Useiden lähetyksien jälkeen palvelin kaatuu, ylikuormituksesta johtuen. UDP Echo hyökkäyksen tarkoituksena on tukkia verkko UDP-sanomilla. Hyökkääjä lähettää koneelle X UDP- sanomaa, jossa hyökkääjän ja vastaanottajan porttinumero on Echo–palvelun porttinumero (numero seitsemän). UDP-sanoma pitää myös väärentää, jolloin Echo- sanoma lähtee tämän IP- osoitteen omistajalle. Smurf- hyökkäyksen ideana on myös lähettää UDP Echo -sanomaa toisen lähdeosoitteesta. Jos tällainen viesti on broadcast– viesti, on hyökkäys valmis. Tällaisessa tapauksessa laite, joka omistaa IP-osoitteen, saa vastauksen lähetettyyn viestiin jokaiselta IP-laitteelta. Isoissa verkoissa, tällaisen sanomaryöpyn jälkeen laite menee ainakin hetkeksi sekaisin. Teardrop-hyökkäys perustuu lohkottujen IP-pakettien käsittelyä joissain TCP/IP- toteutuksissa. Hyökkäys tehdään lohkotuista IP-paketeista. Ensimmäisenä lähetetään TCP/IP –pino sähkeitä pilkottuina ja heti perään toinen, joka sisältyy edelliseen. Jos jälkimmäinen lohko loppuu ensin lähetetyn lohkon loppua, tulee kopioitavasta datasta helposti negatiivinen, ellei ohjelmisto tarkastele asiaa tarkemmin. Kaikki nämä edellä mainitut tietoturva-aukot ovat palvelunestohyökkäyksiä, jotka ovat tarkoitettu lähinnä kiusantekoon tai palvelemisen vaikeuttamiseen. (Kaario, 2002 s. 294 – 300.)

TCP/IP:tä käyttäen voidaan olla yhteydessä myös satelliitilla tietoverkkoihin. Satelliitilla otetaan yhteys eri protokolla kerroksiin, jonka avulla voidaan olla yhteydessä yksityiseen Internetiin, yksittäisiin verkkoihin, yrityksiin, laivoihin, lentokoneisiin ja yksityishenkilöihin. Käytännössä kaikkiin paikkoihin, joissa voidaan päästä ulkopuoliseen verkkoon käsiksi. Tämä toimii, siten että tukikohta sijoitetaan maapallolle harvaan asutulle seudulle, joka vastaan ottaa satelliitti yhteyden, siten voidaan muodostaa TCP/IP-järjestelmä. Tämän järjestelmän tarkoituksena on saada mahdolliseksi viranomaisille vakoilla tietoliiken-nettä ja ehkäistä rikollista toimintaa. Tutkimuksen mukaan kyseinen järjestelmä on kat-sottu poliittiseksi vaikutusvallaksi ja tämä saattaa synnyttää konflikteja eri järjestöjen kanssa. Normaalisti TCP/IP-järjestelmä toimii kahden käyttäjän välillä, mutta tällä ote-taan yhteys kerralla useampaan käyttäjään eli yhteys voi olla auki kerralla moneen paik-kaan yhtä aikaan. (Caupet, Muñoz, Alins, Mata-Díaz & Esparza, 2013.)

Koodi-injektiolla (code injection) tarkoitetaan sitä, että joku ulkopuolinen taho pyrkii murtautumaan nettisivustoille. Tämä toimii siten, että luodaan koodia, joka välitetään Internet-sivulle tai siellä olevaan ohjelmaan. (Wojjie, 2004.) Viime vuosina web- sovelluksista on tullut yhä suositumpia, tämä on myös mahdollistanut tietomurtojen yleistymisen. Hyökkääjät käyttävät hyväksi web-sovellusten haavoittuvuuksia (tietoturva-aukko), joista yleisin on koodi-injektio. Web-palvelimet tuottavat suuren määrän sisältöä asiakkailleen, suurimman osan sisällöstä vastaavaa erilaiset organisaatiot ja ne jotka, tarjoavat asiakkailleen eritasoisia palveluja. (Ollmann, 2007.)

Vaikka web- sovelluksiin kohdistuneet hyökkäykset ovat olleet hyvin tiedossa, viime vuosien hyökkäyksistä johtuen tietoisuus näistä hyökkäyksistä parantunut. Sivustoista on havaittu jo, että ne ovat erityisen alttiita koodi–injektiolle. Web-sovelluksiin pohjautuvat koodi- injektiot hyökkäävät selaimen välityksellä, selain tunnistaa verkkosivuilta HTML-merkkejä/tunnisteita, joita hyökkääjät hyödyntävät koodi-injektiolla. Koodi- injektioita on useita erikaltaisia, joilla on sama päämäärä, hyökätä uhrin tietokoneelle. Koodi-injektio voi olla esimerkiksi Cross-Site Scripting (XSS). (Ollmann, 2007.)

Verkossa liikkuu myös useita muita samankaltaisia injektioita. SQL-injektio on yksi vakavammista WWW-sovelluksen injektiosta. SQL-injektiossa hyökkääjä muuttaa WWW-sovelluksen kyselyn rakennetta lisäämällä kyselyyn omia SQL-avainsanoja tai

operaattoreita. Hyökkääjä voi hyväksi käyttää SQL-injektiohaavoittuvuudessa PHP-koodausta. SQL-injektiossa on olemassa useita mekanismeja. Näistä yleisimpiä ovat käyttäjän syöte, evästeet ja palvelinmuuttajat. Useimmat SQL-injektiohyökkäykset ovat peräisin WWW-sivuilta olevista lomake- elementeistä. XSS (Cross-Site Scripting) on SQL-injektion tapaan koodi- injektio. XSS-hyökkäyksessä WWW-sovellus tulostaa käyttäjän selaimeen lähetettävälle WWW-sivulle hyökkääjän koodia, jonka selain suorittaa WWW-sivun palvelimella. SQL-injektion tapaan XSS-haavoittuvuudet johtuvat käyttäjän syötteen riittämättömästä tarkistamisesta. XSS-injektiossa voidaan käyttää hyväksi saman lähteen käyttöä, koska hyökkääjän injektoima koodi on samalla sivulla. XSS-injektioita on kolmenlaisia: pysyvä XSS (stored XSS), heijastettu XSS (reflected XSS) ja DOM-pohjainen XSS (DOM- based XSS). Esimerkiksi heijastetussa XSS-hyökkäyksessä, WWW- palvelin sisällyttää HTTP- pyynnöissä käyttäjän antamaa syötettä WWW-sivuun, joka lähetetään HTTP – vastauksessa selaimelle. CSRF (Cross-Site Request Forgery)-hyökkäyksessä käyttäjän selain yrittää saada käyttäjän tietämättä lähettämään HTTP-pyyntöjä. CSRF voi tapahtua käyttäjän vieraillessa haitallisilla sivustoilla, joka käskee selainta lähettämään pyyntöjä toiselle sivulle. CSRF-hyökkäyksen onnistuminen riippuu siitä, ettei pyyntöä vastaanottava sivusto tarkista, mistä pyyntö on peräisin. Tämänkaltaisissa tapauksissa sivusto luulee, että pyyntö lähetettiin käyttäjän omasta toimesta. (Lehtinen, 2012.)

Käyttöjärjestelmiin voidaan kohdistaa hyökkäyksiä OS komento- injektiolla ja sitä tukevalla ohjelmalla, kunhan tietoturva-aukko on hyökkääjän tiedossa. Komennot voivat olla esimerkiksi funktio-kutsuja hyökkääjän toimesta. Tyypillisiä käyttöjärjestelmän virheitä ovat: käyttöjärjestelmä on saattanut antaa muistilistan käyttäjälle nollaamatta sitä, hyökkääjä voi tällä tavoin varata paljon muistia ja etsiä siltä saaneelta muistialueelta paljon mielenkiintoista tietoa tai toisena komentona voidaan hyökätä sisältäpäin ja ajaa jotain ohjelmaa ja sammuttaa se hyvissä ajoin. Hyökkäykset voidaan kohdistaa esimerkiksi Windows XP-käyttöjärjestelmiin. (Koskinen, Kervinen, Lehtonen, Vatiainen & Viitanen, 2004.) Unix-käyttöjärjestelmällä on tietoturva-aukkojen takia huono maine ja syystäkin. Unixia ei alun perin suunniteltu turvalliseen käyttöön ja turvallisuusaukkoihin on vaikuttanut myös suurimmaksi osaksi sen lähdekoodin suuri levinneisyys. Unix–käyttöjärjestelmän ohjelmointivirheet voidaan jakaa seuraavasti: suid/grid-ohjelmiin liittyvät virheet, verkko-ohjelmistojen virheet, jotka ovat usein samantyyppisiä kuin suid/grid-ohjelmien virheet, kilpailutilanteet (race conditions), suunnittelu- ja määrittelyvirheet ja lapsukset. (Nikander, Peltonen & Viljainen, 1996 s. 182.)

Sähköposti- injektio (email injection) perustuu nimettömien sähköpostiviestien lähettämiseen, pyrkimyksenä saada vastaanottaja avaamaan lähetetty viesti. Viestin avaamalla kohde saattaa saada koneellensa vakoiluohjelmia. Sähköposti-injektiossa hyökkääjä pyytää antamaan nimettömälle lomakkeelle henkilötietoja, joita voidaan käyttää hyväksi. Myös sähköpostiin voidaan liittää liitetiedostoja tai ohjata tietylle sivustolle, josta käyttäjä saattaa saada koneelleen vakoiluohjelmia. Sähköposti-injektion voi huomata siitä, jos lähettäjä epäilyttää, otsikko on epäilyttävä tai otsikkoa ei ole ollenkaan. Tämä injektio toimii samalla tavalla, kuin koodi-injektio, hyökkääjä iskee koodin kautta (esim. PHP) web-järjestelmään, mutta suoraan valittuun kohteeseen. Hyökkääjä on jostain saanut tietoonsa kohteen sähköpostiosoitteen ja pyrkii lähettämään sille nimettömiä sähköpostiviestejä. (PHPsecure, 2004.)

Haavoittuvuuksia on tutkittu relaatiotietokannan avulla. Tutkijat kehittivät epävirallisen tietokannan, jonka pohjalle rakensivat käyttöliittymän. Tutkimuksessa oli tarkoituksena hakea mahdollisia tietoturva-aukkoja. SQL-kieltä syötettiin tietokantaan Javan avulla. Monien merkkien kanssa tutkimuksessa ilmeni ongelmia, HTML-kieli ei tunnistanut kaikkia englantilaisia merkkejä tai edes välimerkkejä, joilla voitaisiin edesauttaa haa-

voittuvuuksissa. Tässä tutkielmassa käytettiin Secunia ja SecurityFocus tietokantoja, kummassakin tietokannassa on yli 70% mahdollisuus haavoittuvuuksille. Tutkimuksessa tultiin siihen tulokseen, että SQL-kielen haavoittuvuus on merkittävällä tavalla yleistynyt vuoden 1999 jälkeen. (Armold, Hyla & Rowe, 2006.) On myös tutkittu kuinka tunnistaa SQL-injektio hyökkäys. SQL- injektiohyökkäyksen varautumisen ja puolustamisen on tärkeätä koska se on yksi yleisimmistä tietoturvan haavoittuvuuksista ja voi tuottaa yrityksille suurta tappiota. Tutkimuksessa SQL-injektio hyökkäykseen varautuminen jaettiin kahteen eri kategoriaan: 1. Staattinen web-sivu, joka etsii kaikki polut, minne SQL-injektio voi iskeä. 2. Mustan laatikon tunnistaminen, jonka tarkoituksena on simuloida hyökkääjän sovellusohjelman ja paikantaa ongelma. SQL-injektion puolustaminen jaettiin neljään eri katekoriaan: 1. Palvelimen suodatus, joka löytää haittaohjelmat ja SQL-injektion. 2. Rajoitettu tietokantojen käyttämislupa, vähentää SQL-injektioita. 3. Parametrikysely, jossa korkean tason ohjelmointikielet korvaavat SQL-kielen. 4. Tietojen suodatus. Tässä voidaan käyttää kahta listaa, toiselle listalle voidaan merkata esimerkiksi vaarallisia heittomerkkejä. (Tian, Lihao & Hong, 2012.) Koodi – injektio on yleinen nimitys edellä mainituille ongelmille. Ohjelmiin kohdistetut hyökkäykset tulevat olemaan suurin ongelma lähitulevaisuudessa. Tähän tilanteeseen ovat ajaneet ohjelmien puutteelliset tietoturvat ja niiden haavoittuvuudet. Hyökkääjät voivat iskeä tietojärjestelmien muisteihin koodi- injektiolla, C++-kieltä hyödyntäen. (Younan, Joosen & Piessens, 2012.) Näihin haavoittuvuuksiin on kehitetty komento- injektio, jonka tarkoituksena on havaita koodi- injektioita ja ehkäistä niitä. Järjestelmällä on prosessointijärjestelmä, jonka tehtävänä on valvoa tiedonsiirtoa ja erityisesti tiedonsiirto protokollaa. Komento- injektio (suojauksen nimi) on kehitetty, koska tyytymätön yrityksen henkilöstö saattaa syöttää vääriä tietoja koodi- injektion avulla. Komento- injektio kysyy luvan tiedonsiirtoon, ennen sen läpi viemistä. (Gao, Morris, Reaves & Richey, 2010.)

Vuoden 2013 aikana Oulun yliopistolla tutkittiin Internet- selainten haavoittuvuuksia. Haavoittuvuuksia haettiin Oulun yliopiston kehittämän Radamsa-työkalun avulla. Radamsa on täysin automatisoitu tietoturvien testausohjelma. Testauksessa oli mukana selaimista Mozilla Firefox ja Google Chrome. Näistä kahdesta selaimesta löytyi yhteensä yli sata selainhaavoittuvuutta. Suosituin hyökkääjien tapa käyttää haavoittuvuutta hyväkseen on tehdä hakuongelma, joka tekee virheen haettaessa tiettyä ohjelmaa selaimen välityksellä. Haavoittuvuuksien avulla hyökkääjä pyrkii tekemään iskun kohteen koneelle. (Röning, 2013)

3.4 Yksityisyys

Kaikki arkipäiväiset tekomme jättävät sähköisiä jälkiä, esimerkiksi asiointi pankissa tai kaupassa, auton pysäköinti, puhelimensoitto, netissä surffailu ja kaupungilla liikkuminen. Kaupallisen kilpajuoksun takia, erisuuruiset organisaatiot keräävät tietoa asiakkaistaan. Tiedämmekö todella mitä tietoa meistä kerätään? Aluksi kansalaisten tekemisistä olivat kiinnostuneita vain viranomaiset. Suomeen tietokoneet tulivat 1950- luvun lopussa. Ensimmäisenä tietokonetta pääsi käyttämään Postipankki 17.10.1958, mutta vain vuokralle. Muut pankit ja organisaatiot seurasivat perässä ja esimerkiksi seuraavilla organisaatioilla on tallennettuja tietoja kansalaisilta: Ajoneuvokeskus, Kansaneläkelaitos, kirjasto, kunnat, kirkot, lehtikustantamot, oppilaitokset, poliisi, posti, puolustusvoimat, sairaalat, verottaja (Järvinen, 2002 s. 409 – 413.)

Oinas-Kukkoset mainitsevat kirjassaan yksityisyyden kunnioittamisen sosiaalisessa mediassa. Sosiaalisesta mediasta on tullut arkipäiväisempää ihmisten elämästä ja ihmiset käyttävät samanaikaisesti tietokonetta, keskustellessaan toisen kanssa. Suurimmaksi osaksi ennen keskustelun aloittamista pitää rekisteröityä palveluun ja kertoa sinne omia

henkilökohtaisia tietoja. Vaikka monet ajattelevat, että keskustelu on yksityistä, niin todellisuudessa sosiaalinen media on julkista ja monesti ulkopuoliset saattavat nähdä henkilökohtaiset keskustelut. Facebook on nykypäivänä suosituimpia sosiaalisen median tarjoaja, siellä ihmiset voivat myös yksityisesti keskustella keskenään, mutta onko se todellisuudessa näin? Verkossa tapahtuva sosiaalinen median avulla voidaan ottaa yhteyttä eri maihin ja kulttuureihin, yksityisyys on keskustelijan perusoikeus. Toisena asiana on mainittu identiteetti sosiaalisessa mediassa. Tiedämmekö oikeasti kenen ihmisen kanssa juttelemme? Vaan onko keskustelun toinen osa puoli ihan eri henkilö? Chattailussa keskustelijat voivat kehittää nimimerkin, eivätkä ole todellisella henkilöllisyydellä keskustelemassa. (Oinas-Kukkonen, h. & Oinas-Kukkonen, h., 2013 s. 74 – 79.)

Matkapuhelimet viestittävät käyttäjästään monia henkilökohtaisia tietoja. Teknologian perään olevat käyttäjät vaihtavat mallia yhtenään ja kovaa käsittelyä kestäviä puhelimia käyttävät henkilöt ovat todennäköisesti ulkotöissä. Operaattori tietää matkapuhelimen välityksellä kokoajan, missä olet. Operaattorin on seurattava asiakasta tukiasemaverkon kautta, missä puhelin kulloinkin on ja osaa yhdistää puhelun. Matkapuhelimesta on tullut nykyään ihmisen sähköinen tunniste siinä missä henkilötunnuskin. (Järvinen, 2002 s. 418 – 422.) Tässä tutkielmassa mainittiin aikaisemmin TCP/IP-protokollan mahdollistava yhteyden useampaan kohteeseen satelliitin avulla. Tukikeskukset sijoitetaan harvaan asutulle alueelle, josta otetaan yhteys satelliittiin ja sitä kautta myös eri verkkoihin. Tämän avulla voidaan salakuunnella ja vakoilla eri tahoja esimerkiksi meri liikennettä. Tutkimuksessa tätä pidetään poliittisena ja tämä voi lisätä poliittisia konflikteja. Salakuuntelun katsotaan olevan vakoilua ja yksityisyyden loukkaamista. (Caubet, Muñoz, Alins, Mata-Díaz & Esparza, 2013.)

Vuonna 1995 Kaufman, Perlamn ja Speciner kirjoittivat kirjan sähköisestä kommunikoinnista, viestien lähettämisestä sähköisiä verkostoja pitkin, jolloin viestien lähettäminen alkoi menemään julkisempaan suuntaan ja jo silloin alkoi huolestuminen yksityisyydestä. Kirjassa käytetään pretty good privacy (PGP) lausetta, jonka kehitti Philip Zimmerman aikoinaan. Tämä koskee myös verkossa yleistyvää viestien lähettämistä. PGP:en tarkoituksena on viestien salaaminen, jonka tarkoituksena on säilyttää viestin lähettäneen henkilön yksityisyys. PGP:en salaukseen tarvitaan symmetrinen avain, jota voidaan käyttää vain kerran. Viestin lähettäjän voit saada selville ilman salasanaa, mutta viestin sisältöön et pääse käsiksi. PGP- salausta käyttävät viestit ottavat saman tiedoston nimen, mikä on ollut mukana viestissä, joten vastaan ottaja tietää mistä on kyse. Viestit voidaan lähettää salausjärjestelmän välityksellä keksityllä nimellä, mutta jos se on muunneltu nimi omasta oikeasta nimestä, PGP saattaa kertoa alkuperäisen lähettäjän nimen. Kuten tässä huomataan, niin PGP-salausjärjestelmä pyrkii suojaamaan viestin lähettäjän yksityisyyttä ja pitää salassa lähettäjän todellisen henkilöllisyyden. PGP-järjestelmä on erityisen suosittu sähköpostien salaamiseen, mutta se on kuitenkin itsenäinen järjestelmä. (Kaufman, Perlamn & Speciner, 1995 s. 399 – 406.) Paintsil on arvioinut yleisimpiä yksityisyyttä uhkaavia riskejä. Tutkimuksessa arvioitiin mitä henkilökohtaisia tietoja voidaan vuotaa verkossa ulkopuolisille. Riskien arviointi jaettiin kuuteen kategoriaan: 1. Menetys: käyttäjältä häviää tietoja. 2. Väärinkäyttö: Tietoja otetaan luvatta käyttöön. 3. Ilmitulo: joku ulkopuolinen saa omia lähettämiä henkilökohtaisia tietoja. 4. Häiriöt: tiedot eivät toimi. 5. Varkaus: tiedot siirtyvät toiselle käyttäjälle ilman lupaa 6. Korvausarvio: kustannukset nousevat, esimerkiksi resurssit ovat täynnä. Tällä luokitellulla voidaan arvioida, milloin omaisuus voi olla vaarassa, jos ulkopuoliset pääsevät tietoihin käsiksi. (Paintsil, 2013.)

Yritykset seuraavat nykypäivänä järjestelmällisesti ihmisten asiointia kaupoissa (esim. Supermarket) ja pyrkivät keräämään tietoja tietokantaan asiakkaiden mieltymyksistä.

Yritykset seuraavat, mitä asiakkaat ostavat kaupastaan. Asiakas ostaessa lääkkeitä kaupasta, mutta ei halua, että kauppa saa tietoonsa hänen terveystietonsa. Kaikkien yritysten tietoturvaa on mahdoton seurata ja tietoturvapolitiikkaan Ja tällöin on vaarallista, että kuka tahansa voi saada esimerkiksi asiakkaan terveystiedot haltuunsa ja kuka tahansa voi käyttää asiakkaan tietoja hyväksi. Eun, Lee ja Oh mainitsivat tutkimuksessa, että yrityksen ja kaupan välillä mahdollisesti saattaa olla myös kolmas osapuoli. Tähän ongelmaan on annettu ratkaisu NFC (Near field Communication)- protokolla, joka pohjautuu tietoturvaan ja yksityisyyteen. NFC-protokollaan on sisällytettävä seuraavat ehdot: tiedon luottamuksellisuus (on tärkeä suojata tietoja ulkopuolisilta), tiedon eheys (siirrettävissä tiedoissa pitää olla samat tiedot), havaittavuus (käyttäjien tiedot eivät saa erottua toisista datayhteyksistä), kelpoisuus (kaksi eri osapuolta tuottaa tiedot samalla henkilölle, tiedot pitäisi olla tunnistettavissa) ja jäljitettävyys (on tärkeää saada selville kuka on henkilöntiedot luonut tietokantaan). (Eun, Lee & Oh, 2013.) Yksityisyyttä ei aina välttämättä ole edes autoissa, Nykyajan teknologia mahdollistaa myös autoissa viestimien käytön langattomassa verkossa eli autoihinkin on mahdollista saada Internetyhteys. Tätä langatonta teknologiaa voidaan hyödyntää auton paikannukissa. Tätä kyseistä teknologiaa voivat myös hyödyntää matkustajat, jotka voivat kirjautua verkkoon matkan aikana. Auton ajajien käyttäytymistä voidaan seurata verkon välityksillä reaaliaikaisesti ja tehdä havaintoja liikenne turvallisuudesta, johon tällä langattomalla teknologialla alun perin pyrittiin. Liikenneturvallisuutta valvova taho käyttää tiedoissa myös henkilöiden omia henkilötietoja (esim. henkilötunnus) ja tämä voi vaarantaa myös autolla liikkuvien yksityisyyden. Tieto liikkuu näissä samalla tavalla kuin muissakin eli protokolla kerrosten välityksellä ja tähän verkkoon voidaan tehdä samalla lailla tietomurtoja henkilötietorekistereihin. Myös muita autolla liikkuvien henkilötietoja voidaan saada haltuun yksinkertaisesti rekisterinumeroa käyttäen vaikka henkilötietojen pitäisi olla henkilökohtaisia. (Lin, Sun, Ho & Shen, 2007.) On myös tutkittu, kuinka pilvilaskenta vaarantaa yksityisyyden, koska nykyään yritykset ulkoistavat sovelluspalvelujaan. Yksityisyyttä koskeva uhka johtuu siitä, että liiketoimintamalli ja sitä kautta myös asiakkaiden tiedot on viety pilvipalvelimeen. Pilvipalvelimilla käsitellään asiakkaiden luottamuksellisia tietoja, kuten taloustietoja ja terveystietoja. Pilvipalvelun tarjoajan on tärkeätä huolehtia yksityisyyden säilymisestä. (Xiao, Z. & Xiao, Y., 2013.) Yksityisyyden turvaamiseksi on kehitetty useita menetelmiä, joista yleisin on palomuuri. Palomuurin huonona puolena on se, että se on kehitetty edellisien sukupolvien turvaamiseksi, mutta hyökkääjien tietämys kehittyy. Eräässä tutkielmassa suositellaan analysoimaan hyökkäykset ja sen mukaan torjumaan niitä. Hyökkäysten analysoimisen peruslähtökohtana on se, että kaikki ovat syyllisiä ennen kuin toisin todistetaan. Esimerkiksi kun hyökkääjä hyökkää johonkin järjestelmään, hyökkäys analysoidaan ja määritellään, mitä hyökkääjä hyötyy hyökkäyksestään. Hyökkäys pitää aina ensin tunnistaa ja sen jälkeen analysoidaan onko kyseessä oikea hyökkäys, vaan laillinen käyttäjä. Analyysin tehtävänä on myös tunnistaa mahdolliset haittaohjelmat, jotka uhkaavat yksityisyyttä. (Liu, Yu & Mylopoulos, 2003.)

3.5 Suojautumiskeinoja

Tärkein suojautumiskeino verkossa tulevilta tunkeilijoilta kohtaan on palomuuri. Palomuuri muodostaa puolustuksen uloimman linjan. Palomuuri on portinvartija organisaation omaan lähiverkkoon (sisäverkon) ja julkisen tietoverkon välissä, yleensä verkko on Internet. Vartijan ominaisuudessa se pyrkii torjumaan tunkeilijat, jokaisen sisään pyrkivän IP-paketin, tekee sille turvatarkastuksen ja luvan myöntämisen jälkeen päästää sen sisään. Palomuuri voidaan toteuttaa järeällä palvelimella ja siinä pyörivällä palomuurilla. Koneessa on yleensä kaksi verkkokorttia, joista toinen on kiinni sisä- ja toinen ulkopuolella. Ainoana tapana kulkea verkossa on kulkea palomuuriohjelman läpi. Pa-

lomuuri voi olla myös huomaamattoman näköinen laite, joka kytketään organisaatioon tulevaan Internet- yhteyteen ennen tietokonetta. Purkki toimii täysin itsenäisesti ja purkkimallissa palomuuria ohjataan joiltain sisäverkon kautta. Purkkimallissa ei myöskään ole omaa käyttöjärjestelmää. Kotikäyttäjän palomuuri voi olla pelkkä omassa tietokoneessa oleva ohjelma. Ohjelma toimii samassa koneessa niiden ohjelmien kanssa. Joissakin tapauksissa palomuurin voi ostaa omalta Internet- operaattorilta, tällöin tarkistus tehdään operaattorin omasta koneesta. Yksinkertaisimmillaan palomuuri tutkii ainoastaan IP- pakettien lähtö- ja kohde osoitteet sekä portin numerot. (Järvinen, 2002 s. 215 – 316.)

Koodi- injektioiden hyökkäyksen ehkäisemisessä on useita erilaisia keinoja. SQL-injektiohaavoittuvuudet johtuvat useimmiten siitä, etteivät WWW-sovelluskehittäjät ole noudattaneet turvallisia ohjelmointikäytänteitä. SQL-injektioiden ehkäisemiseksi on kaksi tapaa: Parametrisoidut kyselyt ja syötteen koodaaminen. Parametrisoidun kyselyn tarkoituksena on erottaa SQL-kyselyn ”muotti” sekä siihen liittyvät parametrit toisistaan. XSS-injektiot voidaan torjua riittävän syötteen tarkistamisella. Tähän on olemassa neljä tapaa: Syötteessä olevat erikoismerkit voidaan korvata toisilla merkeillä tai poistaa kokonaan, erikoismerkit voidaan myös koodata eli ne pakotetaan tulkitsemana tavallisia merkkejä ja voidaan määritellä vain sallitut merkit, joita käyttäjä voi WWW-sovellukseen syöttää. Ongelmana erikoismerkkien muokkaamisessa tai poistamisessa on se, ettei käyttäjän antaman viestin alkuperäinen merkitys voi hämärtyä. CSRF-hyökkäysten ehkäisemiseksi on useita hyvin yksinkertaisia keinoja. Ensimmäinen keino on varmistaa, että GET-tyyppiset HTTP-pyynnöt voivat ainoastaan hakea sivustolta tietoa, eikä muokata niitä. Tämä keino ei kuitenkaan ole riittävä, sillä esimerkiksi JavaScript- koodin avulla on mahdollista lähettää HTTP-pyyntöjä myös POST-metodilla. Jokaisen POST-pyynnön mukana tulee lähettää satunnaisluku, joka on vaikeasti arvattavissa. Tämän satunnaisluvun tulee olla sama, kuin sivuston evästeessä oleva, koska hyökkääjä ei voi lukea käyttäjän evästeitä saman lähteen käytännöstä johtuen. (Lehtinen, 2012.)

Tietomurron ehkäisemiseksi on tärkeää luoda toimiva ja hyvä salasana. Salasana ei missään tapauksessa saa olla sama kuin käyttäjätunnus tai edes siitä johdeltavissa oleva. Salasanassa ei saa olla mitään henkilökohtaista, esimerkiksi auton rekisterinumero, puhelinnumero, syntymäaika, puolison, lemmikin tai lasten nimet). Tällaisia salasanoja murtautuja kokeilee ensimmäisenä ja yllättäen ne myös toimivat. Kesällä 2002 englantilainen pankki teki tutkimuksen käyttäjien salasanoista ja totesi niiden olevan helposti arvattavissa. Yleisin salasana oli lapsen nimi (23%) ja toiseksi yleisin oli puolison nimi (19%). Myös oma nimi ja lemmikin nimi esiintyivät salasanoissa, kummassakin tapauksessa 8% asiakkaista käyttivät näitä salasanoina. Salasanan pitää olla riittävän pitkä, usein ohjelma antaa minimi pituuden salasanalle. Monilla on se väärä käsitys, että lyhyt salasana riittää, mutta murto-ohjelma brute-force- tekniikkaa hyödyntävät hyökkääjät kokeilevat niitä ensimmäisenä. Salasanoissa pitäisi olla sekä isoja, että pieniä kirjaimia, koska se moninkertaistaa brute-force- hakuun vaadittavan ajan. Esimerkiksi A-Z- kirjaimilla tuottaa 11,8 miljoonaa vaihtoehtoa. Erikoismerkkejä kannattaa käyttää paljon salasanoissa. Ä:tä ja Ö:tä kannattaa myös hyödyntää salasanoissa, koska se lisää tuntuvasti brute-force- haun aikaa, mutta huonona puolena on se, ettei monet ohjelmat salli näiden kirjainten käyttöä. Salasana kannattaa vaihtaa säännöllisesti. Lähiverkon salasanat ovat usein säädelty, jolloin käyttäjän on pakko vaihtaa salasana. Useilla käyttäjillä on moneen eri paikkaan salasanoja, mutta jokaiseen paikkaan pitäisi olla eri salasana, samaa ei saa käyttää. Yritysten kannalta salasana ei saisi olla vain yhden henkilön tiedossa, vaan olisi hyvä jos hätätilainteiden varalta useampi henkilö tietäisi salasanan. Lähiverkossa on mahdollisuus luoda useita käyttäjätunnuksia. (Järvinen, 2002 s. 339 – 343.)

Tietoturvan parantamiseksi teleyritykset tarjoavat sähköpostinsuodattimia, joilla on tarkoitus estää virukset, madot ja muiden haittaohjelmien tuleminen käyttäjien tietokoneille sähköpostien välityksellä. Sähköpostinsuodattimilla lisäksi pyritään torjumaan tietoturvaloukkauksia ja poistetaan tietoturvan häiriöitä. Teleyrityksillä on oikeus ryhtyä välittömiin toimenpiteisiin tietoturvan varmistamiseksi sähköpostiviesteistä ja tekstiviesteistä. Ilman vastaanottajan suostumusta toimiin saa kuitenkin ryhtyä ainoastaan, vain jos ne ovat välttämättömiä verkkopalvelujen tai viestintäpalvelujen viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi. Lisäksi viestien sisältöön saa puuttua vain, jos on aihetta epäillä viestin sisältävän haittaohjelman tai jos on todennäköistä epäillä viestiä käytettävän tietoliikenteen häiritsemiseksi. Joskus voi olla epäselvää, milloin on syytä puuttua viestien sisältöön, mutta lähtökohtaisesti Viestintäviraston varoituksien virus- ja matoepäilyistä voivat aiheuttaa teleyhtiöillä toimenpiteitä. Sähköpostinsuodattimessa on myös se ongelma, mihin suodatin kiinnittää huomion. Esimerkiksi roskapostiksi voidaan epäillä sellaista viestiä, joka normaalistikin lähettää roskapostia. Yksityishenkilökin voi lyhyessä ajassa lähettää tuhansia viestejä samaan osoitteeseen. Monet roskapostiensuodattimet tunnistavat avainsanoja joita ovat esimerkiksi: Viagra, sex, adult, totally free, only for you ja näiden slangiversiot. Jo pelkät avainsanat riittävät roskapostiviestien suodattamiseen. Jos sähköpostinsuodatin poistaa väärän viestin ja käyttäjälle koituu siitä suurta haittaa, on hänellä oikeus hakea normaalia vahingonkorvausta palveluntarjoajalta. (Helepuro, Perttula & Ristola, 2004 s.149 – 158.)

Tietoturvapalvelun verkkosivustolla neuvotaan myös erilaisilla tietoturvaa uhkaavia suojautumismenetelmiä. Sivuston mukaan paras tapa on suojata tietokone pitämällä ajan tasalla torjuntaohjelmat. Tietokoneelle pitää ehdottomasti asentaa ajan tasalla olevat virustorjunta- ja palomuuriohjelmistot. Erikseen on myös saatavilla vakoiluohjelmien tarkastukseen olevia ohjelmistoja. Muita suojautumisessa huomioitavia ohjelmistoja ovat: Verkkoyhteyksien suojaaminen, automaattiset päivitykset, käytönaikainen suojausverkosto, sähköpostisuodatus, selaussuojaus, verkkohuijausten torjunta ja lapsilukko. (Tietoturvapalvelu, s.d.)

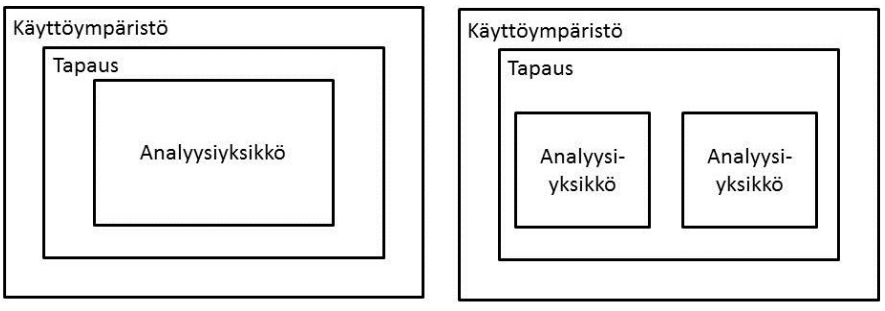
4. Tutkimusmenetelmät

Tutkimusmenetelmänä käytettiin tapaustutkimusta, joka luetaan osaksi laadullista tutkimusta. Laadulliseen tutkimukseen päädyttiin haastateltavien vastauksiin. Myös haastateltavien määrä oli liian pieni (10 + 10), jotta voitaisiin tehdä todellista kvantitatiivista tutkimusta.

Laadullisessa tutkimuksessa paneudutaan ensiksi tutkimuksen aiheeseen ja aikaisempiin tutkimustuloksiin. Aikaisempiin tutkimuksiin tutustumalla saadaan uusia näkökulmia omaan tutkimusaiheeseen ja aikaisempia tutkimustuloksia pitää pystyä myös vertaamaan omiin tutkimustuloksiin tieteellisestä näkökulmasta. Laadullisen tutkimuksen lopuksi, tutkimustulokset analysoidaan. Ennen kuin tutkimustuloksia voidaan analysoida, on ne saatava analysoitavaan muotoon, esimerkiksi muistiinpanoilla ja litteroinnilla. Laadullinen tutkimus raportoidaan samalla tavalla kuin määrällinen tutkimus, raportista pitää käydä ilmi mistä tieto on hankittu ja kuinka luotettavaa tieto on. (Metsämuuronen, 2003 s. 1-9, s. 196 & s. 206.) Tonna ja Edwards ovat tutkineet, mistä laadullinen tutkimus on saanut alkunsa. Heidän määritelmänsä mukaan laadullinen tutkimus on saanut alkunsa sosiaalitieteestä. Laadullinen tutkimus on eräänlainen sosiaalinen kysely, miten ihmiset tulkitsevat erilaisia asioita. (Tonna & Edwards, 2012.)

4.1 Tapaustutkimus

Tapaustutkimuksessa pitää tulla esille tavoite, mitä tutkitaan, teoreettinen viitekehys, tutkimuskysymys (mitä aikaisemmin on tutkittu kyseisestä aiheesta?), tutkimusmenetelmä ja mistä saadaan lisää tietoa tutkimuksen aiheesta. Tutkimusta voidaan lähestyä esimerkiksi havainnoimalla tai kuvailemalla tutkimusongelmaa. Tutkimuksen teoriakatsauksen aikana pyritään selvittämään, mitä tiedetään jo tutkittavasta asiasta, jotta voidaan lähteä itse keräämään aineistoa. Tapaustutkimuksessa tapaukset voivat olla lähes mitä tahansa, mikä on tämän ajan ilmiö. Runeson ja Höst ovat hyödyntäneet tapaustutkimusta tutkiessaan ohjelmistoissa esiintyviä ilmiöitä (tutkimalla, mihin suuntaan ohjelmistot ovat mahdollisesti menossa käyttäjien näkökulmasta?). Tässä kyseisessä tutkimuksessa tapauksen aiheuttaa ihmisen ja tietotekniikan vuorovaikutus, jolloin saadaan selville, millaisia ilmiöitä tietotekniikan käyttö aiheuttaa peruskäyttäjille. Empiiristä aineistoa kerättiin seuraamalla vierestä ihmisten tietokoneen käyttöä. Tapaustutkimuksen kehittämishankkeessa voi olla mukana sekä yksittäisiä henkilöitä, että ryhmiä. (Runeson & Höst, 2009.)



Kuva 3. Tapaustutkimuksen malli. (Runeson & Höst, 2009.)

Kuvassa 3 on esitetty tapaustutkimus, jossa aineisto koostuu kahdesta tapauksesta. Ensiksi määritellään käyttöympäristö, minne voidaan koota yhteen kaksi erilaista henkilöä tai ryhmää. Näistä kohderyhmistä muodostuu tutkimuksen aikana kaksi tapausta, jotka analysoidaan lopuksi omana tapauksena ja tehdään vertailua. (Runeson & Höst, 2009.) Tässä tutkimuksessa on myös toteutettu samaa kaavaa. On kaksi kohderyhmää (Oulun yliopisto ja Tampereen ammattikorkeakoulu), jotka tuottavat oman tapauksen. Molemmat tapauksen analysoidaan omana aineistona ja lopuksi tehdään vertailua.

4.2 Haastattelu

Haastatteluun voidaan käyttää erilaisia tapoja: yksilöhaastattelu kasvoista kasvoihin, ryhmähaastattelu kasvoista kasvoihin, postitettu tai paikanpäällä tehty lomakehaastattelu. Kaikki tutkijat eivät pidä kyselylomaketutkimusta haastatteluna. Haastattelu voidaan toteuttaa strukturoidusti, puolistrukturoidusti tai avoimesti. Haastattelun kestävät yleensä viidestä minuutista useisiin päiviin. Haastatteluja käytetään monesti terapeuttisissa tai psykiatrisissa tilaisuuksissa. Haastattelumenetelmä sopii erityisesti hyvän aineiston hankkimiseen. Kuten aikaisemmin mainittiin, niin haastattelumuotoja on erilaisia. Strukturoitu haastattelu suoritetaan yleensä lomakehaastatteluna. Puolistrukturoitu haastattelua voidaan kuvailla teemahaastatteluna, jossa käydään läpi haastateltavan arkaluonteisia asioita. Ei strukturoitua (avoin haastattelu) haastattelua voidaan nimittää myös vapaaksi, syväksi, tai informaaliksi. Avoin haastattelu muistuttaa lähinnä keskustelua, jossa haastattelija ei välttämättä johda keskustelua. (Metsämuuronen, 2003 s.185 – 189.) Esimerkiksi vuonna 1997 toteutettiin haastattelu yritykseen, johon otettiin käyttöön uutta tietotekniikkaa. Haastateltavina olivat yrityksen työntekijät, joilta kysyttiin 139 kysymystä tietotekniikan täytäntöönpanosta. Haastattelu toteutettiin strukturoidusti. Haastattelusta voitiin todeta, että uuden tietotekniikan käyttöön otto oli hyvä työväline nykyaikaisessa yrityksessä. Haastattelussa kävi ilmi, että tämän kaltaisella tutkimuksella voidaan saada kattavia tietoja työntekijöiltä uuden tietotekniikan käyttöön otosta. Haastattelututkimuksella pyrittiin poistamaan pois vääristymiä ja harhoja subjektiivisista vastauksista. (Korunka, Weiss & Zauchner, 1997.) Tässä tutkielmassa hyödynnettiin haastattelua tapaustutkimukseen, jossa oli kaksi tapausta. Ne analysoitiin kuvan 3 mukaisesti.

5. Tutkimuksen toteutus

Tutkimus toteutettiin kahdessa vaiheessa. Ensimmäisessä vaiheessa tarkasteltiin Viestintäviraston raportteja. Toisessa vaiheessa haastateltiin korkeakouluopiskelijoita Tampereen ammattikorkeakoulusta ja Oulun yliopistosta. Kummastakin oppilaitokselta valittiin kymmenen oppilasta, heiltä kysyttiin tietoturvaan/yksityisyyteen kohdistettuja yleisiä kysymyksiä ja niihin kohdistuvia uhkia/haavoittuvuuksia. Haastattelu toteutettiin lomakkeelle. Oulussa haastateltiin kaikkia tutkimuksessa mukana olleita oppilaita henkilökohtaisesti, haastattelu toteutettiin kokonaisuutena lomakemuodossa. Tampereelle haastattelu suoritettiin osittain sähköpostin välityksellä ja osittain lomakkeella. Eli haastattelut suoritettiin kokonaisuutena strukturoidusti. Haastattelujen pohjalta tehtiin yhteinen analysointi, minkälaisia ajatuksia ja tietämyksiä opiskelijoilla on tietoturvasta ja yksityisyydestä. Tutkimuksessa on kaksi tapausta, Tampereen ammattikorkeakoulu (tuottaa yhden tapauksen) ja Oulun yliopisto (tuottaa yhden tapauksen). Tästä johtuen tutkimusmenetelmänä voidaan soveltaa myös tapaustutkimusta. Loppuanalyysissä voidaan hyödyntää Viestintäviraston julkaisemia raportteja. Näistä suoritettiin yhteinen analyysi.

5.1 Tapahtuneita tietomurtoja ja tietoturvallisuuden loukkauksia

Tapahtuneiden tietomurtojen ja tietoturvallisuuden loukkaukset perustuu Viestintäviraston julkaistuihin raportteihin. Viestintäviraston raportteja otettiin esille yksitoista, tietoturvaloukkauksista pääsääntöisesti Suomesta, mutta osa tapauksista on tapahtunut myös ulkomailla, joilla saattaa olla vaikutusta Suomen tietoturvaan. Tietoturvaloukkaukset ovat tapahtuneet vuosina 2010, 2011, 2012 ja 2013. Raporttien pohjalta voidaan päätellä, että tietoturvahyökkäykset ovat suurimmalta osalta järjestäytyneitä ja niillä hyökkääjän tarkoituksena on hyötyä taloudellisesti tai tehdä yritykselle kiusaa. Hyökkäysten kohteeksi voi joutua yksityishenkilö tai organisaatio. On tapauksia joihin hyökkääjä on kohdistanut murron, sekä organisaatioon, että samanaikaisesti yksityiseen henkilöön. Tällainen tapaus on esimerkiksi tullut esille 17.7.2012, jolloin tietomurto tehtiin Yahoon, Contributor Network- palveluun, Formspringin ja australialaiseen Billaborg Internationaliin. Näiden käyttäjien tunnuksia ja salasanoja oli vuodettu verkkoon. Tässä tietomurron kohteeksi joutui organisaatio ja yksityinen henkilö samanaikaisesti, joka käytti organisaation palveluja. Suomessa palvelunestohyökkäys oli toteutettu mediataloihin (Ilta-Sanomat, Iltalehti, Nelonen, MTV3, YLE). Viestintävirasto raportoi tästä tapauksesta 28.12.2012. On selvää, että tässä hyökkäyksessä oli kyse pelkästä haitan teosta. Viestintävirasto on myös raportoinut 27.11.2012, että suomalaisia verkkosivustoja on sotkettu. Hyökkäyksen kohteeksi oli joutunut sadat webhotelli.fi- palveluiden asiakkaiden sivustot. Tämä hyökkäys kohdistettiin pääsääntöisesti yksityiseen henkilöön suoraan. Viestintäviraston raporteista voidaan päätellä, että useat hyökkääjät pyrkivät saamaan käyttäjien käyttäjätunnuksia ja salasanoja tietoonsa. Esimerkiksi Viestintävirasto on raportoinut 23.2.2011, että suomalaisia verkkopankkien tietoja on yritetty urkkia. Urkkijat ovat tehneet omat sivustot, joilla on pyritty matkimaan verkkopankkien virallisia sivustoja. Verkkopankin palvelujen käyttäjien on ollut tarkoitus kirjautua palveluun omilla verkkopankkitunnuksilla, jolloin urkkijat saisivat omaan tietoonsa tunnukset. Normaalisti ulkomaan hyökkääjät lähettävät viestinsä käyttäjien sähköpostiin, mutta ne on käännetty suomeksi tökerösti Google Translatella, joten käyttäjien on helppo huomata huijausviestit. Viestintävirasto on maininnut että jos omat tunnukset ovat vuotaneet verkkoon, ne pitää vaihtaa heti. 23.4.2013 on raportoitu, että Itellan asi-

akkaiden salasanoja on viety tietomurron seurauksena. Hyökkääjät ovat vuotaneet asiakkaiden salasanalistan Internetiin kaikkien nähtäville. Tässä tapauksessa on kaikkia käyttäjiä kehotettu vaihtamaan salasanansa heti. Kaikissa tietoturvaa uhkaavissa tapauksissa yksityinen käyttäjä tai organisaatio ei voi vaikuttaa hyökkäyksien kulkuun. Viestintävirasto on raportoinut 10.1.2013 tapauksen, jossa on havaittu Java 7 Update 10 haavoittuvuus, jota ei voida korjata. Tätä haavoittuvuutta hankaloittaa se, että jotkut verkkopalvelut vaativat Javaa. Javan käytössä suositellaan käyttämään selainta, jossa Java ei ole päällä. Tällä selaimella hoidat surffailut ja kaikki muut päivittäiset asiat ja toisella selaimella, jossa Java on päällä, hoidat asioinnin palveluissa, jotka kaipaavat Javaa.

Tässä on muutamia mielenkiintoisimpia tapauksia Viestintäviraston julkaisemisista tapauksista:

Suomalaisia IRC- kanavia vallattu: Internet Relay Chat, eli IRC tai tuttavallisemmin irkki, kuuluu internetin vanhimpiin pikaviestintäpalveluihin. Palvelu tarjoaa käyttäjille mahdollisuuden käydä tosiaikaista keskustelua keskusteluhuoneissa tai niin sanotuilla kanavilla. CERT-FI tutkii tapausta jossa tietomurron kohteeksi joutunutta suomalaista palvelinta on käytetty hyväksi IRC-kanavien valtauksessa. Tietomurron tekijä on tehokkaasti peittänyt jälkiään palvelimella, mutta talteen saatu aineisto viittaisi siihen, että palvelimelle tavalla tai toisella on päästy sisään murretun SSH-tunnuksen avulla. Palvelimelta on myös löytynyt jälkiä jotka viittaavat siihen, että käyttövaltuuksia on yritetty laajentaa käyttäen hyväksi Linux-käyttöjärjestelmässä ollutta haavoittuvuutta. Tietomurron yhtenä motiivina lienee ollut hyökkääjän jälkien peittäminen. Hyökkääjä on myös pystynyt hyödyntämään sitä, että murretun palvelimen on tunnistettu olevan Suomessa. Eräiden IRC-kanavien osalta kyseinen tunnistus on riittänyt kanavan valtaamiseen tarvittavien ylläpito-oikeuksien saamiseksi. Nyt tutkitun suomalaisen palvelimen lisäksi IRC-kanavien valtauksessa on hyödynnetty myös ulkomailla sijaitsevia palvelimia.

Viestintävirasto 29.1.2010

Yleensä verkkourkintaa tehdään sähköpostilla, jolloin sähköposti on englanniksi tai käännetty suomeksi jollain netin käännöskoneista, kuten Google Translatella. Varsinkin suomalaiset käännökset viesteistä ovat hyvinkin tökeröjä ja melko helposti huomattavissa väärennöksiksi. Tyypillisesti urkintasähköposteilla kysellään käyttäjän tunnuksia web-sähköpostiin tai verkkopankkiin. CERT-FI:n tietoon tulleissa tapauksissa vastaanottajan saama sähköposti kehottaa siirtymään selaimella sivustolle, mihin käyttäjän tulisi täyttää verkkopankin tunnukset. Sivustojen sisältöä on kopioitu varsinaisten verkkopankkien sivuilta ja ne voivat näyttää hyvinkin aidolta. Selaimen osoitekenttä kuitenkin paljastaa että kyseessä ei ole verkkopankin sivusto.
Jos saat urkintaviestin, poista se, äläkä käy sivustolla mihin sähköpostissa viitataan. Sivusto ei välttämättä sisällä vain urkintatarkoituksessa tehtyä kaavaketta, vaan sivustolta voi saada myös haittaohjelmatartunnan

Viestintävirasto 23.2.2011

Palvelunestohyökkäyksillä useita kohteita Suomessa: Tähän astisissa palvelunestohyökkäyksissä on ollut yhdistäviä piirteitä, joiden perusteella on mahdollista arvioida niiden olevan saman tekijän aikaansaannoksia. Erityisesti valittu hyökkäystekniikka ja hyökkäyksissä nähdyt liikennemäärät ovat olleet samankaltaisia kohteesta toiseen. Kohteena ovat olleet ainakin Ilta-Sanomien, Iltalehden, Nelosen, MTV3:n, YLE:n ja Nelosen uutissivustot sekä viimeksi uutispalvelu Ampparit.com. Sen sijaan Elisan ja suomalaisten lentokenttien lähtöselvityksen tietoliikenneongelmat eivät johtuneet palvelunestohyökkäyksestä. Hyökkäystekniikalle on tunnusomaista se, että hyökkäysliikenteen lähde-

osoitteet ovat väärennettyjä. Kohdeverkon tilatietoisia verkkolaitteita pyritään kuormittamaan yli niiden suorituskyvyn avaamalla suuri määrä yhteyksiä samaan aikaan. Tällaisia laitteita ovat esimerkiksi palomuurit. Lisäksi kohteeseen suunnatut liikennemäärät ovat olleet enimmillään suurempia kuin kohdeverkkojen tietoliikenneyhteyden kapasiteetti. Kuluvan päivän aikana on Viestintävirastolle raportoitu myös palvelunestohyökkäysyrityksistä, jotka hyödyntävät nimipalvelujärjestelmiä. CERT-FI on toimittanut yksilöivämpiä tietoja hyökkäysliikenteestä suomalaisille teleyrityksille, ICT-palveluntarjoajille ja huoltovarmuuskriittisille organisaatioille, jotta nämä pystyisivät suojaamaan omat verkkonsa ja tehostamaan hyökkäysyritysten havainnointia. Kaikkia asianomistajia on kehotettu tekemään poliisille rikosilmoitus.
Viestintävirasto 28.12.2012

Drupal.org–käyttäjien tietoja varastettutietomurrossa: Drupal.org-sivustolle on murtauduttu hyödyntämällä sivustolle asennetussa kolmannen osapuolen komponentissa olevaa haavoittuvuutta. Tietomurron ajankohta ei ole tällä hetkellä tiedossa. Tekijä on saanut käsiinsä drupal.org- ja groups.drupal.org-palvelujen käyttäjien tiedot. Käyttäjien tiedoista on paljastunut ainakin käyttäjätunnus, sähköpostiosoite, maa ja salasanatiiviste. Murrossa paljastuneet salasanat on resetoitu. Sivusto ei kerää luottokorttitietoja, joten niitä ei ole myöskään varastettujen tietojen joukossa.
Viestintävirasto 30.5.2013

5.2 Korkeakouluopiskelijoiden tietoisuus haavoittuvuuksista

Tutkimuksessa käytiin läpi kummatkin korkeakoulut erikseen, jolloin ne analysoidaan ja vertaillaan keskenään. Tutkimuksessa on otettu huomioon molempien oppilaitosten tietojenkäsittelytieteiden suuntautumisvaihtoehdot. Oulun yliopiston tietojenkäsittelyn koulutusohjelmassa on erikoistuttu ohjelmistotuotantoon ja tietojärjestelmiin. Ohjelmistotuotannolla pyritään tuottamaan ohjelmistoja ja palveluja erilaisten organisaatioiden käyttöön. Tietojärjestelmät painottuvat arkielämän ratkaisuihin, esimerkiksi johtamiseen, terveydenhuoltoon, teollisuustuotantoon, markkinointiin, peleihin, viihteeseen ja kuluttajasovelluksiin. (Oulun yliopisto, 2012.) Tampereen ammattikorkeakoulun tietojenkäsittelyn opetuksessa (tradenomi) koostuu yritysten näkökulma ja opinnoissa painotetaan vahvaa liiketalouden osaamista. Opinnot painottuvat alussa erilaisiin ICT (information and communications technology) alan ratkaisuihin ja toimimaan tiimeissä. Myöhemmin on mahdollista suuntautua digitaaliseen viihteeseen ja palveluihin (kuten pelikehitys), ohjelmistojen tuottamiseen ja testaamiseen, tietoverkkojen ja palvelinjärjestelmien palveluihin, tietoturvaan, uusien teknologioiden nopeaan käyttöönottamiseen ja soveltamiseen, terveysalan tietojärjestelmiin, asiakasrajapinnassa toimimiseen sekä ja ICT-alan yrittäjyyteen. (Tampereen ammattikorkeakoulu, 2013.)

Tutkimusta varten haastateltiin Tampereen ammattikorkeakoulun oppilaita ja Oulun yliopiston oppilaita. Haastateltavilta kysyttiin, minkälaisia riskejä ja haavoittuvuuksia liittyy tietoliikenteeseen, minkälainen yleinen tietämys heillä on tietoturvasta ja onko heillä valmiutta ylläpitää tietoturvaa ja yksityisyyttä (esim. omassa tietokoneessa). Ensimmäisenä tutkimukseen osallistuneilta kysyttiin taustatietoa, minkälainen kokemus heillä on ollut ennestään tietoturvasta.

Haastattelu toteutettiin paikan päällä lomakemuodossa eli opiskelijat itse kirjoittivat vastauksen haastattelulomakkeeseen. Oulun yliopistolla haastatteluun saatiin kymmenen opiskelijaa, joista neljä oli naisia ja kuusi miestä, ikärakenne muodostui 21 - 50 vuoden väliin. Suurimmalla osalla ei ollut käytännön tietoturvakokemusta muualta kuin omasta koneesta.

Tampereen ammattikorkeakoulun haastattelu toteutettiin osittain sähköpostilla, mutta suurin osa vastauksista kerättiin paikan päällä. Yhtä vastaajaa lukuun ottamatta opiskelijoiden pääaiheena oli pelituotanto. Vastauksia sain kymmenen, kolme vastaajista oli naisia ja seitsemän miestä. Ikärakenne muodostui 21-52 välille. Kuten Oulussakin niin Tampereella suurimman osan tietoturvakokemus oli tullut oman tietokoneen tietoturvasta huolehtimisesta.

Ensimmäisenä kysyttiin mitä tietoturva opiskelijoille merkitsee.

Oulussa tietoturva määriteltiin omien tietojen suojaamiseksi, voidaan hallita omia tietoja (voidaan itse päättää kenelle tietoa annetaan) ja itseä koskevat tiedot ovat turvassa, eikä vapaasti saatavilla.

”Sitä mitä tietoa halutaan jakaa ja kenelle. Muilla ei tulisi olla tietoturvan takia tämän tietoja.”

Mies 21

”Tarkoittaa, että tiedot ovat turvassa niin, että väärät henkilöt ei pääse niihin käsiksi, pysyvät hallinnassa eli eivät vahingossa katoa.”

Nainen 21

Tampereella tietoturva määriteltiin omien tietojen salaamisella, tietoturvaohjelmistot ovat ajan tasalla ja verkossa voidaan turvallisesti asioida.

”Henkilökohtaisten tietojen suojelua.”

Mies 22

”Henkilökohtaiset tiedot, laitteet eivät joudu ulkopuolisten haltuun”.

Nainen 28

Oulun yliopiston ja Tampereen ammattikorkeakoulun vastaukset eivät suuresti eronneet toisistaan, mutta tamperelaiset määrittelevät tietoturvan enemmän oman koneen turvaamiseksi, kun oululaiset määrittelevät tietoturvan oman yksityisyyden suojaamiseksi.

Toisena kysyttiin, mitä yksityisyys merkitsee.

Oulun yliopiston opiskelijat määrittelevät yksityisyyden omien tietojen hallitsemiseksi, tiedot pysyvät ainoastaan niillä, joille ne kuuluvat. Yksityisyys merkitsi myös suurimmalle osalle pelkästään yksityishenkilön henkilökohtaisten tietojen hallintaa.

”Omien henkilökohtaisten asioiden salassapitoa Hyvin subjektiivinen ja liikkuva määre.”

Mies 27

”Tieto, joka ei muille kuulu (esim. henkilötiedot) ovat yksityisiä ja siten, niihin eivät asianulkopuoliset saa päästä käsiksi.”

Nainen 22

Tampereella yksityisyys määriteltiin, ettei tieto ole julkista, vaan tieto kuuluu vain itselle, ei edes valtio saa selvittää asukkaiden henkilökohtaisia tietoja.

”Ei edes valtio saa tutkia tilejäni.”

Mies 27

”Sitä ettei kukaan saa tietää henkilökohtaisia asioitani ilman minun tietämättäni/sallimatta.”

Nainen 23

Tässä kysymyksessä Tampereen ja Oulun vastaajat olivat kokonaan samoilla linjoilla yksityisyydestä.

Kolmantena kysymyksessä pyydettiin määrittelemään tietoturvakäsitettä, uhat ja haavoittuvuudet.

Oululaisten mielestä uhat voivat vaarantaa tietoturvan tai mahdollinen hyökkäys tietoturvaa kohti. Haavoittuvuus määriteltiin, että se voi olla koodissa ja mitä hyökkääjä voivat käyttää hyväkseen.

Uhka: ”*tietoturvapäätteiden ja järjestelmänpuutteiden aiheuttamat mahdolliset haavoittuvuudet.”*

Mies 25

Haavoittuvuus: *”voi olla ongelma koodissa, jonka kautta tietoturva voi vaarantua. Samoin ongelmia ihmiselementeissä. Esim. huonosti tehdyt salasanat ja huolimattomuus.”*

Nainen 21

Tamperelaiset määrittelivät uhat, että tietoja voi kadota, ohjelmistot eivät ole ajan tasalla ja tiedot voivat levitä ulkopuolisille. Haavoittuvuus määriteltiin huonoilla salasanoilla ja ohjelmistosta on löydetty porsaanreikä.

Uhka: *”käytäntö, jolla tietoturva murretaan.”*

Mies 22

Haavoittuvuus: *”porsaanreiät koodissa ym.”*

Nainen 21

Vastaukset erosivat jonkin verran toisistaan Oulussa uhat ja haavoittuvuus pystyttiin erottamaan toisistaan, mutta Tampereella osa piti näitä kahta samankaltaisina ongelmina

Neljäntenä kysymyksenä pyydettiin kertomaan esimerkkejä, mitä uhkia sisältyy Internet protokollaan (tietoturvassa/yksityisyydessä).

Oulussa monet vastaajista eivät osanneet määritellä, miten Internet protokolla uhkaa tietoturvaa. Useat onnistuivat vastaamaan, että uhkia on mm. salakuuntelu ja hakkerointi.

”Salakuuntelu, tiedon muuttaminen ulkopuolisen toimesta.”

Mies –

”Salasanojen anastaminen. Koneeseen tunkeutuminen ja koneen käyttäminen bot-netissä.”

Nainen 50

Tampereella vastattiin, myös, että uhkana on salakuuntelu. Muita uhkia oli, pakettien kaappaaminen ja IP- osoitteen kautta voidaan jäljittää toisen sijainti. Myös suurena uhkana pidettiin, ettei voida olla varma, onko oman ja vieraan koneen välillä kolmatta osapuolta

”Pakettien katoaminen, kaappaaminen ja muuntelu matkalla.”

Mies 52

”IP:n avulla on mahdollista saada esimerkiksi toisen henkilön sijainti, muuta en nyt muista.”

Nainen 23

Tässä kysymyksessä oululaisten ja tamperelaisten vastaukset olivat lähes täysin identtisiä, Tampereella pohdittiin enemmän sitä, onko oman ja vieraan (PC1-PC2) välillä kolmatta osapuolta. Molempien koulujen opiskelijoilla oli vaikeata määritellä Internet protokollaa koskevaa uhkaa.

Viidentenä kysyttiin mielipiteitä, miten sosiaalisessa mediassa pitäisi ottaa huomioon yksityisyys.

Oulussa oppilaat pohdiskelivat, että sosiaalisessa mediassa ei saisi poimia ihan mitä tietoja tahansa, vaan sosiaalisessa mediassa pitäisi olla hyvät työkalut omien tietojen muokkaamiseen ja ettei tietoja levitetä ilman asianomaisen lupaa ulkopuolisille.

”Ihmisten (käyttäjien) täytyisi olla enemmän tietoisia siitä mihin tietonsa laittavat. Palvelun tarjoajien tulisi selkeästi osoittaa palvelun tietojen käyttötavat.”

Mies 25

”Mielellään kerättyjä tietoja ei levitetä kaikille. Tosin aika paljon omalla vastuulla tietenkin jotain, asiat joita siellä paljastelee.”

Nainen 21

Tampereen ammattikorkeakoulussa pohdittiin, että pitää olla tarkkana mitä tietoja levittää itsestään sosiaalisen median välityksellä ja tietoja ei saa levittää kolmansille osapuolille. Myös ehdotettiin ikärajaa sosiaalisessa mediassa (alaikäiset lavertelevat) ja palvelun pitää kirjata automaattisesti ulos järjestelmästä, kun lopetetaan palvelun käyttäminen.

”Henkilökohtaisia tietoja ei pitäisi luovuttaa kolmansille osapuolille.”

Mies 22

”Yksityisiä tietoja ei saisi kerätä joidenkin yritysten rekistereihin, ellei ne ole välttämättömiä, esimerkiksi palveluiden tarjoamisen kannalta. Lisäksi omien tietojen näyttäminen vain tietyille ihmisille tulisi olevan helppoa asetusten kautta.”

Nainen 23

Vastaukset erosivat välillä aika suuresti toisistaan, oululaisten mielestä vastuu yksityisyydestä on palvelun tarjoajalla, kun tamperelaisten mielestä vastuuta on myös palvelujen käyttäjillä. Molemmissa kouluissa oltiin samaa mieltä, siitä ettei sosiaalisen median ylläpitäjälle tarvitse antaa kaikkia omia (henkilökohtaisia) tietoja.

Kuudentena kysyttiin, että mitä teet jos koneellesi tehdään tietomurto.

Oulun yliopiston oppilaiden mielestä salasana pitää heti vaihtaa, virustorjunnan päivitykset pitää tarkistaa, alustetaan C-asema (format C:) ja kone irti netistä. Eräs opiskelija ehdotti myös panikoimista.

”Koitan korjata tietoturva-aukot offline tilassa ja suojaan tärkeimmät tiedot toisella koneella kuten salasanat.”

Mies 21

”En tiedä, alan ainakin vaihtamaan salasanoja ja panikoimaan.”

Nainen 21

Tampereen ammattikorkeakoulun opiskelijat ehdottivat, että tietomurron seuraukset voidaan itse selvittää, tietomurrosta pitää ilmoittaa viranomaisille, pitää ottaa yhteys palveluntarjoajaan (Internet) ja yhteys poikki netistä.

Vastaukset erosivat jonkin verran toisistaan. Tamperelaiset antoivat enemmän käytännön vinkkejä ja oululaiset pyrkivät suoraan poistamaan virukset koneeltaan. Sama asia toistui vastauksista, tarkasta virustorjunnat ja yhteys poikki netistä.

Seitsemäntenä kysymyksenä pyydettiin kertomaan, kuinka tutkimukseen osallistuneet tunnistavat seuraavat uhat: Hakkerointi hyökkäys, sisäinen uhka, web-sivu hyökkäykset, hyökkäykset älypuhelimiin ja taulutietokoneisiin ja yksityisyyden invaasio.

Oulussa lähes kaikki vastaajat olivat kuulleet tai osasivat selittää kyseiset tietoturvaa koskevat uhat, mutta hyökkäykset älypuhelimiin ja taulutietokoneisiin vastaukset vaihtelivat todella suuresti, osa vastaajista ei ollut kuullutkaan koko uhasta. Kaikki vastaajat eivät ymmärtäneet tai osanneet selittää, mitä tarkoittaa web-sivuihin kohdistuivat hyökkäys.

Tampereen ammattikorkeakulussa kaikki vastaajat osasivat selittää uhat, yksityisyyden invaasiota lukuun ottamatta, joita eivät osanneet määritellä 9/10 vastaajista. Yksi vastaajista tiesi ainoastaan mitä tarkoittaa hakkerointi- hyökkäys ja sisäinen uhka tietoturvassa.

Tietoturvaa koskevista uhista olivat paremmin perille oululaiset, kun tamperelaiset olivat kuulleet kyseisistä uhista jotain, mutta kaikki eivät osanneet selittää mitä kaikki uhat tarkoittavat. Kaksi kaikista vastaajista oli todella hyvin perillä edellä mainituista uhista, yksi Oulusta ja yksi Tampereelta.

Kahdeksantena kysymyksenä pyydettiin kertomaan miten tuttuja ovat seuraavat haavoittuvuudet: SQL-injektio, OS komento- injektio, XSS, sähköposti-injektio ja koodi-injektio.

Oulussa SQL-injektio, OS komento- injektio ja sähköposti-injektio olivat tutuimmat, mutta suurimmalle osalle vastaajista edellä mainitut haavoittuvuudet olivat tuntemattomia tai olivat kuulleet niistä vähäsen. Ainoastaan yksi vastaaja tunsi hyvin kaikki haavoittuvuudet.

Tampereella olivat kaikki haavoittuvuudet lähes tuntemattomia, kaksi vastaaja ymmärsi tai osasi selittää kyseiset haavoittuvuudet. Yksi vastaajista ei ollut kuullut yhdestäkään haavoittuvuudesta.

Molempien koulujen oppilaiden mielestä edellä mainitut haavoittuvuudet olivat aika tuntemattomia, Tampereella osa oppilaista ei osannut selittää ollenkaan mistään haavoittuvuudesta, kun Oulussa löytyi oppilaita, jotka osasivat selittää haavoittuvuuksista jotain. Tampereelta kuitenkin kaksi vastaaja tunsi hyvin kaikki haavoittuvuudet, kun Oulussa ainoastaan yksi vastaajista tunsi hyvin kyseiset haavoittuvuudet.

Viimeisenä kysyttiin, mitä haavoittuvuuksia voisi olla Internet- selaimissa. Tähän kysymykseen kaikkien tutkimukseen osallistuneiden ei tarvinnut vastata.

Oulussa tähän kysymykseen vastasi kolme opiskelijaa. Kysymykseen vastaajien mielestä on olemassa sellaisia selaimia, minkä tietoihin ulkopuoliset voivat päästä käsiksi, kuormituksen kestävyys on myös yksi haavoittuvuus ja selaimilla on myös useita tietoturva- aukkoja.

”Esimerkiksi kuormituksen kestämättömyys. Heikot suojauskäytänteet, kuten SSL:n käyttämättömyys. Vanhojen ympäristöjen hyödyntäminen kuten Java”

Mies 22

”En tiedä muuta kuin, että jotain tietoturva-aukkoja löytyy.”

Nainen 21

Tampereella tähän kysymykseen vastasi kahdeksan oppilasta. Vastauksista kävi ilmi, että koodi- injektio (esim. Java- koodi) on selaimissa oleva haavoittuvuus lisäksi ilmi tuli myös haavoittuvuuksista valelinkit ja selainhistoria.

”Aukot koodissa, joista päästään lisäksi käyttäjän tietoihin.”

Mies 22

”Kolmannen osapuolen ohjelmat, jossa on haavoittuvuuksia ja joita asennetaan mukaan selaimeen.”

Nainen 28

Kysymyksen vastaukset eivät ole vertailukelpoisia, koska Tampereella oli kahdeksan vastaajaa kysymykseen ja Oulussa vain kaksi. Molempien koulujen oppilaiden mielestä selaimissa on nykypäivänä paljon tietoturva- aukkoja.

5.3 Haastattelun analysointi

Kysymyksiin vastasi kymmenen opiskelijaa Oulun yliopistosta ja kymmenen Tampereen ammattikorkeakoulusta. Oulun yliopiston opiskelijat olivat toisella ja kolmannella vuodella. Heidän suuntautumisekseen kerrottiin pääsääntöisesti tietojenkäsittely, josta voidaan päätellä, että heillä ei kandivaiheessa ole vielä tarkempaa suuntautumista. Tampereen ammattikorkeakoulun opiskelijat olivat yhtä aikuisopiskelijaa lukuun ottamatta suuntautuneena pelituotannon puolelle. Oulun yliopiston opiskelijat olivat paremmin perillä haavoittuvuuksista, mutta tiedot olivat lähinnä käytännönläheisiä. Tampereen ammattikorkeakoulussa etenkin IP- osaamisessa oli puutteita, mutta tiedot olivat teknillisempiä, kuten esimerkiksi, mitä haavoittuvuuksia voisi olla Internet- selaimissa. Molemmissa korkeakouluissa oli vaikeuksia kertoa haavoittuvuuksista yksityiskohtaisemmin, mutta uhat olivat paremmin selvillä molempien koulujen opiskelijoiden osalta. Molemmista korkeakoulusta kaikki osasivat hyvin hahmottaa, mitä eroavaisuutta on uhilla ja haavoittuvuuksilla, mutta vaikeuksia oli erotella eri haavoittuvuuksia, kuten esimerkiksi mikä on XSS- haavoittuvuus. Viisi haavoittuvuutta otettiin esille, siitä huolimatta suurin osa vastaajista ei osannut niitä selittää, vaan olivat kuulleet haavoittuvuuden nimen jonkun yhteydessä. Tietoturvaa koskevat uhat olivat paremmin tiedossa Tampereen ammattikorkeakoulussa, kun taas tietoturvaa koskevat haavoittuvuudet olivat paremmassa tiedossa Oulun yliopiston opiskelijoilla. Tutkimuksesta voidaan päätellä, että molemmissa korkeakouluissa on puutteita haavoittuvuuksien tunnistamisissa, vaikka kyseinen ongelma osataankin hyvin määritellä. Kokemuksella oli suuri osa haavoittuvuuksien tunnistamisessa, opiskelijat joilla oli takana jo työhistoriaa IT-alalla tai jotka harrastavat vapaa-ajalla aktiivisesti tietoturvaa, osasivat paremmin määritellä uhat/haavoittuvuudet ja niiden erot. Myös kokeneemmat opiskelijat olivat paremmin tietoisempia haavoittuvuuksista, kuin esimerkiksi alle 25- vuotiaat. Molemmissa kouluissa opitaan lähinnä vain tietoturvasta perusteet, vasta työelämään siirtymisessä tai oman aktiivisuuden kautta opitaan määrittelemään haavoittuvuus ja niihin kohdistuneet uhat paremmin. Suurin osa opiskelijoista molemmista korkeakouluista osasi reagoida, jos omaan koneeseen tehdään tietomurto. Koulujen välisessä tietoisuudessa koskien web- järjestelmien haavoittuvuuksista ei havaittu suuria eroavaisuuksia. Kaikki vastaajat tiesivät, mitä haavoittuvuus on, mutta eivät osanneet selittää esimerkiksi annettuja haavoittuvuuksia.

6. Pohdinta

Tässä tutkielmassa perehdyttiin ensin yleisesti web- järjestelmiin ja niiden eri muotoihin. Web- järjestelmien jälkeen siirryttiin tietoturvaan, niiden uhkiin, haavoittuvuuksiin ja lopuksi pohdittiin mahdollisia suojautumiskeinoja. Kysymykset, joita kysyttiin valituille korkeakouluopiskelijoille, tulivat yleisesti tietoturvasta/yksityisyydestä ja niiden uhista/haavoittuvuuksista. Haastattelu painottui lähinnä web-järjestelmien koskeviin haavoittuvuuksiin, mikä saattaa vaarantaa käyttäjien yksityisyyden. Nämä tuovat omia haavoittuvuuksia, kuten koodi- injektion. Tätä ovat tutkineet Armold, Hyla ja Rowe, jotka saivat Javan avulla selville ihmisten tietoja. He tekivät epävirallisen käyttöliittymän SQL-ympäristöön. Tässä toteutuu, sekä koodi, että SQL-injektio. Haastatteluissa kävi ilmi, että osa tunsi vain toisen injektioista, mutta harva tunsi molemmat haavoittuvuudet. Sähköposti- injektio on yksi yleisistä haavoittuvuuksista, jonka myös suurin osa haastateltavista tunnisti. Tämä voidaan selittää osittain sillä, että sitä käytetään päivittäin korkeakouluissa ja vapaa-ajalla. Tutkimuksesta voitiin havaita se, että kaikki esille otetut haavoittuvuudet, jotka liittyvät web- järjestelmiin, olivat tekemisissä koodi-injektion kanssa. Kaikki haastateltavat eivät tunnistaneet koodi- injektiota, mutta tunnistivat muita samankaltaisia haavoittuvuuksia, joka muistuttaa koodi-injektiota. Kuten tässä tutkimuksessa määriteltiin, web-järjestelmien uhat ovat tietoturva- aukkoja, joita hyökkääjät käytävät hyväkseen. Tässä määriteltiin uhiksi mm. Web-sivuhyökkäykset ja sisäinen uhka. Web-järjestelmiin ei kannata hyökätä, jos se ei sisällä haavoittuvuuksia. Kuten Garfinkel ja Spafford kertoivat, niin Java ei ole tarkoitettu turvalliseen ohjelmointiin, vaan se sisältää paljon haavoittuvuuksia.

Web-järjestelmiä rakennetaan organisaatioiden tietoliikenteen helpottamiseksi. Tietoliikenne kulkee Internet Protokollan välityksellä (IP). IP tuo omia haavoittuvuuksia ja uhka kuvia web-järjestelmien käyttäjien keskuudessa. Satelliitin välityksellä voidaan ottaa yhteys mm. lentokoneisiin ja laivoihin. Sosiaalinen media tuottaa omat ongelmat, viestit kulkevat normaalisti Internet Protokollan välityksellä. Tämän ansiosta voidaan kaapata ihmisten viestejä (esim. sähköposteja). Opiskelijoilta kysyttiin ”mitä uhka-kuvia sisältyy Internet protokollaan”? Suurin osa ei osannut hahmottaa Internet protokollaan, vaan jättivät kokonaan vastaamatta siihen. Kauemmin IT-alalla olleet osasivat vastata, että pakettien kaappaaminen ja salakuuntelu tekee Internet Protokollasta ongelmaisen. Eräs Tampereen ammattikorkeakoulun opiskelija vastasi, että IP-välityksellä voidaan jäljittää toisen käyttäjän tietokone (point-to-point). Haastateltavilta kysyttiin, että miten sosiaalisessa heidän mielestään pitäisi ottaa huomioon yksityisyys. Tämä kysymys oli jatkoa Internet Protokollaan, koska sosiaalisessa mediassa voidaan löytää toinen ihminen Internet Protokollan välityksellä. Vastauksissa kerrottiin, että liikaa ei kannata itsestään kertoa tietoa verkon välityksellä ja vastuuta siirrettiin sekä ylläpitäjälle, että palvelun käyttäjälle. Sosiaalisessa mediassa voidaan helposti vakoilla toisia ihmisiä ja itsestään ei kannata antaa liikaa tietoa (laki määrittelee mitä tietoa saadaan kysyä), kuten kyselyyn vastaajat kertoivatkin. Tutkimuksessa otettiin esille myös pilvipalvelu, jotta yritykset voisivat tuottaa ja ostaa palvelua verkossa (esim. sähköpostit ja tietokannat). Tämä saattaa tuoda lisää ongelmia palveluntarjoajille, koska tässä palvelussa on olemassa aina kolmas osapuoli ja tutkimuksissa havaittiin, että web-järjestelmissä on vielä paljon haavoittuvuuksia ja niihin liittyviä uhkia.

Haastateltavilta kysyttiin myös, miten tulisi reagoida, jos heidän koneeseensa tehtäisiin tietomurto. Tietoturvapalvelun verkkosivut kehottivat pitämään oman tietokoneen vi-

rustorjunnan ajan tasalla, jotta virustorjuntaohjelma tunnistaisi uusimmat uhat. Tutkielmasta voidaan päätellä se, että tärkein suojautumiskeino on asentaa koneelleen palomuuri, jonka avulla voidaan kontrolloida tietoliikennettä, oman tietokoneen ja verkon välillä. Haastatteluissa otettiin esille, että jos tietomurto on jo sattunut, niin paras keino on vaihtaa salasana omalle koneelle välittömästi.. Toisena keinona haastateltavat kehottaisivat ilmoittamaan viranomaisille, jos tietomurto on jo päässyt tapahtumaan.

Kuten tästä voidaan huomata, niin tietoturva/yksityisyys ja niiden haavoittuvuus on erittäin laaja ja monipuolinen käsite. Kaikki opiskelijat osasivat määritellä tietoturvan ja yksityisyyden erot. Heidän mielestään tietoturvalla on tarkoitus suojella omia tietoja ja yksityisyydellä varjellaan omia henkilökohtaisia tietoja. Järvinen jakoi tietoturvan kolmeen osa-alueeseen: Tiedon luottamuksellisuus, eheys ja saatavuus. Näillä kolmella osa-alueella määriteltiin tietojen turvallisen käsittely verkossa, jotta se pysyisi oikeiden henkilöiden ulottuvilla kokonaisina. Oinas-Kukkonen mainitsi yksityisyydestä, että sosiaalisessa mediassa nykypäivänä pitää kirjoittaa omia henkilökohtaisia tietoja rekisteröityessään palvelun käyttäjäksi. Tämä mahdollistaa omien henkilökohtaisten tietojen liikkumisen verkossa ja yksityisyys on silloin uhattuna, koska useat keskustelut ovat julkisia.

Tässä tutkielmassa käytiin tapahtuneita tietomurtoja viestintäviraston julkistamien raporttien muodossa. Raporteista kävi ilmi se, että hyökkäykset ovat kohdistuneet pääsääntöisesti yrityksiin, jonka johdosta hyökkääjät ovat saaneet tietoonsa myös palvelujen käyttäjien yksityisiä tietoja. Tietomurtoja tehtiin myös sosiaalisen median kautta, kuten esimerkiksi Yahoon. Tietomurron lisäksi kyseessä on yksityisyyden loukkaus, koska hyökkääjät ovat saaneet tietoonsa käyttäjien henkilökohtaisia tietoja. Kuten Järvinen kertoo kirjassaan, niin Suomen lain mukaan palveluntarjoajille ei tarvitse antaa itsestään kaikkia tietoja. Raporteista voidaan havaita myös, että useilla verkkopalveluilla on käyttäjiä ympäri maapalloa, joten tietomurrot kohdistuvat kerralla useaan maahan. Hyökkääjät havittelevat normaalisti taloudellista hyötyä, kuten esimerkiksi verkkopankkien tietojen urkintaa. Osa haastateltavista kertoi, että tietomurron kohteeksi joutuneena, kannattaa ottaa yhteys viranomaisiin. Toisena motiivina voidaan kertoa, että hyökkääjät haluavat toiselle tehdä haittaa tai kiusaa. Kuten Porvari kertoi omassa väitöskirjassaan, niin liiketoiminta on siirtynyt hyvin voimakkaasti verkkoon, joka lisää tietoturvariskien syntyä organisaatiota kohden. Hyvänä esimerkkinä voidaan mainita verkkopankkien toiminta, jossa liikkuu paljon pankkien asiakkaiden rahaa. Viestintäviraston raporteista kävi ilmi, että monet hyökkääjät pyrkivät saamaan tietoonsa ihmisten tunnuksia sähköpostin välityksellä.

Tutkimuksessa voitiin havaita, että opiskelijat molemmista oppilaitoksista olivat perillä haavoittuvuuksista, mutta eivät osanneet selittää eri haavoittuvuuksien osa-alueita, mitä tässä tutkimuksessa otettiin esille. Oulun yliopiston opiskelijat tiesivät enemmän haavoittuvuuksia, kuin Tampereen ammattikorkeakoulussa, mutta Tampereella oltiin paremmin tietoisia niihin kohdistuneista uhista. Viestintäviraston raporttien pohjalta voitiin päätellä, että uhat kohdistuvat eri palvelujen kautta suoraan yksityiskäyttäjiin, tästä johtuen viranomaiset ovat osa tietoturvaa, kuten haastatteluissakin tuli esille. Tietoturvien haavoittuvuuksien vaikutukset ja hyökkäyksien kohde ei opiskelijoille tule koulussa kovin laajasti selville, vaan tietoa hankitaan työelämän, kokemuksen ja harrastuksen kautta. Tutkimuksessa havaittiin, että kokeneemmilla opiskelijoilla oli parempi tietämys haavoittuvuuksissa, kuin vasta alalle tulleilla. Molempien koulujen opiskelijoiden vastaukset eivät suuresti poikenneet toisista, vaikka oppi-aineiden pääaine poikkesivatkin toisistaan.

7. Johtopäätökset

Seuraavassa käydään läpi vastauksia tutkimuskysymyksiin ja esitetään mahdollisia jatkotutkimuksen aiheita:

1. **Mitä web-järjestelmien uhat ja haavoittuvuudet merkitsevät?**

Uhilla tarkoitetaan sitä, miten hyökkääjät pyrkivät pääsemään käsiksi kohteen järjestelmiin. Yleisimpiä uhkia olivat APT-hyökkäykset, arvaamaton tuho, hyökkäykset, peitehyökkäykset asiakkaanohjelmistoihin, hyökkäykset web-sivustoihin, hyökkäykset älypuhelimiin ja taulutietokoneisiin, vaara digitaalisissa todistuksissa, sisäiset uhat, uudelleen käytetään samoja tilitietoja ja yksityisyyden invaasio. Uhat ovat niitä joita kohteen pitää olla erityisesti tietoisia, jotta niiltä voitaisiin suojautua. Muita uhkia ovat myös salakuuntelu ja henkilökohtaisten viestien kaappaukset, jotka liittyvät lähinnä Internet protokollaan. Haavoittuvuuksia ovat ne, mitä kanavaa pitkin hyökkääjä pyrkii pääsemään kohteen tietoihin käsiksi tai tuottamalla kohteelle vaikeuksia. Yleisimpiä haavoittuvuuksia olivat injektio, epävarma todennus ja järjestelmän hallinta, Cross-site Scripting, tietoturvan loukkauksille alttiit lähdekoodit, väärät tietoturva-asetukset, arkaluonteisten tietojen altistuminen, web-sovelluksen puutteellinen tietoturvataso, Cross-site request forgery, heikkojen tiedostojen hyödyntäminen sovelluksen hyökkäyksissä ja vahvistamaton tiedonsiirto. Muita haavoittuvuuksia ovat palvelimen ruuhkauttaminen ylimääräisillä tiedonsiirroilla. Hyökkääjän tarkoituksena on saada tietoonsa vastapuolen henkilökohtaisia tietoja (lähinnä taloustietoja) tai aiheuttamalla kiusaa vastapuolelle. Tutkimuksessa havaittiin, että uhat ovat lähinnä hyökkäyksen kohteelle olennaista tietoa, miten hyökkääjä kykenee suorittamaan hyökkäyksensä, kun taas haavoittuvuudet ovat enemmän hyökkääjälle olennaista tietoa, jotta hyökkääjä tietää, mitä reittiä pitkin kyetään suorittamaan isku. Uhat ja haavoittuvuudet tukevat toinen toistaan, kun tiedetään, miten hyökkääjää suorittaa hyökkäyksen ja mitä reittiä pitkin, hyökkäykseen voidaan paremmin varautua. Nykypäivänä tavallisista käyttäjistä on enemmän tullut hyökkääjä kuin kohde, joten molemmat asiat olisi käyttäjien hyvä hallita.

2. **Mikä on opiskelijoiden tietoisuus web-järjestelmien uhista ja haavoittuvuuksista, Tampereen ammattikorkeakoulussa ja Oulun yliopistossa?**

Opiskelijat osasivat paremmin määrittää uhat, koska tavallinen käyttäjä joutuu tekemisiin enemmän uhkien kanssa, mutta haavoittuvuudet tulivat sieltä myös hyvin esille, koska tietojenkäsittelyn opiskelijoista tulee tavallisista käyttäjistä ammattilaisia. Kysymykset viittasivat yleisesti eri injektioihin, koska injektio oli määritelty 2013 suurimmaksi haavoittuvuudeksi. Selkeästi suurin osa osasi selittää uhilla tarkat määritykset, kun taas haavoittuvuuksista oli enemmän epätietoisuutta. Kokemus nousi suureen osaan, ne jotka ovat olleet alalla pidempää, tiesivät hyvin haavoittuvuuksista (ammattilainen), kun taas ne jotka ovat vasta tulossa alalla (peruskäyttäjän ja ammattilaisen murrosvaiheessa olevat). Molempien korkeakoulujen opiskelijoiden osalta tietoliikenne Internet protokollan välityksellä tietämys oli puutteellista, joten suurin osa opiskelijoista ei osannut ottaa erityisesti kantaa sen uhkiin ja haavoittuvuuksiin.

3. Miten opiskelijoiden tietoisuus eroaa toisistaan?

Opiskelijoiden tietous ei eronnut suuresti toisistaan. Oulun yliopiston opiskelijoilla oli laajempaa tietoa teknisistä asioista, kun taas Tampereen ammattikorkeakoulun opiskelijoilla oli enemmän käytännönläheisempää tietoa. Tämä tuli esille myös uhkien ja haavoittuvuuksien määrittelyissä. Vaikka molempien koulujen osalta haavoittuvuuksien eri injektioiden määrittely tuottikin vaikeuksia, niin Oulun yliopiston opiskelijoilla oli niistä parempaa tietoa, kun taas Tampereen ammattikorkeakoulun opiskelijoilla uhat olivat paremmin tiedossa. Haavoittuvuudet viittaavat enemmän teknillisempään osaamiseen, kun uhat ovat enemmän käytännöllisempää osaamista vaativaa.

4. Miten opiskelijoiden tietoisuus eroaa kirjallisuudesta esitetyistä teorioista?

Opiskelijat olivat samalla linjalla kuin kirjallisuudessa esitetyissä teorioissa, Kirjallisuudessa haavoittuvuudet menevät useasti koodin puolelle, kun uhat olivat enemmän konkreettisempia käyttäjän kannalta. Yksityisyys määriteltiin henkilökohtaisten tietojen suojeluksi, samalla kannalla olivat myös opiskelijat. Tietoturvan opiskelijat olivat määritelleet omien tietojen suojeluksi, kun kirjallisuudessa se jaettiin kolmeen osaan: luottamuksellisuus eheys ja saatavuus. Edellä mainitut asiat tarkoittavat käytännössä samaa, eli omien tietojen turvaamista ja tiedot pysyvät niillä, joille ne kuuluvat. Internet protokollaa suurin osa ei osannut määrittää tietoturvan kannalta. Ne jotka osasivat määritellä Internet protokollan, kertoivat että sen välityksellä voidaan kaapata henkilökohtaisia viestejä ja salakuunnella kohteita. Internet protokollan avulla voidaan myös ruuhkauttaa palvelin turhilla tiedonsiirroilla. Tätä ei esiintynyt vastauksissa kertaakaan. Kirjallisuudessa mainittiin, että Internet protokollan avulla voidaan jäljittää toinen henkilö IP-osoitteen avulla, mutta sitä ei määritelty uhaksi.

5. Mahdollisia jatkotutkimusaiheita:

Tutkimuksen mukaan tiedon ruuhkauttaminen olivat ennen suurin haavoittuvuus, mutta kun tavallisista käyttäjistä tuli ammattilaisia injektio-haavoittuvuudet yleistyivät. Miten tällaisilta haavoittuvuuksilta voitaisiin tulevaisuudessa välttyä paremmin? Tutkimusten mukaan Internet tuottaa nykypäivänä paljon riippuvuutta ja se mahdollistaisi tulevaisuudessa monien arkipäiväisten asioiden hoitamisen. Mihin suuntaan web-järjestelmät ovat menossa? Onko havaittavissa jotain suurempaa uhkaa tämän johdosta, kuin pelkästään hyökkäykset toisten henkilökohtaisiin tietoihin? HTML5 kielet ovat viime vuosina yleistyneet voimakkaasti. Mitä mahdollisia uhkia/haavoittuvuuksia voidaan yhdistää HTML5-kieleen?

Tutkimuksessa onnistuttiin selvittämään Tampereen ammattikorkeakoulun ja Oulun yliopiston opiskelijoiden tietoisuus uhista ja haavoittuvuuksista. Tutkimuksessa onnistuttiin myös määrittelemään eroavaisuudet uhkien ja haavoittuvuuksien välille, kuitenkin nykyajan haavoittuvuuden jäivät vähemmälle, esimerkiksi mitä mahdollisia haavoittuvuuksia on HTML5:ssa. Tässä tutkimuksessa ei löydetty suuria eroavaisuuksia Tampereen ammattikorkeakoulun ja Oulun yliopiston vastauksissa. Oliko kysymykset heikosti määritelty vai liian vaikeita, koska osa vastauksista oli aika suppeita ja kaikkiin ei kyetty kunnolla vastaamaan tai ei vastattu ollenkaan.

Lähteet

Alalfi, M., Cordy, J. & Dean, T. (2012). Automated Verification of Role-based Access Control Security Models Recovered from Dynamic Web Applications. *2012 14th IEEE International Symposium on Web Systems Evolution (WSE), 14 (9),* 1-10.

Armold, A., Hyla, B. & Rowe, N. (2006). Automatically Building an Information-Security Vulnerability Database. *Information Assurance Workshop, 2006 IEEE, 23 (6),* 376-377.

Berger, B., Sohr, K. & Koschke, R. (2013). Extracting and Analyzing the Implemented Security Architecture of Business. *2013 European Conference on Applications Software Maintenance and Reengineering (CSMR), 17 (3),* 285-294.

Byrne, D. & Ragin, C. (2009). The SAGE handbook of Case-Based Methods. Lontoo: SAGE publications Ltd.

Caupet, J., Muñoz, J., Alins, J., Mata-Díaz, J., & Esparza, O. (2013). Deploying Internet Protocol Security in satellite networks using Transmission Control Protocol Performance Enhancing Proxies. *INTERNATIONAL JOURNAL OF SATELLITE COMMUNICATIONS AND NETWORKING, 31 (9)*, 51–76.

Chang, R. & Gray, .K. (2013). Ethics of research into learning and teaching with Web 2.0: reflections on eight case studies. *Springer Science+Business Media New York, 25 (9)*, 147-165.

Demchenko, Y., Gommans, L., Laat, C. & Oudenaarde, B. (2005). Web Services and Grid Security Vulnerabilities and Threats Analysis and Model. *GRID '05 Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing, 6 (2005),* 262-267.

Ek, J. & Hellstadius, S. (1998). HTML-opas. Vantaa: Schildts Kustannus Oy/Pagina.

Eun, H., Lee, H. & Oh, H. (2013). Conditional Privacy Preserving Security Protocol for NFC Applications. *Consumer Electronics, IEEE Transactions on,59 (1),* 153-160.

Gao, W., Morris, T, Reaves, B. & Richey, D. (2010). *On SCADA Control System Command and Response Injection and Intrusion Detection. eCrime Researchers Summit (eCrime)*, *20 (10),* 1-9.

Garfinkel, S. & Spafford, G. (1997). Web Security & Commerce. United States of America: O'Reilly.

Ghosh, P. (2013). BBC-news technology. Viitattu 30.5.2013 http://www.bbc.co.uk/news/technology-22249490

Hakala, M. & Vainio, M. (2002). Tietoverkon rakentaminen. Jyväskylä: Docendo Finland Oy.

Hakala, M., Vainio, M. & Vuorinen, O. (2006). Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

Helepuro, S., Perttula, J. & Ristola, J. (2004). Sähköisen viestinnän tietosuoja. Helsinki: Talentum Media Oy.

Hodován, R. & Kiss, A. (2012). Security Evolution of theWebkit Browser Engine. *2012 14th IEEE International Symposium on Web Systems Evolution (WSE),28 (9),* 17-19.

Hämäläinen, P. (2007). Uuden webin uudet uhat. Viitattu 4.12.2013 http://www.tietokone.fi/artikkelit/uuden_webin_uudet_uhat

Jamsa, K. (1997). JAVA ohjelmoinnin perusteet. Jyväskylä: Teknolit Oy.

IPA (Information-technology promotion agency) (2012). 10 Major security threats. IT security center, Japani.

Järvinen, P. (2002). Tietoturva ja yksityisyys. Jyväskylä: Docendo Finland Oy.

Kaario, K. (2002). TCP/IP-verkot. Jyväskylä: Docendo Finland Oy.

Kaufman, C., Perlman, R. & Speciner, M. (1995). Network security-private communication in a public world. New Jersey: Prentice Hall PTR.

Keum, C., Kang, S. & Kim, M. (2013). Architecture-based testing of service-oriented applications in distributed systems. *Information and Software Technology,55 (7),* 1212-1223.

Kommeri, T. (2011). Pilvilaskennan suorituskyky- erityistarkastelussa Drupal- sisällönhallintasovellus Amazonin, Rackspaces ja GoGridin pilvipalvelimilla (pro gradu). Jyväskylän yliopisto, Jyväskylä.

Korpela, J. (2011). HTML5 uudet ominaisuudet. Jyväskylä: WSOYpro Oy.

Korunka, C., Weiss, A. & Zauchner, S. (1997). An interview study of 'continuous' implementations of information technology. Publication models and dates explained*, 16 (11),* 3-16.

Koskinen, J., Kervinen, A., Lehtonen, M., Vatiainen, H. & Viitanen. (2004). Tietoliikenteen turvallisuus (seminaariraportti). Tampereen teknillinen yliopisto, Tampere.

Lehtinen, M. (2012). Haavoittuvuuksien torjunta defensiivisillä ohjelmointikeinoilla PHP- sovelluksissa (kandidaatintutkielma). Jyväskylän yliopisto, Jyväskylä.

Lin, L., Yu, E. & Mylopoulos, J. (2003). Security and Privacy Requirements Analysis within a Social Setting. *Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International, 12 (9),* 151-161.

Lin, X., Sun, X., Ho, P. & Shen, X. (2007). GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications. *IEEE Transactions on Vehicular Technology, 56 (6),* 3442-3456.

MacManus, R. & Porter, J. (2005). Web 2.0 for Designers. Viitattu 29.5.2013 http://www.digital-web.com/articles/web_2_for_designers/

Metsämuuronen, J. (2003). Tutkimuksen tekemisen perusteet ihmistieteissä. Helsinki: International Methelp Ky.

Mitchell, B. (s.d). Wireless/Networking. Viitattu 30.5.2013 http://compnetworking.about.com/cs/worldwideweb/g/bldef_www.htm

Mitchell, B. (s.d). Wireless/Networking. Viitattu 7.6.2013 http://compnetworking.about.com/cs/basicnetworking/f/bitsandbytes.htm

Naker, F. (2006). Safari-Books online. Viitattu 2.6.2013 http://my.safaribooksonline.com/book/networking/network-management/0131747991/foundation-of-networking-protocols/ch02lev1sec1

Nikander, P., Peltonen, T. & Viljainen, L. (1996) Internet tietoturva. Espoo: Suomen ATK-kustannus Oy.

Oinas-Kukkonen, H. & Oinas-Kukkonen, H. (2013). Humanizing the web- Change and social innovation. Yhdysvallat: Palgrave Macmillan.

Ollmann, G. (2007). Technical making sense of security: HTML code injection and cross-site scripting. Viitattu 30.6.2013 http://www.technicalinfo.net/papers/CSS.html

Oulun seudun ammattikorkeakoulu (s.d). Software Business Competence. Viitattu 1.12.2013 http://www.oamk.fi/sbc/testaus/web_sovelluksen_testaus.htm

Oulun yliopisto (2012). Tutustu alaan. Viitattu 24.9.2013 http://www.oulu.fi/tol/hae-opiskelijaksi/tutustu-alaan

OWASP (The open web application security project) (2013). The ten most critical web application security risks.

Paintsil, E. (2013). Evaluation of Privacy and Security Risks Analysis Construct for Identity Management Systems. *Systems Journal, IEEE, 7 (2),* 189-198.

PHPsecure. (2004). Email injection. Viitattu 29.6.2013 http://www.phpsecure.info/v2/article/MailHeadersInject.en.php

Porvari, P. (2012). Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa (väitöskirja). Aalto- yliopisto, Helsinki.

Pozzobon, O. (2013). The Future of GNSS Security Threat Development Parallels Information/Communication Technology (GPS world).

Pressman, R. (2005). Software engineering. Singapore: The McGraw-Hill companies.

Procesi, M., Cantucci, B., Buttinelli, M., Armezzani, G., Quattrocchi, F. & Boschi, E. (2013). Strategic use of the underground in an energy mix plan: Synergies among CO2, CH4 geological storage and geothermal energy. Latium Region case study (Central Italy).The Smithsonian/Nasa Astrophysical Data System*, 110 (4),* 104-131.

Rouse, M.(2005). HTML (Hypertext Markup Language). Viitattu 4.12.2013 http://searchsoa.techtarget.com/definition/HTML

Rouse, M. (2008). SearchNetworking. Viitattu 2.6.2013 http://searchnetworking.techtarget.com/definition/TCP-IP

Rubin, A., Geer, D. & Ranum, M. (1997). Web security sourcebook. Canada: Published simultaneously.

Runeson, P. & Höst, M. (2009). Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering, 14 (2)*, 131-164.

Ruohonen, A. (2013) Service-oriented architecture and Web service. Tampereen teknillisen yliopiston kurssimateriaali.

Röning, J.(2013). Oulun yliopiston tehokkaalla tietoturvan testausohjelmalla löytyi selaimista yli 100 haavoittuvuutta. Oulun yliopisto. Viitattu 17.9.2013 http://www.oulu.fi/yliopisto/uutiset/2013/08/oulun-yliopiston-tehokkaalla-tietoturvan-testausohjelmalla-l%C3%B6ytyi-selaimista-yli-100

Salo, I. (2010). Cloud computing- palvelut verkossa. Jyväskylä: WSOYpro Oy.

Suojelupoliisi (2012). Vuosikertomus 2012.

Stoneburner, G., Hayden, C. & Feringa, A. (2004). Engineering Principles for Information Technology Security (A Baseline for Achieving Security*), Revision A. National institute of Standard and Technology, 4 (12*.

Synergy, Yhdysvallat (s.d). Cloud services. Viitattu 24.6.2013 http://www.synergy.gs/Solutions/CloudServices/

Tampereen ammattikorkeakoulu (2013). Tietojenkäsittelyn koulutusohjelma. Viitattu 24.9.2013 http://www.tamk.fi/cms/tamk.nsf/$all/505A84D3D776119FC2257845005EDF32

Tarchiller, T. & Gerker, T. (2000). Web Application Development with PHP 4.0. Indianapolis, Indiana: New Riders.

Tian, W., Lihao, W. & Hong, Z. (2012). A Java Source-code SQL Injection Attack Detection Algorithm Based on Static Analysis. *National Conference on Information Technology and Computer Science,12 (2012),* 418-420.

Tietoturvapalvelu, Suomi (s.d). Kuinka voin suojata tietokoneeni? Viitattu 4.7.2013 http://www.tietoturvapalvelu.info/johdanto/miten_voin_suojata_tietokoneeni

Tikkunen, T. (2012). Tietoturvan dokumentointi ja fyysinen tietoturva (opinnäytetyö). Lahden ammattikorkeakoulu, Lahti.

Tolvanen, P. (2007). Web sisällönhallinta järjestelmä- ominaisuudet ja käyttöönotto (pro gradu). Jyväskylän yliopisto, Jyväskylä.

Tonna, A. & Edwards, R. (2012). Is there a place for qualitative research methods in pharmacy practice? *European Journal of Hospital Pharmacy: Science & Practice, 20 (11),* 97-99.

Toval, A., Nicolás, J., Moros B., & Garcia, F. (2002). Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach. *Requirement engineering, 6 (4),* 205-219.

Viestintävirasto (2012). Vuosikertomus 2012.

Whitman, M. & Mattord, H. (2008). Management of information security. Canada: Thompson Course Technology.

Wojjie (2004). Code injection vulnerabilities Explained. Viitattu 30.11.2013 http://www.theserverpages.com/articles/webmasters/php/security/Code_Injection_Vulnerabilities_Explained.html

Wongkit, M. & McKercher, B. (2013). Toward a typology of medical tourists: A case study of Thailand. *Tourism management, 38 (10),* 4-12.

Xiao, Z. & Xiao, Y. (2013). Security and Privacy in Cloud Computing. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 15 (2),* 843-859.

Liite A. Viestintäviraston raportit

2013

http://www.cert.fi/tietoturvanyt/2013/06/ttn201306061745.html

http://www.cert.fi/tietoturvanyt/2013/05/ttn201305301603.html

http://www.cert.fi/tietoturvanyt/2013/05/ttn201305090912.html

http://www.cert.fi/tietoturvanyt/2013/04/ttn201304231202.html

http://www.cert.fi/tietoturvanyt/2013/02/ttn201302151507.html

http://www.cert.fi/tietoturvanyt/2013/01/ttn201301101629.html

2012

http://www.cert.fi/tietoturvanyt/2012/12/ttn201212281525.html

http://www.cert.fi/tietoturvanyt/2012/11/ttn201211271133.html

http://www.cert.fi/tietoturvanyt/2012/07/ttn201207171110.html

2011

http://www.cert.fi/tietoturvanyt/2011/02/ttn201102231246.html

2010

http://www.cert.fi/tietoturvanyt/2010/01/ttn201001291059.html

Liite B. Haastattelulomake

Haastattelulomake

Vastaa kaikkiin kysymyksiin lyhyesti. Tämän haastattelu ei ole koe ja kysymyksiin ei ole yhtä oikeaa vastausta, vaan voi olla useita vaihtoehtoja. Kysymykset saattavat olla vaikeita IT- ammattilaisellekin.

yleistietoa

Sukupuoli

Mies Nainen

Ikä

___

Oppilaitos

Tampereen ammattikorkeakoulu Oulun yliopisto

Koulutuksesi pääpaino?

Onko kokemusta tietoturvasta muualta kuin koulusta?

Jos on, mitä?

Kysymykset

1. Mitä sana ’tietoturva’ merkitsee?

2. Mitä sana ’yksityisyys’ merkitsee?

3. Määrittele lyhyesti seuraavat tietoturvaa koskevat asiat

uhat

haavoittuvuus

4. Mitä mahdollisia uhkia sisältyy Internet-protokollaan (tietoturva/yksityisyys)?

Internet protokolla-malli on poistettu tekijänoikeuslain nojalla.

5. Miten mielestäsi sosiaalisessa mediassa pitäisi ottaa huomioon yksityisyys?

6. Mitä teet, jos koneellesi tehdään tietomurto?

7. Seuraavassa on lueteltu viisi yleistä tietoturvauhkaa vuonna 2012

Hakkerointihyökkäykset

osaan selittää ne | ymmärrän | tunnen periaatteet | olen kuullut | en tunne

Sisäinen uhka

osaan selittää ne | ymmärrän | tunnen periaatteet | olen kuullut | en tunne

Web-sivuhyökkäykset

osaan selittää ne | ymmärrän | tunnen periaatteet | olen kuullut | en tunne

Hyökkäykset älypuhelimiin ja taulutietokoneisiin (tablet)

osaan selittää ne | ymmärrän | tunnen periaatteet | olen kuullut | en tunne

Yksityisyyden invaasio

osaan selittää ne | ymmärrän | tunnen periaatteet | olen kuullut | en tunne

8. Seuraavassa on yleisiä tietoturvan haavoittuvuuksia

Structured Query Language (SQL)-injektio

osaan selittää ne | ymmärrän | tunnen periaatteet | olen kuullut | en tunne

Operating system (OS) komento-injektio

osaan selittää ne | ymmärrän | tunnen periaatteet | olen kuullut | en tunne

Cross site scripting (XSS)

osaan selittää ne | ymmärrän | tunnen periaatteet | olen kuullut | en tunne

Sähköposti-injektio

osaan selittää ne | ymmärrän | tunnen periaatteet | olen kuullut | en tunne

Koodi-injektio

osaan selittää ne | ymmärrän | tunnen periaatteet | olen kuullut | en tunne

9. Mitä haavoittuvuuksia mielestäsi voisi olla Internet-selaimissa?