jamk.fi

VAHTI SOVELLUSKEHITYKSEN TIETOTURVA-OHJEEN VAATIMUKSET KETTERÄSSÄ OHJELMISTOKEHITYKSESSÄ

Mikko Hyvärinen

Opinnäytetyö

Toukokuu 2014

Tietojenkäsittelyn koulutusohjelma

Luonnontieteiden ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

KUVAILULEHTI

Tekijä(t) Hyvärinen, Mikko	Julkaisun laji Opinnäytetyö	Päivämäärä 09.05.2014
	Sivumäärä 70	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty (X)

Työn nimi
VAHTI SOVELLUSKEHITYKSEN TIETOTURVAOHJEEN VAATIMUKSET KETTERÄSSÄ OHJELMISTOKEHITYKSESSÄ

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Työn ohjaaja(t)
Kiviaho, Niko

Toimeksiantaja(t)
Salainen

Tiivistelmä

Opinnäytteen toimeksiantajana toimi mm. alihankintaa liiketoimintanaan suorittava kansallinen ohjelmistoyritys, jolla on myös omia tuotteita. Heidän tarkoituksenaan on toteuttaa Valtiohallinnon tietoturvallisuuden johtoryhmän laatiman *VAHTI 1/2103 Sovelluskehityksen tietoturvaohjeen* vaatimukset ja tarjota tietoturvallista sovelluskehitystä asiakkailleen. Tutkimuksen tavoitteena oli tutustua ja laajentaa VAHTI 1/2103 vaatimuksia, analysoida toimeksiantajan prosessia ja tutkia tietoturvallisen sovelluskehityksen tilannetta organisaatiossa tällä hetkellä. Asiaongelma oli tietämättömyyden tila vaatimusten tuoman lisätyön määrästä ja siitä, mitä se tarkoittaa jokapäiväisessä työssä. Haastatteluissa pyrittiin myös kirjaamaan jo käytössä olevia hyviä käytänteitä projekteista, joissa näitä vaatimuksia jo toteutettiin.

Työn teoria on jaettu kolmeen osaan: organisaation tietoturvallisuuteen, projektin aikaiseen tietoturvallisuuteen ja kehitystiimin suorittamaan käytännön toteuttamiseen. Itse kvalitatiivinen tutkimus suoritettiin tutustumalla toimeksiantajan projektikäsikirjaan ja haastattelemalla työntekijöitä tietoturvallisuuteen ja VAHTIn vaatimuksiin liittyen. Toimeksiantaja on kuvattu mahdollisimman tarkkaan siirrettävyyden kannalta. Tutkimukseen osallistui työntekijöitä erilaisista tehtävistä.

Haastatteluiden tuloksista ja nykyisen prosessin analyysistä saatiin opinnäytetyön johtopäätöksiin parannuskohteita ja jo käytössä olevia hyviä käytänteitä. Tutkimuksessa havaittiin mm. koulutuksen tarpeellisuus ja kirjallisen sovelluskehitysprosessin puuttuminen. Kumpikin mainitaan VAHTIn vaatimuksissa. Teoriaosuus ja tutkimuksen tulokset auttavat pieniä ja keskisuuria yrityksiä heidän ponnisteluissaan kohti VAHTI 1/2013 vaatimusten täyttämistä. Toimeksiantaja sai tuloksista käytännön tietoa nykytilanteesta ja parannusehdotuksia**.** Jatkokehitysmahdollisuuksina voisi kehittää toimeksiantajalle kirjallinen sovelluskehitysprosessi ja tutkia tietoturvallisen sovelluskehityksen tilaa erilaisissa yrityksissä.

Avainsanat (asiasanat)
VAHTI, tietoturvallisuus, ketterä sovelluskehitys, alihankinta

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s)	Type of publication	Date
Hyvärinen, Mikko	Bachelor´s Thesis	09.05.2014
	Pages 70	Language Finnish
		Permission for web publication (X)

Title
REQUIREMENTS OF VAHTI SOFTWARE DEVELOPMENT SECURITY GUIDE IN AGILE SOFTWARE DEVELOPMENT

Degree Programme
Business Information Systems

Tutor(s)
Kiviaho, Niko

Assigned by
Confidential

Abstract

This thesis was assigned by a subcontracting software development company that also develops its own products. They aim to implement the requirements in the *VAHTI 1/2013 Software Development Security Guide* specified by the Finnish Government Information Security Management Board. They also wish to offer consultation and secure software development to their clients. The goal of the research was to review and expand the requirements of the VAHTI 1/2013 guide, analyze the current processes of the company, and study the state of secure software development in the company. The main problem was the lack of knowledge of the extra work required when implementing the requirements and what the implementation actually means in everyday work. The aim was also to document existing good practices in secure software development.

The study has been divided into three parts: security in organizations, security during a project, and secure software development in teams. The qualitative research was conducted by analyzing the current written project process manual of the company and interviewing employees of the company concerning questions related to security and the VAHTI requirements. Some background information about the company was also given to provide the context.

Based on the analyses of interviews and the company's current processes, several improvements and good practices are outlined in the discussions. The conclusions of this study highlight the need for security training and the lack of written software development, both of which are mentioned in the VAHTI requirements. The theories and findings of the study help small and medium sized subcontracting companies in their own efforts in implementing the requirements of the VAHTI 1/2013. The company received firsthand knowledge of the current situation and recommendations for improvements. The possibilities for further development could include the composing of a written software development process in addition to researching the state of secure development in various companies.

Keywords
VAHTI, security, agile software development, subcontracting

Miscellaneous

Sisältö

Kuviot

1 VAHTI ja tietoturvallisuus sovelluskehityksessä

1.1 Johdatus aiheeseen

Tietoturvallisuus on ollut ICT-alan kestosuosikki puheenaiheena jo vuosia, mutta siitä on tullut erittäin ajankohtainen nyt, kun eri maiden turvallisuusvirastojen laajamittainen kansalaisten valvonta on tullut julki. Esimerkiksi Yhdysvalloissa suuret yritykset eivät myönnä työskentelevänsä NSA:n (National Security Agency) kanssa, mutta niiden järjestelmiin on tunkeuduttu Snowdenin julkaisemien asiakirjojen mukaan. (Snowden 2014.) Myös Venäjän turvallisuuspalvelu FSB on pyytänyt tietoja Venäjän sosiaalisen median Vkontakte-palvelusta (Hartig 2014). Käyttäjien tietoisuuden lisääntyminen kasvattaa myös organisaatioiden tietoturvallisuuden vaatimuksia. Valtioneuvoston asetus määrittää valtiohallinnon viranomaisten toteuttavan VAHTIn perustason vaatimukset jo tämän opinnäytetyön kirjoittamisen aikaan (Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa 1.7.2010/681). Tietoturvallinen sovelluskehitys kiinnostaa myös yrityksiä, vaikka laissa ei niiden toiminnasta säädetäkään. Tästä syystä aihe on ajankohtainen.

Tutkimuksen aiheena on tarkastella ketterää alihankintasovelluskehitysprojektia ja toimeksiantajan organisaation sovelluskehitysprosessia VAHTI 1/2013 Sovelluskehityksen tietoturvaohjeen vaatimusten näkökulmasta. Tutkimuksessa selvitetään, mitä näiden vaatimusten toteuttaminen tarkoittaa, toteutuvatko ne nyt jo toimeksiantajan projekteissa, ja esitetään nykyiseen prosessiin parannusehdotuksia, jotta vaatimukset toteutuisivat.

1.2 VAHTI Sovelluskehityksen tietoturvaohje

VAHTI on valtionvarainministeriön asettama Valtiohallinnon tietoturvallisuuden johtoryhmä, jonka tavoitteena on tukea julkis- ja valtiohallinnon tietoturvallisuutta kaikilla tietoturvaan liittyvillä osa-alueilla. VAHTIn tehtäviin kuuluu muun muassa ohjata, kehittää ja koordinoida valtiohallinnon toimintojen luotettavuutta ja edistää tietoturvallisuuden integroimista kiinteäksi osaksi prosesseja ja johtamista. (VM, VAHTI ja tietoturvallisuus N.d.) VAHTI Sovelluskehityksen tietoturvaohje on julkistettu tammikuussa 2013, ja se on yksi tuoreimmista ohjekokonaisuuksista VAHTI-ohjeiden perheessä. Nimensä mukaan se käsittelee yksinomaan sovelluskehityksen tietoturvalli-

suuden toteuttamista ja määrittää tälle VAHTI-ohjeiden tyypilliset kolme tasoa: perus-, korotettu ja korkea taso. Sen on tarkoitus toimia tukena valtiohallinnon tietoturvallisuusasetuksen (681/2010) asettaman myös VAHTI Sovelluskehityksen tietoturvaohjeen määrittämän perustason vaatimusten täyttämiselle 30.9.2013 mennessä valtiohallinnon organisaatioissa ja niiden noudattamiselle tulevissa projekteissa. (VAHTI 1/2013, 7.)

VAHTI Sovelluskehityksen tietoturvaohje on laadittu auttamaan riittävän tietoturvallisuuden määrittämisessä suhteessa sovelluksen käyttötarkoitukseen ja ympäristöön sovelluskehitysprojektissa. Ohje on tarkoitettu tukemaan erityisesti julkishallinnon alihankintana tilattujen ohjelmistokehityshankkeiden ja valmisohjelmistojen hankinnassa sekä jo olemassa olevien sovellusten ylläpitoon liittyvissä tietoturvakysymyksissä. Yksi ohjeen noudattamisen tavoitteista on julkishallinnon organisaatioiden tietojärjestelmien toimivuuden turvaaminen kaikissa tilanteissa, niiden tietoaineiston luottamuksellisuuden ja eheyden turvaaminen sekä täten toiminnan jatkuvuuden turvaaminen varmistamalla sovellusten tietoturvallinen toteutus. Muita tavoitteita ovat myös sovelluskehityksen arviointi perustuen VAHTI Sovelluskehityksen tietoturvaohjeen määrittämiin tasoihin ja vaatimusmäärittelyn tuki alihankintaprojekteissa. (VAHTI 1/2013, 12.)

1.3 Toimeksiantaja

Tutkimuksen tulosten siirrettävyyden kannalta lähtötilanne on kuvattu mahdollisimman tarkasti ottaen kuitenkin huomioon, että toimeksiantaja ei halua nimeään julkisuuteen. Toimeksiantajan yritys on ohjelmistopalveluyritys, joka tekee projekteja, tuotekehitystä ja asiantuntijapalvelua. Toimeksiantaja lukeutuu pk-yrityksiin alle 10 miljoonan liikevaihdollaan ja noin sata työntekijää kattavalla henkilöstöllään (Komission suositus 2003/361). Toimeksiantajalla on useilla paikkakunnilla toimipisteitä, ja osa paikkakuntien toimipisteistä on keskittynyt alihankintaprojekteihin. Alihankintana suorittavissa projekteissa voi olla mukana joko vain yksi henkilö asiakkaan projektissa konsulttina tai kokonainen scrumtiimi. Koko projekti voidaan myös suorittaa toimeksiantajan toimesta. Yleisimmin tämänlaisen tutkimuksen tulokset keskittyvät scrumtiimin tai useamman tiimin yhteistyönä muodostuvaan projektiin.

2 Tutkimusasetelma

2.1 Lähtötilanne

Tutkimuksen aiheena on VAHTI Sovelluskehityksen tietoturvaohjeen vaatimusten soveltaminen käytännön sovelluskehitystyössä, sen haasteet ja mahdollisuudet. Asiaongelmana toimeksiantajalla on tietämättömyys lisätyön määrästä, jota VAHTI Sovelluskehityksen tietoturvaohjeen ottaminen mukaan projektisopimuksen vaatimuksiin ja tarjousprosessiin tarkoittaa käytännössä scrumtiimin jokapäiväisessä työssä ja siitä, miten se pitäisi määrittää nykyiseen sovelluskehitysprosessiin koko ketjun läpi. Tätä tarkoitusta varten tutkimuksessa kerrotaan alihankintaprosessista, scrumprosessista, tietoturvallisen sovelluskehityksestä ja testauksen perusperiaatteista. Lisäksi haastatellaan eri projektien työntekijöitä parannuskohteiden ja hyvien käytänteiden löytämiseksi.

Lähtökohtana tutkimustyölle on kartoittaa tietoturvallisen kehittämisen nykytilanne toimeksiantajan yrityksessä, saada parempi kuva tietoturvan toteutuksesta projekteissa ja kehittää nykyistä prosessia. Tämä tutkimus on prosessinkehityshanke, jossa tutkitaan toimeksiantajan projektien prosessia analysoimalla projektikäsikirjaa ja haastatellaan useiden eri projektien työntekijöitä. Yhdessä projektissa on nyt jo otettu VAHTIn vaatimukset huomioon. Tämän projektin hyvät käytännöt halutaan tallentaa ja kehittämisen kohteet kirjata ylös huomioiden ja parannusehdotusten kera. Tutkimuksen rajauksena ovat erityisesti julkishallinnon ohjelmistoprojektit, joissa VAHTI-vaatimuksia eritoten vaaditaan. Tutkimusongelmana on, miten VAHTI Sovelluskehityksen tietoturvaohjeen vaatimukset vaikuttavat scrumtiimin työskentelyyn ja miten tätä prosessia tulisi hallinnoida.

2.2 Tutkimusmenetelmä

Laadullinen tutkimus

Tutkimusongelmaan on kaksi päälähestymistapaa: kvalitatiivinen eli laadullinen ja kvantitatiivinen eli määrällinen (Kananen 2008, 18). Siinä, missä määrällisessä tutkimuksessa kyselyn vastaajien otos on satunnaisesti valittu, on laadullisen tutkimuksen vastaajat valittu perustuen heidän tietoonsa käsiteltävästä aiheesta. Määrällisessä

tutkimuksessa kysymyksen laatu on strukturoitu, ja laadullisessa se on avoin kysymys. Laadullinen tutkimus keskittyy ei-numeeriseen tietoon aiheesta, ja sen tutkimuksen tulokset esitetään tekstimuotoisena. Määrällisessä tutkimuksessa erottamattomana osana ovat numeerisen tiedon tiivistäminen, esittäminen ja analysointi. Yhdessä tutkimuksessa voidaan käyttää kumpaakin lähestymistapaa ristiin tutkimusongelman ratkaisemiseksi. (Laadullisen ja määrällisen tutkimuksen erot N.d.)

Määrällinen tutkimus perustuu hypoteesin asettamiseen, jonka paikkansapitävyyttä yritetään todistaa. Laadullisessa tutkimuksessa ei vielä tiedetä, mitä odottaa, ja siinä pyritään muodostamaan uusia hypoteeseja empirian ja teorian avulla. Laadullinen tutkimus pyrkii löytämään merkityksiä, kokemuksia ja sitä, miten reaalimaailma nähdään tutkittavien näkökulmasta. (Kananen 2008, 25.) Laadullisen tutkimuksen havaintoyksiköiden määrän tulisi olla niin suuri, että saavutetaan saturaatio eli kyllääntymispiste. Kyllääntymispiste on saavutettu, kun haastateltavien vastaukset alkavat toistaa edellisiä tuloksia, jolloin tulkinta ei enää muutu. Määrää tärkeämpää on kuitenkin aineiston laatu. (Kananen 2008, 34−35.) Hyvin pienellä määrällä haastateltavia voidaan saavuttaa enemmän tietoa kuin suurella määrällä, jos osataan kysyä oikeat kysymykset oikeilta ihmisiltä.

Tutkimuksen toteuttaminen

VAHTI Sovelluskehityksen tietoturvaohje on uusi, ja sitä ollaan vasta ottamassa käyttöön monissa julkishallinnon organisaatioissa ja projekteissa. Tutkimuksessa käsitellään VAHTI Sovelluskehityksen tietoturvaohjeen vaatimukset vaihe vaiheelta läpi, tarkastellaan niiden toteutumista eräässä projektissa perustuen haastatteluihin ja tarkastellaan prosessin muutoksia, jotta vaatimukset voidaan toteuttaa. Haastatteluiden tiedonkeruutapa on teemahaastattelu. Tutkimus on suunnattu ennen kaikkea toimeksiantajan päätöksenteon tueksi, mutta myös muille vastaavassa tilanteessa oleville organisaatioille ja tietoturvallisesta sovelluskehityksestä kiinnostuneille.

Koska tutkimuksella pyritään ymmärtämään maailmaa käsitteellisellä tasolla analysoimalla haastateltavien näkökulmia ja ilmaisuja, kyselyyn vastaavat henkilöt on valittu perustuen heidän empiiriseen tietoonsa aiheesta. VAHTI Sovelluskehityksen tietoturvaohjeen ja sen lähteiden sisältämän teorian perusteella voidaan määrittää lähtötilanteessa esitettyyn asiaongelmaan ratkaisumalleja, joten tutkimus on vahvas-

ti teorialähtöinen (Kananen 2008, 22). Tutkimus esittää teoriaosuudessa paitsi taustaa tietoturvallisuuteen liittyviin ongelmiin, myös mahdollisia ratkaisuja yksittäisten vaatimusten täyttämiseksi juuri tässä kontekstissa. Tutkimus on kiinnostunut prosessista, sen kehittämisestä, tiedon lisäämisestä ja ihmisten käsitysten kartoittamisesta, joten tutkimusmenetelmä on kvalitatiivinen. Laadullisen tutkimuksen haastattelun kyllääntymispisteen saavuttamiseksi haastatteluun otetaan mukaan henkilöitä eri projekteista mahdollisimman paljon sekä johtavasta asemasta että itse työn ammattilaisista.

2.3 Tutkielman rakenne

Teoriassa käsitellään alihankintana suoritettavaa ohjelmistoprojektia ja erityisesti julkishallinnon projekteja. Lisäksi käsitellään ketterää sovelluskehitystä ja erityisesti scrum-mallia. Teoriassa kerrotaan myös tietoturvasta, tietoturvallisesta sovelluskehityksestä ja tietoturvatestauksesta. VAHTI Sovelluskehityksen tietoturvaohje jakaa määrittämänsä vaatimukset kahteen osa-alueeseen: hallinnollisiin ja sovelluskehitykseen liittyviin vaatimuksiin. Koska tutkielman tavoitteena on kehittää toimittajan roolissa olevan alihankkijan projektikäsikirjaa, on vaatimukset jaettu tässä tutkielmassa kolmeen osaan: asiakasorganisaation vastuulla oleviin, projektiorganisaation vastuulla oleviin ja kehitystiimin vastuulla oleviin. Tietoturvallisuus lähtee organisaation tasolta, ja yksittäisen projektin tietoturva on vain osa sitä. Teoriaosuus jakautuu näihin kolmeen osaan, joista suositellaan lukemaan ainakin omaan sidosryhmään kuuluvat luvut. Haastatteluissa keskityttiin projektiorganisaation ja kehitystiimin vaatimuksiin ja niiden toteuttamiseen. Tuloksena esitellään muutokset projektikäsikirjaan ja prosessiin alihankintaprojektissa, mutta sivutaan myös organisaatioanaalisia vaatimuksia, joiden täyttäminen on yhtä tärkeää.

2.4 Tutkimuskysymykset

Tutkimuksen tavoitteena on lisätä tietoa tietoturvallisesta sovelluskehittämisestä. Halutaan ymmärrys siitä, mitä tietoturvavaatimusten huomioiminen sovelluskehityksessä vaatii sekä asiakkaan että toimittajan näkökulmasta. Tutkielman teoriaosuudessa, luvuissa 3, 4 ja 5 vastataan kysymykseen:

1. Mitä tietoturvan huomioiminen tarkoittaa ohjelmistokehitysprojektissa?

Jos nykyinen prosessi ottaa huomioon tietoturvan, toimitaanko todella näin? Tähän kysymykseen vastataan tutkimalla nykyistä projektikäsikirjaa ja haastatteluiden avulla. Tässä kysymyksessä pyritään selvittämään jo nykyisessä prosessissa olevat hyvät käytänteet.

2. Miten yrityksen nykyinen prosessi huomioi VAHTI Sovelluskehityksen tietoturvaohjeen vaatimukset?

Toimeksiantaja on jo nyt ottanut VAHTI Sovelluskehityksen tietoturvaohjeen vaatimukset huomioon yhdessä projektissa, vaikka vakiintunutta prosessimallia niiden toteuttamiselle ei ole olemassa. Tähän halutaan muutos, ja siksi tutkielman soveltava osa käy läpi kaikki tietoturvavaatimukset, käsittelee niitä haastattelujen ja teorian pohjalta sekä ehdottaa, miten kyseessä oleva vaatimus voidaan toteuttaa. Tutkielman soveltavassa osassa vastataan tutkimuksen pääkysymykseen:

3. Miten yrityksen prosesseja tulisi muuttaa, jotta ne vastaisivat VAHTI Sovelluskehityksen tietoturvaohjeen vaatimuksia?

2.5 Aikaisempi tutkimus aiheesta

Varsinainen VAHTI 1/2013 Sovelluskehityksen tietoturvaohje ei ole vielä ollut tutkimuksen kohteena uutuutensa vuoksi, mutta VAHTI-ohjeista on tehty tutkimusta aikaisemminkin. Merkittävin tämä tutkielman kannalta, VAHTI-ohjeisiin liittyen, on Lauri Hämäläisen (2007) tekemä tutkimus, jossa hän vertailee ja yhdistelee British Standards Instituten 7799, VAHTI-tietoturvaohjeiden ja the IT Infrastucture Libraryn prosessikuvauksia. Tutkimuksen kohteena on Hämeen ammattikorkeakoulun organisaation tietoturvallisuuden kehittämishanke, jossa tehdään riskianalyysi, tietoturvan kartoitus ja kehittämissuunnitelma. (Hämäläinen 2007, 1.) Tämä tutkimus on lähellä tätä tutkimusta, mutta tämän tutkimuksen tavoitteen on kehittää nimenomaan sovelluskehityksen tietoturvaa.

Jari Råman (2006) on tehnyt väitöskirjan aiheesta tietoturvallisen sovelluskehityksen sääntely (Regulating Secure Software Development), joka on erittäin lähellä tätä tutkielmaa, sillä tavoitteena on parantaa tietoturvallista kehittämistä ottaen huomioon muun muassa VAHTI-tietoturvaohjeet. Råman määrittää, että valtion virastojen tai ministeriöiden asetukset ovat juuri tämän kaltaista säätelyä sovelluskehityksen to-

teuttamiseen (Råman 2006, 27). Tästä on hyvänä esimerkkinä Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa (681/2010), joka säätää yleisistä tietoturvavaatimuksista, asiakirjojen luokittelusta ja niiden käsittelystä (Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa 2010).

Tietoturvan ja tietosuojan kehittämisestä pilviteknologiassa on Vesa Lehtinen (2010) tehnyt pro gradu -tutkielman, joka sivuaa tätä tutkielmaa ja toimii hyvänä lähtökohtana laadullisesta tutkielmasta tietoturvallisuuden aihealueelta. Lehtinen keskittyy käsittelemään aihetta tietojenkäsittelystandardien ja -kehitysmallien avulla ja toteaa niiden määrittämisen ja käyttämisen vähentävän tietoturvan ja tietosuojan pettämisen riskejä. (Lehtinen 2010, 80−81.)

3 Tietoturvallisuus organisaatiossa

Tässä luvussa keskitytään VAHTI Sovelluskehityksen tietoturvaohjeen vaatimusten täyttämiseen organisaation tasolla ja tietoturvallisuuden toteuttamisen haasteisiin ennen varsinaisen hankkeen aloittamista ja sovelluskehitysprosessin aikaisia toimia tietoturvallisuuden edistämiseksi. Tämä luku antaa tietoa tietoturvallisuudesta vastuussa oleville henkilöille organisaation tietohallinnossa ja projektiorganisaatioissa työskenteleville henkilöille. On selvää, että suuri osa tietoturvallisuudesta tulee toteuttaa organisaation tasolla, koska tietoturvallinen sovellus ei pysty suojaamaan tietoja ilman turvallista ympäristöä. Organisaation tason tietoturvavaatimukset on toteutettava sekä asiakasorganisaation (mahdollisesti julkishallinnon) sekä toimittajaorganisaation toimesta. Lisäksi kun toimittajaorganisaatiossa toteutuvat nämä vaatimukset, on sovelluskehitysprojektin aikaisia vaatimuksia helpompi toteuttaa.

3.1 Tietoturvallisuus

Tietoturvallisuudella tarkoitetaan sitä toimintaa, jossa suojataan ja varmuuskopioidaan tietoja ja palveluita sekä ohjataan järjestelmien ja tietoliikenneyhteyksien riskienhallintaa (VAHTI 5/2009, 9). Tietoturvallisuuden tarkoitus on suojata tiedon luottamuksellisuutta, eheyttä, saatavuutta ja jäljitettävyyttä. Luottamuksellisuus tarkoittaa sitä, että tietoon on pääsy vain siihen oikeutetuilla henkilöillä (VAHTI 1/2013, 15). Luottamuksellisuus on se tiedon ominaisuus, joka kertoo tiedon salaamisen tärkey-

destä sen tallennuksen, prosessoinnin ja siirron aikana (Kumar & Bhargav 2011). Luottamuksellisuuden menetys tapahtuu, kun henkilö tarkoituksellisesti pääsee käsiksi tietoihin ilman valtuutusta tai ylittää hänelle annetut valtuudet tiedon näkemisen suhteen (Kouns & Minoli 2010). Luottamuksellisuus menetetään esimerkiksi, kun henkilö pystyy tarkastelemaan toisen käyttäjän henkilökohtaisia tietoja, joita toinen ei ole jakanut julkiseksi.

Eheydellä tarkoitetaan tiedon muuttumisen hallintaa, jotta sen tahaton tai hyökkäyksestä johtuva muuttuminen on estetty tai ainakin heti havaittavissa (VAHTI 1/2013, 15). Tiedon eheyden menetys tapahtuu, kun itse järjestelmää tai sen tietoa on muutettu tai poistettu ilman valtuuksia tahattomasti tai tahallisesti. Virukset voivat muokata sovelluskoodia haavoittuvuuden paljastamiseksi järjestelmässä. Tällöin sovelluksen eheys on menetetty. (Kouns & Minoli 2010.) Vakava tiedon eheyden menettämiseen johtava haavoittuvuus on esimerkiksi se, jos käyttäjä pystyy poistamaan toisen käyttäjän tietoja ainoastaan tietämällä URI:n (Uniform Resource Identifier), mihin lähettää pyyntö. Tämä on mahdollista, jos sovellus ei tarkasta käyttäjän valtuuksia joka pyynnön yhteydessä.

Tiedon pitää olla aina tarvittaessa saatavilla (VAHTI 1/2013, 15). Saatavuudessa on ongelmia, jos sovelluksen lailliset valtuutetut käyttäjät estyvät pääsemästä sovellukseen tai sen tietoihin käsiksi väliaikaisesti ja luotettavasti. Verkkosivustolle voidaan tehdä hajautettu palvelunestohyökkäyshyökkäys (Distributed Denial-of-Service), jolloin sovelluspalvelin ei pysty ottamaan vastaan sen todellisten käyttäjien palvelupyyntöjä suuren turhien pyyntöjen määrän vuoksi. (Kouns & Minoli 2010.) Jäljitettävyys tarkoittaa kaikkien järjestelmässä tehtyjen toimenpiteiden selvitettävyyttä, josta selviää mitä, kuka ja milloin ko. toimenpide on tehty (VAHTI 1/2013, 15).

Näihin tiedon ominaisuuksiin liittyviin ongelmiin voi olla syynä rauta- tai ohjelmistovika, ulkopuolinen luonnollinen ilmiö, tahallinen, piittaamaton käytös tai tahaton onnettomuus (VAHTI 5/2009, 9). Tietoturvallisuuden taso täytyy määrittää tiedon luottamuksellisuuden mukaan ja löytää tasapaino perustuen riskiarvioihin. Esimerkiksi maanpuolustuksen kannalta kriittisen tiedon luottamuksellisuuden turvaaminen on sen saatavuutta ja eheyttä tärkeämpää. (Kumar & Bhargav 2011.)

Sovellusten tietoturvallisuuden toteutuksen tarve on muuttunut julkisten verkkojen ja pilvipalveluiden myötä organisaatioissa. Aikaisemmin sovelluksen tietoturvasta ja pääsystä huolehti sisäverkon rajaava palomuuri. Nykypäivänä jokaisen sovelluksen pystyttävä huolehtimaan omasta tietoturvallisuudestaan, sillä ne saattavat olla näkyvissä julkiseen verkkoon ja alttiina hyökkäyksille. (VAHTI 1/2013, 11.)

Tietoturvallisuudesta on säädetty myös laissa, ja sovelluskehityshankkeissa mukana olevien organisaatioiden, mukaan lukien asiakas- ja toimittajaorganisaatioiden, on oltava kulloinkin perillä niiden toimintaa ja sovelluskehitystä koskevista laeista, asetukista ja muista vaatimuksista. Jokaiselle sovellukselle voi olla sen käyttötarkoitukseen liittyviä vaatimuksia, joiden toteutuminen on varmistettava jo suunnitteluvaiheessa sekä itse kehityksen aikana. (VAHTI 1/2013, 15.) Muun muassa Arkistolaki (831/1994), Henkilötietolaki (523/1999), Perustuslaki (731/1999) ja Laki yksityisyyden suojasta sähköisessä viestinnässä (516/2004) ottavat kantaa tietoturvallisuuteen (VAHTI 5/2009, 10).

3.2 Riskienhallinta

Riskienhallinta on jatkuva prosessi (Kouns & Minoli 2010). Sitä tulee suorittaa koko projektin ajan säännöllisin väliajoin ja jokaisessa sovelluksen elinkaaren aikana esitutkimuksesta ja käytöstä poistoon. Kouns & Minoli (2010) määrittävät, että organisaation on oltava tietoinen siitä,

- mitä IT-resursseja ja omaisuutta sillä on koko liiketoiminnan laajuudella
- miten niitä kaikkia käytetään ja
- kuka ja miten niihin voisi mahdollisesti hyökätä.

Valmista riskienhallinnan ratkaisua ei ole olemassa yritysten liiketoimintojen ja omaisuuden erojen takia. Tästä syystä riskienhallinta tulee aina tehdä nimenomaan sille organisaatiolle, jonka liiketoiminnasta on kyse. Hyväksi todettuja toimintamalleja ja ohjeita kannattaa käyttää, mutta yleisellä tasolla tehty riskiarvio on turha ja jättää paljon yrityksen liiketoiminnalle ominaisia riskejä arvioimatta. (Hämäläinen 2007, 32.)

Haavoittuvuudet ja uhat

Haavoittuvuus on turvallisuudessa oleva heikkous, jota voidaan mahdollisesti käyttää hyväksi (Kumar & Bhargav 2011). Tällainen heikkous voi olla esimerkiksi salasanojen lähettäminen suojaamattomana verkon yli. Tämä itsessään ei altista kirjautumistietoja vahingossa kolmansille osapuolille, mutta jättää vahingollisille tarkoituksille keinon saada tiedot. Hyökkääjä voi käyttää huonoa suunnittelua hyväkseen ja tunkeutua järjestelmään ilman lupaa. Hyökkääjä on siis uhka tietojärjestelmän turvallisuudelle, koska se voi tunnistaa haavoittuvuuden ja mahdollisesti käyttää sitä hyväkseen. Uhkia voivat olla mitkä tahansa tekijät ihmisistä ja eläimistä aina luonnonmullistuksiin ja metallin ruostumiseen. (Kumar & Bhargav 2011.)

Riski

Riski on määrällinen arvo mahdollisesta haitasta, jonka aiheuttaa uhka, haavoittuvuus tai jokin tahallinen tai tahaton tapahtuma. Riski on se haitta, joka koituu tapahtumasta, joka altistaa jonkin organisaation omaisuuden (palvelu, data, laitteet, palvelimet jne.) vaaraan. (Kouns & Minoli 2010.) Riski on uhkakuvan ja haavoittuvuuden tuotos, joten ilman jompaakumpaa ei ole olemassa riskiä. Jos uhka ei ole tiedossa, ei mahdollinen haavoittuvuus ole riski tai se on olematon, koska emme tiedä, miten sitä voisi hyväksikäyttää ja aiheuttaa tietoturvallisuuden heikkenemisen. (Kumar & Bhargav 2011.)

Sama pätee haavoittuvuuden suhteen, eli ilman tiedossa olevia haavoittuvuuksia eivät mahdolliset uhkaavalta vaikuttavat vihamieliset toimijat ole suuri riski. Loppujen lopuksi haavoittuvuuden hyväksikäytöstä johtuva haitta tarvitsee tahattoman tai tahallisen tapahtuman toteutumisen. Esimerkiksi ohjelmoija voi epähuomiossa jättää sovellukseen haavoittuvuuden, joka altistaa sen tietojen pääsemisen tahoille, joiden ei pitäisi niitä nähdä. Tässä tapauksessa ei ole tehty tahallista hyökkäystä, mutta tietoturvallisuuteen on tullut vakava aukko. Suora hyökkäys organisaation palvelimia, verkkosivuja tai muuta infrastruktuuria kohtaan on tahallinen, josta voi aiheutua myös tietoturvallisuuden heikkeneminen. (Kouns & Minoli 2010.)

Riskienhallintaprosessi

Riskienhallintaprosessista löytyy viisi vaihetta, joita toistetaan jatkuvasti. Ne ovat (Kouns & Minoli 2010):

- Riskien tunnistaminen
    1. Mitä omaisuutta organisaatio pyrkii suojelemaan?
    2. Mistä organisaatio on huolissaan?
    3. Miten uhat voisivat toteutua? Haavoittuvuudet?
    4. Mitkä seikat jo nyt vähentävät riskiä?
- Arviointi
    1. Mikä vaikutus riskin toteutumisella on organisaatiolle?
    2. Miten todennäköisiä riskit ovat?
- Torjuntatoimenpiteiden määritys
    1. Mitä uusia keinoja riskien minimoimiseksi tarvitaan?
- Torjuntatoimenpiteiden toimeenpano
    1. Miten torjuntatoimenpiteet voidaan parhaiten toteuttaa?
- Toimenpiteiden tehokkuuden arviointi
    1. Toimivatko torjuntatoimenpiteet?
    2. Onko mahdollista vaihtaa torjuntatoimenpide toiseen riskin pienentämiseksi?

3.3 Tietoturvallisuuden osa-alueet

Tietoturvallisuus koostuu useista osa-alueista, jotka pitää ottaa huomioon organisaation tietoturvapolitiikassa, ei ainoastaan sovellusten uuskehityksessä. VAHTI 9/2008 Hankkeen tietoturvaohje (21−28) määrittää tietoturvan osa-alueet seuraavasti:

- Hallinnollinen turvallisuus
- Yritys- ja henkilöstöturvallisuus
- Tietoaineistoturvallisuus
- Fyysinen turvallisuus
- Ohjelmistoturvallisuus
- Tietoliikenneturvallisuus
- Laitteistoturvallisuus

- Käyttöturvallisuus

Hallinnollinen turvallisuus

Hallinnollinen tuvallisuus koostuu määrittelystä, kuten turvallisuusluokka ja toiminnalliset tietoturvavaatimukset, riskienhallinasta ja organisoinnista. Hankkeella on aina turvallisuusluokka tai se on julkinen. Turvallisuusluokat ovat seuraavat matalimmalta tasolta korkeimpaan: käyttö rajoitettu, luottamuksellinen, salainen ja erittäin salainen. Hankkeessa käsiteltävien tietojen luottamuksellisuusmäärittely määrää hankkeen turvallisuusluokan, koska luokan on vastattava tietojen luottamuksellisuuden tasoa, jotta tietoja voidaan käsitellä turvallisesti. Jos hankkeessa täytyy käsitellä korkeamman turvallisuusluokan tietoja, pitää niille soveltaa tiukempia käsittelysääntöjä tai jättää ne käsittelemättä kyseessä olevassa hankkeessa. (VAHTI 9/2008, 21.) Tietoturvariskien hallinta on jatkuva toimenpide, eikä sitä voi tehdä tyhjentävästi projektin alussa.

Tietoturvallisuuden hallinnoinnissa on tärkeää vastuuttaa se selkeästi avainhenkilöille. Hankkeesta vastaava päällikkö on vastuussa tietoturvallisuudesta kokonaisuudessaan. Hän suunnittelee vastuutuksen, vastuuhenkilöiden ohjeistuksen, heidän koulutuksensa ja valtuutuksen tietojenkäsittelyyn. Hankkeen ohjausryhmä hyväksyy suunnitelman ja vastuutuksen. (VAHTI 9/2008, 23.) Tällä tavalla varmistetaan sekä valmiin sovelluksen tietoturvallisuus, että koko projektin aikaisen tietoturvallisuuden toteutuminen. Vastuutetuilla avainhenkilöillä on oltava perustuntemus tietoturvallisuudesta. Useiden toimittajien ja sidosryhmien projekteissa tietoturvallisuuden toteutumisen valvontavastuu on tilaajalla. (VAHTI 1/2013, 19−20.)

Vastuut tulee jakaa pyrkien välttämään vaarallisten työtehtäväyhdistelmien syntyminen. Tällaisia ovat esimerkiksi samanaikaisesti käyttäjä-, sovelluskehitys-, testaus- ja tuotantotehtävissä toimivat henkilöt. Pienissä organisaatioissa tätä ei aina voida välttää, mutta tällöin täytyy tehdä riskianalyysi, arvioida riskin suuruutta ja suunnitella mahdollisia toimenpiteitä riskin pienentämiseksi. Erittäin tärkeää on kuitenkin erottaa sovelluskehitys ja järjestelmätestaus, jossa tarkastetaan toiminnallisuudet ja tietoturvallisuusvaatimusten vastaavuus määrittelyyn. (VAHTI 1/2013, 20.) Dokumentin tai ohjelmakoodin laatija voi arvioida omaa koodiaan toisen ohjelmoijan kanssa pa-

riohjelmointina. Kun koodikatselmointeja tehdään, tulee katselmoijana toimia jonkun muun henkilön kuin ohjelmoijan itse. (Kumar & Bhargav 2011.)

Yritys- ja henkilöstöturvallisuus

Pitkissä hankkeissa ja yhteistyötoiminnassa on hyvä laatia puolustusvoimien yritysturvallisuussopimusmenettelyn tyylinen yritysturvallisuussopimus. Koko julkishallinnon ulkopuolisesta henkilöstöstä tulee laatia hankkeessa käsiteltävän tiedon turvatason mukaan suppea tai perusmuotoinen turvallisuusselvitys. Kaikkien hankkeeseen osallistuvien tulee allekirjoittaa Hankkeen tietoturvaohjeen (8/2009) liitteen 3 mukainen vaitiolositoumus. Hankkeesta tiedottaminen ulkopuolisille on hankepäällikön vastuulla, eikä kenenkään muun tulisi sitä suorittaa. Hankepäällikkö myös vastaa turvallisuusselvityksistä ja vaitiolositoumusten allekirjoituksesta. Kaikkia materiaaleja tulee käsitellä niiden turvatason mukaisesti kuljettamalla niitä julkisissa paikoissa suojattuna. (VAHTI 8/2009, 25−26.)

Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan sitä, että kaikelle hankkeessa käsiteltävälle ja sen seurauksena tuotettavalle tietoaineistolle tulee asettaa tietoturvallisuusluokitus eli turvataso. Tietoaineiston tuottaja määrittää luokituksen ja hankkeen hankepäällikkö tarkastaa ja vahvistaa luokituksen mahdollisten ali- tai yliarviointien varalta. Turvallisuustaso tulee määrittää kulloinkin voimassa olevan käytännön mukaisesti, ja jos tietoaineistoa ei merkitä lainkaan, se on julkinen. Tämä julkisuus pitää huomioida kaikkien hankkeessa olevien. Materiaalia tulee säilyttää luokittelun mukaisessa paikassa ja kuljettaa asianmukaisesti. Salaisten ja erittäin salaisten materiaalien käsittely tulee määrittää erikseen. (VAHTI 9/2008, 26.)

Fyysinen turvallisuus

Fyysinen tuvallisuus on tarkoittaa tilojen ja tietojen suojaamista luvattomalta tarkastelulta ja pääsyltä, kuten murtovarkailta tai terroristeilta. Esimerkiksi pankissa on korkea fyysinen turvallisuustaso pankkiholviin, joka on suojattu vartioilla, pääsynvalvonnalla, vahvoilla seinillä ja kameroilla. (Kumar & Bhrgav 2011.) Samaa periaatetta täytyy noudattaa hankkeen tietojenkäsittelyssä ottaen huomioon tietojen tietoturvatason. Jotta hankkeessa ja valmiissa sovelluksessa käsiteltävät tiedot eivät päädy ul-

kopuolisten haltuun, tulee tilojen suunnittelussa ottaa huomioon äänieristys, näkösuoja, kuluvalvonta ja murtosuojaus (VAHTI 9/2008, 27).

Ohjelmistoturvallisuus

Sovellukset ja tietokannat ovat helppoja hyökkäyskohteita, koska nykyään ne ovat vielä suoraan yhteydessä Internetiin, eikä niitä välttämättä suojaa sisäverkon palomuuri. Tästä syystä niiden on pystyttävä puolustautumaan hyökkäyksiä vastaan. Ohjelmistoturvallisuudessa on kaksi puolta: konfiguraatio ja ohjelmistokehitys. Ohjelmistoturvallisuudessa täytyy ottaa huomioon ohjelmiston ja sen riippuvuudet (kuten rajapinnat toisiin sovelluksiin ja tietokannat) sisältävän infrastruktuurin konfiguraatio. Esimerkiksi sovelluspalvelimen ja tietokantapalvelinten konfiguraation tarkastaminen on tärkeää. Se tarkoittaa konfiguraation jatkuvaa päivittämistä, tarpeen mukaista riittävää salasanasuojausta palvelinten käyttäjille, ylimääräisten palveluiden käytöstä poistoa palvelimella, vain tarvittavien palveluiden aktivointia ja sovellusten, laitteiden ja palvelinten lokien kirjoituksen aktiivisuuden varmistamista. Tämä on erittäin tärkeä osa tietoturvallisuutta, koska yksikään tietoturvallinen ohjelmisto ei mahda mitään huonolle infrastruktuurin tietoturvalle. Toinen puoli on ohjelmistokehitys, joka menee myös käsi kädessä konfiguraation kanssa, mikä tarkoittaa, että hyvin konfiguroitu palvelin ei auta itse ohjelmiston ollessa heikosti suojattu. (Kumar & Bhrgav 2011.) Tähän puoleen paneudutaan tarkemmin luvussa viisi.

Hankkeen tietoturvaohjeen (9/2008) mukaan julkishallinnon hankkeissa tulee käyttää organisaatioiden sopimia lisensoituja ohjelmistoja. Avoimen lähdekoodin ohjelmistojen käytöstä tulee sopia erikseen, mutta kaikkien ohjelmistojen täytyy olla ylläpidettyjä ja tietoturvapäivitettyjä. Sähköisten dokumenttien käsittelyssä ei saa käyttää suojausta, jossa muokkaus- ja käsittelysalasana on vain dokumentin laatijan hallussa.

Tietoliikenne- ja laitteistoturvallisuus

Sähköpostiviestinnässä tulee ottaa huomioon sähköpostiliikenteen ja itse viestin salaaminen valtiohallinnon käyttöön hyväksytyillä menetelmillä, kuten tiedostojen pakkaamisella itsepurkautuviksi paketeiksi. Sähköpostin käytön sijaan tulisi tiedostojen jakoon olla tietoturvallinen sähköinen ryhmätyötila, jonka turvallisuutta voidaan valvoa. Laitteistoturvallisuudesta jokaisella organisaatiolla tulee olla tietoturvaohjeistus. (VAHTI 9/2008, 27−28.)

Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan yrityksen tietojärjestelmiin tehtävien etäyhteyksien sekä yhteydessä käytettävien laitteiden ja suojausmekanismien turvallisuuden varmistamista. Keskeisiin järjestelmiin tulee välttää myöntämästä etäkäyttömahdollisuutta kokonaan. Jos tämä on erityisestä syystä tehtävä, tulee etäyhteyteen tarkoitettu tietokone olla asetettu vain tähän tarkoitukseen ja sen on vastatta tietoturvatasoltaan kohdejärjestelmän tasoa. Tunnistautumis- ja salausmenettelyn tulee olla tietoturvatason mukaiset. Käyttöturvallisuuteen liittyvät tietojärjestelmien käytön kaikki normaalit operointi- ja hallintatoimet on koulutettava työntekijöille. (VAHTI 5/2004, 90−91.)

3.4 Miksi web-sovellusten tietoturvallisuus on tärkeää?

Organisaatiot ottavat web-sovelluksia Internetin yli käyttöön enenevissä määrin joka vuosi, kun ne huomaavat niiden tuomat hyödyt. Aikaisemmin arkaluontoiset tiedot käsiteltiin varmasti suljetun verkon puolella. Nyt yhä useammin tietoturvaluokiteltua tai muuta arkaluontoista tietoa liikutellaan suurten ja pienten organisaatioiden eri maantieteellisten paikkojen välillä Internetin yli. Tällaisia tietoja ovat yksityöhenkilöiden luottokortti- ja henkilötiedot, yritysten verotus tai muut taloudelliset tunnusluvut. (Kumar & Bhargav 2011.)

Web-sovellusten kehittämisestä on tullut vuosien saatossa entistä helpompaa ja nopeampaa. Uudet sovelluskehykset mahdollistavat sovellusten kehittämisen ja käyttöönoton nopeasti ja ketterästi kirjoittamatta paljoa uuttaa koodia. Organisaatioiden hankkeiden aikataulut myös sanelevat kehityksen nopean läpiviennin, jolloin sovelluskehysten ja ulkoisten kirjastojen käyttöä suositaan ymmärtämättä välttämättä nopeuden ja tietoturvallisuuden suhdetta. Kun käytetään ulkoisia kirjastoja, pitää tietoturvallisuuden toteuttamisen olla viime kädessä kehittäjällä, sillä joskus sovelluskehysten tietoturvallisuudesta ei ole taetta. (Kumar & Bhargav 2011.)

Moni ei ymmärrä tietoturvallisen ohjelmiston kehittämisen olevan halvempaa kuin sen laiminlyönnin. Tietoturvallisten ohjelmointikäytänteiden, koodikatselmointien, haavoittuvuusanalyysien ja muiden tietoturvallisuuteen liittyvien työvaiheiden toteuttaminen ohjelmistoprojektissa voi olla kallista, mutta niiden hinta on pieni ver-

rattuna siihen kustannukseen, joka koituu, kun haavoittuvuutta käytetään hyväksi ja arkaluontoista tietoa pääsee ulkopuolisten käsiin. Haavoittuvuuden korjaamisen ollessa jälkikäteen kallista, voidaan yritykset tuomita maksamaan myös tuntuvia sakkoja tietoturvallisuuden laiminlyönnistä hyökkäyksen tapahtumahetkellä. Tietoturvallisuuden parantaminen vahingon jälkeen ei enää korjaa yrityksen mainetta, ja sen menetys tulee erittäin kalliiksi menetettyjen asiakkaiden kautta. Brändin arvon huomaa parhaiten, kun se on menetetty, ja tämän pitäisikin olla yksi suurimmista motivaation lähteistä tietoturvalliselle sovelluskehitykselle. (Kumar & Bhargav 2011.)

3.5 Tietoturvallisuuden toteuttamisen haasteet

Selaimen tietoturvallisuus

Web-sovellusten tietoturvaan vaikuttaa merkittävästi käytettävä selain ja sen turvallisuustaso. Selaimia on monia, eikä niitä voida kaikkia tukea. Lisäksi myös suosituimmissa selaimissa tulee tietoturva-aukkoja esille jatkuvasti. Vaikka itse selaintoimittaja huolehtisikin tietoturvapäivityksistä, voi jokin selaimessa oleva lisäosa tai liitännäinen sisältää tietoturva-aukon. Selain voi sisältää tietoturvallisuutta parantavia ominaisuuksia, kuten Cross-site scripting (XSS) -esto, joka tunnistaa mahdollisesti haitallista JavaScript-koodia web-sivulta estäen sen suorittamisen. Selain ei voi luottaa web-sivun turvallisuuteen sataprosenttisesti, mutta toisaalta myös selain voi olla saastunut eikä web-sovellus voi luottaa kaikkien sen käyttäjien selainten turvallisuuteen. Tästä syystä web-sovelluksen täytyy minimoida riskit, jotka voivat johtua niin sanotuista hyökkääjistä selaimessa (man-in-the-browser), vaikka täydellistä kontrollia ei voidakaan toteuttaa. (Kumar & Bhargav 2011.)

Toimittajan vastuu ja sovelluskehityksen elinkaari

Vaikka käytetään vapaan lähdekoodin tai muita mahdollisia ulkopuolisia kirjastoja, on web-sovellusten tietoturvallisuuden toteuttaminen toimittajan vastuulla (Kumar & Bhargav 2011). Tietoturvallisuuden varmistaminen jätetään liian usein elinkaaren loppuvaiheeseen ulkopuoliselle toimijalle tietoturva-auditointiin ymmärtämättä, että kaikki piilevät haavoittuvuudet eivät tule esiin tällä toimintatavalla (VAHTI 1/2013, 18). Sovelluksen tilaaja eli asiakas on kuitenkin loppukädessä vastuussa tietoturvallisuudesta sen omassa organisaatiossa, ja sen täytyy ottaa asia huomioon ohjelmiston elinkaaren joka vaiheessa suunnittelusta ylläpitoon vaatien tietoturvallisuutta toimit-

tajalta. Monet yritysten käyttämät ohjelmistokehityksen elinkaarimallit eivät ota automaattisesti huomioon tietoturvallisuutta. Tietotuvallisuutta ei rakenneta kehityksen aikana, vaan se pitää suunnitella jo ennen sitä. Myös testaus keskittyy toiminnallisuuden testaamiseen ja tietoturvallisuuden osa-alueet voivat unohtua, ellei niitä oteta jo aikaisemmissa elinkaaren vaiheissa huomioon. (Kumar & Bhargav 2011.)

Tietoturvallinen ohjelmistokehityksen elinkaari edellyttää riskiarviointia ennen kehityksen aloittamista ja jokaisen sovellukseen tehtävän muutoksen yhteydessä. Koodikatselmoinnit tietoturvan varalta ja tietoturvallisuuden arviointi sekä haavoittuvuuksien korjaaminen ovat osa elinkaarta. Kaikkien muutoksien koodiin ja määrittelyyn täytyy mennä muodollisen muutoksenhallinnan kautta ja hyväksyttää projektipäällikköllä tai vanhemmalla kehittäjällä projektissa, jotta vastuuvelvollisuus on taattu. (Kumar & Bhargav 2011.)

Tietoisuuden puute ja liiketoimintalähtöinen ajattelu

Kun uuskehitystä tehdään, keskitytään sovelluksen toiminnallisuuteen, koska näille toiminnoille on olemassa tarve ja niiden toteuttamiselle löydetään helposti taloudellinen liiketoiminnallinen hyöty. Sovelluksen päätoiminnallisuuden tai muun kriittisen osa-alueen epävakautta korjaamaan löydetään helposti resursseja. (Kumar & Bhargav 2011.) Tietoturvallisuuden puutetta taas ei nähdä esteenä sovelluksen julkaisemiselle, ja yleensä se nähdään väärin vain lisätyönä ja hidasteena kehitystyössä, koska se on sovelluksen ei-toiminnallinen ominaisuus (VAHTI 1/2013, 17).

Johto ei yleensä tajua tietoturvallisuuden tarvetta, ennen kuin ensimmäinen vahinko sattuu. Tämän jälkeen sille löytyy resursseja, vaikka se on jo myöhäistä. Tietoturvallisuus ei ole liikevaihtoa kasvattava ominaisuus, mutta sen puutteella voi olla merkittäviä taloudellisia seurauksia. Liiketoimintalähtöisyydestä johtuen myös kehittäjät keskittyvät toiminnallisuuksien toteuttamiseen tiukoissa aikatauluissa ja monesti eivät ole edes tietoisia web-sovellusten tietoturvallisuuden konsepteista tai käytännön toteuttamisesta. Tietoturvalliset ohjelmointikäytänteet, SQL-kyselyiden parametrisointi, lomakkeiden syötteiden tarkastukset (validointi) ja tietoturvallisuuteen liittyvien toimintojen lokimerkinnät ovat tärkeässä roolissa sovelluksen tietoturvallisuudessa. Ne on kuitenkin helppo jättää tekemättä, kun toiminto on jo kerran todettu toimivaksi. Organisaatiot eivät myöskään käytä aikaa ja rahaa kehittäjien tietotur-

vakoulutukseen, vaikka sillä olisi kauaskantoisia positiivisia seurauksia kaikissa projekteissa. (Kumar & Bhargav 2011.) Ohjelmointia ja sovelluskehityksen projektien läpivientiä opettavat oppilaitokset eivät myöskään ota huomioon tietoturvallisuutta osana opetussuunnitelmaa, jolloin uusien alalle tulevien ohjelmoijien tietoisuuden tietoturvallisuuden toteuttamisesta täytyy tulla organisaatiolta (VAHTI 1/2013, 17). He saattavat huomaamattaan tehdä virheitä, joiden havaitseminen on hankalaa.

Kehittäjät ja testaajat eivät ota huomioon mahdollisia hyökkäystilanteita, joita valmis sovellus mahdollisesti tulee kohtaamaan. Kehittäjien tulisi harrastaa niin sanottua defensiivistä ohjelmointia ja testaajien pyrkiä rakentamaan testitapauksia, joissa käyttäjällä on vahingolliset aikeet. Tiedossa olevien virhetilanteiden ja ennalta määrittelemättömien tilanteiden käsittely ja virheestä palautuminen on usein heikkoa. Sovellusten riskianalyysit jäävät usein tekemättä tai ne ovat puutteellisia. (VAHTI 1/2013, 18.) Vaikka tietoturvatestaus suoritettaisiinkin oikein ja se löytäisi ongelmia, on testausorganisaation ja johdon vastuulla arvioida haavoittuvuuksien vakavuus. Jos tietotaito ei riitä ongelmien vakavuuden arviointiin, on seurauksena haavoittuvuuksien vakavuuden yli- tai aliarviointi, joista kummassakin tapauksessa tulee ylimääräisiä kustannuksia. (Kumar & Bhargav 2011.) Tietoisuuden puutteeseen ja työntekijöiden asenteisiin voidaan vaikuttaa kouluttamisella.

Organisaatioiden vanhat järjestelmät ja rajapinnat

Organisaatioiden vanhat järjestelmät ovat suuri ongelma tietoturvallisuuden toteuttamisessa kokonaisuudessaan. Usein organisaatioiden sovellusalusta on kehitetty useita vuosia sitten, siitä on tullut massiivinen kokonaisuus, joka koostuu useista rajapinnoista toisiin sovelluksiin ja ulottuu mantereelta toiselle, ja sitä kehitettäessä ei ole otettu huomioon tietoturvallisuutta tai järjestelmän alasajoa uuden tieltä. Pääsynvalvonta, vahvat salasanat, kriittisten toimintojen lokimerkinnät ja tiedon salaus eivät olleet järjestelmää toteuttaessa suuressa roolissa. Monille yrityksille on mahdotonta siirtyä kerralla uuteen järjestelmään, koska vanhat järjestelmät sisältävät miljoonia rivejä asiakastietoja, joiden turvallinen siirtäminen voi tulla kalliiksi, ja se pitäisi hoitaa mahdollisimman lyhyellä katkolla, jotta liiketoiminta ei pysähtyisi. Näiden järjestelmien korvaaminen on haasteellista ja siirtymisen riskit ovat suuret eikä epäonnistuneisiin kokeiluihin ole varaa. (Kumar & Bhargav 2011.) Tietojärjestelmäympäristöt monimutkaistuvat jatkuvasti uusien rajapintojen, pilvipalveluiden käyttöön-

oton, uusien ohjelmointikielten ja verkon laajenemisen myötä. Tämä aiheuttaa haasteita tietoturvallisuudelle, koska tietojärjestelmän yhden komponentin toimittajan on mahdotonta huolehtia kokonaisturvallisuudesta. (VAHTI 1/2013, 18.)

3.6 Yhteenveto

Tietoturvallisuus on useiden toimenpiteiden summa. Absoluuttista tietoturvaa ei ole, vaan tietoturvallisuus on riskienhallintaan perustuvaa toimintaa. Riskienhallinta on jatkuva toimenpide ja riski on aina määrällinen arvio siitä vahingosta, jonka uhka ja haavoittuvuus aiheuttavat jonkin tapahtuman sattuessa. Tietoturvallisuus koostuu useista tekijöistä, ja sen tarkoitus on suojata tiedon luottamuksellisuutta, eheyttä, saatavuutta ja jäljitettävyyttä (VAHTI 1/2013, 15). Nykyisellään tietoturvasta huolehtiminen on siirtynyt sisäverkkojen palomuurien vastuulta jokaisen Internetiin yhteydessä olevan sovelluksen itsensä vastuulle.

Tietoturvallisuudessa organisaatiossa on useita osa-alueita, jotka pitää hallita erikseen. Näitä ovat muun muassa hallinnollinen, yritys- ja henkilöstö-, ohjelmisto- sekä tietoliikenne- ja laitteistoturvallisuus. Liitteessä 1 ovat organisaation toimintaan liittyvät vaatimukset kysymysmuodossa. Yhä useammin arkaluontoista tietoa liikutellaan julkisessa verkossa, joten kaikkien osa-alueiden on oltava kunnossa, mukaan lukien päätelaitteiden ja selainten. Usein tietoturvallisuuden heikkeneminen johtuu tietoisuuden puutteesta ja lyhytkatseisuudesta voittojen suhteen. Tietoturvallisuus nähdään usein kuluna, joka ei tuota voittoa suoraan, joten se jätetään huomiotta.

Jotta organisaatiolla olisi uskottava ja kypsä tietoturvallisuuden hallinta, tulee sen dokumentoida se tarkkaan. Vasta kun asiat kirjoitetaan ylös, niistä tulee selviä. Organisaation tasolla määritettävät asiat:

- Tietoturvallisuuspolitiikka (ks. Hämäläinen 2007, liite 2)
- Tietojärjestelmien käyttösäännöt (ks. Hämäläinen 2007, liite 3)
- Sähköpostin käsittelysäännöt (ks. Hämäläinen 2007, liite 4)
- Tietojärjestelmien ylläpitosäännöt (ks. Hämäläinen 2007, liite 5)
- Tietoturvapoikkeamiin reagoiminen (ks. Hämäläinen 2007, liite 6)
- Tiedottaminen poikkeamatilanteissa (ks. Hämäläinen 2007, liite 7)

4 Tietoturvallisuus alihankintaprojektissa

Koska VAHTI 1/2013 Sovelluskehityksen tietoturvaohje, kuten kaikki muutkin VAHTI-ohjeet, on laadittu julkishallinnon hankintoja silmällä pitäen, ja koska toimeksiantajalla on liiketoiminnallisia intressejä saavuttaa VAHTI-ohjeiden mukainen vaatimustaso. Tämän se haluaa tehdä voittaakseen julkishallinnon ICT-hankintojen toimittajaprojekteja itselleen. Siksi tässä luvussa on keskitytty erityisesti kyseessä oleviin projekteihin ja niiden vaatimaan prosessiin. Aluksi kerrotaan julkishallinnon hankinnoista, kilpailutuksen aikaiseen valintaan ja tietoturvallisuusvaatimuksiin pohjautuen VAHTI 9/2008 Hankkeen tietoturvaohjeeseen. Scrum-menetelmä käydään pääpiirteittäin läpi ketterän sovelluskehityksen esimerkkinä. Sen jälkeen keskitytään projektin aloittamiseen liittyviin VAHTI 1/2013 Sovelluskehityksen tietoturvaohjeen vaatimuksiin, kuten esitutkimukseen ja vaatimusmäärittelyyn.

4.1 Julkishallinnon hankintaprosessi

Julkiset hankinnat

Alihankinta tarkoittaa sellaista yhteistyötä, jossa yritys toimittaa toiselle yritykselle tai julkishallinnon organisaatiolle tuotteen osan, tuotteen valmistuksen työvaiheen tai jonkin palvelun, kuten koko sovelluskehitysprojektin (Antila 2012, 3). Julkisella hankinnalla tarkoitetaan sitä hankintalainsäädännössä (Laki julkisista hankinnoista 30.3.2007/348) määritellyn julkishallinnon organisaation tekemää tavara-, palvelu- tai rakennusurakkahankintaa, joka suoritetaan organisaation ulkopuolella. Nämä hankinnat tehdään hankintalainsäädännön ja EU-hankintadirektiivien menettelytapoja seuraten (Mitä julkiset hankinnat ovat? 2014).

Julkisten hankintojen tavoitteena on löytää julkishallinnon organisaation hankinnalle mahdollisimman taloudellinen vaihtoehto. Kilpailutus on läpinäkyvää, ja toimittajien valintakriteerit ovat tiedossa jo etukäteen. (Mitä julkiset hankinnat ovat? 2014.) Tämä koskee siis myös tietoturvallisuuteen liittyviä valintakriteereitä ja vaatimuksia. Sillä on merkittäviä vaikutuksia valittavaan toimittajaan, sillä halvin toimittaja ei välttämättä ole paras vaihtoehto, kun analysoidaan koko sovelluksen elinkaarta aina sen käytöstä poistoon saakka.

> *"62 §: Tarjouksista on hyväksyttävä se, joka on hankintayksikön kannalta kokonaistaloudellisesti edullisin hankinnan kohteeseen liittyvien vertailuperusteiden mukaan, tai se, joka on hinnaltaan halvin." (Laki julkisista hankinnoista 30.3.2007/348).*

Laki julkisista hankinnoista kuudeskymmenes toinen pykälä toteaa, että kokonaistaloudellisesti kannattavin tarjous tulee valita. Jos kaikki tarjouksen osa-alueet ovat kunnossa ja siinä on huolellisesti otettu huomioon myös tietoturvallisuuden toteuttaminen perusteluineen liiketoiminnan kannalta, voi hyväksytty tarjous olla vaikka kallein saaduista tarjouksista.

Julkisten hankintojen tarjouspyynnöt ja vaatimukset

Julkiset hankinnat on suoritettava kilpailutusprosessin määrittämien sääntöjen mukaan. VAHTI Sovelluskehityksen tietoturvaohje määrittää myös, mitkä tietoruvallisuuteen liittyvät vaatimukset täytyy sisällyttää jo tarjouspyyntöön mukaan. Hankkeen asettajan muodostama hankkeen ohjausryhmä hyväksyy, minkälaisia tietoturvallisuuden toteuttamisen periaatteita ja käytänteitä hankkeessa käytetään. Tämä tarkoittaa sitä, että tietoturvallisuuden toteuttaminen alkaa jo hankkeen alussa. Hankepäällikkö on vastuussa kokonaisturvallisuudesta hankkeen aikana. (VAHTI 9/2008, 16.)

Esitutkimuksen vaatimuksien tulee olla kunnossa jo tarjouspyyntövaiheessa, mutta toimittajan on hyvä tarkastaa muutama asia, etenkin jos se joutuu konsultoimaan asiakasorganisaatiota. Sovellukselle pitäisi olla määritetty sen tarkoitus, kriittisyys (ks. ESI-001) ja vaikutusanalyysi liiketoiminnan kannalta (ks. ESI-002). Onko vaaditut sovelluskehityksen karkean tason tietoturvavaatimukset listattu tarjouspyynnössä (ks. VTM-003)? Mikä on toteutettavan järjestelmän tietoturvallisuustaso (ks. VTM-004)?

Hankkeelle laaditaan VAHTI 9/2008 Hankkeen tietoturvaohjeen liitteen 1 mukainen tietoturvaohje, jossa on kuvataan muun muassa tietoturvallisuusperiaatteet, hankkeeseen liittyvät säädökset, hankkeen tietoturvataso ja tietoturvallisuuteen vaikuttavat tekijät hankkeen aikana. Asiakasorganisaatio myös arvioi ulkopuolisen toimittajan soveltuvuutta hankkeeseen tietoturvallisuusperiaatteiden toteutusmahdollisuuksien

mukaan. Ne ovat yksi keskeisistä valintakriteereistä ottaen erityisesti huomioon hankkeelle määritelty tietoturvataso. Lisäksi hankkeesta kirjoitetaan yritystason turvallisuussopimus ja mahdollisesti suoritetaan toimittajan auditointi. Kaikki hankkeeseen osallistuvat henkilöt tulee kouluttaa ja tiedottaa hankkeen tietoturvaohjeesta. Kun toimittaja on valittu, tulee tietoturvan ylläpidolle ja valvonnalle luoda toimintatavat toimittajaorganisaation kanssa. (VAHTI 9/2008, 18.)

Se, käytetäänkö hanke- vai projektitermiä, voi vaihdella organisaatiosta riippuen (VAHTI 1/2013, 19), mutta tästä eteenpäin tässä tutkielmassa käytetään pääasiassa termiä projekti.

Julkisia sovelluskehitysprojekteja ohjaavat lait ja säädökset

Vaatimusmäärittelyn perustason vaatimus VTM-002 edellyttää, että kaikki sovelluskehitykseen, kyseiseen projektiin ja kehitettävään järjestelmään liittyvät lainsäädännölliset seikat tulee huomioida. Toteutettavan sovelluksen tietoaineiston tietoturvatasot ja niiden suojaamiseen liittyvät seikat määritellään Julkisuuslaissa (JulkL 621/1999) ja Asetuksessa viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (JulkA 1030/1999). Tiedon saatavuudesta säätää Laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011). Kun käsitellään EU-lainsäädännön alaisia tietoja, tukeudutaan EU:n neuvoston päätökseen turvallisuussäännöistä 31.3.2011 (2011/292/EU). (VAHTI 1/2013, 69−70.)

Sovelluksen luonteesta riippuen tietojärjestelmään tallennetaan erilaisia tietoja, joista yleensä yksi ovat sen käyttäjät tai tietovarastoon tallennettavat muut henkilötiedot. Näiden tietojen tallennusta ja tietosuojaa säätelee Henkilötietolaki (523/1999). (VAHTI 1/2013, 69.) Tietojärjestelmään tallennettavista henkilötiedoista kannattaa tallentaa kuitenkin vain tarpeelliset tiedot, ja suunnittelun perustason vaatimus Salausratkaisut (SNT-013) määrittää myös, että luottamukselliseksi luokiteltavan tai salaisemman datan tallentaminen varmuuden varalta on kiellettyä. Tiedoille tulee aina olla käyttötarkoitus ja Henkilötietolain (523/1999) 10 § määrittää myös, että rekisteristä on laadittava rekisteriseloste, jossa tämä tarkoitus käy ilmi.

VAHTI 9/2008 Hankkeen tietoturvaohjeen liite 3 määrittää esimerkin vaitiolovelvollisuussitoumuksesta, joka viittaa lakeihin Laki työelämän tietosuojasta (759/2004) ja

Laki viranomaisten toiminnan julkisuudesta (JulkL 621/1999) 23 §, 24 §, 35 §. Lisäksi auditointeihin ja laadunvarmistukseen voidaan käyttää KATAKRI kansallista turvallisuusauditointikriteeristöä (VAHTI 1/2013, 70).

Tietoturvallisuuteen otetaan kantaa useissa laeissa. Näitä ovat muun muassa (Hämäläinen 2007, 76):

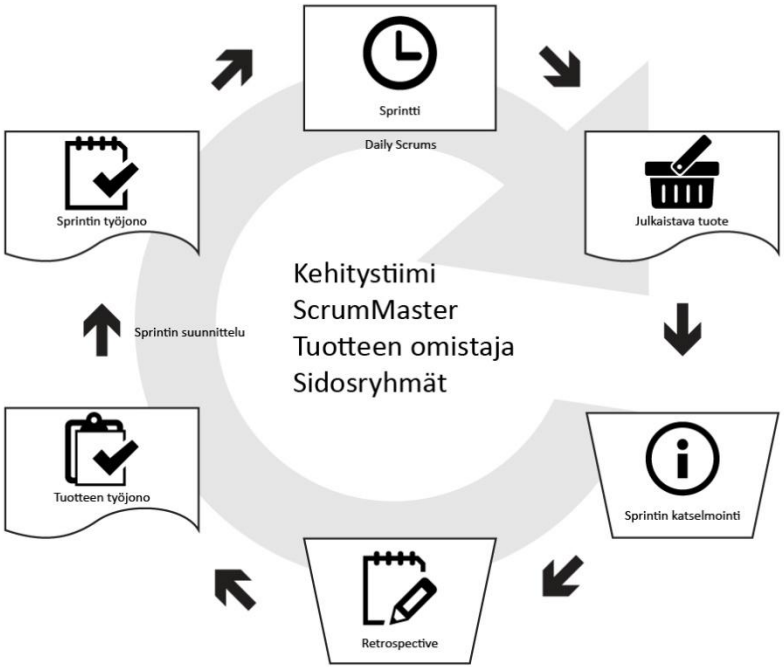
- Rikoslaki luku 38 Tieto- ja viestintärikoksista (39/1889)
- Suomen perustuslaki 10§ (731/1999)
- Valmiuslaki (1080/1991)
- Viestintämarkkinalaki (393/2003)
- Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)
- Henkilötietolaki (523/1999)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki eräiden suojausten purkujärjestelmien kieltämisestä (1117/2001)
- Laki tietoyhteiskunnan palvelujen tarjoamisesta (282/2002)
- Laki yksityisistä turvallisuuspalveluista (458/2002)
- Työturvallisuuslaki (738/2002)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki sähköisestä allekirjoituksesta (14/2003)
- Verkkotunnuslaki (228/2003)
- Sähköisen viestinnän tietosuojalaki (516/2004)
- Laki yksityisyyden suojasta työelämässä (759/2004)

Henkilöstön tietoturvaohjeen (4/2013) liite 1: Tietoturvallisuuteen keskeisesti liittyvät säädökset listaa myös tärkeimmät säädökset.

4.2 Scrum

Kehityksen rakenne

Scrum on ketterä inkrementaalis-iteratiivinen sovelluskehityksen menetelmä, jonka eri osaamisalueita yhdistelevää, yhteistä päämäärää tavoittelevaa kokoonpanoa verrattiin rugbyn scrum-muodostelmaan, josta se sai myös nimensä. Se esiteltiin ensimmäisenä Hirotaka Takeuchin ja Ikujiro Nonakan artikkelissa Harvard Business Revirew:ssä vuonna 1986. (Pham & Pham 2012.) Kehittäminen tapahtuu useiden iteraatioiden ketjuttamisesta, joista jokaisesta syntyy julkaistava tuote, eli kaikki iteraatioon määritellyt tehtävät saadaan valmiiksi sille varatussa ajassa. Scrumissa iteraatiota kutsutaan sprintiksi. Scrumissa on määritettyjä rooleja ja palaverikäytänteitä, jotka määrittävät kehityksen toimenpiteitä. (Shrimp & Rawsthorne 2009.) Scrumissa käytetyt termit tulevat Suomenkielisestä scrum-sanastosta (Eskelinen, Heiramo, Haukilehto, Kirjavainen, Koskela, Laanti, Lekman, Lilja, Lindström, Nyman, Taipale, Tikka, Virtanen & Zieg, 2014).



Kuvio 1. Scrum-sprintti (Shrimp & Rawsthorne 2009)

Roolit

Scrummasterin (engl. Scrum Master) tehtävä on auttaa, valmentaa ja sovitella asioita yhteisen tavoitteiden saavuttamiseksi sprintin aikana. Hän hoitaa kommunikaation

tuoteomistajan ja kehitystiimin välillä. Hän kerää jatkuvasti tietoa kehitystiimin tilanteesta ja esteistä suorittaa tehtävää. Esteiden tai ongelmien ilmaantuessa, hänen tehtävänsä on poistaa ne kehitystiimiltä. Tämä voi tarkoittaa myös huomion keskittämistä ongelmaan ja sen ratkaisemisen kehitystiimin sisällä. (Shrimp & Rawsthorne 2009.)

Tuoteomistaja (engl. Product Owner) on itse kehitystiimin kannalta tärkein henkilö. Scrum-projektin ulkopuoliset sidosryhmät ovat tärkeässä osassa koko projektin kannalta, kuten budjetoinnin ja tavoitteiden. Tuoteomistaja keskustelee sidosryhmien kanssa ja esittää tehtäviä ja toiveita kehitystiimille. Hän antaa kehitykselle suuntaviivat ja priorisoi toteutettavat tehtävät. Hän on ensisijaisesti vastuussa tiimin suorituskyvystä ja sidosryhmien tyytyväisyydestä projektin aikana. (Shrimp & Rawsthorne 2009.)

Kehitystiimi on scrumin yksi tärkeimmistä osista. Kehitystiimin jäsenet vastaavat toisilleen tuottavuudestaan ja työskentelevät yhdessä yhteisten tehtävien saavuttamiseksi. Kehitystiimi organisoituu parhaaksi katsomallaan tavalla, eikä erillisiä työnimikkeitä jaeta, vaikka jokainen olisikin erikoistunut johonkin kehityksen osa-alueeseen. Ideaalitilanteessa tiimin kaikki jäsenet pystyvät tekemään kaikkia osa-tehtäviä kokonaisuuden ja julkaisuvalmiin tuotteen saamiseksi valmiiksi sprintin aikana. (Shrimp & Rawsthorne 2009.)

Toiminnot ja palaverit

Tuotteen kehitysjono on priorisoitu lista kaikista tehtävistä tai ominaisuuskokonaisuuksista, joita tuotteelle ollaan aikeissa tehdä projektin aikana. Kaikkien tehtävien tulee olla kehitystiimin tiedossa näkyvyyden vuoksi. Tuotteen ja sprintin kehitysjonot mahdollistavat Kanban-periaatteen eli tehtävien vetämisen työn alle itsenäisesti, kenenkään projektipäällikön tai scrummasterin työntämättä niitä projektiryhmälle tai yksittäiselle jäsenelle. (Pries & Quigley 2011.)

Yksi **sprintti** on iteraatio eli lyhyen ajan aikataulu. Sprintin ideana on toteuttaa tehtäviä tuotteen kehitysjonosta valmiiksi saakka esimerkiksi kahden viikon ajanjakson aikana. Sprintin pituus voi vaihdella. (Pries & Quigley 2011.) Tuoteomistaja suunnittelee tulevan sprintin kehitystiimin kanssa toteutettavista tehtävistä. Jokaiselle tehtä-

välle laaditaan sen valmiuden kriteerit (definition of done), ja ne laitetaan kehitystiimin **sprintin kehitysjonoon**.

Päiväpalaverin (engl. Daily Scrum) tarkoituksena on jakaa tietoa scrummasterin ja kehitystiimin jäsenten meneillään olevista töistä, suunnitelmista ja ongelmista. Jokaisen tiimin jäsenen tulee kertoa, mitä teki eilen, mitä tulee tekemään tänään ja mitä ongelmia on tullut vastaan. Muita kysymyksiä tai asioiden pidempää pohtimista ei suositella tämän palaverin puitteissa. (Pries & Quigley 2011.)

Sprintin katselmointi pidetään sprintin päätteeksi, jolloin kehitystiimi ja tuoteomistaja esittelevät kehitystiimin aikaansaannoksia sprintin aikana ulkoisille sidosryhmille. Tähän palaveriin voi osallistua kuka tahansa projektista kiinnostunut. Sen tarkoituksena on toimia palautekanavana tiimille ja todistaa tiimin edistyvän tavoitteissaan. Ennen uuden sprintin suunnittelun aloittamista kehitystiimi ja scrummaster vielä arvioivat edellisen sprintin tehokkuuden ja prosessin sprintin **retrospektiivi**palaverissa. Siinä päätetään parannettavat asiat seuraavaan sprinttiin. (Shrimp & Rawsthorne 2009.)

4.3 Tietoturvallisen sovelluskehityksen roolit ja vastuualueet

VAHTI 1/2013 Sovelluskehityksen tietoturvaohje (21−23) määrittää muun muassa seuraavia rooleja:

- Johto, projektin asettaja
- Projektin ohjausryhmä
- Tietoturvaryhmä
- Sovelluksen omistaja
- Projektipäällikkö
- Projektiryhmä
- Tietohallintovastaava
- Tietoturvavastaava
- Auditoija
- Katselmoija
- Sovelluksen pääkäyttäjä ja käyttäjä

Kaikki tietoturvallinen kehittäminen lähtee johdon sitoutumisesta ja halusta. Organisaation johdolla on oltava selkeä suunta tietoturvallisuuden suhteen osana toiminta- ja tietohallintostrategiaa. Projektin asettaja, joka yleensä on organisaation johdon edustaja, toimii projektin ohjausryhmän puheenjohtajana. Hän ja ohjausryhmä ovat tilivelvollisia tietoturvallisuuden huomioimisesta hankkeessa. He vastuuttavat työn projektipäällikölle, projektiryhmälle ja tietoturvavastaavalle. (VAHTI 1/2013, 21.) Seuraavassa käydään läpi sovelluksen toimittajan kannalta tärkeät roolit ja heidän vastuunsa tietoturvallisuuden suhteen. Nämä roolit on valittu, koska tavallisesti muut roolit täytetään asiakasorganisaation toimesta ja sovelluksen omistaja on tärkein toimittajaorganisaation projektiryhmän kanssa työskentelevä toimija. Auditoija ja katselmoija saattavat myös tulla toimittajaorganisaatiosta.

Projektipäällikkö

Organisaation laajuisen tietoturvallisuuden toteutumisen vastuu on luonnollisesti johdolla ja sen periaatteet määritetty osana strategiaa (VAHTI 1/2013, 21). Projektin tietoturvallisuuden toteutuminen on kuitenkin projektipäällikön vastuulla jo ennen projektin alkua. Projektipäällikön tulee hallita, toteuttaa, valvoa ja raportoida ohjausryhmälle tietoturvasta projektissa. Hän määrittää tulosdokumenttien ja lähteinä käytettävien materiaalien tietoturvatason ja vastuuttaa tietoturvatehtävät projektin aikana. Hän on myös ensi kädessä vastuussa koko projektiorganisaation henkilöiden ohjeistamisesta, koulutuksesta ja valvonnasta tietoturvankin suhteen. (VAHTI 9/2008, 16.) Tämä koskee myös jatkuvan tietoturvallisuuden ylläpidon ja valvonnan toimintatapojen määrittämistä toimittajaorganisaation kanssa (VAHTI 9/2008, 18).

VAHTI 9/2008 Hankkeen tietoturvaohjeen mukaan projektipäällikkö vastaa uhka- ja riskiarvioiden tekemisestä suunnitteluineen. Julkishallinnon organisaation tulee laatia uhka- ja riskiarviot mukaan lukien tietoturvariskit jo ennen hankkeen aloittamista. (VAHTI 9/2008, 17.) Lisäksi projektipäällikkö vastaa yritysten välisten turvallisuussopimusten ja muiden auditointien suorittamisesta toimittajaorganisaation kanssa. Tämä kohta ilmentää vahvasti projektipäällikön tai toisin sanoen hankintapäällikön tulevan asiakasorganisaatiosta. Projektipäällikkö ja hankepäällikkö voivat myös olla kaksi eri henkilöä, joista hankkeen päällikkö tulee asiakasorganisaatiosta ja työskentelee toimittajaorganisaation projektipäällikön kanssa tiiviissä yhteistyössä. Joka tapauksessa nämä roolit ovat periaatteessa sama asia. Projektipäällikkö vastaa myös

hankkeen valmistumiseen ja lopettamiseen liittyvistä tietoturvakysymyksistä. Lisäksi hänen vastuullaan on hoitaa projektin aikainen ulkoinen viestintä. Viestintään liittyvät periaatteet ja toimintatavat täytyy käsitellä projektin ohjausryhmän kanssa projektin aloituskokouksessa. (VAHTI 9/2008, 20.)

Sovelluksen omistaja

Sovelluksen (tai tuotteen) omistajan (engl. Product Owner) vastuulla on itse toteutettavan sovelluksen tietoturvallisuus ja kaikki siihen liittyvät tekijät, kuten vaatimukset, kaikki järjestelmää koskevat päätökset, hyväksymistestaus, käyttäjien koulutus ja tietoturvavaatimusten ottaminen kehitysjonoon iteraatiossa. Sovelluksen omistaja saa apua esimerkiksi tietoturvaryhmältä kaikkien vastuidensa ja tietoturvavaatimusten kanssa, tai hän voi määrittää jonkun henkilön vastaamaan yhdestä osa-alueesta edellyttäen kuitenkin sovelluksen omistajan valvovan kyseisen henkilön toimintaa. (VAHTI 1/2013, 21.)

Scrum-projektissa ja muissa inkrementaalis-iteratiivisissa ketterissä ohjelmistokehitysmalleissa tuoteomistaja on keskeisessä roolissa. Hyvällä tuoteomistajalla on seitsemän ominaisuutta (Pham & Pham 2012):

1. hän hallitsee eri sidosryhmien usein ristiriitaiset vaatimukset
2. omaa selvän näkemyksen tuotteesta
3. tietää, miten vaatimukset kerätään järkeväksi kehitysjonoksi
4. on aina täysin tiimin saatavilla jokaisessa vaiheessa
5. pystyy organisoimaan useaa omaa tehtäväänsä pitäen tietyn perspektiivin kehitettävään tuotteeseen
6. pystyy välittämään tuotteen vision tiimin lisäksi myös liiketoimintajohdolle rakentaen heidän luottamustaan projektin aikana ja
7. olemaan hyvä johtaja, ohjaaja, valmentaja sekä tuki tiimille koko projektin ajan.

Projektiryhmä

Projektiryhmän tavoitteena on toimia itsenäisenä yksikkönä toteuttaen sovelluksen omistajan määrittämästä kehitysjonosta aina ominaisuuksia, mukaan lukien tietoturvaominaisuuksia, noudattaen määritettyjä menetelmiä ja standardeja. Projektiryh-

män jokaisen jäsenen tulee olla itsekin tietoinen ja aktiivinen sovelluksen tai projektin tietoturvallisuuteen liittyvissä asioissa ja tuoda epäkohtia aktiivisesti esille sovelluksen omistajalle ja projektipäällikölle. (VAHTI 1/2013, 22.) Heidän on huomioitava projektin aikainen tietoturvallisuus kaikessa, mitä he tekevät, pitäen mielessä luvussa 3.3 esitellyt tietoturvallisuuden osa-alueet, kuten tietoaineistoturvallisuus ja käyttöturvallisuus. Projektiryhmän tietoturvallisuuden käytännön suunnitteluun, toteuttamiseen ja testaamiseen paneudutaan vaatimusten kanssa tutkielman luvussa 5 Tietoturvallinen sovelluskehitys.

4.4 Kirjallinen sovelluskehitysprosessi

VAHTI 1/2014 Sovelluskehityksen tietoturvaohjeen (41) perustason vaatimuksiin kuuluu, että toimittajalla on olemassa kirjallinen sovelluskehitysprosessi (SKM-001), joka ottaa kantaa kaikkiin sovelluskehityksen vaiheisiin esitutkimuksesta aina käytöstä poistoon ja niille asetettuihin tietoturvavaatimuksiin. Tämän prosessin kouluttaminen kaikille sovelluskehitykseen osallistuville on suotavaa. Tietoturvatehtävien on oltava luonnollinen osa kehitystyötä. (VAHTI 1/2013, 42.)

SKM-001-vaatimus ehdottaa sovelluskehitysprosessin määrittävän uudelleenkäytettäviä tietoturvallisuusvaatimuksia eri projekteille, jotta niiden toteuttaminen ei varmasti unohdu mistään. Valmiista listasta on myös helpompi poimia kulloinkin kehityksessä olevaan sovellukseen valmiita vaatimuksia perustuen VAHTIn vaatimuksiin. Tätä laadittua prosessia tulee myös käyttää kaikessa organisaation sovelluskehityksessä. (VAHTI 1/2013, 41.)

> *”Tietoturvallisuus tulee ottaa huomioon jokaisessa elinkaaren vaiheessa.” (VAHTI 1/2013, 42).*

Lainauksen lauseen merkitys heijastuu siihen, että toimittavalla yrityksellä on oltava suunniteltuna, miten tietoturvallisuus otetaan huomioon kussakin vaiheessa projektia. Ennen kuin projektiryhmä pääsee aloittamaan ensimmäistäkään iteraatiota, on projektin esitutkimus- ja vaatimusmäärittelyvaiheen VAHTI-tietoturvavaatimukset käytävä läpi. Nämä vaatimukset elävät projektin aikana, mutta on tärkeää määrittää tietoturvavaatimukset ja yleinen turvallisuustaso jo ennen projektia. Projektia aloitettaessa esitutkimusvaiheessa laaditaan projektille tietoturvallisuusohje asiakasor-

ganisaation strategian mukaisesti. Lisäksi tarkastellaan sovelluksen liiketoiminnallinen tarkoitus, määritellään tietoturvallisuustaso sen käsittelemille tiedoille (ks. ESI-001) ja laaditaan vaikutusanalyysi mahdollisten sovelluksesta koituvien uhkakuvien seurauksista yrityksen toiminnalle (ks. ESI-002). (VAHTI 1/2013, 45.) Jotta tuoteomistaja voi määrittää tietoturvavaatimuksia projektitiimin työjonoon, on hänen laadittava uhka-analyysin (vaikutusanalyysin) pohjalta tietoturvakertomuksia ja väärinkäyttötapauksia. Tietoturvakertomukset kertovat, miten tietoturvallisuus on toteutettu sovelluksessa karkealla tasolla, ja väärinkäyttötapaukset pyrkivät löytämään jo nyt kaikki mahdolliset tavat, joilla organisaation ulko- ja sisäpuoliset toimijat voisivat käyttää sovellusta hyväkseen. Näiden pohjalta voidaan asentaa puolustautumiskeinoja, ja niistä saadaan suoraan testaukseen testitapauksia ja heikkoja kohtia sovelluksen turvallisuudessa. (VAHTI 1/2013, 44.)

Iteraatiossa toteutettaville ominaisuuksille kannattaa kirjata tietoturvallisuuteen liittyviä hyväksyntäkriteereitä, joita testaus voi käyttää hyväkseen. Tämä auttaa myös ohjelmoijia ja arkkitehtejä tietoturvallisen komponentin suunnittelussa, koska he tietävät jo toteuttaessaan tietoturvan huomioon ottamisesta testauksessa. (VAHTI 1/2013, 44.)

4.5 Yhteenveto

Julkiset hankinnat pyrkivät löytämään kokonaiskustannuksiltaan taloudellisimman vaihtoehdon, mutta tietoturvallisuuden kannalta ajateltuna halvin hintalappu ei välttämättä ole halvin vuosien päästä hankkeesta. VAHTI Sovelluskehityksen tietoturvaohjeen vaatimuksista osa laitetaan jo mukaan tarjouspyyntöön ja toisista sovitaan erikseen. Perustason vaatimuksiin kuuluu (ks. VTM-002), että kaikki sovelluksen käsittelemään tietoon ja yleiseen tietoturvallisuuteen liittyvät säädökset ja lait ovat tiedossa ja että ne on huomioitu.

Tietoturvallisuuden kannalta organisaation johto on keskeisessä roolissa. Projektipäällikkö on vastuussa kokonaisturvallisuudesta projektin aikana. Sovelluksen omistaja vastaa tietoturvavaatimusten toteuttamisesta ja projektiryhmä vastaa niiden toteuttamisesta ammattimaisella tietoturvallisilla toimintatavoilla. Liitteessä 2 kuvataan projektin aikaiset VAHTI-vaatimukset kysymyslistana.

Toimittajalla on oltava kirjallinen sovelluskehitysprosessi, joka ottaa kantaa kaikkiin vaiheisiin ja tietoturvallisuuteen. Dokumentaatio, joka tulee laatia VAHTI Sovelluskehityksen tietoturvaohjeen mukaan perustason saavuttamiseksi:

- Kirjallinen sovelluskehitysprosessi
- Hankkeen tietoturvaohje (suositus)
- Liiketoiminnan vaikutusanalyysi
- Sovelluksen tarkoitus ja kriittisyys asiakasorganisaatiossa
- Tietoturvavaatimukset eri osa-alueille
- Tietoturvallisuustason määrittäminen tiedoille ja itse järjestelmälle

5 Tietoturvallinen sovelluskehitys

Tässä luvussa kerrotaan tietoturvallisesta sovelluskehityksestä käytännössä iteraation aikana tiimin näkökulmasta. Siitä selvitetään, mitä se tarkoittaa projektin kannalta, tukeutuen VAHTI Sovelluskehityksen tietoturvaohjeen vaatimuksiin ja käyden sen esittämät osa-alueet läpi. Tarkoitus ei ole kuitenkaan kopioida VAHTI-ohjeen sisältöä vaan tuoda lisätietoja joihinkin osa-alueisiin, joten jokaisen osa-alueen kokonaisvaltainen ymmärtäminen vaatii tietoturvallisuuteen, VAHTI-ohjeeseen ja sen lähdemateriaaliin tutustumista.

5.1 Suunnittelu iteraatiossa

Iteraation suunnittelupäivä alkaa tuotteen kehitysjonon (engl. Product Backlog) tarkastelulla. Tuotteen Tuoteomistaja määrittää iteraation tietoturvavaatimuksia ja väärinkäyttötapauksia toteutettaviksi sekä testattaviksi. (VAHTI 1/2013, 19.) Arkkitehtuurin suunnittelun aikana ja ensimmäisen iteraation suunnittelupäivänä olisi hyvä tarkastaa, että arkkitehtuuri noudattaa yleisesti käytössä olevia ja hyväksyttyjä standardeja (ks. SNT-001). Niitä on hyvä käyttää integroitavuuden, tietoturvallisuuden ja tunnettuuden takia. Etenkin web-sovellusten kehityksessä kannattaa käyttää avoimia standardeja muun muassa tiedonsiirrossa ja tiedostomuodoissa, koska tämä ei rajoita käyttäjiä. Lisäksi niiden tietoturvaominaisuudet ovat suljettuja standardeja paremmin tiedossa. (VAHTI 1/2013, 48−49.) World Wide Web Consortium (W3C) määrittää avointen standardien web-alustan (engl. Open Web Platform), joka käsittää

muun muassa avoimia standardeja web-sovellusten kehittämisestä, arkkitehtuurista, web-palveluista (Web Service) ja mobiilikehityksestä (Standards N.d.).

Tietoturvapäivitysten ja muiden korjausten asentaminen tulee tehdä helpoksi huomioimalla se jo arkkitehtuuria suunniteltaessa. Tämä saavutetaan käyttämällä sovelluskehystä tai muuten toteuttamalla kaikki sovelluksen konfiguraatio erillisissä konfiguraatiotiedostoissa kovakoodauksen sijaan. Lisäksi kirjastojen täytyy olla helposti päivitettävissä ja sovelluksen koodin pyrkiä olemaan käyttämättä käytöistä poistettuja metodeja luokkakirjastoista, jotta sovellus ei ole riippuvainen yhdestä kirjaston versiosta ja päivittäminen on mahdollista muuttamatta sovelluskoodia. (VAHTI 1/2013, 49.)

5.2 Tietoturvalliset ohjelmointikäytänteet

VAHTI Sovelluskehityksen tietoturvaohjeen vaatimuksista suurin osa määritellään jo ennen itse toteutuksen aloittamista, mutta käytännön ohjelmointityössäkin on pidettävä mielessä muutama vaatimus, joiden toteutuminen joka puolella järjestelmää on ohjelmoijan itsensä vastuulla. Teknisen sovelluskehitysympäristön vaatimuksissa määritellään Arkkitehtuuri- ja sovelluskehitysohjeistus (ks. TSK-001), jonka määrittämiin asioihin ohjelmoinnissa kannattaa kiinnittää huomiota ja ohjelmoijana olla ajan tasalla tietoturvaongelmista, joita käytettävä ohjelmointikieli ja/tai sovelluskehys sisältää. Vaikka organisaatiolla ei olisikaan kyseessä olevaa ohjetta, pitää ohjelmoijan pitää vaatimuksen listaamat ongelmat mielessä. Toteutustiimin vastuulla on seurata, että kaikki koodi katselmoidaan tasaisin väliajoin hyvien käytäntöjen ylläpitämiseksi ja tietoturvallisuushaavoittuvuuksien havaitsemiseksi (ks. TOT-008). (VAHTI 1/2013, 38.)

Ohjelmoijan yksi tärkeimmistä tehtävistä on huolehtia virhetilanteiden oikeanlaisesta ja tietoturvallisesta käsittelystä. Virhetilanteita tulee aina, mutta niiden käsittelyllä voidaan estää tietoturva-aukkojen syntyminen ja virheistä palautuminen sekä järjestelmän että käyttäjän näkökulmasta. Perustason vaatimus TOT-001 (VAHTI 1/2013, 54) määrittää asioita, jotka on hyvä toteuttaa jokaiseen järjestelmään. Esimerkiksi poikkeusten käsittelyn suunnittelu ja sen keskitetty toteuttaminen on erittäin suotavaa ylläpidettävyyden ja testauksen kannalta. Jokaiselle ohjelmoijalle tulisi olla selvää, miten poikkeusluokkia käytetään ja miten virheiden todelliset syyt raportoidaan

eteenpäin. Vaikka kuvaavien poikkeusluokkien heittäminen on hyvä, voi se olla työlästä määrittää jokaiselle poikkeukselle oma luokkansa ja tällöin olisi hyvä olla geneerinen yhden komponentin tai toiminnallisuuden poikkeus, jolle määritellään viestiin poikkeuksen todellinen syy (Kumar & Bhargav 2011).

Virheilmoitukset eivät saa kuitenkaan sisältää sovelluksesta liikaa tietoja tai ylläpitäjien yhteystietoja, jotta vältetään sosiaalista manipulointia hyväksikäyttävät hyökkäykset (engl. social engineering) ja muut virheilmoituksista saatavat järjestelmään murtautumista helpottavat tiedot (VAHTI 1/2013, 54). Virheilmoituksessa ei esimerkiksi saa olla ylläpitäjien yhteystietoja. Virheiden käsittelystä kannattaa muistaa, että virheitä kannattaa heittää heti, kun virhetilanteeseen joudutaan, ja ottaa virhe vastaan mahdollisimman myöhään suoritusketjussa, jotta kaikki tieto voidaan käsitellä ja kerätä rauhassa (Kumar & Bhargav 2011). Ohjelmoijan on pidettävä virheiden olemassaolo mielessään ja rakentaa sovellusta olettaen, että se sisältää virheitä. Tämä tarkoittaa, että virhetilanteissa pitää ennemmin estää komponenttien ja tietojen käyttö kuin riskeerata tietoturva-aukkoa. Myös ohjelmiston sisäisten komponenttien ei tulisi luottaa liikaa toistensa tekemiin syötteiden tarkastuksiin ja mahdollisiin väärinkäyttötilanteiden huomioimiseen, vaan sitä pitäisi tehdä joka tasolla. Tämä on niin sanottua monien tasojen suojausta (engl. layered defence).

Poikkeusten käsittelyssä pitää myös muistaa lokimerkintöjen tekeminen sekä onnistuneista että epäonnistuneista tietoturvallisuuteen liittyvistä tapahtumista sovelluksessa (ks. TOT-002). Tämä mahdollistaa kaikkien tapahtumien selvittämisen jälkikäteen, koska tietoturvallisuutta vaarantanut tapahtuma on saattanut olla sovelluksen näkökulmasta onnistunut, vaikka se on vaikuttanut merkittävästi tietoturvallisuuteen. Tällaisia tietoturvallisuuteen liittyviä tapahtumia ovat muun muassa onnistuneet ja epäonnistuneet kirjautumisyritykset, pääsynhallintapäätökset, epäonnistuneet syötteiden käsittelyyn liittyvät päätökset, kaikki ylläpitotoimet ja kriittisten tietojen luku, muutokset ja poisto. Lisäksi jokaiseen lokimerkintään tulee kirjata ainakin TOT-003-perustason vaatimuksien määrittämät tiedot. Lisäksi lokimerkintöjen aikaleimojen tulee olla koko järjestelmässä yhdenmukaiset, ja tämä tarkoittaa, että kaikilla järjestelmän komponenteilla on oltava yhteinen aikalähde (ks. TOT-004). Lokit tulee tallentaa niin, että niiden lukuoikeudet voidaan määrittää sekä puskuroimatta tallentaa jokainen merkintä erikseen (ks. TOT-005). (VAHTI 1/2013, 55.)

HTTP-yhteyksien sessioiden tietoturvallinen käsittely on erittäin tärkeää. Session tunnistusavaimen paljastuminen, kaappaaminen tai arvaaminen voi johtaa käyttäjien sessioiden kaappaamiseen, jossa hyökkääjä voi täysin esittää oikeaa käyttäjää sovelluksen näkökulmasta (Session Management Cheat Sheet 2014). Perustason vaatimus TOT-006 määrittää useita hyviä käytäntöjä istuntojen suojaukseen hyökkäyksiä vastaan, joita ovat muun muassa yhteyden salaus SSL/TLS (Secure Sockets Layer tai Transport Layer Security, myös HTTPS), istunnon aikakatkaisu, vaikeasti arvattava istuntotunniste ja session avanneen IP-osoitteen tallentaminen (VAHTI 1/2013, 56). Evästeeseen tallennettavaa istuntotunnistetta ei kannata muodostaa itse ainakaan mistään tunnukseen, kirjautumisaikaan, sovellukseen liittyvästä tai käyttäjään liittyvästä määreestä, vaan käyttää web-sovelluskehyksen tarjoamia valmiita sessioidenhallintakirjastoja. Näissäkin pitää kuitenkin muistaa vaihtaa evästeenä tallennettavan sessioavaimen oletusnimi pois, jotta siitä ei voida arvata käytettävää teknologiaa. Esimerkiksi “JSESSIONID” tai “PHPSESSID” ovat yleisimmin käytettyjen web-ohjelmointikielien JavaEE ja PHP oletusistuntoavaimet. Lisäksi pitää muistaa, että nämäkään sovelluskehysten tarjoamat kirjastot eivät ole tietoturva-aukkovapaita, vaan aina täytyy pitää huolta viimeisimpien päivitysten asentamisesta niihin. Yhteyden salaus SSL/TLS (HTTPS) ei kuitenkaan suojaa tunnisteen arvausta, brute force -hyökkäystä, asiakasselaimen turvan heikkenemisestä johtuvaa tai istunnon määräystä (engl. fixation) vastaan, vaikka se on yksi tärkeimmistä tietoturvallisuuteen vaikuttavista ominaisuuksista. (Session Management Cheat Sheet 2014.)

Käyttäjien ja heidän istuntojensa hallintaan suositellaan käytettävän valmiita sovelluskehysten tarjoamia kirjastoja. Perusvaatimus TOT-007 määrittää, että käyttäjienhallinnan on oltava keskitettyä ja ajantasaista ja sovelluksen on tuettava esimerkiksi ulkoista LDAP-palvelinta (Lightweight Directory Access Protocol), johon käyttäjienhallinta voidaan keskittää. (VAHTI 1/2013, 56.) Tällaisen mahdollisuuden JavaEE-ympäristöön tarjoaa muun muassa Spring Security, joka tukee erilaisia autentikointimalleja. Näitä ovat muun muassa LDAP, perinteinen lomakepohjainen kirjautuminen, OpenID, Kerberos ja Java Open Source Single Sign On. Spring Security huolehtii sovellukseen kirjautumisesta ja käyttöoikeuksien/valtuuksien hallinnasta. (Alex, Taylor & Winch 2014.)

5.3 Koodikatselmoinnit

Projektin tietoturvavastaavalla on testauksen kannalta paljon vastuuta. Hän on vastuussa tietoturvatestauksesta projektin aikana ja sen jälkeen käytön aikana. Hänen tulee katselmoida tietoturvasuunnitelmat. Perustason vaatimus OSK-005 määrittää, että organisaation nimeämä Security Coach eli tietoturvavastuullinen huolehtii myös koodikatselmoinneista järjestelmän kriittisiin osiin. (VAHTI 1/2013, 58.)

Katselmointeja voidaan pitää hyvin muodollisesta täysin epämuodolliseen pariohjelmointiin. Katselmointien tyyppi riippuu sovelluskehitysprosessin maturiteetista, turvallisuustason edellyttämästä tai muun lainsäädännöllisen määrityksestä. (Foundation Level Syllabus 2011, 33.) Epämuodollinen katselmointi voi olla esimerkiksi pariohjelmointia tai koodin läpikäyntiä yhdessä. Tavoitteena on saada ymmärrystä dokumentista tai koodista käyttämättä paljoa aikaa ja rahaa katselmoinnin valmisteluun ja dokumentointiin. Myös epämuodolliset katselmoinnit voidaan dokumentoida. (Foundation Level Syllabus 2011, 34.) Epämuodollisissa katselmoinneissa kannattaa käydä koodia läpi suunnitteluvaiheessa määriteltyjen ja yleisesti tiedossa olevien tietoturvavaatimusten pohjalta. Pariohjelmoinnissa tai kollegan koodin analysoinnissa kannattaa kiinnittää huomiota erityisesti virheidenkäsittelyn laatuun ja syötteiden käsittelyyn.

Läpikäynti ja tekninen katselmointi ovat hieman muodollisempia katselmointityyppejä. Siinä, missä läpikäynti ei välttämättä ole dokumentoitu, on teknisen katselmoinnin tuloksena aina katselmointiraportti löytöineen ja lausuntoineen. Läpikäynti on yleensä dokumentin laatijan vetämä, ja tekninen katselmointi pidetään koulutetun vetäjän toimesta. (Foundation Level Syllabus 2011, 34.) Näitä katselmointityyppejä voidaan käyttää suurempien kokonaisuuksien tietoturvallisuuden arviointiin. Projektille voi olla määritetty erikseen myös katselmoija, joka huolehtii sekä dokumentaation, että myös koodin muodollisista katselmoinneista.

Muodollisin katselmointityyppi on tarkastus, jonka vetää aina koulutettu vetäjä ja jolle on määritetty tarkat roolit. Tarkastukseen valmistaudutaan, ja se sisältää tarkan prosessin, säännöt ja tarkastuslistat. (Foundation Level Syllabus 2011, 35.) Tätä katselmointityyppiä tarvitaan lähinnä, kun turvallisuustaso on korkea ja tietoturvallisuudesta tarvitaan tarkkaa metriikkaa ja dokumentaatiota päätöksenteon tueksi.

Sovelluksen tietoturvatasosta riippuen tulee päättää, minkälaisia katselmointeja tarvitaan, ja niille on varatta aikaa. Viime kädessä tästä on vastuussa projektipäällikkö, mikäli tietoturva-asiantuntijaa ei nimetä. Katselmoinnit tulee suunnitella, ja suunnitelmaan pitää kirjata katselmointien pohjana käytettävät kriteerit. (VAHTI 1/2013, 24.) Katselmointien tyypeistä, niiden tehtävistä ja tavoitteista kannattaa lukea ISTQB Foundation Level Syllabuksesta (2011, 33−35) lisää.

5.4 Tietoturvatestaus

VAHTI Sovelluskehityksen tietoturvaohje määrittää testaukselle muutamia vastuualueita koodikatselmointien lisäksi, joita testaajien on hyvä myös suorittaa. Testaajien tulee suunnitella testitapaukset tietoturvatestaukselle perustuen sovellukselle asetettujen tietoturvavaatimusten, toiminnallisten vaatimusten, jo tiedossa olevien aikaisempien ongelmien ja sovellukselle määritettyjen mahdollisten väärinkäyttötapausten pohjalta sekä muistaa tarkastaa viimeisimmät tietoturvatrendit ja tyypilliset ongelmat toteutuksessa käytettäviin teknologioihin ja kirjastoihin (ks. TST-001). Tällaisia listoja ovat muun muassa OWASP Top 10 -lista (www.owasp.org). Testaajien tulee suorittaa suunnittelemansa tietoturvatestit ja laatia niiden suorittamisesta raportti (ks. TST-002). Testaajien tulee pitää tietoturvallisuus mielessä koko testausprosessin aikana, ja jos testauksessa käytetään hyväksi jotain oikeaa dataa tuotantotietokannasta, tulee salassa pidettävä tieto poistaa testidatan joukosta sekä sekoittaa tietueiden tiedot (ks. TST-005). Näin varmistetaan, ettei yksittäistä tietuetta kokonaisuudessaan voida saada selville. (VAHTI 1/2013, 57−58.) Myös testausvaiheessa kannattaa kirjoittaa testitapauksia käyttäen hyväkseen OWASP Testing Guide v4:ää, josta löytyy myös tarkastuslista kaikista siinä käsitellyistä ongelmista.

Testauksessa tulee pitää mielessä toteutuksessakin käytetty defence-in-depth-periaate. Se tarkoittaa monien tasojen suojausta pidemmälle vietyä ajattelumallia, jossa toteutetaan suojausta jokaisella mahdollisella tavalla ja mietitään turvallisuuden säilymistä myös silloin, kun vahinko on jo sattunut. (Perrin 2008.) Tietoturvatestaukseen tulee käyttää erilaisia testaustekniikoita eikä tyytyä tuloksiin ainoastaan yhdeltä automaatiotestityökalulta. Siis defence-in-depth-ajattelulla suoritettu tietoturvatestaus käyttää hyväkseen useita eri tekniikoita, jotta jonkin tekniikan puutteet voidaan täyttää toisella ja varmistaa järjestelmän kokonaisturvallisuus kaikissa tilan-

teissa. (Kumar & Bhargav 2011.) Tekniikat jaetaan karkeasti black-box ja white-box -tekniikoihin.

Black-box-tekniikat

Haavoittuvuuksien arviointi

Haavoittuvuuksien arviointi (engl. vulnerability assessment) on prosessi, jossa arvioidaan sovellusten ja koko tietojärjestelmän tietoturvallisuutta. Haavoittuvuuksia voidaan arvioida erilaisten manuaalisten ja automaattisten keinojen avulla. Markkinoilla on useita automaatiotyökaluja, jotka arvioivat sovelluksen ja antavat tietoa haavoittuvuuden tyypistä, niiden vakavuudesta ja mahdollisista keinoista paikata haavoittuvuus. Automaattisilla työkaluilla ei kuitenkaan voida löytää kaikkia mahdollisia haavoittuvuuksia, joten tarvitaan myös manuaalista testaamista. Ihmismielen kognitiivisia ja luovia aivoja tarvitaan tietoturvallisuuden testaamisessa. (Kumar & Bhargav 2011.)

Penetraatiotestaus

Penetraatiotestausta suorittavat hyväksytyt ammattilaiset, jotka pyrkivät simuloimaan mahdollisimman tarkkaan todellisia tiedonkalastelu- ja järjestelmään pääsyhyökkäyksiä. Näin mahdolliset heikkoudet tietoturvallisuudessa voidaan tunnistaa ja korjata, ennen kuin uhkaava pahaenteinen toimija löytää ne. Penetraatiotestausprosessissa kerätään tietoa järjestelmästä, listataan sen haavoittuvuudet ja käytetään niitä vielä hyväksi järjestelmään luvattoman pääsyn aikaansaamiseksi. Siinä mielessä se menee vielä pidemmälle kuin haavoittuvuuksien arviointi. (Kumar & Bhargav 2011.)

White-box-tekniikat

White-box-tekniikat tarkoittavat ohjelmakoodin tarkastelua ja siitä tietoturvaongelmien arviointia. White-box-tekniikoilla ei voida arvioida koko ohjelmakoodia, mutta sillä voidaan saada tietoa tietoturvallisista ohjelmointikäytänteistä tai niiden puutteesta. (Kumar & Bhargav 2011.) Koodikatselmointeja ja muuta koodin arviointia tekemällä voidaan saada varmuus koodin kypsyydestä. Jos ohjelmakoodi ei ota tietoturvallisuutta huomioon yhdessä paikassa, on todennäköistä, että se ei ota sitä huomioon toisaallakaan. Varsinkin suurten projektien ja useiden ohjelmoijien tietoturval-

listen ohjelmointikäytänteiden seuraaminen on tärkeää kokonaisturvallisuuden kannalta. Haavoittuvuuksien tunnistaminen ohjelmakoodista ja niihin ratkaisujen ehdottaminen vaativat ammattitaitoa myös testaajalta. (Kumar & Bhargav 2011.)

5.5 Yhteenveto

Tietoturvallinen sovelluskehitys lähtee tietoturvavaatimusten määrittämisestä. Liitteessä 3 on kuvattu projektitiimin kehitystyöhön liittyvät vaatimukset kysymyslistana, josta vaatimuksia voidaan tarkastaa projektin edetessä. Vaikka ohjelmoijat voivat ammattitaidollaan paikata huonoa sovelluskehitysprosessia, eivät hekään keskity tietoturvallisuuteen, ellei heille aseteta tietoturvallisuutta yhdeksi tavoitteeksi vaatimusten muodossa. Sovelluksen omistaja on keskeisessä roolissa määrittäessään tietoturvavaatimuksia projektiryhmän työjonoon.

Kaikki koodi tulee katselmoida säännöllisin väliajoin jonkin muun kuin sen laatijan toimesta. Tällä ylläpidetään hyviä käytänteitä ja pyritään tunnistamaan haavoittuvuuksia (ks. TOT-008). Sovelluskehittäjän on huolehdittava virheiden käsittelystä, yhteyksien salauksesta ja tiedon tallennuksen turvallisuudesta. Hänen tulee myös ylläpitää ajantasaista tietoa viimeisimmistä tietoturvaongelmista.

Tietoturvavastuullinen henkilö vastaa katselmoinneista kriittisimpiin sovelluksen osiin (ks. OSK-005). Katselmointeja on erityyppisiä: hyvin formaaleja ja toisaalta erittäin epäformaaleja, kuten pariohjelmointi. Sovelluksesta, sen sisältämästä tiedosta ja projektin tietoturvatasosta riippuu, minkälaisia katselmointeja pidetään ja allokoidaanko niille aikaa projektin aikana.

Tietoturvallisuuden testitapaukset tulee johtaa tietoturva- ja toiminnallisista vaatimuksista, jo tiedossa olevien aikaisemmista ongelmista ja sovellukselle määritetyistä väärinkäyttötapauksista. Testauksessa tulee käyttää montaa erilaista lähestymistapaa ja muistaa defence-in-depth-periaate. OWASP Testing Guide v4 on hyvä materiaali testausten laatimiselle.

6 Nykyinen prosessi

Tässä luvussa käydään läpi toimeksiantajan kirjalliset projektin läpivienti- ja sovelluskehitysprosessit sekä muu materiaali, joka tukee sovelluskehitystä.

6.1 Projektikäsikirja

Projektikäsikirja on tarkoitettu kaikkiin alihankintana tehtäviin sovellustoimitusprojekteihin sekä sisäiseen sovelluskehitykseen. Se määrittää prosessin, dokumentit ja vastuut jokaisessa toimeksiantajan projektissa. Tarjouksen ja sopimuksen tekeminen on kuvattu laatukäsikirjassa. Projektikäsikirjassa määritellään projektin roolitus, toteutus ja päättäminen. (Toimeksiantajan projektikäsikirja 2013, 3.)

Ohjausryhmä

Projektin asettajan on oltava budjettivastuullinen. Hän määrittää projektille ohjausryhmän ja toimii tämän ohjausryhmän johdossa tai vastuuttaa sen jollekulle toiselle. Ohjausryhmän jäsenten tulee kuulua toimeksiantajan laatuorganisaatioon, mutta tapauskohtaisesti sovitaan asiakkaan kanssa, muodostetaanko ohjausryhmä myös tämän edustajista. Projektipäällikkö ei ole osa ohjausryhmää ja vastaa ainoastaan ohjausryhmälle projektiin liittyvissä asioissa. (Toimeksiantajan projektikäsikirja 2013, 5.)

Ohjausryhmä katselmoi ja hyväksyy tarjouksen sekä projektisuunnitelman lopullisen sitovan tarjouksen jättämistä asiakkaalle. Ohjausryhmän tehtävänä on valvoa projektia laadun, budjetin, resurssien, riskien ja itse sovelluksen toimituksen suhteen. Erityisesti se kiinnittää huomiota asiakastyytyväisyyteen, ja se on vastuussa projektin kannattavuudesta yrityksen liiketoiminnalle. Ohjausryhmä asettaa projektille tavoitteet, niiden seurantaa vaadittavat mittarit ja jakaa vastuut ja tehtävät. (Toimeksiantajan projektikäsikirja 2013, 5.)

Ohjausryhmän tehtävät (Toimeksiantajan projektikäsikirja 2013, 6):

- Tavoitteet: aika, tekninen ja talous
- Vastuunjako
- Projektidokumentaation hyväksyntä

- Kiistojen ratkaiseminen
- Projektipäällikön vastuisiin kuulumattomien päätösten tekeminen, kuten lisäinvestoinnit
- Vaaditun raportoinnin määrittely, seuranta ja hyväksyntä
- Projektin tulosten seuranta
- Projektin keskeyttämis- tai lopetuspäätökset
- Loppuraportin hyväksyntä.

Projektipäällikkö

Projektipäällikkö on vastuussa projektisuunnitelman laatimisesta ja siksi myös edistymisestä, budjetista ja laadusta. Projektipäällikkö voi delegoida tehtäviään muille, mutta hänen on seurattava niiden toteuttamista.

Projektipäällikön tehtävät (Toimeksiantajan projektikäsikirja 2013, 6−7):

- Projektisuunnitelma
- Tekninen vaatimusmäärittely
- Arkkitehtuurisuunnitelman hyväksyminen
- Viikkoraportit/väliraporttien laatiminen sprinttien päätteeksi
- Raportointi asiakkaalle ja ohjausryhmälle
- Projektisalkun ylläpito
- Loppuraportti
- Ylläpitosuunnitelma
- Työnteon etenemisen seuraaminen
- Laskutustietojen eteenpäin toimittaminen
- Retrospektiivi-koostepalaverien koollekutsuminen ja raportointi.

Projektiryhmän vastuut (Toimeksiantajan projektikäsikirja 2013, 7):

- Teknisen vaatimusmäärittelyn tekeminen asiakkaan kanssa ja projektipäällikön johdolla
- Arkkitehtuurisuunnitelma
- Testaussuunnitelma
- Sovelluksen suunnittelu, toteutus ja testaus

- Projektipäällikölle raportointi
- Ylläpitosuunnitelman laatiminen projektipäällikön johdolla.

Projektisuunnitelmassa määritellään seuraavat asiat (Toimeksiantajan projektikäsikirja 2013, 8−9):

- Projektin tavoite
- Rajoitteet ja oletukset: integroinnit muihin järjestelmiin, tuetut selaimet
- Projektin organisaatio ja resursointi
- Projektin aikataulu, vaiheistus ja työmäärät
- Viestintäsuunnitelma
- Budjetointi: myös käyttöönotto ja ylläpitovaiheessa tarvittavat resurssit
- Projektin tuotokset: mitä missäkin vaiheessa tuotetaan, virstanpylväät
- Riskienhallinta: tekniset riskit, aikataulun riskit, taloudelliset riskit, henkilö/tiedonkulkuriskit, asiakkaaseen liittyvät riskit ja sopimukseen liittyvät riskit.

Projektin ohjaus- ja seurantakäytännöt noudattavat scrum-mallia. Sprintin retrospektiivi-palaverien tulokset kerätään taulukkoon. Matka- ja muiden kulujen seurantaan löytyvät liitteinä pohjat. Lisäksi erilaiset mittarit on sovittava asiakkaan kanssa erikseen. (Toimeksiantajan projektikäsikirja 2013, 10−11.)

Projektin päättäminen

Ohjausryhmän päätettyä käyttöönotosta ja ylläpitovaiheeseen siirtymisestä vastuu siirtyy ylläpito-organisaatiolle. Tämä kostuu yleensä osasta projektitiimin jäseniä. Kaikkia ei yleensä kuitenkaan tarvita. Projektipäällikkö laatii ylläpitosuunnitelman ja liittää sen laatimaansa loppuraporttiin liitteeksi. Ohjausryhmä hyväksyy kummankin. Projektipäällikkö järjestää retrospektiivin, jossa käydään läpi kaikkien sprinttien retrospektiivi-palaverien tulokset ja käydään läpi onnistumiset ja epäonnistumiset projektin aikana. (Toimeksiantajan projektikäsikirja 2013, 13.)

6.2 Projektin aloittamisen tehtävälista

Kirjallisen projektikäsikirjan liitteenä on projektin aloittamisen tehtävälista, jolla projektin aloittamisen tehtäviä seurataan. Tehtävien teemoja ovat muun maussa sopimusten kirjoittamiseen liittyvät ja työkaluihin liittyvät tehtävät. Jokaiselle tehtävälle

määritellään tavoiteaikataulu, vaikutus ja vastuuhenkilöt sekä asiakas- että toimeksiantajan organisaatiosta. Kun jokainen tehtävä on suoritettu, se merkataan tehdyksi. (Toimeksiantajan projektikäsikirja 2013, liite 7.)

Sopimusten tekemiseen liittyviä tehtäviä ovat seuraavien dokumenttien laatiminen (Toimeksiantajan projektikäsikirja 2013, liite 7):

- projektisopimus
- projektisuunnitelma ja
- aikataulusuunnitelma.

Työkaluihin liittyviä tehtäviä ovat muun muassa verkkolevytilan allokointi projektille, etätyökalujen määrittäminen, projektin luonti erilaisiin projektia tukeviin sisäisiin järjestelmiin, kuten versionhallinta, työajanseuranta, wiki ja bugienseuranta. Yhteyksiin liittyy VPN-yhteyksien muodostaminen toimittajalta asiakkaalle ja toisinpäin tarvittaessa. (Toimeksiantajan projektikäsikirja 2013, liite 7.)

7 Tutkimuksen toteutus

Tässä luvussa kuvataan tutkimuksen tavoitteet ja selostetaan itse tutkimuksen toteutusta.

7.1 Tavoitteet ja viitekehys

VAHTI Sovelluskehityksen tietoturvaohje on itsessään kattava kokonaisuus tietoturvallisesta kehittämisestä, ja se sisältää paljon viittauksia ulkoisiin lähteisiin, joita analysoimalla saadaan lisätietoa aiheesta. Tutkimuksen teoriapohjaan analysoitiin muutamaa ulkoista lähdettä, mutta teorian rakenne tulee VAHTI Sovelluskehityksen tietoturvaohjeesta. Ohjeessa vaatimukset on jaettu kahteen osaan: organisaatioon ja sovelluskehitykseen liittyviin. Kaikki sovelluskehitykseen liittyvät vaatimukset eivät kuitenkaan ole projektiorganisaation vastuulla, tai niistä pitää sopia erikseen. Tällaisia ovat esimerkiksi käyttöönoton jälkeiset sovelluksen elinkaaren vaiheet ylläpito ja käytöstä poisto. Ylläpito-organisaatio voidaan muodostaa ainakin osittain projektiryhmästä. Käytöstä poistosta huolehtii yleensä sovellusta käyttävä organisaatio. Tämä tutkimus tarkasteli vaatimuksia toimittajaorganisaation alihankintaprojektin nä-

kökulmasta. Tästä syystä osa sovelluskehityksen vaatimuksista on siirretty näennäisesti takaisin tilaavan organisaation vastuulle. Tavoitteena oli analysoida VAHTI Sovelluskehityksen tietoturvaohjetta, sen lähteitä ja muuta materiaalia ensimmäiseen tutkimuskysymykseen vastausta varten. Tässä selvitettiin tietoturvallisen kehittämisen tarkoitusta sovelluskehityksessä.

7.2 Haastatteluiden toteutus

Itse kvalitatiivinen tutkimus eli toiseen ja kolmanteen tutkimuskysymykseen vastaaminen toteutettiin tutustumalla nykyiseen toimittajan projektikäsikirjaan ja haastattelemalla työntekijöitä. Haastatteluun osallistui sekä organisaation johtoa että sovelluskehittäjiä ja testauspäällikkö. Haastatteluun haluttiin ottaa mukaan mahdollisimman eri tehtävissä olevia henkilöitä, jotta saataisiin mahdollisimman hyvä kuva tietoturvallisesta sovelluskehittämisestä nykyisellään organisaatiossa. Haastateltavat poimittiin harkinnanvaraisesti niin, että saatiin hyvä kattavuus erilaisista projekteista ja erilaisista työtehtävistä. Lopullisen haastateltavien valinnan tekivät toimeksiantajan liiketoimintajohtaja ja projektipäällikkö, koska he pystyivät arvioimaan parhaiten, kuka soveltuu haastatteluun annettujen kriteerien perusteella. Toimeksiantajalla on myös yksi projekti, jossa otetaan jo VAHTI Sovelluskehityksen vaatimuksia tietoisesti huomioon. Tämän projektin työntekijöitä haastateltiin, jotta saatiin esimerkkejä hyvistä käytänteistä. Muiden projektien työntekijät toimivat kontrolliryhmänä, jotta tiedetään, miten yleisellä tasolla tietoturvallisuudessa ollaan. Haastattelu oli teemahaastattelu, joka suoritettiin sekä puhelinhaastatteluna että henkilökohtaisesti. Tämä johtui siitä, että toimeksiantajan toimipisteet sijaitsevat eri paikkakunnilla.

Haastattelun aihealueet olivat seuraavat, joista jokaisesta noin 4 kysymystä:

- Henkilön taustatiedot
- Prosessin taustatiedot
- Projektiorganisaatiota koskevat perustason VAHTI-vaatimukset
- Kehitystiimiä koskevat perustason VAHTI-vaatimukset
- Prosessin ja toiminnan kehitysehdotukset

Henkilön taustatiedoilla selvitettiin sitä, minkälaisia henkilöitä haastatteluihin saatiin, ja heidän henkilökohtaiset tietonsa ja kiinnostuksensa tietoturvallisuuteen. Prosessin

taustatiedoissa kysyttiin nykyisen projektikäsikirjan tuntemusta, nykyisen projektin ohjelmistokehitysmenetelmää ja tietoturvallisuuden huomioimista meneillään olevassa projektissa. Koska perustason vaatimukset määrittävät tiettyjä osa-alueita toteutettaviksi, kysyttiin projektiorganisaatioon liittyviin vaatimuksista kirjallisen sovelluskehitysprosessin, tietoturvavaatimusten ja tietoturvatasomäärityksen olemassaoloa. Kehitystiimin vaatimuksissa kysyttiin arkkitehtuurin standardeista, tunnistautumismenetelmän turvatasosta ja salausratkaisuista. Sekä projektiorganisaation että kehitystiimin kysymykset johdettiin VAHTI Sovelluskehityksen tietoturvaohjeen perustason vaatimuksista, koska se on tällä hetkellä Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa (1.7.2010/681) määrittämä taso, joka tulee toteuttaa. Kaikki vaatimukset käännettiin kysymysmuotoon työn liitteiksi 1−3. Lopuksi kysyttiin yleisesti kehitysehdotuksia työntekijöiltä nykyiseen prosessiin. Haastattelurunko on kokonaisuudessaan liitteessä 4.

8 Tutkimuksen tulokset ja johtopäätökset

Tässä kappaleessa esitellään tutkimuksen tulokset jokaisen aihealueen osalta, esitellään johtopäätökset prosessin analysoinnista ja lopuksi vastataan tutkimuskysymyksiin lyhyesti.

8.1 Teemahaastattelun tulokset

Haastatteluun osallistuneiden taustatiedot

Haastatteluun valikoitui kahdeksan henkilöä erilaisista sovelluskehitykseen liittyvissä tehtävissä työskentelevistä toimeksiantajan työntekijöistä. Mukana oli testauspäällikkö, projektipäällikkö, scrummaster ja sovelluskehittäjiä. Haastateltavien ja toimeksiantajan pyynnöstä anonyymiyden säilyttämiseksi henkilöihin viitataan koodauksella H1-H8.

- H1: Työskentelee Senior Software Designer -nimikkeellä sovelluskehittäjänä nykyisessä projektiorganisaatiossa. Hän ei ollut tutustunut VAHTI-ohjeisiin.

- H2: Työskentelee Senior Software Designer -nimikkeellä scrummasterin tehtävässä ja sovelluskehittäjänä nykyisessä projektiorganisaatiossa. Hän tulee

miettineeksi tietoturvallisuutta mahdollisimman usein. Hän on käynyt VAHTI-ohjeisiin liittyvässä koulutuksessa muutama vuosi sitten.

- H3: Työskentelee Senior Software Designer -nimikkeellä sovelluskehittäjänä nykyisessä projektiorganisaatiossa. Hän ei ollut tutustunut VAHTI-ohjeisiin.

- H4: Työskentelee Senior Software Designer -nimikkeellä sovelluskehittäjänä nykyisessä projektiorganisaatiossa. Hän ei ollut tutustunut VAHTI-ohjeisiin.

- H5: Työskentelee laatu- ja turvallisuusjohtajana sekä testauspäällikkönä nykyisessä projektiorganisaatiossa. Hänelle tietoturvallisuuden toteuttaminen sovelluskehityksessä on ainakin osittain arkipäivää. Tietoturvallisuuteen liittyvää uutisointia tulee seurattua RSS-syötteen avulla päivittäin.

- H6: Työskentelee Senior Software Designer -nimikkeellä sovelluskehittäjänä. Hän ottaa tietoturvallisuuden huomioon kaikessaan työssään, mutta tiedostaa, ettei siihen ole mitään tiettyä prosessia eikä hänellä ole siihen mitään erityistä koulutusta. VAHTI Sovelluskehityksen vaatimukset on otettava huomioon nykyisessä projektissa, joten siihen hän on tutustunut osittain.

- H7: Työskentelee Software Designer -nimikkeellä sovelluskehittäjänä. Hänelle tietoturvallisuuden toteuttamisessa jokapäiväisessä työssä on vielä paljon asioita, joita pitäisi oppia. VAHTI Sovelluskehityksen vaatimukset on otettava huomioon nykyisessä projektissa, mutta muihin ohjeisiin hän ei ole tutustunut.

- H8: Työskentelee laadunvarmistuksen ja ohjelmistotuotannon projektijohtotehtävissä. Nykyisessä projektissa hän on projektipäällikkö. Hänelle tietoturvallisuuden toteuttaminen ei ole vieras asia, mutta se voisi olla myös tiiviimmin mukana jokapäiväisessä työssä. Hän on tutustunut VAHTI Sovelluskehityksen tietoturvaohjeeseen nykyisen projektin vaatimusten kautta huolellisesti ja tämän lisäksi myös infrastruktuuriin liittyviin VAHTI-ohjeistukseen. Hänellä on käytössä myös postituslista, johon tulee tietoturvailmoituksia.

Kaikkia vastanneita yhdisti lisäksi se, että he seuraavat kaikkea alaan liittyvää uutisointia, ja niiden joukossa tulee usein tietoturvallisuuteen liittyvää tietoa.

Prosessin taustatiedot

Täysin oletettavasti toimeksiantajan projektikäsikirja oli tuttu vain johtavassa asemassa oleville henkilöille, mutta sekä H4 ja H7 sovelluskehittäjistä sanoivat joskus selanneensa sitä. Kaikkien haastateltavien projekteissa käytettiin ketterää sovelluskehityksen mallia, joista scrum tai siitä sovellettu malli oli käytöissä kaikilla muilla paitsi haastateltavalla H3. Hänen ylläpitoprojektissaan käytettiin Kanban-menetelmää bugien ottamiseen työn alle.

Kysyttäessä, miten nykyinen sovelluskehityksen prosessi ottaa huomioon tietoturvallisuuden, H1-H5 vastasivat: heikosti tai ei lainkaan. H5 kommentoi, että sitä toteutetaan täsmäiskuina, mutta itse sovelluskehitysprosessi ei sitä huomioi, eikä se ole jokapäiväistä. H6-H8 työskentelevät samassa projektissa, jossa jo tarjouspyyntövaiheessa on vaadittu VAHTI Sovelluskehityksen tietoturvaohjeen vaatimusten täyttämistä. Tässä projektissa tietoturvallisuuden toteuttaminen on tapahtunut sekä testauksessa koko ajan että erillisissä tietoturvasprinteissä. Tietoturvasprinteissä käydään VAHTI tietoturvavaatimuksia ja OWASP Top 10 -haavoittuvuuksia tarkemmin läpi ja otetaan niitä työjonoon. Projektiryhmän kanssa on myös sovittu niin sanotuista definition-of-done (DoD) -määrittelystä tietoturvallisuuden osalta. Lisäksi on otettu käyttöön SonarQube-työkalu. Siihen liitetty OWASP Top 10 -liitännäinen analysoi paketin staattisin keinoin jokaisen ohjelmakoodin kääntämisen yhteydessä.

Kysyttäessä riskianalyysin olemassaoloa nykyisessä projektissa vastasivat kaikki paitsi haastateltava H8 kielteisesti. Myös H8 tarkensi, että kyseinen riskianalyysi oli hyvin pinnallinen ja sitä ei viety kovin pitkälle.

Projektiorganisaatiota koskevat perustason VAHTI-vaatimukset

Perustason vaatimuksen SKM-001 mukaisesta kirjallisen sovelluskehitysprosessin olemassaolosta kysyttäessä vastaajat, paitsi haastateltava H8, vastasivat yksimielisesti, että sellaista ei ole tai he eivät ainakaan ole siitä tietoisia. Vaatimuksen mukaan prosessin tulisi ottaa kantaa kaikkiin sovelluskehityksen vaiheisiin ja niiden tietoturvahaasteisiin (VAHTI 1/2013, 41). Haastateltava H8 on mukana jo käynnistetyssä pro-

jektissa kehittää tämän tyyppinen kirjallinen sovelluskehitysprosessi. H8:n mukaan tähän mennessä on jo tehty paljon työtä prosessin eteen, ja tarkoituksena on käydä kaikki vaatimukset läpi sekä yhdistää ne jo käytössä oleviin hyviin käytäntöihin. Monet vaatimuksista täytetään jo jotenkin, mutta yhtenäinen ohjeistus kaikille puuttuu.

Positiivisena yllätyksenä haastatteluissa huomattiin, että karkean tason tietoturvavaatimuksia oli mietitty kaikkien paitsi haastateltavien H3 ja H4 projekteissa. Kun karkean tason tietoturvavaatimukset (ks. VTM-003) oli määritetty, se ei välttämättä ollut virallinen listaus. Tuoteomistaja oli määritellyt tietoturvallisuustason ja tietoaineiston arkistoinnin vaatimukset (ks. VTM-004) haastateltavien H2, H3 ja H6−H8 projekteissa.

Kehitystiimiä koskevat perustason VAHTI-vaatimukset

Yleisesti käytössä olevat ja hyväksytyt standardit olivat hyvin vaihtelevasti käytössä projekteissa. Haastateltavan H3 projektissa oli esimerkiksi käytössä Java 1.5, ja muut eivät osanneet sanoa tai niitä ei ollut. Sovelluksen tunnistautumismenetelmä oli tiedon tietoturvatason mukainen (ks. SNT-009) haastateltavien H3−H8 projekteissa, ja H1 ja H2 eivät osanneet sanoa. H6−H8:n projekteissa käsiteltävä tieto vaatii erillisen sirukorttitunnistuksen. Projekteissa oli käytössä salausratkaisuja ja tiivisteistä, kuten SHA-1, SHA-256, MD5 ja SSL. Haastateltavat H1, H3, H5, H7 ja H8 eivät osanneet ottaa kantaa salauskysymykseen.

Prosessin ja toiminnan kehitysehdotukset haastateltavilta

Tutkimuksessa kysyttiin mahdollisia kehitystarpeita toimeksiantajan organisaation tai asiakkaan sovelluskehitysprosessiin. H1 sanoi, että kaikille sovelluksen osakomponenteille pitäisi olla vastuuarkkitehdit, joille tietoturvallisuuden toteuttaminen tulisi myös vastuuttaa. H2 ehdotti tietoturvakatselmointien säännöllistä pitämistä riippuen projektista ja asiakkaan tarpeista. H3, H4 ja H5 olivat kaikki sitä mieltä, että kunnollinen kirjallinen prosessi tulisi saattaa kaikkien käyttöön ja erityisesti tietoturvatestausta tulisi terävöittää. H4 lisäsi vielä, että laatukäsikirjan käyttö tulisi pakottaa kaikille käyttöön. H7 ehdotti, että olisi olemassa valmis lista VAHTIn ja OWASP Top 10:n vaatimuksista ja haavoittuvuuksista sekä niiden toteuttamisesta, jotta jokaisen projektiryhmän ei tarvitsisi joka kerta analysoida varsinaisia määrityksiä, vaan ne olisivat nopeasti otettavissa työjonoon. Haastateltavan H8 aloittama projekti sovellus-

kehityksen prosessin laatimisesta olisi saatettava loppuun ja tiedotettava tästä työntekijöille. Hänen mielestään suurin ongelma tällä hetkellä on myös, että asiakkaat eivät ymmärrä, mitä tietoturvallisuuden toteuttaminen maksaa ajassa ja rahassa.

> *H8: "Tämä meidän tietoturvallinen kehitysprosessi tulisi tarpeeseen siinä, että tuodaan esiin sitä, että jos vaaditan jotain, mitä se tarkoittaa. Toisaalta myös toisinpäin, että jos asiakas ei ole vaatimassa tietoturvallisuutta, voidaan osoittaa, että mitä ne mahdolliset riskit ja ongelmat ovat, jos ne jätetään pois."*

Kaikki paitsi H3 halusivat yleistä käytännönläheistä tietoturvakoulutusta, ja H3 halusi erityisesti verkkojen turvallisuuteen liittyvää koulutusta. H8 lisäsi myös, että jonkinlainen VAHTI Sovelluskehityksen tietoturvaohjeen osa-alueisiin paneutuva sertifiointikoulutus olisi hyväksi. Kysymyksenä oli eniten tällä hetkellä tarvittavan tietoturvakoulutuksen laatu.

8.2 Johtopäätökset

Haastattelut

Haastateltavien henkilöiden asema yrityksessä vaikutti hieman VAHTI-ohjeisiin perehtyneisyyteen ja tietoturvallisen kehityksen tiedostamiseen jokapäiväisessä työssä. Vastuutehtävissä scrummasterista projektipäällikköön olivat kaikki tutustuneet VAHTI-ohjeistukseen. Tämä oli myös totta sovelluskehittäjillä, joiden projektissa otettiin aktiivisesti huomioon VAHTI Sovelluskehityksen vaatimuksia. Toisissa projekteissa työskentelevillä tämä ei pitänyt paikkaansa. Kaikkia haastateltavia yhdisti kuitenkin kiinnostus tietoturvallisuuteen, joten oikeanlaisella koulutuksella tietoturvallisesta kehittämisestä saadaan arkipäivää kaikille. Hyviä käytänteitä haastateltavilta poimittuna olivat tietoturvaan liittyvien RSS-syötteiden ja postituslistojen käyttäminen, joka helpottaa aiheeseen liittyvän uutisoinnin seuraamista.

Kaikissa projekteissa käytettiin ketteriä menetelmiä, ja usein se oli sovellettu scrum. Ainoastaan yhdessä projektissa otettiin tietoturvallisuus huomioon jo prosessitasolla sekä projektiryhmän käytännön ohjeistuksessa että heidän työtavoissaan. Hyvänä käytäntönä pidettiin erityisten tietoturvasprinttien pitämistä, joissa keskityttiin erityisesti esimerkiksi OWASP Top 10 -haavoittuvuuksien karsintaan tai muihin tietoturva-

ongelmiin. Lisäksi oli otettu käyttöön SonarQube niminen staattisen analyysin työkalu, jonka OWASP Top 10 -liitännäinen etsii kaikkien ohjelmistopakettien käännön yhteydessä ilmenneitä haavoittuvuuksia. Tietoturvavaatimuksien määrittäminen jo projektin alussa helpottaa myös tietoturvallisuuden ottamista huomioon testauksessa jokaisessa iteraatiossa, ei ainoastaan tietoturvasprintissä.

Ehdotuksia sovelluskehitysprosessiin olivat muun muassa vastuuarkkitehdit kaikille komponenteille, suunnitellut tietoturvakatselmoinnit, kirjallinen sovelluskehitysprosessi, lista tietoturvavaatimusten toteuttamisen käytännön ohjeista ja tietoturvan toteuttamisen hinnan perustelukyvyn nostaminen asiakkaalle. Lähes kaikki haastateltavat myös halusivat käytännönläheistä tietoturvakoulutusta.

Hyvät käytänteet ja ehdotukset haastatteluista:

- Työntekijöiden kiinnostus tietoturvaan on käytettävä hyväksi.
- Tietoturvaan liittyvien RSS-syötteiden ja postituslistojen käyttö lisää tietoturvallisuuden lähestyttävyyttä ja tietojen ylläpitoa.
- Hyvänä käytäntönä huomattiin erillisten tietoturvasprinttien käyttöönotto, jossa tietoturvallisuuteen paneudutaan kunnolla.
- OWASP-projektin keräämien tietoturvatiedon hyväksikäyttö sekä manuaalisesti että staattisten analyysityökalujen kanssa oli todettu hyödylliseksi.
- Tietoturvavaatimusten listaaminen jo projektin alussa ja sprinttien yhteydessä helpottaa niiden huomioimista.
- Vastuuarkkitehdit jokaiselle komponentille
- Kirjallinen sovelluskehitysprosessi
- Yleistä tietoturvakoulutusta koko henkilökunnalle

Teoria

Vaikka tässä tutkielmassa keskityttiin ainoastaan sovelluskehityksen ja projektien tietoturvavaatimuksiin, kannattaa toimeksiantajaorganisaation tarkastaa myös kaikki organisaation toimintaa koskevat vaatimukset, jotta sen omat prosessit olisivat myös VAHTI Sovelluskehityksen tietoturvaohjeen vaatimusten mukaiset. Kun vaatimukset ovat sen mukaiset, on niiden toteuttaminen kaikille asiakasorganisaatiolle helpommin perusteltavissa ja tuo asiantuntevuutta.

Projektikäsikirjaa tule päivittää ottamaan huomioon tietoturvallisuus kaikissa projekteissa. VAHTI Sovelluskehityksen tietoturvaohje määrittää muun muassa, että ilman erillistä tietoturva-asiantuntijaa, on tietoturvallisuus projektipäällikön ja projektitiimin vastuulla. Tämä tulisi lisätä vastuulistaan.

Kehitettävät asiat projekteissa:

- Hankkeen tietoturvaohje joka projektille (ks. VAHTI 9/2008 Hankkeen tietoturvaohje)
- Kirjallinen tietoturvallinen sovelluskehitysprosessi, jota noudatetaan ja joka koulutetaan sovelluskehittäjille (ks. SKM-001)
- Koulutusta tietoturvallisesta kehittämisestä ja testaamisesta henkilöstölle (ks. OSK-001, OSK-002, OSK-003, OSK-006, OSK-007)
- Projektikäsikirjan vastuulistoja tulee kasvattaa myös tietoturva-asioissa
- Tietoturvavaatimukset erilliseen dokumenttiin (ks. VTM-001), josta niitä voidaan poimia projekteihin. Niihin voidaan myös liittää esimerkkitoteutus esimerkiksi lokimerkinnöille vaatimusten TOT-002 ja TOT-003 mukaiseksi.

8.3 Vastaukset tutkimuskysymyksiin

1. Mitä tietoturvan huomioiminen tarkoittaa ohjelmistokehitysprojektissa?

Ensimmäisenä tutkimuskysymyksenä oli selvittää, mitä tietoturvan huomioiminen tarkoittaa sovelluskehitysprojektissa. Tähän tutkimuskysymykseen vastataan luvuissa 3−5. Yhteenvetona voidaan sanoa, että sovelluskehityksen tietoturvallisuus alkaa jo ennen itse projektin alkua organisaation tasolla, ja kaikki tietoturvallisuus lähtee johdon halusta toteuttaa se. Organisaatiolla on oltava selkeä ohjeistus, politiikat ja riskienhallinta tietoturvallisuudesta sen koko liiketoiminnan laajuisesti. Tämän jälkeen voidaan siirtyä sovelluskehitysprojektiin ja sen asettamiin projektikohtaisiin tietoturvahaasteisiin. Projektille ja sen seurauksena toteutettavalle sovellukselle on laadittava kattavat tietoturvavaatimukset ja seurattava niiden toteutumista. Tähän auttavat VAHTI Sovelluskehityksen tietoturvaohjeen vaatimukset, jotka listaavat tarvittavat osa-alueet. Viimeisenä kerroksena sovelluskehittäjillä on vastuu toteuttaa toiminnalliset ja tietoturvavaatimukset. Heidän ammattitaitonsa ja kiinnostuksensa tietoturvallisuutta kohtaan on avainasemassa. Organisaation on tarjottava kaikki mahdollinen

tuki ja koulutus tietoturvallisuuden toteuttamiseen sovelluskehitysprojektissa, jotta tietoisuuden puute ei ole haavoittuvuuksien ilmestymisen syy.

2. Miten yrityksen nykyinen prosessi huomioi VAHTI Sovelluskehityksen tietoturvaohjeen vaatimukset?

Toinen tutkimuskysymys pyrki selvittämään nykyisen prosessin ja hiljaisen tiedon toimeksiantajan työntekijöiden keskuudessa. Nykyinen projektikäsikirja ei ota kantaa tietoturvallisuuden toteuttamiseen, ja yrityksen tasolla tietoturvallista sovelluskehittämisen ohjetta on vasta alettu laatia, mutta siitä ei vielä ole julkaistua versiota. Haastatteluista kävi ilmi, että työntekijöillä on harrastuneisuutta tietoturvalliseen kehittämiseen ja kiinnostusta löytyy. Projektiohjeet ja vaatimukset eivät kuitenkaan vaadi tietoturvallisuuden ehdotonta toteuttamista, joten se jätetään yleensä vain pienelle huomiolle ja korjataan vain räikeimmät virheet, joiden havaitseminen on helppoa. Yhdessä toimeksiantajan projektissa vaatimukset otettiin huomioon, ja niitä toteutettiin erillisissä tietoturvasprinteissä sekä testauksessa jatkuvasti. Näitä käytäntöjä ei kuitenkaan ole kirjattu ylös koko organisaation tasolla.

3. Miten yrityksen prosesseja tulisi muuttaa, jotta ne vastaisivat VAHTI Sovelluskehityksen tietoturvaohjeen vaatimuksia?

Kolmas tutkimuskysymys on koko tutkimuksen pääkysymys, jonka vastaus tarjoaa ratkaisumallit toisen tutkimuskysymyksen vastauksena esiteltyyn nykyisen prosessin kehityskohteisiin. Hyviä käytänteitä oli havaittavissa työntekijöiden työssä, ja sekä haastatteluissa että VAHTI Sovelluksen tietoturvaohjeen vaatimuksia tarkastelemalla päästiin samoihin kehityskohteisiin. Näitä olivat kirjallinen tietoturvallinen sovelluskehitysprosessi, koulutus ja vaatimusten listaus helpompaan muotoon. Lisäksi teoriassa todettiin, että tulisi laatia jokaiselle projektille myös erillinen hankkeen tietoturvaohje ja olemassa olevan projektikäsikirjan vastuulistoja tulisi muuttaa kattamaan myös tietoturvallisuus, jotta ne otetaan varmasti huomioon kaikissa projekteissa.

9 Pohdinta

Pohdinnassa arvioidaan saatuja tuloksia ja tutkimuksen toteutusta. Siinä myös esitellään jatkokehitysmahdollisuuksia ja arvioidaan mitä prosessin aikana opittiin.

9.1 Tavoitteet ja tulokset

Toimeksiantaja ymmärtää VAHTI Sovelluskehityksen vaatimusten toteuttamisen tärkeyden, mutta siltä ei löytynyt tietoa tämän hetkisestä tilanteesta tai niiden toteuttamisen vaiheista. Tavoitteena oli löytää olemassa olevat hyvät toimintatavat, poimia vaatimuksista prosessille kehityskohteita ja tuoda lisätietoa VAHTI Sovelluskehityksen tietoturvaohjeen rinnalle laajentamalla siinä käsiteltyjä aiheita.

Toimeksiantajaa opinnäytetyö hyödyttää erityisesti, koska haastattelut kohdistuivat sen työntekijöihin ja koska prosessia voidaan kehittää räätälöidysti juuri toimeksiantajan organisaatiossa. Toisaalta koska toimeksiantaja on pk-yritys ja sen ominaisuudet on kuvattu hyvin, voidaan tämän tutkielman huomioita soveltaa myös muiden alalla toimivien pk-yritysten toiminnan kehittämiseen. Opinnäytetyön avulla voidaan tutustua ohjeessa esiteltyihin käsitteisiin, niiden selityksiin ja vaatimuksiin lukematta jokaista vaatimusta itse ohjeesta. Opinnäytetyllä voidaan tutustua oman sovelluskehitysvastuualueen vaatimuksiin ja tarkastaa niiden toteutuminen liitteenä olevien vaatimuksista johdettujen kysymyslistojen avulla. Vaikka VAHTI Sovelluskehityksen tietoturvaohje on tarkoitettu ensisijaisesti julkishallinnon projekteihin, voivat myös yksityiset organisaatiot saada ohjeesta hyödyllistä tietoa tietoturvallisuuden toteuttamisesta.

Tutkielman alkuperäinen tutkimuksen kohde oli ainoastaan yksi projekti toimeksiantajan projektisalkussa. Tarkoitus oli tutkia ja kirjata ylös hyvät ja huonot toimintatavat VAHTI Sovelluskehityksen tietoturvavaatimusten toteuttamisesta projektissa. Tämän projektin aikataulu kuitenkin venyi keväällä 2014 niin pahasti, että pystyin haastattelemaan projektiryhmää vasta huhtikuun lopussa. Haastatteluajankohdan venyessä jo helmikuussa päätettiin tehdä suunnanmuutos niin, että haastattelen myös muissa projekteissa työskenteleviä sovelluskehittäjiä ja muita sidosryhmiä. Tutkielman kannalta tämä oli kuitenkin hyvä asia, sillä yhteen projektiin keskittymisen sijaan tutkin toimeksiantajan yleistä sovelluskehitysprosessia ja etsin hyviä käytänteitä muistakin projekteista. Vastoinkäymisten jälkeen sain alkuperäisen projektin ryhmääkin haastateltua, mikä toi taas toisenlaista tietoa tietoturvallisuudesta yleisen tietoisuuden lisäksi.

Kirjoittaja oppi tietoturvallisuudesta yleisellä tasolla ja sen suhteen, mitä sen toteuttaminen sovelluskehitysprojektissa käytännössä tarkoittaa. Tietoturvallisuus on monen asian summa ja vaatii erilaisia vastuuhenkilöitä. Kirjoittajan mielenkiinto oli jo ennen työn aloittamista suuri, mutta se kasvoi työn edetessä. Kirjoittaja työskenteli kokopäiväisesti koko opinnäytetyöprosessin aikana, joten ajankäytön hallintaa ja venymistä tarvittiin puolin ja toisin.

9.2 Tutkimuksen luotettavuus

Haastattelut olivat onnistuneet niiden tulosten sisältämien uusien ehdotusten ja työtekijöiden työtehtävien erojen takia. Kvalitatiivisen tutkimuksen haastatteluiden luotettavuuden kannalta niin sanottu kyllääntymispiste saavutettiin, koska haastateltavien vastaukset alkoivat muistuttaa toisiaan, vaikka he kaikki työskentelivät eri tehtävissä ja projekteissa. Haastatteluissa oli myös hyvä huomata, että työntekijät ehdottivat samoja kehityskohteita, jotka olivat jo VAHTI Sovelluskehityksen tietoturvaohjeen vaatimuksia. Tämä osoittaa sekä tietotaitoa toimeksiantajan organisaatiossa että myös kuvastaa VAHTI-ohjeen ja siitä tehtyjen tämän opinnäytetyön havaintojen luotettavuutta.

Haastatteluiden tulokset ovat selkeitä, mutta muutaman kysymyksen kysymyksenasettelu jäi liian rajaavaksi. Kvalitatiiviseen tutkimukseen olisi kuulunut käyttää avoimia kysymyksiä ja tässä haastattelussa oli monta suljettua kysymystä. Tavoitteeseen selvittää VAHTI Sovelluskehityksen tietoturvaohjeen yksittäisiä vaatimuksia päästiin, mutta kehitystiimiä koskevien kysymysten kohdalla ei löydetty tutkimusta hyödyttävää uuttaa tietoa.

9.3 Jatkokehitysmahdollisuudet

Tahtotila oli alussa, että työstä olisi saanut toimeksiantajalle suoraa tietoa sen omaan sovelluskehitysprosessiin vaatimusten esimerkkitoteutuksena. Jotta opinnäytetyö olisi ollut alkuperäisen kattava, olisi teoriaosuudessa keskitytty koodiesimerkein esimerkiksi käytännön tietoturvalliseen sovelluskehittämiseen. Käytännön syistä ja rajauksen takia ei teoriaosuudesta tehty alkuperäisen suunnitelman mukaisesti tarkkaa, vaan paneuduttiin asioihin yleisemmällä tasolla. Tällaisia käytänteitä voisi kehittää toimeksiantajan käyttöön.

Jatkokehitysmahdollisuuksina olisi kehittää toimeksiantajalle kirjallinen tietoturvallisuuden huomioon ottava sovelluskehitysprosessi ja laatia pohjat dokumentaatiosta, joita tarvitaan jokaisessa projektissa liittyen tietoturvaan. Lisäksi tämän prosessin käyttöönoton jälkeen tulisi tehdä kontrollikysely, jossa selvitettäisiin, onko tietoturvallisesta kehittämisestä tullut sovelluskehittäjille arkipäivää ja millä tavalla sen aikainen prosessi ottaa tietoturvallisuuden huomioon. Lisäksi mielenkiintoista olisi tietää, miten tietoturvallisuuden tarjoaminen asiakkaalle on muuttunut uusien prosessien myötä ja onko se lisännyt myyntiä. Tutkimuksen voisi laajentaa myös koko ICT-alalle ja kartoittaa VAHTI Sovelluskehityksen tietoturvaohjeen vaatimusten täyttäminen organisaatiotasolla ja projekteissa. Tämä tutkimus toisi parhaiten tietoa kvantitatiivisena tutkimuksena.

Lähteet

Alex, B. Taylor, L. & Winch, R. 2014. Spring Security Reference. Päivitetty 25.3.2014. Viitattu 6.4.2014. http://docs.spring.io/spring-security/site/docs/3.2.3.RELEASE/reference/htmlsingle/

Antila, T. 2012. Alihankintaprosessin kehittäminen levyosavalmistuksessa. Diplomityö. Tampereen teknillinen yliopisto, Konetekniikan koulutusohjelma. http://URN.fi/URN:NBN:fi:tty-201209101274

Eskelinen, A. Heiramo, P. Haukilehto, A. Kirjavainen, A. Koskela, L. Laanti, M. Lekman, L. Lilja, S. Lindström, J. Nyman, R. Taipale, M. Tikka, A. Virtanen, P. Zieg, L. 2014. Suomenkielinen scrum-sanasto. Viitattu 8.5.2014. Päivitetty 1/2014. http://lekman.fi/scrumguide/, Sanasto.

Foundation Level Syllabus. 2011. ISTQB Foundation Level Syllabus. Päivitetty 1.4.2011. Viitattu 23.4.2014. http://www.istqb.org, Downloads, Syllabi, Foundation Level Syllabus.

Hartig, O. 2014. “Venäjän Facebookin” perustaja paljastaa: FSB vaati Euromaidan-mielenosoittajien tietoja. Artikkeli Tietoviikon sivuilla. Viitattu 3.5.2014. http://www.tietoviikko.fi/kaikki_uutiset/quotvenajan+facebookinquot+perustaja+paljastaa+fsb+vaati+euromaidanmielenosoittajien+tietoja/a982777

Hämäläinen, L. 2007. Case-tutkimus: BS7799-vaatimusten, VAHTI-tietoturvaohjeiden ja ITIL-prosessikuvausten vertailusta ja yhdistämisestä. Pro gradu -tutkielma. Tampereen yliopisto, Tietojenkäsittelytieteiden laitos. http://urn.fi/urn:nbn:fi:uta-1-16677

Kananen, J. 2008. Kvali. Jyväskylä: Jyväskylän ammattikorkeakoulun julkaisusarja.

Komission suositus 2003/361. 2003. I OSASTO, KOMISSION HYVÄKSYMÄ MIKROYRITYSTEN SEKÄ PIENTEN JA KESKISUURTEN YRITYSTEN MÄÄRITELMÄ, 2 Artikla. Viitattu 26.2.2014. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:fi:PDF

Kouns, J. & Minoli, D. 2010. Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams. Viitattu 15.3.2014. John Wiley & Sons. http://www.jamk.fi/kirjasto, Nelli-portaali, books24x7.

Kumar, B.V. & Bhargav, A. 2011. Secure Java: For Web Application Development. Auerbach Publications. http://www.jamk.fi/kirjasto, Nelli-portaali, books24x7.

Laadullisen ja määrällisen tutkimuksen erot. N.d. Viitattu 4.3.2014. http://tilastokeskus.fi/virsta/tkeruu, 1. Teoreettiset lähtökohdat, Laadullisen ja määrällisen tutkimuksen erot.

Laki julkisista hankinnoista 30.3.2007/348. Viitattu 8.4.2014. http://www.finlex.fi/fi/laki/ajantasa/2007/20070348

Lehtinen, V. 2010. Tietoturvan ja tietosuojan kehittäminen pilviteknologiassa - Standardit ja kehitysmallit sekä riskienhallinnan näkökulma. Pro gradu -tutkielma. Jyväskylän ylipisto, Tietojenkäsittelytieteiden laitos. http://urn.fi/URN:NBN:fi:jyu-201012093149

McDowell, M. 2009. Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks. Viitattu 19.4.2014. Päivitetty 22.10.2009. http://www.us-cert.gov/ncas/tips/ST04-014

Mitä julkiset hankinnat ovat? 2014. Artikkeli Työ- ja elinkeinoministeriön sivuilla. Viitattu 5.3.2014. Päivitetty 5.3.2014. http://www.tem.fi, Kuluttajat ja markkinat, Julkiset hankinnat.

Perrin, C. 2008. Understanding layered security and defense in depth. Blogikirjoitus. Päivitetty 18.12.2008. Viitattu 25.4.2014. http://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/

Pham, A. & Pham, P-V. 2012. Scrum in Action: Agile Software Project Management and Development. Viitattu 3.5.2014. Cengage Learning. http://www.jamk.fi/kirjasto, Nelli-portaali, books24x7.

Pries, K. & Quigley, J. 2011. Scrum Project Management. Viitattu 4.5.2014. Auerbach Publications.

Råman, J. 2006. Regulating Secure Software Development. Väitöskirja. Lapin yliopisto, Oikeustieteellinen tiedekunta.
http://www.doria.fi/bitstream/handle/10024/66729/Jari_Råman_väitöskirja.pdf

Session Management Cheat Sheet. 2014. Wiki-sivu OWASP.org sivustolla. Päivitetty 20.3.2014. Viitattu 6.4.2014.
https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

Shrimp, D. & Rawsthorne, D. 2009. Scrum In A Nutshell. Artikkeli Scrum Alliancen sivuilla. Viitattu 4.5.2014. Päivitetty 21.12.2009. http://www.scrumalliance.org, Community, Member Articles, 2009, December, Scrum In A Nutshell.

Snowden, E. 2014. Here's how we take back the Internet. Viitattu 19.4.2014. Päivitetty maaliskuu 2014.
http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet

Standards. N.d. Standards. Sivu World Wide Web Consortium (W3C) sivustolla. Viitattu 3.4.2014. www.w3.org, Standards.

Toimeksiantajan projektikäsikirja. 2013. Projektikäsikirja.

VAHTI 1/2013. 2013. VAHTI Sovelluskehityksen tietoturvaohje. Päivitetty 7.2.2013. Viitattu 16.12.2013. www.vm.fi, Julkaisut ja asiakirjat, Julkaisut, Valtiollinen tietoturvallisuus, Sovelluskehityksen tietoturvaohje VAHTI 1/2013.

VAHTI 4/2013. 2013. VAHTI Henkilöstön tietoturvaohje. Päivitetty 25.11.2013. Viitattu 27.4.2014. http://www.vm.fi, Julkaisut ja asiakirjat, Julkaisut, Valtiohallinnon tietoturvallisuus, VAHTI 4/2013 Henkilöstön tietoturvaohje.

VAHTI 5/2009. 2009. VAHTI Effective Information Security. Päivitetty 29.06.2009. Viitattu 24.02.2014. www.vm.fi, Julkaisut ja asiakirjat, Julkaisut, Valtiollinen tietoturvallisuus, Effective Information Security VAHTI 5/2009.

VAHTI 5/2013. 2013. VAHTI Päätelaitteiden tietoturvaohje. Viitattu 8.4.2014. Päivitetty 10.12.2013. www.vm.fi, Julkaisut ja asiakirjat, Julkaisut, Valtiollinen tietoturvallisuus, Päätelaitteiden tietoturvaohje, VAHTI 5/2013.

VAHTI 9/2008. 2008. VAHTI Hankkeen tietoturvaohje. Päivitetty 11.12.2008.Viitattu 24.02.2014. www.vm.fi, Julkaisut ja asiakirjat, Julkaisut, Valtiollinen tietoturvallisuus, Hankkeen tietoturvaohje VAHTI 9/2008.

Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa 1.7.2010/681. 2010. Viitattu 24.2.2014. http://www.finlex.fi/fi/laki/alkup/2010/20100681

VM, VAHTI ja tietoturvallisuus. N.d. Tietosivu Vahtiohjeen sivuilla. Viitattu 26.2.2014. https://www.vahtiohje.fi/web/guest/vm-vahti-ja-tietoturvallisuus

Liitteet

Liite 1: Organisaation vaatimukset

Perustaso

- Onko asiakasorganisaation sovelluskehityksen kannalta merkittävät henkilöt tunnistettu ja heille varattu riittävästi aikaa tietoturvatehtäviin? (STR-001)
- Onko organisaatiolle määritetty kirjallinen VAHTI Sovelluskehityksen tietoturvaohjeen mukainen tietoturvapolitiikka? (POL-001)
- Onko organisaatiolla kartoitettuna ne roolit, joiden haltioista pitää olla turvallisuusselvitys ja onko tämä turvallisuusselvitysprosessi dokumentoitu? (POL-002)
- Onko organisaation kaikille tietojärjestelmille määritelty omistaja? (POL-003)
- Tehdäänkö organisaatiolle säännöllisesti kokonaisriskianalyysi, joka ottaa huomioon myös tietoturvallisuuteen liittyviä riskejä, niistä seuraavat ehkäisytoimenpiteet ja seurannan? (RSK-001)
- Onko sovelluskehityksestä vastuussa oleville henkilöille järjestetty tietoturvatietoisuuskoulutusta säännöllisesti vuosittain, jossa käydään läpi sovellusten tyypillisiä tietoturvaongelmia? Tämä on erittäin tärkeää uusille sovelluskehittäjille. (OSK-001)
- Onko organisaatiolla olemassa ylläpidetty lista dokumenteista, joista löytyy tietoturvaohjeistusta organisaatiossa käytettäville teknologioille ja työkaluille? (OSK-002)
- Onko tietoturvakoulutus osa organisaation perehdytyskoulutusta? (OSK-003)
- Seurataanko organisaation tietoturvasääntöjen noudattamista, tiedotetaanko sen seuraamisesta ja puututaanko sen noudattamatta jättämiseen? (OSK-004)
- Onko organisaatiolla ainakin yksi tietoturvalliseen sovelluskehitykseen perehtynyt henkilö, joka vastaa tietoturvallisuuskoulutuksesta ja jolta projektitiimit saavat tietoturvakonsultaatiota? (OSK-005)
- Onko organisaatiolla kirjallinen toipumisstrategia ja -suunnitelma? (JTH-001)
- Onko jatkuvuus turvattu sen kannalta avainasemassa olevien roolien ja henkilöiden osalta, mikäli avainhenkilö ei olisi saatavilla? (JTH-002)

- Onko kaikkien ulkoisten kirjastojen, sovelluspalvelinten, tietokantojen, jne. ja itse sovelluksen kriittiset tietoturvapäivitykset tunnistettu ja asennettu? Tämän toiminnan pitää olla organisoitua ja vastuutettua. (YLP-001)
- Seurataanko sovelluksen käyttämien komponenttien elinkaarta, jotta mahdollinen siirtyminen uuteen voidaan aloittaa hyvissä ajoin? (YLP-002)
- Onko tuotannon tietokannan muokkaaminen ohi sovelluksen tuoteomistajan hyväksymää ja jääkö siitä merkintä tietokannan lokiin, johon voidaan tarvittaessa palata? (YLP-003)
- Dokumentoidaanko sovelluksen tyypillisimmät virhetilanteet ja toimenpiteet niistä toipumiseksi? (YLP-004)
- Onko sovelluksen tietoturvapäivitysten ja korjauksien asennus dokumentoitu, organisoitu, vastuutettu ja dokumentti katselmoitu? (YLP-005)
- Onko tietoturvapoikkeamien luokittelulle suunniteltu periaatteet, jotta tiedetään mitkä korjaukset on saatettava tuotantoon välittömästi? (YLP-006)
- Onko organisaation asiakkaille ja sidosryhmille tarjottu ja tiedotettu mahdollisuudesta raportoida vakavia tietoturvapuutteita tai haavoittuvuuksia? (YLP-007)
- Varmuuskopioidaanko ainakin sovelluksen tiedot ja konfiguraatiot säännöllisesti sovelluksesta riippumattomalle järjestelmälle? Onko tietojen palautusmenettely kuvattu toipumissuunnitelmassa?
- Onko sovelluksen tiedoille tehty arvon määrittely? (KTP-001)
- Hoidetaanko käytöstä poistettavan tiedon tuhoaminen tietoturvallisesti? (KTP-002)
- Onko tieto muunnettu formaattiin, jossa sitä voidaan lukea tulevaisuudessakin? (KTP-003)
- Onko säilytettävä tieto luokiteltu ja luokittelu perusteltu? (KTP-004)

Korotettu taso

- Onko organisaatiolle määritetty tietoturvatyön vastuualueet määrittävä ja organisaation liiketoimintasuunnitelman kanssa linjassa oleva tietoturvastrategia? (STR-002)
- Onko organisaation tietoturvapolitiikalle määritetty katselmointi- ja päivitysprosessi vastuuhenkilöineen? (POL-004)

- Onko organisaatiolla lokipolitiikka? (POL-005)
- Onko organisaatiolla käyttövaltuuspolitiikka? (POL-006)
- Onko organisaation riskienhallintaprosessi kuvattu sen riskienhallintapolitiikassa? (RSK-002)
- Järjestetäänkö projektiorganisaation henkilöille räätälöityä tehtäväkohtaista koulutusta? Tämä tarkoittaa testaajille, toteuttajille ja tuoteomistajille erikseen järjestettävää tietoturvakoulutusta. (OSK-006)
- Onko organisaation tietoturvakoulutus kuvattu kirjallisesti, sen päivittäminen ja katselmointi vastuutettu, jotta se pysyy ajantasaisena? (OSK-007)
- Onko organisaation tärkeimmille järjestelmille laadittu toipumissuunnitelmat sekä niiden katselmointi ja päivittäminen vastuutettu? (JTH-003)
- Ovatko eri vakavuusluokkien päivitysten tavoiteajat, huoltoikkunat, roolit, jne. määritelty sovelluksen päivitysten hallintaprosessissa, joka on kirjallinen katselmoitu ja vastuutettu prosessi? (YLP-010)
- Auditoidaanko sovellusympäristön tietoturvallisuuteen vaikuttavien asetukset säännöllisesti? (YLP-011)
- Onko tietoturvapoikkeamien käsittelyprosessi dokumentoitu? (YLP-012)
- Onko mahdollisten tietoturvapoikkeamien julkinen tiedottaminen laadittu, dokumentoitu ja vastuutettu? (YLP-013)
- Onko korotetun tason sovelluksen tietoturvapoikkeamien raportoinnille dokumentoitu menetelmä ja dokumenttipohjat? (YLP-014)
- Suoritetaanko tietoturvapoikkeamien ja -puutteiden korjauksen jälkeinen analyysi syiden etsimiseksi ja korjaavien toimenpiteiden määrittämiseksi? (YLP-015)
- Onko päivitys- ja muutosperiaatteet dokumentoitu? (YLP-016)
- Seurataanko sovelluksen tuottamaa lokia automaattisesti tai manuaalisesti jatkuvasti, jotta väärinkäytökset ja hyökkäykset voidaan havaita välittömästi? (YLP-017)
- Onko sovelluksesta laadittu kirjallinen varmuuskopiointipolitiikka? (YLP-018)
- Onko korotetun tason sovelluksesta olemassa varmuuskopioiden lisäksi suojakopiot, jos varmuuskopiot eivät ole jostain syystä käytettävissä? (YLP-019)

Korkea taso

- Ottaako riskienhallintaprosessi huomioon organisaation toiminnan suuret muutokset ja niistä seuraavien tietoturvariskien uudelleenarvioinnin? (RSK-003)
- Pystyykö koulutus reagoimaan organisaation äkillisiin muutoksiin nopealla aikataululla toteutetulla lisäkoulutuksella tai tiedotuksella, jotka vaikuttavat merkittävästi tietoturvallisuuden tilaan? (OSK-008)
- Onko organisaation jatkuvuus- ja toipumissuunnitelmia testattu käytännössä ja tehdäänkö sitä säännöllisesti? (JTH-004)
- Seurataanko organisaation järjestelmien häiriöitä ja niiden syitä riskianalyysien ja yhteistyösopimusten laatimisen tueksi? (JTH-005)
- Onko tuotantoympäristössä mekanismi yllättäviin tietoturvatilanteisiin reagointiin? (YLP-020)
- Onko korkean tason sovelluksen varmuuskopioiden palauttamista testattu säännöllisesti? (YLP-021)
- Laaditaanko sovelluksessa havaituista tietoturvapoikkeamista vuosittain yhteenvetoraportti? (YLP-022)
- Seurataanko sovelluksen tietoturvapäivitysten onnistumista ja ajantasaisuutta? (YLP-023)
- Tilastoidaanko korkean tason sovelluksen palautettujen tietojen määrää ja syitä toiminnan ja sovelluskehityksen parantamiseksi? (YLP-024)

Liite 2: Projektiorganisaation vaatimukset

Perustaso

- Onko organisaatiolla kirjallinen sovelluskehitysprosessi, joka ottaa kantaa kaikkiin kehitysvaiheisiin ja niiden tietoturvahaasteisiin (secure SDLC)? (SKM-001)
- Onko toteutettavan sovelluksen tarkoitus ja sen kriittisyys asiakasorganisaation liiketoiminnan kannalta määritelty? (ESI-001)
- Onko toteutettavalle sovellukselle laadittu liiketoiminnan vaikutusanalyysi? (ESI-002)
- Onko toteuttajille suunnittelun pohjaksi tulevat tietoturvavaatimukset toteuttavat ratkaisut dokumentoitu? (VTM-001)
- Onko sovelluksen käsittelemään tietoon, toimintaympäristöön tai muuhun seikkaan vaikuttavat lainsäädännölliset vaatimukset otettu huomioon? (VTM-002)
- Onko toteutettavalle sovellukselle laadittu karkean tason lista tietoturvavaatimuksista eri osa-alueilta, kuten luottamuksellisuus, eheys ja saatavuus, perustuen esitutkimusvaiheessa määriteltyyn sovellusprofiiliin? (VTM-003)
- Onko tuoteomistaja määrittänyt toteutettavan järjestelmän tietoturvallisuustason ja sen tietoaineiston arkistoinnin vaatimukset? (VTM-004)
- Onko toteutettavalle sovellukselle laadittu riskianalyysi?`(VTM-005)
- Onko sovellukselle laadittu tietoturvavaatimukset? (VTM-006)
- Onko tietoturvavaatimusten laatimisessa käytetty soveltuvia lakeja, määräyksiä, standardeja ja hyvien käytäntöjen ohjeistuksia? (VTM-007)
- Onko toteutettavan sovelluksen toimintaympäristö (mm. prosessoriarkkitehtuuri, käyttöjärjestelmien versiot, tarvittavat kirjastot) kuvattu ja ylläpidetäänkö sitä? (KTY-001)
- Ovatko sovelluksen käyttöönottovaiheessa tietoturvallisuuteen vaikuttavat oletusasetukset ja muut asetukset listattu, jotta ne huomioidaan asennuksessa? Onko sovelluksesta laadittu kovennusdokumentti? (KTY-002)
- Onko tuoteomistajan määrittelemän tiedon suojaustason mukaiset tiedon käsittelyyn liittyvät vaatimukset otettu huomioon? (KTY-003)

- Onko asiakasorganisaation riskikarttaan lisätty toteutettavan sovelluksen huomioiva osa? (KTY-004)

Korotettu taso

- Onko toteutettavalle sovellukselle suoritettu johonkin valittuun metodiin tai malliin pohjautuva uhkamallinnus? (VTM-008)
- Onko asiakasorganisaation määrittämän arkkitehtuurilinjauksen mukaiset tietoturva- ja muut vaatimukset otettu huomioon? (VTM-009)
- Onko sovelluksen toteuttamiseen ja arkkitehtuuriin liittyvät uhat, kuten käyttäjäroolit, tietototurvaoletukset tai teknologiat, otettu huomioon uhkamallinnuksessa? (VTM-010)
- Onko sovelluksen asentamisesta laadittu sen käsittelemän tiedon asettamat tietoturvallisuusasetukset huomioon ottava kirjallinen dokumentti? (KTY-005)

Korkea taso

- Onko toteutettavan sovellukseen liitettävien ja sen käyttämien kolmansien osapuolten komponenteille, kuten avoimen lähdekoodin kirjastot, tehty uhkamallinnusta? (VTM-011)

Liite 3: Projektiryhmän vaatimukset

Perustaso

- Onko arkkitehtuurin suunnittelussa suosittu yleisesti käytössä olevia ja hyväksyttyjä standardeja? (SNT-001)
- Huomioidaanko helppo korjausten ja tietoturvapäivitysten asentaminen jälkikäteen kovakoodausta ja tietyistä ajoympäristöistä riippumattomuutta välttämällä? (SNT-002)
- Onko sovelluksen käyttämistä ohjelmistokomponenteista, kirjastoista ja sovelluskehyksistä olemassa ylläpidetty lista toiminnallisuuden mukaan? (SNT-003)
- Ovatko sovelluksen ulkoiset rajapinnat käyty läpi ja verrattu organisaation ohjeistukseen vaatimuksessa TSK-001? (SNT-004)
- Käytetäänkö arkkitehtuurin suunnittelussa turvallisia suunnittelumalleja? (SNT-005)
- Onko sovelluksen hyökkäyspinta tunnistettu? (STN-006)
- Onko sovelluksen arkkitehtuuri analysoitu tietoturvavaatimusten kanssa? (SNT-007)
- Onko perustason vaatimusten mukaiset TSK-002 tietoturvaratkaisut varmistettu katselmoinneissa? (SNT-008)
- Onko valitun tunnistautumismenetelmän tietoturvallisuuden taso tuoteomistajan määrittämän sovelluksen käsittelemän tiedon turvatason mukainen? (SNT-009)
- Onko salasanavaatimusten uudelleenkonfigurointi otettu huomioon tai mahdollisesti siirretty sovelluksen hallinnasta kokonaan ulkoiseen LDAP-hakemistotietokantaan? (SNT-010)
- Huomioidaanko käyttäjien roolin vähimpien välttämättömimpien käyttöoikeuksien asettaminen ja sovelluksen komponenttien suorittaminen pienimmällä mahdollisilla käyttöoikeuksilla? (SNT-011)
- Onko sovelluksen luottamusrajat määritelty ja validoidaanko kaikki data tuon rajan toiselta puolelta ns. white list tyyppisesti? (SNT-012)
- Onko VAHTI Sovelluskehityksen tietoturvaohjeen mukaiset SNT-013 määrittämät salausratkaisut toteutettu? (SNT-013)

- Onko mahdolliset tuki- ja ylläpitoyhteydet huomioitu ja tarkastettu salauksen osalta? (SNT-014)
- Onko poikkeusten- ja virheiden käsittely suunniteltu ja toteutettu huomioimalla TOT-001 vaatimuksen kohdat? (TOT-001)
- Kirjoittaako sovellus lokimerkinnät TOT-002 vaatimuksen määrittämän listan tapahtumista? (TOT-002)
- Sisältääkö lokitapahtuman merkintä ainakin TOT-003 vaatimuksen mukaiset tiedot? Noudattaako lokimerkintä ennalta määrättyä rakennetta?(TOT-003)
- Synkronoivatko kaikki ympäristöön kuuluvat laitteet kellonsa samasta lähteestä? (TOT-004)
- Onko lokin lukuoikeudet määritetty tietoturvallisesti ja kirjoitetaanko jokainen merkintä erikseen puskuroimatta? (TOT-005)
- Onko istunnon suojaamiseen toteutettu ainakin TOT-006 vaatimuksen mukaiset toimenpiteet? (TOT-006)
- Onko käyttäjätunnusten hallinta toteutettu keskitetysti, ajantasaisesti ja mahdollisesti tukemaan tai ulkoistettu LDAP-hakemistotietokannalle? (TOT-007)
- Suoritetaanko koodikatselmointeja säännöllisesti huomioiden TSK-001 ja TSK-002 vaatimukset sekä yleisimmät sovelluskehitykseen liittyvät tietoturvaongelmat? (TOT-008)
- Onko tietoturvallisuuden testitapaukset johdettu useista ainakin TST-001 vaatimuksen määrittämistä lähteistä? (TST-001)
- Onko tietoturvasuunnitelmat katselmoitu ja arvioitu tietoturvavastaavan toimesta? (TST-002)
- Onko tietoturvatestaus suoritettu ja testiraportti laadittu niiden suorittamisesta? (TST-003)
- Onko sovelluskehityksen tietoturvavastaava suorittanut ja dokumentoinut epäformaaleja koodikatselmointeja tietoturvallisuuden kannalta kriittisiin komponentteihin? (TST-004)
- Onko testidatan tietoturvallisuudesta pidetty huolta generoimalla se kokonaan, poistettu salassa pidettävät tiedot ja sekoitettu tiedot keskenään, jotta tietueet eivät ole kokonaisuudessaan koskaan aitoja, vaikka yksittäiset tiedot ovatkin? (TST-005)

Korotettu taso

- Onko vaatimusmäärittelyvaiheessa tehtyä uhkamallinnusta päivitetty valittujen teknisten ratkaisujen ja toiminnallisuuksien pohjalta? (SNT-015)
- Onko mahdollisen monitasoarkkitehtuurin eri komponenttien välinen tietoliikenne suunniteltu, dokumentoitu ja salattu? (SNT-016)
- Toteuttaako sovellus korotetun tason sovellukselle asetettavat lokien muokkaamiseen liittyvät TOT-009 vaatimukset? (TOT-009)
- Käytetäänkö tietoturvatestaamisessa automaattisia testaustyökaluja? (TST-006)
- Onko korotetun tason sovellukselle suoritettu riippumaton tietoturva-auditointi ennen tuotantoon viemistä? (TST-007)
- Onko sovelluksen tietoturvamekanismit tarkastettu, kuten autentikaatio, istunnon käsittely ja syötteiden validointi? (TST-008)

Korkea taso

- Tukeeko korkean tason järjestelmä vahvaa useamman tietolähteen tunnistautumista? Käyttääkö sovellus eri palvelimille sijoiteltua monitasoarkkitehtuuria? (STN-017)
- Toteuttaako sovellus korkean tason sovellukselle asetettavat lokien muokkaamiseen liittyvät TOT-010 vaatimukset? (TOT-010)
- Onko tietoturvatestitapausten läpäisy määritetty vaatimukseksi siirryttäessä vaiheesta toiseen ja niiden läpäisy todettu? (TST-009)
- Onko sovelluskehityksen aikainen tietoturvallisuus auditoitu ainakin tarkastuspisteissä? (TST-010)
- Onko koodikatselmointien läpäisy määritetty vaatimukseksi siirryttäessä vaiheesta toiseen ja mahdollisten tietoturvapuuteiden riskiarviointi suoritettu? (TST-011)

Liite 4: Haastattelukysymykset

Haastattelurunko: VAHTI Sovelluskehityksen tietoturvaohjeen vaatimukset ketterässä sovelluskehityksessä

Henkilön taustatiedot

1. Missä tehtävässä työskentelette yrityksessä?

2. Missä tehtävässä työskentelette nykyisessä projektiorganisaatiossa?

3. Onko tietoturvallisuus ja sen toteuttaminen websovelluksessa teille arkipäivää?

4. Oletteko tutustunut VAHTI-ohjeisiin ja kuinka moneen?

5. Seuraatteko tietoturvallisuuteen liittyvää uutisointia, blogeja tai muuta ajankohtaista tietoa?

Prosessin taustatiedot

6. Onko yrityksen projektikäsikirja teille tuttu?

7. Minkälaista ohjelmistokehityksen menetelmää projektissa käytetään?

8. Miten nykyinen prosessi ottaa huomioon tietoturvallisuuden projektin aikana?

9. Onko nykyiselle projektille tehty riskianalyysi?

Projektiorganisaatiota koskevat perustason VAHTI vaatimukset

10.1 Onko organisaatiolla kirjallinen sovelluskehitysprosessi, joka ottaa kantaa kaikkiin kehitysvaiheisiin ja niiden tietoturvahaasteisiin (secure SDLC)? (SKM-001)

10.2 Onko esimerkiksi tietoturvatestaus, turvallinen arkkitehtuuri, tietoturvavaatimukset ja noudatettavat standardit dokumentoitu sekä käytettävissänne?

11. Onko toteutettavalle sovellukselle laadittu karkean tason lista tietoturvavaatimuksista eri osa-alueilta, kuten luottamuksellisuus, eheys ja saatavuus, perustuen esitutkimusvaiheessa määriteltyyn sovellusprofiiliin? (VTM-003)

12. Onko tuoteomistaja määrittänyt toteutettavan järjestelmän tietoturvallisuustason ja sen tietoaineiston arkistoinnin vaatimukset? (VTM-004)

Kehitystiimiä koskevat perustason VAHTI vaatimukset

13.1 Onko arkkitehtuurin suunnittelussa suosittu yleisesti käytössä olevia ja hyväksyttyjä standardeja? (SNT-001)

13.2 Jos kyllä, niin mitä?

14. Onko valitun tunnistautumismenetelmän tietoturvallisuuden taso tuoteomistajan määrittämän sovelluksen käsittelemän tiedon turvatason mukainen? (SNT-009)

15. Oletko tietoinen millaisia salausratkaisuja kuten salausalgoritmeja tai tiivisteitä sovelluksessa käytetään?

15.2 Jos kyllä, niin mitä?

Prosessin ja toiminnan kehitysehdotukset

16. Millaisia kehitystarpeita näkisitte nykyisessä prosessissa?

17. Minkälaista koulutusta tai tietoa tarvitsisitte eniten tällä hetkellä tietoturvallisuudesta?

18. Haluaisitteko vielä sanoa jotain joka saattaisi auttaa yrityksen ponnisteluita kohti VAHTI vaatimusten täyttämistä organisaationa?