TIETOTURVA

Case oldtimerTimer

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Visamäki, syksy 2015

Nico Heinimäki

HAMK
HÄMEEN AMMATTIKORKEAKOULU

VISAMÄKI
Tietojenkäsittelyn koulutusohjelma
eLearning ja multimedia

Tekijä Nico Heinimäki **Vuosi** 2015

Työn nimi Tietoturva: Case oldtimerTimer

TIIVISTELMÄ

Opinnäytetyön toimeksiantajana olivat Linnan Ateria Oy ja Hämeen ammattikorkeakoulu. Opinnäytetyön tavoitteena oli suorittaa kesän 2014 oldtimerTimer-projektijärjestelmän tietoturvakartoitus teemahaastattelun avulla. Tietoturvakartoituksessa hyödynnettiin teoriaa, ja teorian tutkimusmenetelmänä käytettiin kvalitatiivista tutkimusmenetelmää.

Työn teoriaosuudessa perehdyttiin tietoturvaan yleisesti, sen osa-alueisiin, tietoturvauhkiin ja tekniseen tietoturvaan sekä siihen, mikä on lainsäädännön vaikutus tietoturvaan. Teoriatietoa sisältävä aineisto oli kerätty aiheeseen liittyvistä kirjoista ja internetistä.

Tutkimuksen ohella otettiin selville, mitä laitteistoja ja ohjelmistoja projektissa oli käytetty. Tutkimus toteuttiin hyödyntämällä joitakin tietoturvan osa-alueita.

Työn tuloksena löydettiin lähes jokaisen projektin osa-alueista lukuisia tietoturvahaavoittuvaisuuksia, mutta nettiportaalin tietoturva oli toteutettu kaikista pisimmälle. Syksyn 2014 opintojakso ICT project, johon oldtimerTimer-järjestelmä kuuluu, tulisi tietoturvaa korostaa enemmän.

Avainsanat Tietoturva, tietoturvakartoitus, tietoturvaselvitys

Sivut 25 s. + liitteet 3 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

VISAMÄKI
Degree programme in Business Information Technology
eLearning and multimedia

Author Nico Heinimäki **Year** 2015

Subject of Bachelor's thesis Data Security: Case oldtimerTimer

ABSTRACT

The goal of this thesis was to complete the oldtimerTimer project system security mapping by interviews according to themes. This was completed in the summer 2014 and the participants were Linnan Ateria Oy and Hamk University of Applied Sciences. Security mapping was used in theory, and as research method the qualitative research method was used.

A part of the theory was to give a briefing about the basics of data security, their scope of fields, threats to data security, technical data security and the influence of the law to data security. A knowledge of theory that includes materials was collected from books and from the internet.

During the research commissioning hardware and software for the project and for their premises was decided. The research was executed to use some of fields of data security.

In the results of the work vulnerabilites were found in almost all parts of data security, but net portal's data security was completed further. In the autumn 2014, a study module that included oldtimerTimer system was emphasized.

Keywords Data security, security mapping, security clearance

Pages 25 p. + appendices 3 p.

SISÄLLYS

Liite 1 TIETOTURVAKYSYMYKSIEN RUNKO

PHP (Hypertext Preprocessor)
WWW-ympäristössä käytetty ohjelmointikieli, jolla saa aikaan muun muassa dynaamisia verkkosivuja.

XML (eXtensive Markup Language)
Kuvauskieli.

MySQL
Tietokantaohjelmisto, joka on suosittu Web-ympäristöissä.

Java
Laitteistoriippumaton ohjelmointikieli.

HTTP (Hypertext Transfer Protocol)
Selaimen ja verkkopalvelimen kesken välittävä verkkoprotokolla.

HTTPS (Hypertext Transfer Protocol Secure)
Sama kuin edellinen, mutta verkkoprotokolla on suojattu ulkopuolisilta.

TCP/IP (Transmission Control Protocol / Internet Protocol)
Yleinen verkkoprotokolla.

Sprint
Osa projektinhallintamenetelmää.

1 JOHDANTO

Tämän opinnäytetyön aiheena oli kartoittaa oldtimerTimer-projektin tietoturvaa ja tutkia tietoturvaa yleisesti. Tietoturva itsessään on kuitenkin laaja käsite, ja sen vuoksi rajauksesta on jätetty pois dokumentoinnin yksityiskohtaisemmat osiot sekä asiat, jotka kuuluvat kokonaan oldtimerTimer-projektin ulkopuolelle.

Taustalla oli Digital Service Development -opintojakso, jossa jokainen kurssin osallistuja sai valita oldtimerTimer-järjestelmästä oman tehtävän vastuualueeksi ja tehdä siitä myöhemmin opinnäytetyön. OldtimerTimerin ideana oli ilmoittaa asiakkaidensa puhelimen kautta, mitä on ruokana Linnan Ateriassa. Kurssin aikana jokainen tehtäväalueestaan vastannut keräsi siitä mahdollisimman kattavia tietoja kesän 2014 projektia varten. Opintojakson jälkeen osa osallistujista jatkoi kesällä projektin kehittämistä eteenpäin, ja osa heistä samaan aikaan opinnäytetyötä. Projektiin kuuluivat päivä- ja sprint-palaverit, joissa tiedusteltiin jokaiselta osallistujalta töiden etenemisestä. Projektinseurannassa käytettiin Scrum-projektinhallintamenetelmää.

Opinnäytetyön toimeksiantaja oli Linnan Ateria Oy, joka tuottaa asiakkailleen ateriapalveluita. Yhtiö perustettiin vuonna 2010 ja sen omistaa Hämeenlinnan kaupunki. Linnan Ateriasta esitettiin toive, että saataisiin toteutettua sovellusohjelma, jonka avulla ikäihmiset voisivat löytää lähimmät ruokailupaikat helpommin ja joka toisi tiedon ruokailupaikkojen ruokalistoista. Linnan Aterian toiveiden pohjalta alettiin kehittämään sovellusta, jonka omistaa Hämeen ammattikorkeakoulu.

Tietoturvaan liittyvät asiat olivat opinnäytetyön kirjoittajalle yksi tietotekniikan mielenkiintoisimmista aiheista sekä halu kartoittaa järjestelmän tietoturvaa. Tekijällä ei ollut aiempaa kokemusta tietoturvasta, mutta hän on käynyt aiheeseen liittyvän kurssin. Opinnäytetyön toteuttamisen myötä kirjoittaja saattaa tulevaisuudessa sijoittua tietoturva-asiantuntijaksi.

Opinnäytetyön tavoitteena oli kartoittaa kesän 2014 oldtimerTimer-projektin nykytilanne ja tutkia tietoturvaa yleisellä tasolla. Opinnäytetyötä kirjoittaessa aihe kallistui enemmän tietoturvan yleiselle tasolle, koska aihetta oli tarkoitus hyödyntää muissakin, korkeintaan kymmenhenkisissä projekteissa. Tämän vuoksi opinnäytetyön ei ollut tarkoitus täyttää ainoastaan oldtimerTimer-järjestelmän tarpeita. Lopulta rajaus tuli vastaan ja aihe keskittyi tarkemmin tietoturvauhkiin ja tekniseen tietoturvaan. Näistä luotiin teoriaosio, jonka pohjalta toteutettiin tietoturvakartoitus.

Opinnäytetyön tutkimuskysymykset:
- Mikä on tietoturva?
- Mitä laitteistoja ja ohjelmistoja käytetään OTT-projektissa?
- Mikä on OTT-järjestelmän tietoturvan nykytilanne projektin lopussa?
- Miten järjestelmän tietoturvaa voisi kehittää jatkossa?

Opinnäytetyön ensimmäisissä luvuissa kerrotaan teoriassa, mitä tietoturva on. Tämän jälkeen kerrotaan teoriassa tietoturvan määritykset, osa-alueet, tietoturvauhat ja tekninen tietoturva. Lopuksi esitetään oldtimerTimer-projektin tietoturvakartoitus, jossa kerrotaan muun muassa projektissa toteutettujen järjestelmien nykytilanne ja mitä osa-alueita voisi jatkossa kehittää tulevaisuudessa.

Opinnäytetyön luonne on empiirinen, ja tutkimusmenetelminä hyödynnettiin laadullista eli kvalitatiivista tutkimusta sekä teemahaastattelua. Tietoa tietoturvasta on kerätty opinnäytetyöhön käyttäen sekä internetiä ja kirjoja. Osaltaan näiden kerättyjen tiedon pohjalta suoritettiin tietoturvakartoitus oldtimerTimer-projektille teemahaastattelulla.

Koska tietoturva on hyvin laaja käsite, aiheen rajaaminen kesän 2014:n oldtimerTimer-projektiin oli hyvin haasteellista. Alkuperäisen suunnitelman mukaan aiheeseen tulisi mukaan myös paljon asiaa hallinnollisesta tietoturvasta ja tietoturvasuunnitelmasta. Lopulta Nämä aiheet kuitenkin rajattiin opinnäytetyön ulkopuolelle, koska niitä ei ole otettu kesän 2014:n projektiin lainkaan käyttöön.

2 TIETOTURVA

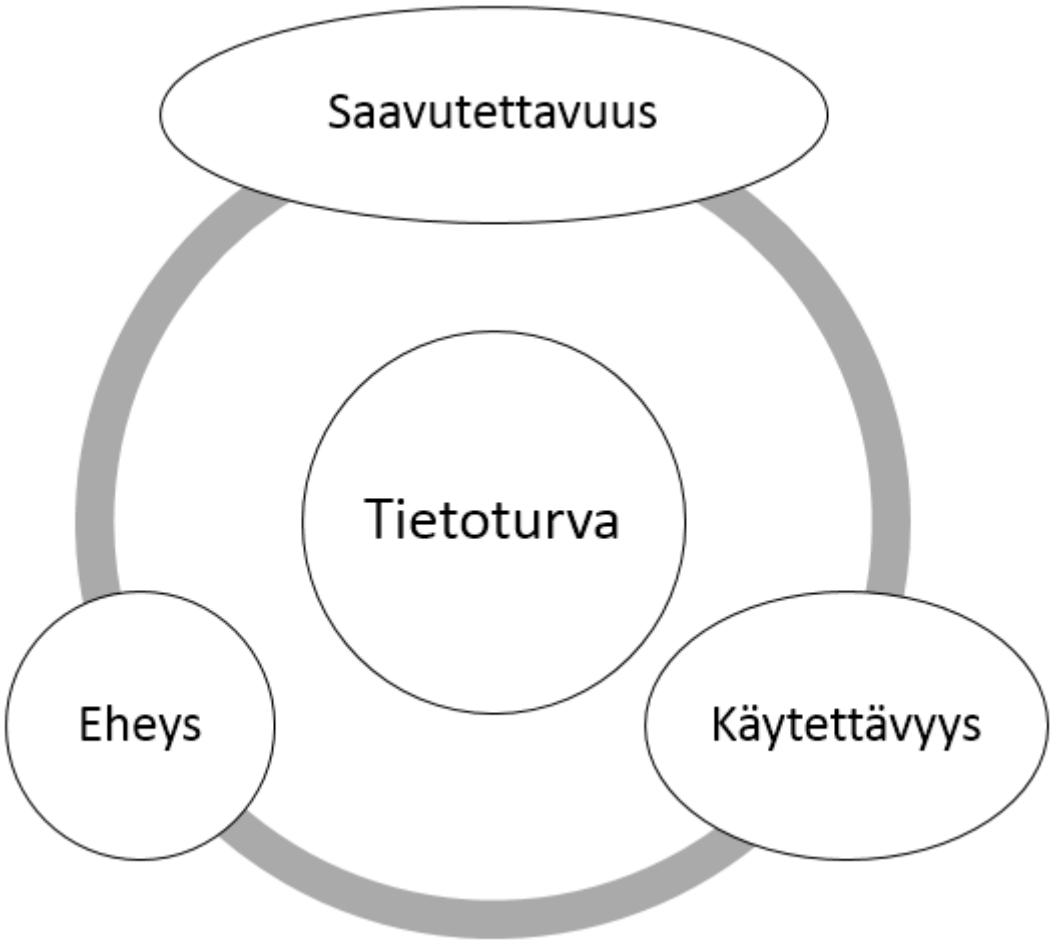
Tässä luvussa käsitellään tietoturvaa, sen käsitteitä, osa-alueita ja lainsäädännön vaikutus tietoturvaan. Koska tietoturva itsessään on hyvin laaja käsite, sille ei ole olemassa yksiselitteistä määritelmää (Kuivanen 2005). Tiivistettynä tietoturvalla tarkoitetaan suojaamaan tietoja, järjestelmiä ja tietoliikennettä ulkopuolisilta tahoilta erilaisissa olosuhteissa (VAHTI-tietoturva 2004). Ilman minkäänlaista tietoturvaa ulkopuolisilla on mahdollisuus tehdä mitä tahansa käsiin saaduilla tiedoilla, muun muassa muokata, lukea, tarkastaa, tallentaa tai hävittää. Tietoturva ei ole ainoastaan tietojen suojaamista, vaan siihen liittyvät sekä fyysinen turvallisuus ja tiedonkäsittelijöiden osaaminen. (Tirronen 2003)

Tietoturva on tärkeää erityisesti yrityksissä ja julkishallinnoissa. Näissä organisaatioissa käsitellään monia erilaisia tärkeitä tietoja, muun muassa henkilötietoja, finanssitietoja ja muita asiakirjoja. Koska osa näistä tiedoista ovat luottamuksellisia ja arkaluonteisia, niiden salassa pitäminen on välttämätöntä. Joissakin tilanteissa näihin tietoihin laaditaan käsittelevälle henkilölle salassapitosopimus, joka perustuu lakiin. Näin tiedot eivät päädy ulkopuoliselle. VAHTIn mukaan salassapidon säätämisestä mainitaan esimerkiksi henkilötieto- ja julkisuuslaissa. (VAHTI-tietoturva 2004)

Tietoturva ja tietosuoja ovat eri asioita. Tietosuojalla tarkoitetaan eri ihmisten henkilötietojen keräämistä ja käsittelyn rajoittamista siten, että henkilön tiedot eivät päädy vääriin käsiin. (Tirronen 2003)

2.1 Tietoturvan määritykset

Aikaisemmin katsottiin, että eheys, käytettävyys ja saavutettavuus (englanniksi confidentiality, integrity & availability) olivat riittäviä tavoitteita tietoturvan määrittämisessä. (Kuvio 1.) Nykyään kuitenkin katsotaan, että olennaisia tietoturvan määrityksiä ovat myös kiistämättömyys, pääsynvalvonta ja todentaminen (Kuvio 2.). Jotta nämä jälkimmäiset kohdat olisi mahdollista toteuttaa, kolme ensimmäistä määritystä eivät huomioi tiedon muokkaajan tai omistajan henkilöllisyyttä. (Kitunen 2014, 10.)



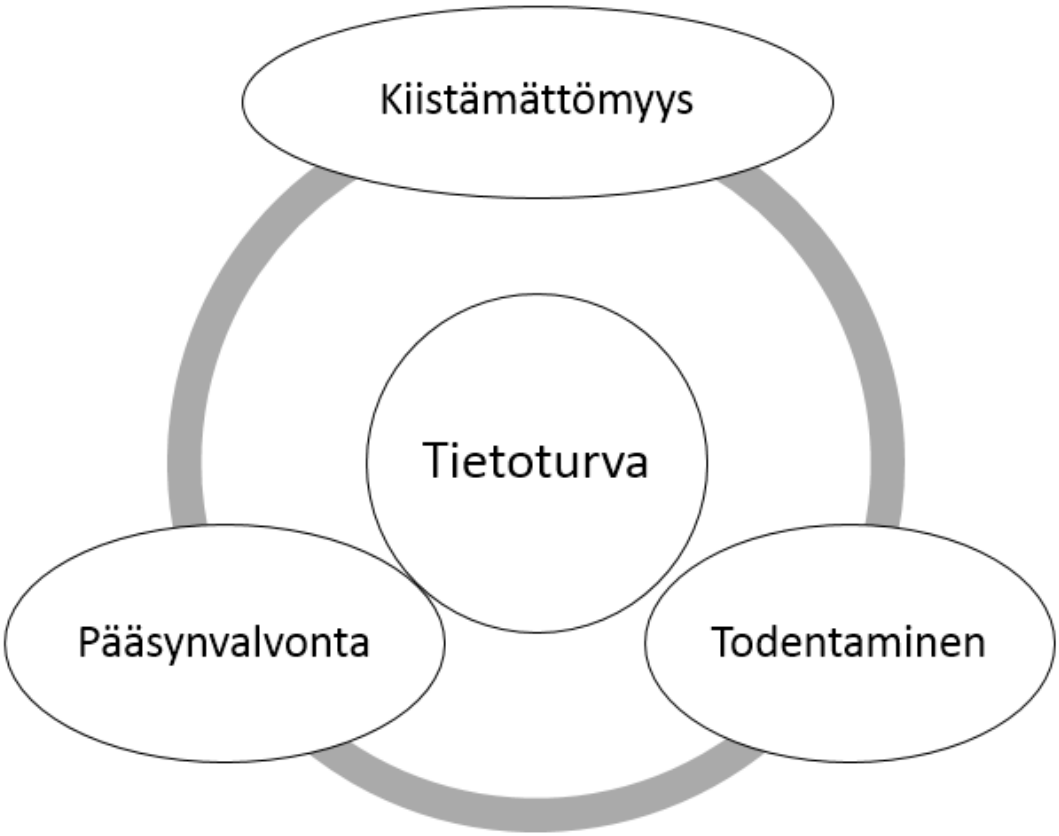
Kuvio 1. Havainnollinen kuva kertoo alkuperäisen tietoturvan määrittämisestä.

Saavutettavuudella tarkoitetaan, että tietojärjestelmissä olevat tiedot annetaan käytettäväksi vain niille taholle, jotka tarvitsevat työssään. Näin ollen mikä tahansa taho ei voi muuttaa, katsoa tai tuhoa tietoja ilman näihin valtuuksilla annettuja käyttöoikeuksia (VAHTI-tietoturva 2004.). Joillekin tahoille annetaan kuitenkin työhönsä sopivia oikeuksia tarvitseviinsa tietoihin, esimerkiksi käyttäjällä on oikeus muuttaa tietoja, mutta ei oikeutta tuhota niitä. Luottamuksellisuuden pääasiallinen idea on suojata yksityisyyttä ja varmistaa tietojen omistusoikeudet. Luottamuksellisuus menetetään, kun ulkopuolinen taho pääsee luvatta käsiksi tietoihin, joihin sillä ei ole käyttöoikeutta. (Kitunen 2014, 10.)

Eheydellä tarkoitetaan järjestelmissä olevia tietoja, jotka ovat luotettavia, oikeita ja ajantasaisia, mikäli tietojen muokkaamista valtuutetut tahot eivät ole muokanneet tietoja hallitsemattomasti tai eivät ole muuten muuttuneet laitteisto-, ohjelmistovian tai jonkun muun vastoinkäymisen seurauksena. (VAHTI-tietoturva 2004) Jos jokin taho pääsee tavalla tai toisella muokkaamaan tietoja lupaamatta, tiedon eheys menetetään (Kitunen 2014, 9.) .

Käytettävyys tarkoittaa, että luotu tieto tai järjestelmä on saatavilla ja käytettävissä etukäteen valtuutetuille tahoille. Tietojärjestelmästä

katsottuna käytettävyys vaikuttaa muun muassa laitteistojen lukumäärä, käyttäjien käyttö tietojärjestelmässä ja tiedostojensiirron kapasiteetti. Käyttäjä voi kiertää vaikeasti käytettävissä olevan tiedon ja se on riskialtillista tietoturvalle. Ylläpidolle haastavampi saavutettava tavoite on tasapainottaa käytettävyys sopivaksi turvallisuuden ja käytettävyyden välille. (Kitunen 2014, 9.)



Kuvio 2. Havainnollinen kuva muista olennaisista tietoturvan määrityksistä.

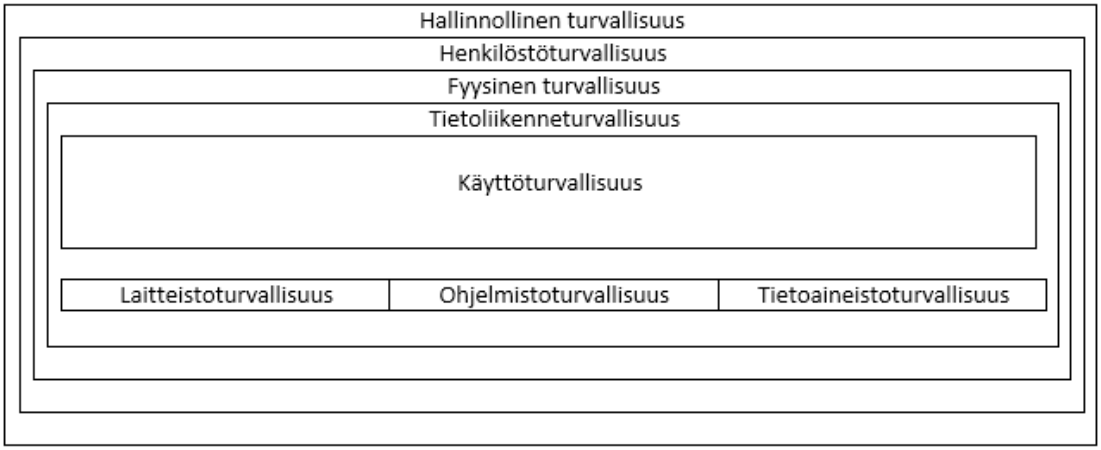
Todentaminen eli autetikointi tarkoittaa, että etukäteen valitulla henkilöllä tai järjestelmällä on oikeus päästä käyttämään järjestelmää. Autetikointi suoritetaan henkilön tai järjestelmän varmalla tunnustautumisella esimerkiksi sormenjälkitunnistimella. (VAHTI-tietoturva 2004.)

Kiistämättömyys pohjautuu käsitteeseen, että dokumentit suojataan ja todennetaan varmenteilla ja aikaleimoilla, jolloin henkilö ei voi väittää muokanneensa tietoja, jos hän ei ole näin tehnyt. (VAHTI-tietoturva 2004.)

Pääsynvalvonta tarkoittaa yleistä pääsyä tietoihin, jonka todennetaan tunnuksilla, salasanalla ja oikeuksien määrityksellä. Pääsynvalvontaan kuuluu myös seurantajärjestelmä, joka tallentaa lokitiedostoja käyttäjien muokkaamista tiedostoista. (Verkkopedakologi s.a.)

2.2 Tietoturvan osa-alueet

Tiivistettynä tietoturva jaetaan perinteiseen tapaan kahdeksaan eri osa-alueeseen. Allaoleva kuva (Kuvio 3.) kertoo, miten tietoturvan osa-alueet vaikuttavat toisiinsa.



Kuvio 3. Havainnollinen kuvaus tietoturvan osa-alueista. (Kitunen 2014)

Hallinnollisella turvallisuudella on tarkoitus varmistaa tietoturvan hallinta ja johtaminen. Näihin kuuluvat myös yhteyden ottaminen turvallisuudesta vastaaviin henkilöihin. Näiden henkilöiden tärkeä tehtävä on arvioida lakien mukaisia sopimuksia, jotka liittyvät tietoturvakäytäntöihin. Mikäli hallinnolla ei ole minkäänlaista kiinnostusta panostaa tietoturvaan, todennäköisesti hallinto ei ylläpidä tietoturvan tasoa ja henkilöstön tietoturvaosaamista. Suuremmissa organisaatoissa hallinnollisen turvallisuuden ylläpito kuuluu yleensä tietohallintoa edustava osasto ja pienemmissä organisaatioissa tietoturvasta vastaava henkilö. Hallinnollinen turvallisuus vaikuttaa kaikkiin muihin tietoturvan osa-alueisiin. (Hakala, Vainio & Vuorinen 2006, 10.)

Henkilöstöturvallisuuteen kuuluvat sellaiset toimenpiteet, jossa rajataan joidenkin käyttäjien mahdollisuus käsitellä organisaatioon kuuluvia tietoja ja järjestelmiä. Suuremmissa organisaatioissa henkilöstöturvallisuudesta vastaa henkilöstöosasto, joka on yhdessä tietohallinnon ja muiden tietoturvavastaavien kanssa. Henkilöstöturvallisuus vaikuttaa kaikkiin muihin tietoturvan osa-alueisiin, lukuun ottamatta hallinnollista turvallisuutta. (Hakala, Vainio & Vuorinen 2006, 11.)

Fyysiseen turvallisuuteen kuuluvat kiinteistöjen tilojen ja niihin kuuluvien laitteiden suojaaminen fyysisiltä uhkilta, kuten murroilta, ilkivalloilta, luonnonkatastrofeilta, tulipaloilta, vesivahingoilta ja muilta järjestelmien toimintahäiriöiltä. Fyysisestä turvallisuudesta vastaavat kiinteistöalaan eritoistuneet ammattilaiset. Tietohallinnon ammattilaisten on myös hyvä osallistua fyysiseen turvallisuuteen liittyvään suunnitteluun ja ylläpitoon. Muun muassa palvelimentilojen fyysinen suojaaminen on oltava korkeatasoinen. Fyysinen turvallisuus vaikuttaa kaikkiin muihin tietoturvan

osa-alueisiin, lukuun ottamatta hallinnollista turvallisuutta ja henkilöstöturvallisuutta. (Hakala, Vainio & Vuorinen 2006, 11.)

Tietoliikenneturvallisuudella varmistetaan sisäisten ja ulkoisten verkkojen tiedonsiirtoratkaisuja ja muiden viestintäjärjestelmien turvallisuudesta. Tietohallinto on vastuussa tietoliikenneturvallisuudesta. Hakalan, Vainion ja Vuorisen mukaan edellämainittu tietoturvan osa-alue on keinotekoinen, koska tietoliikenneturvallisuus vaikuttaa jokaiseen muuhunkin tietoturvan osa-alueeseen ja niissä on runsaasti yhtenäisiä tekijöitä. Käytännöstä katsottuna tietoliikenneturvallisuus vaikuttaa yleensä käyttöturvallisuuteen ja sitä kautta vaikuttaa laitteistoturvallisuuteen, ohjelmistoturvallisuuteen ja tietoaineistoturvallisuuteen. (Hakala, Vainio & Vuorinen 2006, 12.)

Käyttöturvallisuuteen liittyvät tietojärjestelmien käytöstä aiheutuvat riskit ja niihin varautuminen. Käyttöturvallisuus sisällyttää käytännössä laitteistoturvallisuuden, ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden. (Hakala, Vainio & Vuorinen 2006, 12.)

Laitteistoturvallisuudessa huolehditaan tietokoneiden ja muiden tietojärjestelmien kytkettyjen laitteiden mitoitus, testaaminen, huoltojen järjestäminen ja laitteiston kuluminen sekä vanheminen. Laitteistoturvallisuuteen kuuluvat myös käytöstä aiheutuvat vaarat, kuten sähköiskun ja muiden luokkaantumisvaarojen arviointi ja minimointi. Yleensä laitteistoturvallisuudesta vastaa tietohallinto. (Hakala, Vainio & Vuorinen 2006, 12.)

Ohjelmistoturvallisuuteen kuuluvat esimerkiksi ohjelmistojen testaus ja toimivuus, joilla varmistetaan muun muassa ohjelmiston sopivuus käyttötarkoitukseen, ohjelmistojen yhteensopivuus laitteistoon sekä toiseen ohjelmistoon, ohjelmiston toiminnollisuus sekä virheettömyys. Ohjelmistoturvallisuuteen liittyvät myös ohjelmistoversioiden ja lisenssien hallinta. Tietohallinta vastaa ohjelmistoturvallisuudesta. (Hakala, Vainio & Vuorinen 2006, 12.)

Tietoaineistoturvallisuuteen kuuluvat ne toimenpiteet, joihin liittyvät tietoaineistojen säilyttäminen, turvaaminen, varmistaminen, palauttaminen ja tuhoaminen. Tietoaineistoturvallisuudesta vastaavat tietohallinto ja organisaation arkistoinnin vastaava osasto. (Hakala, Vainio & Vuorinen 2006, 11.)

2.3 Lainsäädännön vaikutus tietoturvaan

Tietoturvan toteuttamisessa on huomioitava tietoturvaan kuuluvia lainsäädäntöjä. Suomen laissa ei kuitenkaan ole suoranaisesti olemassa olevaa tietoturvaa koskevaa lakia, vaan nämä säädökset ovat osa muuta olemassa olevia lakipykäliä. Ne ovat muun muassa henkilötietolaki. Haastetta tuovat myös Euroopan unionin asettamat direktiivit, jotka on toteutettu joko väliaikaisesti tai välittömästi, jotka on liitetty osaksi Suomen lainsäädäntöä. (Pappinen 2013)

Henkilötietolaki on vuonna 1999 voimaan tullut henkilötietoja käsittelevä peruslaki. Lain tarkoituksena on taata henkilöiden yksityiselämän suojaa ja muita henkilötietoja käsiteltäessä yksityisyyden suojaa takaavia perusoikeuksia (Finlex 1999). Tietoyhteiskuntakaari on vuonna 2015 osittain voimaan tullut lakikokoelma, joka on korvannut muun muassa sähköisen viestinnän tietosuojalain. Uuden lain on tarkoitus parantaa viestintäpalveluiden käyttäjien oikeuksia sekä varmistaa viestintäpalveluiden korkea laatu ja tietoturva. (Finlex 2014)

Suomen ja kansainvälinen laki asettaa yhteisöille sekä suoria ja epäsuoria velvoitteita tietoturvan huolehtimiseksi. Yleensä nämä velvoitteet ovat yleisluonteisia, käytännön toteutus ja määrittely yleisen tietoturvan taso. Tietoturvan suunnittelu, ylläpito ja kehittäminen ovat keskeisiä säädöksiä tietoturvan kartoittamisessa. Lainsäädännön lisäksi on hyvä tunnistaa sopimuksiin kuuluvat velvoitteet tietoturvasta. (Laaksonen, Nevasalo & Tomula 2006, 18.)

Viime vuosikymmenen aikana on tullut merkittäviä määrä tietoturvaan liittyviä säädöksiä, joilla on osaltaan pyritty määrittelemään tietoturvaan liittyviä toimenpideitä erilaisissa tilanteissa. Teknisen tietoturvan kannalta on haastavaa huomioida lainsäädäntöä, koska tekniikka ja sovellukset kehittyvät nopeasti. Laaksosen, Nevasalon ja Tomulan mukaan ne tuovat uusia tilanteita ja mahdollisuuksia, joihin ei lain kannalta ole varauduttu. (Laaksonen, Nevasalo & Tomula 2006, 18.)

3 TIETOTURVAUHAT

Tietoturvauhka on tietoturvaan kohdistuva uhka, joka aiheuttaa vaaraa jonkin tai useamman tietoturvan osa-alueen. (Koppa 2011) Tässä luvussa luetellaan yleisempiä käsiteltäviä tietoturvauhkia ja kerrotaan niiltä suojautumisesta.

3.1 Tulipalo tai vesivahinko

Kun suunnitellaan tietokonetiloja, on kiinnitettävä huomiota erityisesti tilojen paloturvallisuuteen. Paloturvallisuutta lisätään ilmastoinnilla, joka on varustettu lämpötarkkailujärjestelmällä. Ilmastointia tulisi olla asentamatta suoraan koneiden tai paloherkkien laitteiden yläpuolelle ilmastoinnista mahdollisien aiheutuvien vuotojen takia. Tietokonetilan suojaaminen tulipalolta automaattisilla sammutuslaitteella voi olla vaarallista. Mikäli sammutuslaitteessa on vettä, on kiinnitettävä huomioon sähkölaitteiden vedensietokyky. Muuttaessa uuteen tietokonetilaan on huomioitava viemäreiden sijainti. Tietokonetilaksi vältetään ne tilat, joissa viemärit ovat tilojen yläpuolella.

3.2 Sähköhäiriöt

Sähköhäiriöstä, salamaniskusta tai muusta sähkökatkoksesta johtuvat virtajohdot ovat odottamattomia ja aiheuttavat todennäköisiä riskejä. Liiallinen sähkönsaanti voi tuhota sähkölaitteita käsitteleviä tietoja. Myös odottamaton sähkökatkos voi hävittää sähkövirtaa tarvitsevan laitteen tietoja. Yksi tapa sähköhäiriöiden estämiseksi on käyttää ylijännitesuojia sisältäviä pistorasioita tai vikavirtasuojakytkintä.

3.1 Luonnonkatastrofit ja muut ympäristöuhat

Luonnonkatastrofeihin lukeutuvat muun muassa pyörremyrskyt, tulvat ja maanjäristykset. Muilla ympäristöuhkilla tarkoitetaan muun muassa ihmisien aiheuttamia uhkia, kuten sodat ja ydinonnettomuus. Nämä uhat ilmenevät olosuhteista ja sijainnista riippuen. Yllämainittuja uhkia voidaan ennaltaehkäistä varmuuskopioimalla tiedostoja pilvipalveluihin.

3.2 Haittaohjelmat

Haittaohjelma voi olla jonkin ohjelman osa tai skriptillä toteutettu komento, joka lähetetään Internetistä suoraan tai sähköpostin kautta tietokoneille. Haittaohjelmat tietokoneessa aiheuttavat tahallisesti erilaisia tapahtumia, kuten tiedon hävittämistä, kaappausta tai muuta väärinkäyttöä. Haittaohjelmilta suojaudutaan asentamalla koneisiin tietoturvaohjelmia. Seuraavassa kappaleessa kerrotaan yleisimpiä ilmestyviä haittaohjelmia.

Virus on tietokoneelle vahinkoa aiheuttava ohjelma. Virukset pääsevät käsiksi tietokoneisiin sähköpostin liitteenä, Internetistä ladatun tiedoston tai käyttäjän vierailevan verkkosivun kautta. (Tietoturvapalvelu .s.a)

Troijan hevonen on haittaohjelma, joka on naamioitunut tavalliseksi ohjelmaksi, joka vahingoittaa tietokonetta. Tietoturvapalvelun mukaan yksi tavanomainen esimerkki troijalaisesta on tietomurrettu tietokonepeliohjelma, joka mahdollistaa alkuperäisen pelin toimivuuden ilman CD/DVD-levyä, mutta samalla pelin aikana troijalainen poistaa tiedostoja tietokoneesta. (Tietoturvapalvelu .s.a)

Madot ovat nopeasti leviäviä ohjelmia. Madot yrittävät tunkeutua niihin Internetiin kytkettyihin tietokoneisiin, joissa jäivät asentamatta tietoturvapäivitykset. Madot leviävät myös sähköpostin osoitekirjoihin, joiden kautta lähettävät osoitteisiin ja liittävät mukaan tiedostoja. Madot voivat myös tunkeutua aktivoituihin bluetooth-laitteisiin noin 15 metrin päästä. (Tietoturvapalvelu .s.a)

Vakoiluohjelma jäljittää ja kerää käyttäjän tiedostoja sekä lähettää niitä käyttäjän tietämättä kolmannelle osapuolelle. Vakoiluohjelma voi olla asennettu tietokoneeseen tai osana tavallista ohjelmistoa käyttäjän tietämättä. Esimerkiksi julkisilla paikoilla olevissa yhteiskäyttöisissä tietokoneissa saattaa olla asennettuna vakoiluohjelmia. Näihin koneisiin ei suositella käyttävän henkilötietoja ja salasanoja. (Tietoturvapalvelu .s.a)

Mainosohjelma on verkkoselaimessa oleva ohjelma, joka näyttää mainoksia. Osa mainosohjelmista voi kerätä käyttäjän tietoja tietokoneen käytöstä. Näiden perusteella mainosohjelma lataa ja näyttää automaattisesti tietokoneelle mainosmateriaalia. (Tietoturvapalvelu .s.a)

Roskaposti on ei-toivottu sähköpostiviesti, jota lähetetään käyttäjän sähköpostilaatikkoon suurina määrinä. Roskapostille voi altistua esimerkiksi osallistumalla kilpailuun netissä, jossa pyydetään sähköpostiosoitetta ja kilpailu olikin huijaussivusto. Roskapostin tunnistaa tyypillisesti siitä, että lähettäjän nimi pelkkänä etunimenä ja viestin sisältö näyttää epäilyttävältä tai kuulostaa liian hyvältä. (Tietoturvapalvelu .s.a)

Verkkohuijaus on menetelmä, jolla varastetaan käyttäjän henkilökohtaisia tietoja. Verkkohuijauksia esiintyy muun muassa sähköpostiviesteissä, joiden sisältö väittää tulevan laillisesta organisaatiosta, mutta linkit menevät aitoihin, mutta valheellisiin verkkosivustoihin. Huijaussivustojen tarkoituksena on harhauttaa käyttäjiä syöttämään niihin muun muassa pankkitunnukset, salasanat ja muita henkilötietoja. Todellisuudessa pankit ja viranomaiset eivät pyydä sähköpostitse salasanoja tai pankkitunnuksen numeroita. (Tietoturvapalvelu .s.a)

3.3 Henkilöstö

Tietoturvariskeistä suurimpana pidetään henkilöstöä, joka voi tehdä hallitsemalleen järjestelmälleen virheitä joko tahattomasti tai tahallisesti. Useimmiten henkilö ei tiedä tai suhtautuu välinpitämättömästi tietoturva-

asioihin. Henkilöstön muu uhka on epäluotettavuus, johon kuuluvat esimerkiksi työaikojen laiminlyöminen, salassapitovelvollisuuden rikkominen, työntekijän asiaton pääsy suojattuun materiaaliin tai tilaan. Riskejä voi ennaltaehkäistä laatimalla salassapitosopimuksen, annetaan vain työtehtäviin kuuluvat käyttöoikeudet ja työajan seuraaminen. (SecMeter 2008)

3.4 Ilkivalta ja varkaus

Murtautuminen tietojärjestelmään ja sen käyttäminen luvatta, tarkoituksena on joko varastaa tai hävittää tiedostoja. Tiloissa ilkivaltaa ja varkautta voidaan estää asentamalla valvontakamerat, murtohälytykset ja asettamalla ei-käytössä olevat laitteistot lukittuun tilaan. Myös vakuutukset olisi hyvä ottaa ja pitää niitä kunnossa.

3.5 Internet-yhteyden katkeaminen

Internetiä vaativat aktiivilaitteet pitää tarkistaa, että Internet-yhteys on kunnossa. Mikäli laajakaistassa Internet-yhteys ei ole syystä tai toisesta toiminnassa, on syytä tarkistaa reitittimessä olevia valoja, ovatko ne päällä Internetin ja ADSL:n puolella. Kun molemmissa ei pala valo, ensimmäisenä on ilmoitettava viasta Internet-yhteyden tilaamisesta saadulta operaattorille.

4 TEKNINEN TIETOTURVA

Teknisessä tietoturvassa varmistetaan, että käytettävissä olevissa järjestelmissä ei ilmene tietoturvahaavoittuvaisuuksia. Näiden tietoturvaa on hyvä pohtia aikaisintaan järjestelmien hankintavaihteessa. Tässä luvussa kerrotaan tekniseen tietoturvaan liittyvät järjestelmät kuten sähköposti, palomuuri, mobiili ja tietokanta.

4.1 Tietoturvaohjelma

Tietoturvaohjelma on sovellus, joka estää haittaohjelmien pääsyn laitteeseen. Tietoturvaohjelmia ovat muuan muassa palomuurit, virustentorjuntaohjelmat ja anti-spyware-ohjelmat, jotka ovat yleisimpiä tietoturvaohjelmia kotikäytössä.

Palomuuri suojaa tietokoneen liikennettä ulkopuolisilta hyökkäyksiltä. Virustentorjuntaohjelma torjuu nimensä mukaisesti viruksia ja muita haittaohjelmia. Virustentorjuntaohjelmia on saatavilla maksullisina ja ilmaisina. Roskanpoistaja hävittää tietokoneissa tarpeettomia loki- ja väliaikaistiedostoja. Ohjelmaa käytäessä on kuitenkin pidettävä huolta, ettei ohjelma poista myös tarpeellisia tiedostoja. Salasanojen hallintaohjelman tarkoituksena on ylläpitää ohjelmistoihin ja verkkosivuille asetettuja salasanoja. Anti-spyware-ohjelma jäljittää sekä hävittää tietokoneelta vakoilu- ja muita haittaohjelmia.

4.2 Tietoliikenne

Tietoliikenne tarkoittaa sähköisen tiedon siirtämistä lähettäjältä vastaanottajalle. Tieto voi siirtyä joko langallisen tai langattoman verkon kautta. Alun perin TCP/IP-protokollia suunniteltaessa tietoturva jätettiin kokonaan huomiotta. Toisin kuin IPv4:ssa, IPv6:ssa pyrittiin ottamaan tietoturva paremmin huomioon.

TCP/IP:n heikkouksia ovat kuitenkin verkon salakuuntelu, yhteyksien kaappaus ja väärillä tunnustiedoilla esiintyminen. Verkon salakuuntelu on TPC/IP-verkossa helppoa, jos kaappaava laite pääsee fyysisesti lähelle verkkoelementtejä. Sitä on mahdollista suorittaa myös etäältä, mutta silloin se on työläämpää, riippuen siitä, mikä kytkin tai reititin on käytössä. Ne on toteutettu eri tekniikoilla. Useat verkon perusprotokollat ovat täysin salaamattomia, esimerkkeinä ftp (tiedostojen siirtäminen kahden tietokoneen välille), http ja smtp (viestien välittämisen sähköpostipalvelimien kesken). Näiden suojatut verkot ovat ftps ja https.

4.3 Palomuurit

Palomuuri tarkoittaa laitetta tai ohjelmistoa, jonka tarkoituksena on suodattaa tietoliikennettä ulkopuolisilta hyökkäyksiltä. Aikoinaan

palomuuri oli tehokas suojaamaan organisaation ulkopuolelta tulleita ennalta-arvaamattomia hyökkäyksiä vastaan. Samoin oli mahdollista rajoittaa organisaatiosta ulospäin menevää verkkoliikennettä ja estää tiettyjen Internet-palvelujen käyttö. IP-osoitteiden ja porttinumeroiden rajoituksien asettaminen oli helppoa. (Järvinen 2006, 105.)

Nykyään kannettavien tietokoneiden ja WLAN-yhteyksien yleistyessä palomuurin merkitys on tietoturvan kannalta vähentynyt. Uusien laitteiden myötä tietoliikenne liikkuu uusien porttien kautta. Organisaation henkilökunta ja erityisesti vieraat tuovat sisään kytkettäviä kannettavia tietokoneita. Tällöin koneissa olevat haittaohjelmat voivat levitä organisaation sisäiseen verkkoon. WLAN on tietoliikenteen kannalta haavoittuvainen, koska se päästää liikennettä sisään ja ulos ohittaen näin palomuurin. (Järvinen 2006, 105.)

Porteista pahin kohta on porttinumero 80, joka on aina auki Internetiä käyttäessä. Tämän vuoksi monet muutkin käyttävät, ja vakoiluohjelmat käyttävät yllämainittua porttia hyödyksi. Jotta palomuuri voisi tunnistaa sen, on tutkittava jokainen tietoliikenteessä oleva IP-osoite ja analysoida näyttääkseen aidon http-protokollan mukaiselta. (Järvinen 2006, 105.)

4.4 Palvelin

Palvelin on tietokone, johon on asennettu yleensä useita erilaisia palvelinohjelmistoja. Palvelin voi olla muun muassa sähköposti-, peli- tai www-palvelin. Hyvän palvelimen ympäristö on suljettu ja lukittu tila, jotta henkilökunnan ulkopuolisilta tahoilta on sinne pääsy kielletty. Tilassa on oltava toimiva ilmastointi ja se on sijoitettava muualle kuin suoraan palvelimen yläpuolelle, koska ilmastointiin voi tulla vuotoja, jonka vuoksi se saattaa aiheuttaa palvelimelle kosteusvaurioita.

Suuremmissa organisaatioissa palvelimet on hajautettu eri tiloihin ja palvelimien käyttöä hyödynnetään fyysisien palvelimen lisäksi myös virtuaalipalvelimia. Virtuaalipalvelimet antavat mahdollisuuden testata uusia sovellusohjelmia, käyttöjärjestelmiä ja kehittää niitä ilman, että palvelin menee fyysisesti rikki. Koulutuskäytössäkin hyödynnetään virtuaalipalvelimia, joissa opetetaan muun muassa verkkoasetuksien konfigurountia. Virtuaalipalvelimen hyvänä puolena ovat kustannustehokkuus, kloonaus ja se, että se ei aiheuta fyysisesti vahinkoja. Vaikka virtuaalipalvelimet tuovat paljon hyviä puolia, ne ovat fyysisiä palvelimia hitaampia silloin, kun virtuaalipalvelinta käyttää useampi käyttäjä samaan aikaan. Mitä alhaisempi laitteisto virtuaalipalvelimelle annetaan käyttöön, sitä hitaammaksi se tulee. (Pulli 2012)

4.5 Mobiili

Mobiili on laite, joka on älypuhelin, tabletti, älykello tai PDA-laite eli kämmentietokone. Laitteet ovat yleensä mukana kulkevia ja niillä on yleensä mahdollisuus päästä Internetiin. Nykyisillä mobiililaitteilla on lukuisia eri tietokoneiden ominaisuuksia, jotka ovat muun muassa Internet-

selain, toimisto-ohjelmat sekä video- ja kuvanmuokkausohjelmia. Ennen vuosituhannen vaihtumista mobiililaitteet eivät olleet yhtä merkittävässä käytössä kuin nykyään. Ensimmäinen mobiililaite oli matkapuhelin, jolla voi soittaa ja lähettää tekstiviestejä. (Järvinen 2012, 30.)

Erityisesti Android-järjestelmiin on suotavaa asentaa viruksentorjunta ja palomuuri, koska kyseinen käyttöjärjestelmä on avoimen lähdekoodiin pohjautuva sekä maailman suosituin mobiilikäyttöjärjestelmä. (Teknavi 2014) Etenkin yrityksen puhelimet, tabletit ja muut mobiililaitteet tulisi suojata vastaavin keinoin kuin tietokoneet.

4.6 Sähköposti

Sähköpostit liikkuvat salaamattomana julkisessa verkossa ja siten niissä ei ole suojausta. Tämän vuoksi viestien salakuuntelu on helppoa. Toisaalta on myös helppo väärentää viestin lähettäjän tunnistustiedot, ja vastaanottaja ei ole varma viestin lähettäjästä. (Hakala, Vainio & Vuorinen 2006, 39.)

Epäilyttävän lähettäjän pystyy yleensä tunnistamaan helposti esimerkiksi epäilyttävän viestin otsikosta: viesti on lähetetty pelkästään lähettäjän etunimellä tai viesti on kirjoitettu kielellä, jota lähettäjä ei yleensä käytä. Sähköpostin liitteenä voivat olla troijalaisia, viruksia, matoja tai muita haittaohjelmia. Etenkin ne tiedostonpäätteet, jotka ovat .com, .exe, .shs, .pif ja .vbs ovat tyypillisesti haittaohjelmien merkkejä, ja niiden avaamista on syytä välttää. (Viestintävirasto 2014)

Hakalan, Vainion ja Vuorisen mukaan sähköpostiviestien suojaamiseen on kehitetty muuan muassa ilmainen Pretty Good Privacy (PGP) -ohjelmisto. Ohjelmisto suojaa viestin ulkopuolisilta, toteuttaa varmentamisen ja varmentaa viestin alkuperän. Viestin lähettäjän lisäksi myös vastaanottajan on käytettävä samaa ohjelmistoa avatakseen suojatun viestin. (Hakala, Vainio & Vuorinen 2006, 381.)

Yksi tapa varmistaa viestin muokkaamattomuus ja viestin lähettäjän henkilöllisyys on digitaalinen allekirjoitus. Viestin lähettäjän julkisella avaimella mahdollistaa allekirjoittamalla viestin, ja lähettämisen jälkeen viestin vastaanottaja todentaa viestin lähettäjän henkilöllisyyden lähettäjän viestin julkisella avaimella. Digitaaliset allekirjottamisohjelmat ovat usein kaupallisia. Yllämainittu ohjelma PGP:n (Pretty Good Privacy) heikkoutena on takaamattomuus viestin lähettäjän ja hänen julkisen avaimensa kuuluvuus. Tämä mahdollistaa sen, että lähettäjän julkinen avain voi kuuluakin jollekin ulkopuoliselle. Tämän ongelman ratkaisevat esimerkiksi julkisen avaimen infrastruktuurissa käytetyt henkilövarmenteet, jotka sitovat sekä lähettäjän että hänen julkisen avaimensa luotettavuuden toisiinsa. (Viestintävirasto 2014)

4.7 Salasanat

Helppoja ja käytetyimpiä salasanoja, muun muassa salasana, 12345 ja qwerty, on syytä välttää. Muista helpoista salasanoista ei saisi olla

käyttäjään liittyviä nimiä tai numeroita. Väärinkäyttäjä voi kirjoittaa helpon sanasanan kirjautumiskenttään ja kaapata tunnuksen. Vaihtoehtoisesti väärinkäyttäjä voi hyödyntää salasanaohjelmistoa, joka pitää listaa tavallisesta nimistä ja helpoista salasanoista.

Jotkut sivustoista, esimerkkeinä Google ja Dropbox, ilmoittavat sähköpostin kautta tilin omistajalle, että muulla kuin omalta päätelaitteelta on kirjauduttu sisään. Ilmoituksen lisäksi annetaan vaihtoehto, jossa nollataan salasana ja sen tekemisen jälkeen väärinkäyttäjä ei voi tehdä tilillä enää mitään.

Hyvän salasana on ulkopuolisille vaikeasti arvattava, mutta käyttäjälle hyvin muistettava. Suositeltu salasanan pituus yli 12 merkkiä ja se sisältää erikoismerkkejä, numeroita, pieniä sekä isoja kirjaimia. Mitä pidempi salasana ja enemmän käytetty erilaisia näppäinmerkkejä, sitä vaikeasti salasana on arvattavissa. Salasanaa suositellaan vaihtamaan usein ja säännöllisesti. Jokaiselle tilille suositellaan eri salasana.

4.8 Käyttöoikeudet

Käyttöoikeuksien rajaaminen käyttäjille on tehokas tapa parantaa tietoturvaa. Käyttäjälle annetaan ne oikeudet, jotka ovat työnsä kannalta välttämättömiä. Oikeuksien rajaaminen mahdolliseksi on vaadittava harkintaa ja suunnittelua. Vaikka tulos vie aikaa ja vaivaa, hyvin toteutetuilla rajoituksilla käyttäjällä ei ole pääsyä muokkaamaan tietokoneen asetuksia tai työnsä ulkopuolella olevia tiedostoja. Näin virheitä ei tapahdu ja käyttöoikeuksien kannalta tietokone on lähes haavoittumaton. Windowsissa käyttöoikeudet eivät ole kuitenkaan yhtä kattavia kuin muut käyttöjärjestelmät. Käyttöoikeuksien rajaaminen mahdollistaa kiertämisen, mikä on Windows-ympäristöissä ongelma. Järvisen mukaan yksi ongelmista ovat sovellusohjelmien antamat epäselvät ja harhaanjohtavat virheilmoitukset, joiden takia ohjelmat eivät ole tietoisia oikeuksien rajaamista. (Järvinen 2006, 195.)

Rajoitetuilla käyttöoikeuksilla toimivat käyttäjät pystyvät käyttämään konetta ja ohjelmia, mutta eivät muuttamaan asetuksia eivätkä niinkään sotkemaan mitään. Vaikka rajoitetulla käyttöoikeuksilla omaava henkilö käynnistäisi vahingossakin haittaohjelman, se ei pystyisi tekemään koneella vahinkoa. (Järvinen 2006, 196.)

Käyttöjärjestelmissä käyttöoikeudet määritellään hyvin tarkkaan. Jotta jokaiselle ei tarvitse määritellä oikeuksia yksi kerrallaan, oikeudet asetetaan ryhmiin. Pääkäyttäjäryhmällä on kaikki oikeudet tietokoneeseen, kun tavallisella käyttäjäryhmällä on yleensä ohjelmien käytössä tarvittavat perusoikeudet. Kun käyttäjä liitetään jonkin ryhmän jäseneksi, hän saa ryhmään kuuluvat oikeudet. Käyttäjä voi myös kuulua useampaan eri ryhmään. Pääkäyttäjien ja tavallisien käyttäjien ryhmien välissä on myös muita ryhmiä. Näille ryhmille voidaan antaa joitakin pääkäyttäjien oikeuksia, muun muassa ylläpitotehtäviin varten, kuten varmuuskopiointia tai ohjelmien päivittämistä. Käyttäjäryhmien oikeuksia voi myös rajata pääsyn joihinkin kiintolevyn hakemistoihin. (Järvinen 2006, 196.)

4.9 Salaus

Salauksella salataan tieto siten, että sen haltuun saava ulkopuolinen ei voi sitä avata. Salauksen tarkoitus on saattaa tieto sellaiseen muotoon, jonka voi palauttaa alkuperäiseen muotoon vain tietoon oikeutetut henkilöt.

Symmetrinen salaus on menetelmä, jonka salauksessa ja sen purkamisessa käytetään samaa avainta. (Viestintävirasto 2007) Tässä luvussa on listattu yleisimpiä symmetrisiä salausjärjestelmiä. (Taulukko 1.)

Symmetriset salaukset			
Nimi	Kuvaus	Avainkoko (bit)	Salauslohko(bit)
DES	IBM:n kehittämä laajasti käytetty vanha salausjärjestelmä.	56	64
AES	Yleinen käytössä oleva tietotekniikan salaus. DESin seuraaja.	128, 192, 256	128
Blowfish	Käyttää 16-kerrosta 64 bitin lohkoissa.	32-448	64
Twofish	Lohkosalausjärjestelmää käyttävä salaus.	128, 192, 256	128
3DES	Sama salausalgoritmi kuin DES:ssa, mutta tuo useamman suojauskerran.	168, 112	168

Taulukko 1. Taulukko yleisimmistä symmetrisistä salauksista.

Epäsymmetrisessä salauksessa käytetään kahta avainta, joista toinen on julkinen ja toinen yksityinen. Avaimet ovat yhteensopivia siten, että julkisella avaimella salattu viesti on mahdollista purkaa yksityisellä avaimella ja päinvastoin. Epäsymmetrinen salaus on hitaampi ja avaimen on oltava pidempi kuin symmetrisellä salauksella. (Viestintävirasto 2007)

Diffie-Hellman on salausprotokolla, jonka avulla kaksi osapuolta keskustelevat keskenään turvattoman tietoliikenneyhteyden yli käyttäen samantapaista salausmenetelmää, joka salaa molemmat osapuolet, tehden näin keskustelusta yksityisen. RSA on salausalgoritmi, joka luo julkisen avaimen ja yksityisen avaimen, joita käytetään viestien/tiedon lähettämisessä ja avaamisessa. ElGamal on julkisten avainten salausalgoritmi, jossa avaimia vaihdetaan. Ensiksi avain luodaan, tämän jälkeen salataan ja lopuksi puretaan.

Tiedon salaukseen tarkoitettuja ohjelmia on monia, muun muassa TrueCrypt. TrueCrypt on avoimen lähdekoodin sovellusohjelma, jolla voi salata kiintolevyn sisältö osiona tai kokonaan. Sen voi asentaa myös sellaiselle kiintolevylle, jossa on asennettu käyttöjärjestelmä, mutta silloin tietokoneen käynnistyessä TrueCrypt pyytää salasanan ennen kuin antaa käyttöjärjestelmän käynnistyä. (Koivisto 2012)

4.10 Varmuuskopiointi

Säännöllinen varmuuskopiointi tietyn ajan välein olisi hyvä tiedostojen katoamisen varalta. Aiemmin hyviä varmuuskopiontipaikkoja olivat

tallennusmediat, CD/DVD-levyt, muistitikut, levykkeet ja kiintolevyt. Nykyajan hyödyllisiä varmuuskopiointipaikkoja ovat pilvipalvelut, joista osa synkronoi automaattisesti aina sitä mukaa, kun aiemmin tallennettu tiedosto muutettiin. Maailman ensimmäisenä pilvipalveluna oli pidetty vuonna 1999 perustettu Salesforce.com. (ComputerWeekly 2009)

Lopullisesti hävitettäviä tiedostoja hävitetään kunnolla siten, että tiedoston varmuuskopioidutkin hävitetään samalla tavalla. Kunnolla hävittämisellä tarkoitetaan tiedoston hävittämiseen tarkoitettua ylikirjoitusohjelmaa.

4.11 Tietokanta

Tietokanta on tietotekniikassa käytetty termi, jossa on kokoelma yhteen liitettyjä tietoja. Ne sisältävät muun muassa henkilötietoja, käyttäjätunnukset salasanoineen ja asiakkaan tilaukset. Tietokannassa oleva tieto on järjestelmistä tärkein ja kriittisin ominaisuus.

Tietokannan tietoturvallisuus alkaa asennuksesta, jossa muun muassa asetetaan porttinumeroksi 1521 ja käyttöoikeuksien muuttaminen. Jos tietokannassa on käyttäjätunnuksia, niiden salasanat on oltava kryptattuja. Esimerkiksi salaus algoritmi md5. Tietokannan tietoturvallisuus on hyvä testata ennen käyttöönottoa.

4.12 Pilvipalvelu

Pilvipalvelulla tarkoitetaan järjestelmää, jota voi käyttää missä vaan paikasta riippumatta. Pilvipalvelimet ovat jaettu kolmeen eri pääluokkaan IaaS- (Infrastructure as a Service; infrastruktuuripalvelin), PaaS- (Platform as a Service; alustapalvelin) ja SaaS (Software as a Service; sovellusohjelmapalvelin)–palveluihin. Uusi, yleistyvä pilvipalvelimen luokka on XaaS (Anything as a Service; yleispalvelin). (Takkinen 2013, 6 & 11.)

Pilvipalveluiden huonona puolena on se, että niiden käyttö edellyttää yleensä netin käyttöä. Pilvipalveluiden teknisinä riskeinä ovat pilviteknologiasta aiheutuva haavoittuneisuus, heikot rajapinnat ja tietojen todennäköinen tuhoutuminen. (Kiviharju 2014)

4.13 WWW-sisällönhallintajärjestelmä

WWW-sisällönhallintajärjestelmällä tarkoitetaan verkossa olevaa tietojärjestelmää, johon voi lisätä helppokäyttöisesti tarkoituksenmukaisesti olevia sisältöjä, kuten tekstejä ja muita mediatiedostoja. Tällaiset ovat kuvat, äänitteet ja videot. Esimerkiksi blogien ja verkkosivujen taustalla voi toimia sisällönhallintajärjestelmä.

Tämän hetkisen käytetyimmät sisällönhallintajärjestelmät ovat Wordpress, Joomla ja Drupal. Etenkin näihin järjestelmiin kohdistuvat haittaohjelmat, jotka pyrkivät murtautumaan sisällönhallintajärjestelmiin kaikin keinoin ja sitä kautta aiheuttaa järjestelmälle vahinkoa. Www-

sisällönhallintajärjestelmiä kohdistuvia haittaohjelmia voi ennaltaehkäistä asentamalla tietoturvaan liittyvät lisäosat ja muuttamalla oletushallintapaneelin ja -pääkäyttäjän nimi joksikin muuksi.

5 OLDTIMERTIMER-PROJEKTI

oldtimerTimer-projektin tekijät koostuivat kymmenestä henkilöstä. Heistä kaksi vastasi mobiilisovelluksen kehittämisestä, kaksi Wordpress/nettiportaalin kehittämisestä, yksi tietokannan suunnittelusta, yksi tuotantopalvelimen hankkimisesta sekä ylläpitämisestä, kaksi mobiilin ja nettiportaalin käyttöliittymien suunnittelusta. Kirjoittaja vastasi tietoturvasta, ja yksi oli projektipäällikön tehtävissä. Tässä luvussa kerrotaan oldtimerTimer-järjestelmän tietoturvan nykytilanne ja se, mitä järjestelmän tietoturvassa otetaan huomioon.

Aikaisemmissa luvuissa mainitut tietoturvan osa-alueet olisi kaikki näistä otettu mukaan tietoturvasuunnitelmaan, mutta asiaa pohdittiin vasta kesän 2014:n jälkeen ja siten jätettiin osa tietoturvan osa-alueista kokonaan pois. Esimerkiksi hallinnollista turvallisuutta vastaisi projektipäällikkö yhdessä tietoturvavastaajan kanssa. Tietoturvan osa-alueista otettiin mukaan kartoitettavaksi tietoliikenneturvallisuus, ohjelmistoturvallisuus, käyttöturvallisuus ja fyysinen turvallisuus yhdessä laitteistoturvallisuuden kanssa.

5.1 Projektin tietoturvakartoitus ja tulokset

Tietoturvakartoitusta varten projekti jaettiin projektityöntekijöiden vastuualueiden mukaan, joiden tietoturvan joidenkin osa-alueet sekoitettiin keskenään. Ainoastaan fyysinen ja laitteistoturvallisuus kartoitettiin tietoturvan osa-alueiden mukaan. Osa tietoturvakartoituksen tulokset perustuivat teemahaastatteluilla ja siihen perustuvilla kirjallisilla merkinnöillä. Haastattelun ulkopuolelle jäivät projektipäällikkö ja käyttöliittymien suunnittelijat, koska tietoturvakartoitus suoritettiin pääosin teknisellä tasolla. Tietoturvan teemahaastattelu suoritettiin koko kesän 2014:n aikana yhden kerran ja kokonaisuudessaan se kesti noin kaksi tuntia. Teemahaastattelu liittyy myös tietoturvan osa-alueisiin, joihin kuuluvat tietoliikenneturvallisuus, käyttöturvallisuus ja erityisesti ohjelmistoturvallisuus.

5.2 Fyysinen turvallisuus ja laitteistoturvallisuus

oldtimerTimer-projektin tila pidettiin Hämeen ammattikorkeakoulun C-talon tietokoneluokissa. Tilat oli yleisesti ottaen hyvin järjestetty. Tietokanta ja www-sisällönhallintajärjestelmä sijaitsivat virtuaalipalvelimessa, joka vastaavasti sijaitsi Hämeen ammattikorkeakoulun tiedonhallinnan palvelintiloissa. Osaltaan tästä syystä hallinnollinen turvallisuus jäi toteutumatta. Mobiilisovellus sijaitsi kannettavissa tietokoneissa, joista vastasivat kyseisen järjestelmän kehittäjät. Tietokoneluokan tietokoneiden ja kannettavien tietokoneiden käynnistämisen jälkeen kysytään käyttäjätunnusta ja salasanaa.

Järjestelmään pääsi kirjautumaan vain, jos oli Hämeen ammattikorkeakouluun kuuluvat aktiivisessa käytössä olevat tunnukset.

5.3 WWW-sisällönhallintajärjestelmä

Projektinimi nettiportaali, eli WWW-sisällönhallintajärjestelmänä käytettiin avoimeen lähdekoodiin pohjautuvaa Wordpressiä, joka on tällä hetkellä maailman käytetyin julkaisujärjestelmä. Laajasta käytöstä huolimatta Wordpress voi olla riskialtis tietoturvalle: mitä käytetympi julkaisujärjestelmä, sitä riskialttiimpi se voi olla tietoturvalle.

Wordpress valittiin julkaisujärjestelmäksi, koska se oli projektityöntekijöille tuttu ja turvallinen. Muina ehdokkaina olisivat olleet Drupal ja Liferay, mutta ne jätettiin pois edellä mainittujen syiden vuoksi.

Lisäosissa on huomioitu version yhteensopivuus Wordpressin nykyisen version kanssa ja se, milloin järjestelmä oli viimeksi päivitetty. Lisäosien etsiminen oli tuottanut hankaluuksia koska monet mainitsemisen arvoiset lisäosat olivatkin ehtineet vanhentua lyhyessä ajassa. OldtimerTimer-projektin Wordpressiin asennettiin tietoturvaan liittyvät lisäosat. (Taulukko 2.)

Wordpressin lisäosat	
Nimi	Kuvaus
All in one WP security	Laaja tietoturvaan liittyvä lisäosa, jossa voi muun muassa nimetä kirjautumisosoitteen uudelleen.
Login Lockdown	Jos yrittää kirjautua sisään kolmesti väärällä salasanalla, järjestelmä lukkiutuu 15:ksi minuutiksi.
Members	Laajempi käyttöoikeuksiin kuuluva lisäosa.
Ready! Backup.	Varmuuskopiointilisäosa.

Taulukko 2. OTT-projektissa käytetyt Wordpressin lisäosat.

Wordpressin rekisteröinnissä pyydettiin käyttäjätunnusta ja sähköpostiosoitetta, jonka jälkeen rekisteröijän sähköpostilaatikkoon tuli viesti, jossa oli salasana. Näin jäi epäselväksi, millä tavalla salasana luotiin ja lähetettiin sähköpostissa.

Käyttäjärooleissa olivat ylläpitäjä, hoitajat ja omaiset. Ylläpitäjä antoi manuaalisesti hoitajille omat tunnukset, koska muuten rekisteröijät olivat automaattisesti omaisia. Näin kuka tahansa ei voinut olla hoitaja ilman ylläpitäjän valtuuttamana. Mikäli käyttäjäkunta kasvaa järjestelmän käytön myötä, ylläpitäjälle on työläämpää antaa hoitajalle rooleja.

Nimen, sähköpostin ja salasanan vaihto onnistuivat menemällä Omat näkymät -sivulle.

Wordpressin oletuspääkäyttäjän (admin) nimi oli vaihdettu, mutta kirjautumisosoitetta (wp-admin) ei ollut vielä vaihdettu. Näiden oletusnimien vaihtaminen oli kannattavaa, koska verkossa liikkuivat Wordpress-julkaisujärjestelmään suunnattuja haittaohjelmia, jotka yrittävät murtautua järjestelmään oletushakemistojen perusteella ja murron jälkeen aiheuttaa järjestelmälle vahinkoa.

Sivustolla oli edelleen tietoturvaongelmia. Käyttäjiltä tulleet syötteet tarkistettiin PHP:n funktiolla ennen niiden käyttämistä, jonka piti estää esimerkiksi koodien syöttämisen tekstikentän kautta. PHP:n tietokantayhteys oli ohjelmoitu sivuille, eli jos sivu "meni rikki" ja näytti PHP-koodit selkokielisinä, sieltä pystyi helposti noukkimaan tietokannan tiedot, käyttäjätunnuksen ja salasanan. Tämän takia PHP:n funktion käyttö ei ollut hyvä ratkaisu, mutta tuolloin resurssit eivät riittäneet erilaisten kansiorakenteiden muokkailuun yms.

5.4 Mobiilisovellus

Mobiilin käyttöjärjestelmänä käytettiin Androidia. Android on ohjelmoitu Javalla. Ehdokkaina mobiilisovelluskehitystyökaluksi olisivat olleet Corona SDK, PhoneGap, Xamarin ja AppGyver Steroids. Loppulliseksi valinnaksi otettiin käyttöön ehdokkaiden ulkopuolelta oleva Eclipse-mobiilisovelluskehitystyökalu.

Rekisteröintijärjestelmä toimi PHP-palvelimen kautta, jonka tiedot olivat tallennettu. Rekisteröitymisen aikana järjestelmä pyysi käyttäjätunnuksen, salasanan, etu- ja sukunimen. Niissä olivat GET-komennot, joiden avulla pystyi helposti murtautumaan järjestelmään. Järjestelmän rekisteröityessä puuttui käyttäjätunnuksen tarkistus. Ilman tarkistusta kuka tahansa pystyi rekisteröitymään järjestelmään mobiilisovelluksen kautta.

Järjestelmän tietokanta ei tallentunut mobiiliin, kun verkko oli alhaalla. Mobiilissa voi kuitenkin lisätä kalenterimerkinnät palvelimen ollessa alhaalla. PHP:ssa on käytetty msql-koodi mysqlin sijaan, joka on huonompi tietoturvaratkaisu toisin kuin jälkimmäinen koodi.

5.5 Tietokanta

Tietokantana oli MySQL, ja asiakaspuolen syötteet tallennettiin XML:ään. Tietokannan hallintaohjelmistona käytettiin PhpMyAdminia. Tietokannan salasanoja ei ole toteutettu md5:lla, koska se muuttaisi salasanan salaukseksi, minkä myötä edes järjestelmän ylläpitäjäkään ei tietäisi sitä. Myöstään PhpMyAdminin pääkäyttäjän (root) nimeä ei muutettu. XML:n sijaan JSONia olisi voitu käyttää tietojen esittämiseen, koska JSON on XML:ään verrattuna riippumaton JavaScriptistä. Näin ollen sitä olisi voinut hyödyntää muilla ohjelmointikielellä.

5.6 Palvelin ja tietoliikenne

Palvelimeksi valittiin virtuaalipalvelin fyysisen palvelimen sijaan. Virtuaalipalvelin oli hankittu Hämeen Ammattikorkeakoulun tiedonhallinnolta. Palvelimen käyttöjärjestelmänä oli käytössä Linux.

Palvelimessa oli PhpMyAdmin ja www-sisällönhallintajärjestelmä. Palvelin oli väliaikaisesti virtuaalipalvelimella siihen asti, kunnes järjestelmä siirrettiin fyysiselle palvelimelle tuotantotarkoitukseen. HAMKin tiedonhallintoa ei hyväksynyt kaupallisia tuotteita virtuaalipalvelimelle. Myös fyysisen palvelimen osalta olisi jouduttu vastaamaan enemmän tietoturvasta.

Tietoliikenteen liikkuminen järjestelmien väliltä oli käytetty http-protokollaa, joka on hyvin tietoturva-altis kaappaamiseksi. Tämän ongelman ratkaisisi muuttamalla HTTP HTTPS-protokollaksi. Ongelmana on virtuaalipalvelimen tuki HTTPS:lle, koska se jäi testaamatta.

6 POHDINTA JA JOHTOPÄÄTÖKSET

Tietoturvakartoittamisen aikana huomattiin järjestelmissä olevan runsaasti aukkoja, mutta nettiportaalin tietoturva oli toteutettu kaikista muista järjestelmän osa-alueista pisimmälle. Nettiportaalin Wordpress-sisällönhallintajärjestelmään oli asennettu lukuisia eri tietoturvan lisäosia, jotka tekivät järjestelmästä lähes haavoittumattoman. Mobiilisovelluksen tekninen toteutus oli ohjelmoitu kokonaan tyhjästä, ja siihen oli monimutkaista toteuttaa tietoturvaan liittyviä järjestelmiä jälkikäteen. Palvelimen tarkempi tietoturvakartoitus ei ollut tarpeen, koska palvelin toimi virtuaalisessa ympäristössä.

Noin kymmenhenkisessä odtimerTimer-projektissa tietoturvapolitiikkaa oli pidetty liian muodollisena eikä sitä otettu käyttöön. Myös tietoturvan yksityiskohtainen dokumentointi jäi toteuttamatta edellä mainitun syyn vuoksi. Näiden sijaan toteutettiin yksinkertainen tietoturvakartoitus, joihin asetettiin kartoituksen kohteelle kriittisimmille kohdille kysymykset.

Opinnäytetyön käytännön osuus keskittyi kesän 2014 projektin tietoturvaan. Osuus suoritettiin teemahaastattelulla ja kartoittamalla projektiin käytettäviä laitteistoja sekä ohjelmistoja. Haastattelussa kävi useassa osa-alueessa ilmi, että panostaminen tietoturvaan oli jäänyt kokonaan tekemättä. Opinnäytetyössä otettiin myös kantaa kesän 2014 projektin tietoturvan nykytilanteeseen.

6.1 Tietoturvakartoituksen rajoitukset

Tietoturvan tutkimista rajasi eniten ajan puute. Tietoturvakartoitukseen kootut kysymykset jäivät analysoimatta tarkemmin ja laajemmin. Tietoturvakartoitukseen suoritettu teemahaastattelu järjestettiin koko kesän 2014 projektin aikana kerran ja se tapahtui aivan projektin päätyttyä. Projektinhallintamenetelmänä käytettiin Scrumia koko projektin aikana, joihin kuuluivat noin kymmenen minuuttia kestävät päiväpalaverit. Suurin osa päiväpalavereista jäi väliin juuri ajan puutteen vuoksi. Päiväpalavereissa kysyttiin jokaiselta projektityöntekijältä mitä tehtiin päivän työnä. Näiden tiedustelujen pohjalta olisi voitu suorittaa tietoturvaselvitys.

Aineiston pohjalta toteutettu tietoturvakartoitusta rajasi myös aiheen rajaus. Tietoturva on aiheena niin laaja, että kesän 2014:n oldtimerTimer-projektiin oli hyvin haastavaa. Opinnäytetyöhön tulivat alusta lähtien myös projektiin liittymättömät tietoturva-asiat. Näihin kuuluivat tietoturvan hallinnointi ja vaiheittain etenevä tietoturvakartoitus. Lopulta nämä aiheet kuitenkin poistettiin kokonaan lopullisesta opinnäytetyöstä.

6.2 Jatkokehitys

Koska oldtimerTimer-järjestelmä oli toteutettu vasta prototyyppivaiheeseen, järjestelmän tietoturvan kartoittaminen ei ollut kriittisin osa-alue. Kehittyneempi järjestelmä toteutettiin syksyn 2014 ICT-Project -opintojaksossa. Jatkossa tietoturvaa tulisi korostaa enemmän tulevassa projektissa.

7 YHTEENVETO

Opinnäytetyön alkuperäisenä tavoitteena oli suunnitella ja toteuttaa tietoturvakartoitus oldtimerTimer-projektille. Kokonaisuudessa järjestelmän kartoitus oli riittämätön, mutta se kuitenkin onnistui jossain määrin. Tietoturvakartoituksessa tutkittiin ensisijaisesti järjestelmän kriittisimmät kohdat. Suurin ongelma oli tietoturvan käsittely, koska se oli aiheena hyvin laaja ja sen kirjoittaminen ja rajaaminen tuotti hankaluuksia.

Mikäli kirjoittajalle menetelmät olisivat olleet tuttuja ennestään, kesän 2014:n projektissa lukuisilta virheiltä olisi voitu välttyä ja kirjoittaminen sekä aiheen rajaus olisivat olleet paljon selkeämpää. Joka tapauksessa kesän 2014:n projekti toi kuitenkin kirjoittajalleen paljon uusia kokemuksia tietoturvavastaajana.

Opinnäytetyöprosessin edetessä tutkimuskysymykset muuttuivat. Alun perin tutkimuskysymykset liittyivät tietoturvakartoitukseen, riskianalyysiin ja toipumissuunnitelmaan. Projektin hahmotuttua osa tutkimuskysymyksistä poistettiin ja laajennettiin tietoturvan yleiselle tasolle. Ensimmäinen tutkimuskysymys oli tietojen turvaamista, toinen oli järjestelmien käyttöönotto projektissa. Myöhemmin tutkimuskysymyksiä tuli kolme lisää. Ensimmäinen oli mitä tietoturva on, viimeiset kysymykset liittyivät projektin tietoturvan nykytilanteeseen ja projektin tietoturvan jatkokehitykseen.

Ennen projektia ja opinnäytetyöprosessia tietoturva oli kirjoittajalle tuttu aihealue, erityisesti Linuxin tietoturvan osa-alue. Projektin aikana käsitys tietoturvasta laajeni huomattavasti ja tietoturvakartoituksen toteuttaminen toi mahdollisuuden tutustua eri järjestelmän osa-alueisiin, joissa järjestelmän tietoturva oli enemmän tai vähemmän kunnossa. Projektin hallintamenetelmä Scrum toi myös käytännön kokemusta.

Opinnäytetyön aihe oli kirjoittajalle hyödyllinen. Projektin aikana tietoturvan merkitys korostui ja tulevassa projekteissa huomion kiinnittäminen tietoturvaan on jatkossa tärkeää. Vaikka kirjoittajan käsitys tietoturvasta on laajentunut teoriassa, tietoturvan käytännön kokemuksen lisääminen olisi tarpeen.

LÄHTEET

ComputerWeekly. 2009. computerweekly.com
Viitattu 2.9.2015. http://www.computerweekly.com/feature/A-history-of-cloud-computing

Finlex. 1999. finlex.fi
Viitattu 8.3.2015. http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Hakala, Vainoa & Vuorinen. 2006. Tietoturvallisuuden käsikirja
Viitattu 18.1.2015.

Järvinen. 2006. Paranna tietoturvaasi.
Viitattu 19.1.2015.

Järvinen. 2012. Arjen tietoturva.
Viitattu 1.2.2015.

Kitunen. 2014. Yksityisen syöpäsairaalan tietoturvakartoitus. Helsinki: Haaga-Helia ammattikorkeakoulu, pdf-tiedosto. Viitattu 24.8.2014.
http://www.theseus.fi/bitstream/handle/10024/73259/kitunen_martti_yksityisen_syopasairaalan_tietoturvakartoitus.pdf/

Kiviharju. 2014. Viestintävirasto, pdf-tiedosto.
Viitatty 1.2.2015,
https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20140519Tietot/Pilvipalveluiden_arviointi_Compatibility_Mode.pdf

Koivisto. 2012. Tiedon salaus ja tietoliikenteen suojaus. Vaasa: Vaasan Ammattikorkeakoulu, pdf-tiedosto. Viitattu 23.3.2015. https://www.theseus.fi/bitstream/handle/10024/44642/Koivisto_Markus.pdf?sequence=1

Laaksonen, Nevasalo & Tomula. 2006. Yrityksen tietoturvakäsikirja
Viitattu 6.7.2015

Laakso. 2010. Tietojesiturvaksi.fi.
Viitattu 25.8.2014. http://www.tietojesiturvaksi.fi/content/tietoturvan-osa-alueet/

Leino. 2013. Pk-yrityksen tietoturva. Helsinki: Haaga-Helia ammattikorkeakoulu, pdf-tiedosto. Viitattu 25.8.2014. https://www.theseus.fi/bitstream/handle/10024/63975/Leino_Satu.pdf/

Mobiilia liiketoimintaa ja teknologiaa. 2014. ristola.wordpress.com

Viitattu 7.2014, http://ristola.wordpress.com/2014/02/05/mobiilitermit-tutuksi/

Pappinen. 2013. PK-yrityksen tietoturvasuunnitelma. Joensuu: Pohjois-Karjalan ammattikorkeakoulu, pdf-tiedosto. Viitattu 28.7.2015. http://www.theseus.fi/bitstream/handle/10024/54539/Pk-yrityksen%20tietoturvasuunnitelma.pdf?sequence=1

Pulli. 2012. Katastrofinkestävän ICT-järjestelmän toteutus, case Pirkanmaan sairaanhoitopiirin potilastietovarasto. Hämeenlinna: Hämeen Ammattikorkeakoulu, pdf-tiedosto. Viitattu 1.2.2015. http://theseus.fi/bitstream/handle/10024/49646/Pulli_Ismo.pdf?sequence=1

SecMeter. 2008. Secmeter.com
Viitattu 18.4.2015
http://www.secmeter.com/henkilostoturvallisuus.html

Teknavi. 2014. teknavi.fi
Viitattu 5.8.2015.
http://teknavi.fi/elektroniikka/google-esitteli-uuden-android-kayttojarjestelman-tassa-tarkeimmat-uudistukset

Takkinen. 2013. Palvelinvirtualisointi ja pilvipalvelut. Helsinki: Metropolia ammattikorkeakoulu, pdf-tiedosto. Viitattu 1.2.2015. https://www.theseus.fi/bitstream/handle/10024/54199/Palvelinvirtualisointi%20ja%20pilvipalvelut.pdf?sequence=1

Tietoturvapalvelu. Tietoturvapalvelu.info
Viitattu 18.4.2015
http://www.tietoturvapalvelu.info/johdanto/haittaohjelmat_ja_muut_uhat

Tietoturvan perusteita. 2005. Metropolia.
Viitattu 24.8.2014. http://users.metropolia.fi/~kuivi/tietoturva/

Tietoturva ja tietosuoja. 2003. Tuotantorenkaat.
Viitattu 24.8.2014. http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/

VAHTI-tietoturva. 2004. Lapin Ammattikorkeakoulu.
Viitattu 24.8.2014. http://ta.ramk.fi/VAHTI/

Verkkopedakologi. verkkopedagogi.net
Viitattu 14.4.2015.
http://www.verkkopedagogi.net/vanhat/fi/sisalto/materiaalit/tietoturva/luku016e4a.html?C:D=419124&selres=419124

Viestintävirasto. 2014. viestintavirasto.fi
Viitattu 18.1.2015,
https://www.viestintavirasto.fi/tietoturva/palveluidenturvallinenkaytto/sahkoposti.html

Liite 1

TIETOTURVAKYSYMYKSIEN RUNKO

Mobiilisovellus

Miten rekisteröinti toimii?

Onko olemassa olevan käyttäjätunnuksen tarkistusta?

Tuleeko vahvistus, kun rekisteröinti on suoritettu?

Ketkä voivat rekisteröityä?

Toimiiko mobiilisovellus ja sen tietokanta, kun verkko ei ole käytössä?

Onko PHP-tietokannassa käytetty mysqli-komentoa?

Tietoliikenne

Millä tietoliikenteellä rekisteröitymis- ja muut tiedot tallentuvat tietokantaan sekä mikä protokolla on käytössä?

Nettiportaali/Wordpress

Mitä tapahtuu, kun kirjoittaa salasanan monta kertaa väärin?

Miten kirjautumista tarkistetaan ja onko kirjautumisyrityksiä rajoitettu?

Miten rekisteröityminen toimii?

Kuka määrittää uudelle käyttäjälle aseman? (omainen, hoitaja)

Miten nimen, s-postin ja salasanan vaihto toimii?

Mitä tietoturvalisäosat ovat käytössä?

Onko varmuuskopiointijärjestelmää?

Onko oletuspääkäyttäjän nimi vaihdettu?

Onko tietokannan oletusarvo vaihdettu?

Onko kirjautumisosoite vaihdettu?

Onko kansioiden ja kirjoituslukuoikeudet muutettu järkeviksi?

Tietokanta

Tietokannan nykytilanne?

Onko salasanat toteutettu md5:lla?

Pääkäyttäjän nimi muutettu?

Onko muita kuin pääkäyttäjiä?

Miksi juuri XML:llä toteutetaan tiedonsiirrolla JSONin sijaan?

Palvelin

Mikä palvelin on käytössä?

Mitä palvelimessa voi muokata?

Onko palomuuri käytössä ja voiko siinä tehdä määritykset?

Onko virustentorjuntaohjelmaa?

Onko palvelin väliaikainen vai pysyvä?

Onko tietoturvapäivityksiä asentamatta?

Onko asennettu ylimääräisiä sovelluksia?