VAASAN YLIOPISTO

TEKNILLINEN TIEDEKUNTA

TIETOTEKNIIKKA

Tommi Hartonen

TIETOJÄRJESTELMÄN TIETOTURVALLISUUSARVIOINTI

Tietotekniikan
pro gradu -tutkielma

VAASA 2017

SISÄLLYSLUETTELO **sivu**

TERMIT JA LYHENTEET

Auditointityökalu	on auditointia nopeuttamaan ja helpottamaan kehitetty asia, joka voi esimerkiksi automatisoida osan auditointiprosessia, sopia tarkistuslistaksi tai varmistaa auditoinnin laatua.
Eheys	tiedon ominaisuus, joka ilmentää sitä, että tiedon sisältö ei ole muuttunut.
False positive	tarkoittaa suomeksi vääriä positiivisia virheitä eli "väärä hälytys". Kyseinen tulos osoittaa virheellisesti, että ehto on täyttynyt.
Hyökkäys	toimenpide, jolla pyritään vahingoittamaan tai käyttämään oikeudettomasti tietojärjestelmää tai tietoverkkoa.
IoT	eli Internet of things, joka tarkoittaa esineiden internetiä.
Kiistämättömyys	siihen pyritään mm. käyttämällä sähköistä allekirjoitusta tai aikaleimaa.
Käytettävyys	ominaisuus, joka ilmentää sitä, miten tieto, järjestelmä tai palvelu on niihin oikeutettujen hyödynnettävissä haluttuna aikana.
Luottamuksellisuus	tiedon ominaisuus, joka ilmentää sitä, että tieto on vain sen käyttöön oikeutettujen käytettävissä.
Mato	on haittaohjelma, joka leviää itsenäisenä ohjelmana.
OWASP	Open Web Application Security Project on sovellustietoturvan ympärille muodostunut oma organisaatio, joka levittää sovellustietoturvaan liittyvää informaatiota.
Robustisuus	testauksessa valitaan testitapauksia parametrien arvoalueiden ulkopuolelta.
Rootkit	eli piilohallintaohjelma. Se on myös usein troijalainen, joka välitetään toisen ohjelmiston avulla asennettavaksi.

SOAP	eli Simple Object Access Protocol on XML-kieleen pohjautuva tietoliikenneprotokolla.
Tietoturva	järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus.
Tietoturva-auditointi	tarkoittaa kohteen tietoturvan nykytason kattavaa arviointia.
Tietoturva-aukko	on tietojärjestelmässä tai suojauksessa oleva heikkous tietoturvassa.
Tietoturvauhka	voi olla sisäinen tai ulkoinen. Sisäisellä uhkalla tarkoitetaan organisaation oman henkilökunnan toiminnasta muodostuvaa tietoturvauhkaa ja ulkoisella uhkalla organisaation ulkopuolisesta seikasta, kuten viruksesta, muodostuvaa tietoturvauhkaa.
Tietoturvapolitiikka	on kokoelma organisaation laatimia tietoturvaan liittyviä säädöksiä, joita noudattamalla pyritään ehkäisemään organisaatiota koskevien tietoturvariskien toteutuminen.
Tietoturvaprosessi	on käytännön toimintatapa, joka panee täytäntöön jonkin tietoturvapolitiikassa mainitun tietoturvasäädöksen.
Todentaminen	menettely, jolla varmistutaan tiedon eheyden säilyminen.
Troijalainen	on naamioitu ohjelma, johon on piilotettu haittaohjelma. Se ei leviä automaattisesti viruksen tai madon tavoin, vaan leviäminen edellyttää käyttäjän toimia tai muuta ulkoista tapahtumaa.
VAHTI	on valtiovarainministerin asettama tietoturvallisuuden asiantuntemusta laajasti edustava ryhmä, joka kehittää ns. VAHTI-ohjeistoa.
Virus	on haittaohjelma, joka leviää kopioitumalla muihin ohjelmiin. Yleisesti tunnetuin haittaohjelmakategoria johon kuuluvat mm. tiedostovirukset ja käynnistyslohkovirukset.

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Tommi Hartonen
Tutkielman nimi: Tietojärjestelmän tietoturvallisuusarviointi
Ohjaajan nimi: Jouni Lampinen
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Tietotekniikka
Opintojen aloitusvuosi: 2009
Tutkielman valmistumisvuosi: 2017 **Sivumäärä**: 66

TIIVISTELMÄ:

Tässä tutkielmassa tutustutaan valtionhallinnon käytössä olevaan web-pohjaisen tietojärjestelmän tietoturvallisuusarviointiin. Tavoitteena tutkimuksessa on selvittää, kuinka tietojärjestelmän tietoturvallisuusarviointi suoritetaan ja millaisia tarkastusmenetelmiä arvioinnissa käytetään. Tutkielma keskittyy tekniseen tietoturva-auditointiin. Tutkielman ulkopuolelle on rajattu kokonaisvaltaiseen tietoturva-auditointiin kuuluvat hallinnollisen turvallisuuden, henkilöstöturvallisuuden sekä fyysisen turvallisuuden osa-alueet. Tekninen osuus käsittää vain tietojärjestelmän sovelluskerrokseen. Tutkielman työn lopputuloksena syntyy tarkastusraportti, josta selviää kohdeorganisaation tarkastuksen kohteena olevan sovelluksen teknisten puutteiden korjausehdotukset.

Tutkimuksen tekninen toteutus suoritettiin melko tarkasti tutkimussuunnitelman mukaisesti. Case-yrityksen web-sovelluksen teknisen tietoturvallisuuden tilan todentamisessa käytettiin suunnitelman mukaisesti aktiivista rajapinta-analyysi menetelmää. Haavoittuvuuksien havaitseminen verkossa ja porttiskannaus suoritettiin Nmap ja Burp Suite -ohjelmilla. Tutkimus suoritettiin etäyhteyden välityksellä case-yrityksen testausympäristössä.

Tutkimuksessa löydetyt havainnot olivat vakavuudeltaan vähäisiä. Havainnot eivät johtaneet välittömiin tietoturvallisuutta korjaaviin toimenpiteisiin. Sovellustestauksen tuloksena löytyi muutamia pienempiä korjausehdotuksia tietojärjestelmän omistajalle. Kohdeorganisaation kokonaisvaltaisesta tietoturvasta voidaan todeta, että se on erittäin hyvällä tasolla. Suositeltavat jatkotoimenpiteet sekä arviointiraportti lähetettiin arvioinnin kohteena olevalle case-yritykselle. Case-yrityksen tietojärjestelmään tehtävät tulevat ohjelmistopäivitykset on edelleen jatkossa hyväksyttävä kolmannen osapuolen toimesta ennen uusien päivitysten asentamista, jotta tarkastuspäätös pysyy voimassa. Kansallisesta tietojärjestelmästä ollessa kyse lopullisen tietojärjestelmän käyttöönottopäätöksen tekee tiedon omistaja.

AVAINSANAT: Tietoturva, Tietojärjestelmätarkastus, Tarkastusmenetelmä

UNIVERSITY OF VAASA
Faculty of technology
Author: Tommi Hartonen
Topic of the Master´s Thesis: Information security assessment of the information system
Instructor: Jouni Lampinen
Degree: Master of Science in Economics and Business Administration
Major: Computer Science
Year of Entering the University: 2009
Year of Completing the Master´s Thesis: 2017 **Pages**: 66

ABSTRACT:

This thesis explores the information security assessment of a web-based information system in use by the State administration. The aim of the study is to find out how the information security assessment of the information system is performed and what kind of methods of inspection are used in the evaluation. The thesis focuses on technical security auditing, excluding the areas of administrative security, personnel safety and physical security. The technical part comprises an application layer of information technology. As a result of the thesis work an audit report will be produced that will explain the technical deficiency repair plan of the target organization.

The technical implementation of the research was carried out with percission in accordance with the research plan. A systematic active interface analysis method was used to verify the technical information security status of the Case company web application. Network vulnerability detection and port scanning were performed with Nmap and Burp Suite -tools. The research was carried out remotely in a case study environment.

The findings from the study were minor in severity. Observations did not lead to immediate data security remedial measures. As a result of the application testing, a few minor repair solutions were recommended to the owner of the information system. From the overall information security of the target organization, it can be stated that it is at a very good level. The recommended follow-up measures and the evaluation report were sent to the company under review. The tasks of the Case company's IT system will come from software updates that will continue to be approved by 3rd party prior to installing the new update to ensure that the audit decision remains in effect. In the case of a national information system, the data owner will make a final decision on the introduction of an information system.

KEYWORDS: Information Security, Information Systems Audit, Method of Inspection

1 JOHDANTO

1.1 Tutkielman tavoitteet ja rajaus

Tutkielmassa tutustutaan valtionhallinnon käytössä olevaan web-pohjaisen tietojärjestelmän tietoturvallisuusarviointiin. Tutkielmassa tutkitaan tapausta, jossa kolmas osapuoli on saanut toimeksiannon kohdeorganisaation tietojärjestelmän tietoturvallisuusauditoinnista. Tutkimuksen tavoitteena on selvittää, kuinka tietojärjestelmän tietoturvallisuusarviointi suoritetaan ja millaisia tarkastusmenetelmiä arvioinnissa käytetään.

Tutkielmassa pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

Onko web-pohjainen kohdetietojärjestelmä tietoturvallinen?
Miten tietojärjestelmän turvallisuusarviointi toteutetaan?

Tämä tutkielma ei suoranaisesti muuta auditoinnin kohteena olevan organisaation tietoturvaa tai tietojärjestelmistä vastaavan ylläpidon prosesseja, vaikka auditoinnin yhteydessä ilmenevät tulokset tulevat parantamaan kohdeorganisaation tietoturvaprosessien implementaatiota. Tutkielman ulkopuolelle on rajattu kokonaisvaltaiseen tietoturva-auditointiin kuuluvat hallinnollisen turvallisuuden, henkilöstöturvallisuuden sekä fyysisen turvallisuuden osa-alueet. Tutkielman tekninen osuus kohdentuu pelkästään tietojärjestelmän sovelluskerrokseen. Tietoturvallisuusauditoinnin ulkopuolelle tässä tapauksessa on rajattu OSI-mallin kerrosten muut osa-alueet. Tutkielman työn lopputuloksena syntyy tarkastusraportti, josta selviää kohdeorganisaation tarkastuksen kohteena olevan sovelluksen teknisten puutteiden korjausehdotukset toimenpiteineen.

Tutkimuksen testausosiossa oli käytettävissä rajallinen aikataulu, minkä takia käytettyjä työkaluja ei voitu maksimaalisesti testiajaa koko testiympäristössä. Kohdeorganisaation

omassa käytössä olevia työkaluja tai työskentelytapoja ei käsitellä tässä tutkimuksessa. Auditoinnissa käytetyt työkalut ovat kaikki kaupallisia lisensoituja ohjelmia.
Johtopäätöksenä kohdeorganisaation kokonaisvaltaisesta tietoturvasta voidaan todeta, että se on hyvällä tasolla. Kohdeorganisaatiolla on vuosien kokemus tietojärjestelmiensä tietoturva-auditoinneista. Tämä todennettiin, kun kävimme aikaisemman auditointiraportin tuloksia läpi ja vertasimme niitä uusimpiin haavoittuvuuslöydöksiin. Sovellustestauksen tuloksena löytyi muutamia pienempiä korjausehdotuksia tietojärjestelmän omistajalle. Kohdeorganisaation tietojärjestelmiä tullaan testaamaan myös jatkossa Viestintäviraston toimesta.

1.2 Tutkimusmenetelmä

Pro gradu tutkielman luonne on empiirinen ja sen menetelmäsuuntaus on kvalitatiivinen. Tutkimusstrategiana käytetään tapaustutkimusta, haavoittuvuuksien todentamiseen ja havainnollistamiseen käytetään kokeellista tutkimusta, joka antaa vahvistusta tapaustutkimuksessa ilmenneille teorioille. Tutkimusmenetelminä ovat selittävä metodi ja kontrolloitu koe. Aineistonhankintamenetelmänä on käytetty muun muassa harkinnanvaraisesti valittuja valmiita dokumentteja. Aineiston analysoimisessa käytetään induktiivista, eli yleistävää päättelyä.

1.3 Tutkielman rakenne

Tutkielman ensimmäinen kappale sisältää johdannon, jossa käydään läpi tutkielman rajaus ja tavoitteet. Tutkielman toisessa kappaleessa käydään läpi tutkielman kannalta oleelliset käsitteet jotka koskevat tietoturvaa sekä tietoturvan historiaa ja taustaa. Toisen kappaleen loppupuoliskossa käydään läpi tietoturvan nykytilaa ja tulevaisuutta.

Kolmas kappale käsittelee tietojärjestelmien arviointi- ja hyväksyntäprosesseja. Kappaleessa tarkennetaan muun muassa hyväksyntä, arviointi ja tarkastus -käsitteet. Kolmannessa kappaleessa käydään myös läpi lainsäädäntöosuus sekä tietoturvallisuuden arviointikriteeristöt ja tietoaineistojen luokittelu. Neljännessä kappaleessa käydään ylätasolla case -yrityksen järjestelmäkuvaus läpi.

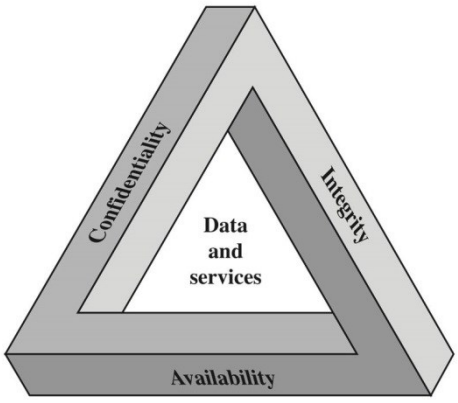
Viides kappale sisältää tutkimussuunnitelman. Tämä viides kappale sisältää myös tarkastuksessa käytettävät työkalut sekä menetelmät. Kuudes kappale käsittää tutkimuksen toteutuksen. Seitsemäs kappale pitää sisällä tutkimustulokset ja havainnot. Viimeinen kahdeksas kappale pitää sisällään johtopäätökset.

2 TIETOTURVA

2.1 Tietoturvan käsitteet

Tietoturva on tietojen, järjestelmien, palveluiden ja tietoliikenteen suojaamista. Tietoturvaan kuuluu tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Tietoturvan järjestelyjä ovat esimerkiksi salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. (Sanastokeskus 2004)

Tietoturvajärjestelyillä pyritään varmistamaan tiedon luottamuksellisuus, eheys ja käytettävyys. Tätä tietoturvallisuuden ominaisuuksien jaottelua kutsutaan CIA-malliksi joka tulee englanninkielisistä sanoista confidentiality, integrity ja availability (Kuva 1). Jaotteluun on lisätty myös käsitteet kiistämättömyys sekä autenttisuus eli todentaminen. (Stallings 2012: 609 – 610)



Kuva 1. CIA-malli. (Stallings W. 2008)

Luottamuksellisuudella tarkoitetaan sitä, että tietoa voivat käsitellä vain henkilöt, joilla on siihen oikeus. Luottamuksellisuutta voidaan tehostaa salasanoilla, käyttäjäoikeuksien rajoituksilla ja salausalgoritmeilla. (Järvinen 2012: 10)

Käytettävyydellä tai saatavuudella varmistetaan että tieto ja palvelut on saatavilla ja koneiden käytettävissä aina kun niitä tarvitaan. Saavuttamisen toteuttaminen on haasteellista sillä koneet hajoavat, nettiyhteydet pätkivät ja sovellukset kaatuilevat. (Järvinen 2012: 10)

Suuret pankit ja maailman isoimmat nettipalvelut kärsivät myös ajoittain katkoksista, miljoonien dollareiden panostuksetkaan toimintojen varmistamiseen ei aina riitä. Käytettävyysongelmista on kärsinyt myös Internetin suosituin suoratoistovideopalvelu YouTube.com. (Digitoday 2010)

Tiedon eheys tarkoittaa että tietoihin kohdistuu vain oikeutettuja muutoksia käsittelyn ja käytön aikana. Virukset, jotka leviävät esimerkiksi sähköpostin mukana, on tietoturvaongelma, koska viesti ei ole enää alkuperäinen ja ehyt. (Järvinen 2012: 10)

Tiedon luottamuksellisuutta ja eheyttä voidaan edistää teknisillä toimenpiteillä kuten salauksilla. Ulkopuoliset tahot eivät pysty lukemaan tai muokkaamaan tietoa mikäli suojattava kohde on salattu, tallennettu fyysiselle ulkoiselle medialle ja toimitettu turvattuun tilaan. Tällöin voidaan puhua hyvästä luottamuksellisuudesta ja eheydestä. (Järvinen 2002: 22 – 24)

CIA-mallia täydennetään kiistämättömyydellä ja todentamisella. Todentaminen eli autentikointi tarkoittaa henkilön tai järjestelmän luotettavaa tunnistamista esimerkiksi sähköisessä asiointipalvelussa ja tietojen siirrossa. Kiistämättömyydellä tarkoitetaan jonkin tapahtuneen todistamista jälkeenpäin. Kiistämättömyyden tavoite on juridinen sitovuus. Kiistämättömyys varmistaa, ettei toinen osapuoli voi kieltää toimintaansa jälkeenpäin. (Valtiovarainministeriö 2009: 4)

2.2 Tietoturvan historia ja tausta

Haittaohjelmilla on digiajan mittapuun mukaan pitkä historia, sillä ensimmäiset tietokonevirukset ilmestyivät jo 1980-luvulla. Aluksi kohteina olivat Macintosh-koneet, mutta sitten tekijöiden huomio kääntyi nopeasti yleistyviin pc-koneisiin ja niiden DOS -käyttöjärjestelmään. (Järvinen 2012: 178)

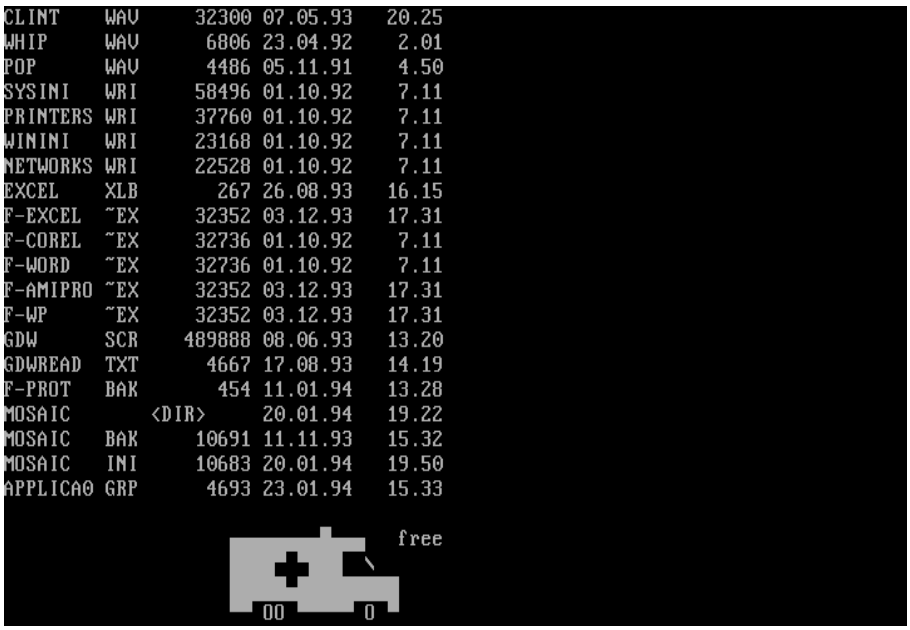
Vuonna 1971 Bob Thomasin toimesta kirjoitetaan ensimmäinen virus nimeltä Creeper, Creeper -virus oli kokeellinen itseään monistava ohjelma. Se saastutti DEC PDP-10 tietokoneita, joissa oli käyttöjärjestelmänä TENEX. Creeper sai pääsyn järjestelmiin ARPANETin välityksellä ja se kopio itsensä etäjärjestelmään, jossa näkyi viesti ”I´m the creeper, catch me if you can!”. Reaper-ohjelma luotiin myöhemmin poistamaan Creeper -virus. (Timeline of computer viruses and worms 2014)

Ensimmäisen varsinaisen tietokoneviruksen teki Rich Skrenta 15 vuoden ikäisenä Yhdysvaltain Pittsburghista. Rich Skrenta kirjoitti vuonna 1981 Apple II -tietokoneen Apple DOS 3.3 -käyttöjärjestelmälle Elk Cloner nimisen käynnistyslohkoviruksen. Elk Cloner levisi 5,25 tuuman levykkeiden välityksellä. Kun kone käynnistettiin saastuneella levyllä, virus latautui koneen muistiin, josta se kopioitui kaikille levyasemaan syötetyille levykkeille. Kun levyke siirrettiin fyysisesti toiseen koneeseen, virus tarttui siihenkin ja jatkoi leviämistään. (Tekniikan Maailma 2011.)

Ensimmäinen pc-koneille suunniteltu tietokonevirus, Brain, lähti liikkeelle vuonna 1986 syyskuussa Basit ja Amjad Farooq Alvi nimisten pakistanilaisten veljesten toimesta. Brain oli Elk Clonerin ja myöhempien virusten tapaan käynnistyslohkovirus. Samalla se oli niin sanottu rootkit -ohjelma. (Tekniikan Maailma 2011.)

Virukset levisivät koneesta toiseen lähinnä levykkeiden mukana ja ohjelmatiedostoihin tarttumalla. Virukset piileskelivät aikansa ja kertoivat sitten itsestään esittämällä animaatioita ruudulla (Kuva 2) tai soittamalla musiikkia koneen kaiuttimesta. Pahimmat

virukset sotkivat tahallaan tiedostoja tai tuhosivat kiintolevyn kuten Dark Avenger ja Disk Killer -virukset. Nykypäivän haittaohjelmat ovat ihan toista maata. Ohjelmia levittävät suureksi osaksi rikolliset, jotka hakevat haittaohjelmilla taloudellista hyötyä. Mitä kauemmin haittaohjelma pysyy piilossa, sitä enemmän siitä on myös hyötyä ohjelman tekijöille. (Järvinen 2012: 178)



Kuva 2. Ambulance virus. (F-secure 2014).

2.3 Tietoturvan nykytila ja tulevaisuus

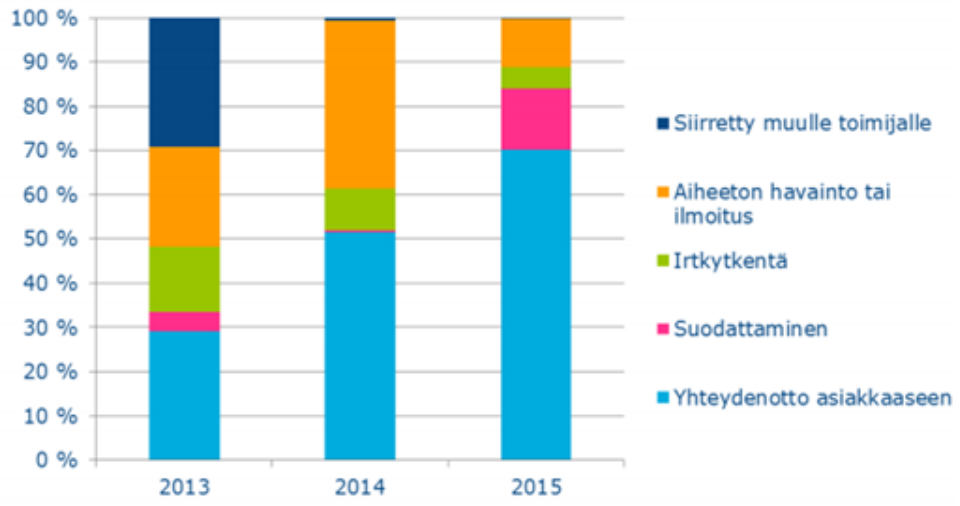
Tietoturva on vakava uhka tänä päivänä aivan kaikille tietokoneiden ja mobiililaitteiden käyttäjille. Ei ole merkitystä käytätkö laitteita kotimaassa tai maailman metropoleissa, uhka on läsnä paikasta tai ajasta riippumatta.

Verkkohuutokauppa eBay joutui vuonna 2014 erittäin laajan tietomurron uhriksi. Se ilmoitti tietomurrosta, jonka seurauksena 145 000 000 asiakkaan käyttäjätiedot vaarantuivat. (Viestintävirasto 2014a)

Vaikka ilmoitettujen tietoturvahyökkäysten määrä maailmalla on kasvanut vuosittain ja suomessa aina vuoteen 2013 asti, on suomessa tietoliikenneverkkojen tietoturva pääsääntöisesti hyvällä tasolla, joka käy ilmi useista eri lähteistä kerätyistä tilastoista, joissa Suomi sijoittuu kärkijoukkoon. Teleyritykset käsittelivät vuonna 2013 peräti 677 146 tietoturvaloukkausta, joista 15 908 aiheutti toimenpiteitä. (Viestintävirasto 2016)

Tietoturvahavaintojen kokonaismäärä laskussa

Teleyritysten käsittelemien tietoturvatapausten määrä on selvässä laskussa vuodesta 2013 lähtien. Viestintäviraston selvityksen (2016) mukaan vuonna 2015 tietoturvatapauksia oli yhteensä noin 200 000. Näistä havainnoista valtaosa oli Viestintäviraston Autoreporter-järjestelmän havaitsemia haittaohjelmia.



Kuva 3. Teleyritysten tietoturvahavaintojen ratkaisemiseksi tekemät toimenpiteet vuosina 2013 − 2015. (Viestintävirasto 2016: 16)

Asiakkaiden liittymiin kohdistuvat tietoturvaloukkaukset saadaan yhä useammin selvitettyä teleyritysten neuvonnan kautta. Yllä olevassa pylväsdiagrammissa on kuvattuna teleyritysten tietoturvahavaintojen ratkaisemiseksi tekemät toimenpiteet vuosina 2013 − 2015. Vuoden 2015 tilasto pitää sisällään vain vuoden toisen puoliskon

(Kuva 3). Vuonna 2015 196 000 tapauksesta jopa 70 prosentissa yhteydenotto asiakkaaseen oli riittävä korjaava toimenpide. Useassa tapauksessa myös verkkoliikenteen suodattaminen oli riittävä korjaustoimenpide. Vuonna 2015 verkkoliikennettä oli suodatettu 14 prosentissa tapauksista. Teleyritykset joutuvat entistä harvemmin kytkemään tietoturvaa vaarantavan liittymän kokonaan irti. Viime vuonna tähän toimenpiteeseen jouduttiin turvautumaan vain viidessä prosentissa tapauksista. Täysin aiheettomia havaintoja ja ilmoituksia viime vuonna oli noin 11 prosenttia. (Viestintävirasto 2016)

Tietoturvan tulevaisuus

Viime vuonna kiristyshaittaohjelmamarkkinat kokivat kehityksen askeleen eteenpäin kun poliisi-aiheiset huijaukset siirtyivät syrjään ja tilalle tulivat salakirjoittavat kiristyshaittaohjelmat (Crypto Ransomware). Jäljempänä mainittu haittaohjelma salakirjoittaa käyttäjän tiedostot ja vastaavasti vakuuttaa purkavansa salauksen kohteen maksettua vaaditun summan. (Ficora TTN 2016) Tulevaisuudessa saatamme törmätä myös IoT-kiristystroijalaisiin. Tänä päivänä esineiden internet on yksi kuumista puheenaiheista. Halpojen IoT-laitteiden turvataso on usein huono ja näin ollen laitteissa on haavoittuvuuksia, joiden kautta IoT-laitteen saa haltuun tai sen voi mädättää haittaohjelmilla. "Kuvittele, että auto ei käynnisty ja sen näytölle ilmestyy kiristysviesti. Pitää käydä netissä ja maksaa parisataa euroa ennen kuin auton saa takaisin käyttöönsä. Kiireinen saattaa mieluummin maksaa lunnaat kuin hinauttaa auton korjaamolle", kirjoittaa F-Securen tietoturva-asiantuntija Mikael Albrecht mahdollisista tulevaisuuden tietoturva skenaariosta. (Ficora TTN 2016)

3 TIETOJÄRJESTELMIEN ARVIOINTI- JA HYVÄKSYNTÄPROSESSIT

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista, kansainvälisistä tietoturvallisuusvelvoitteista sekä turvallisuusselvityksistä annettujen lakien mukaisesti Viestintäviraston tehtäviin kuuluu erilaiset tietojärjestelmien turvallisuusarvioinnit ja tietoturvallisuushyväksynnät. Viestintäviraston NCSA-FI eli National Communications Security Authority:n suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit sisältävät arvioinnin tai hyväksynnän tilaajalta vaadittavat suoritteet.

3.1 Hyväksyntä, arviointi ja tarkastus

Hyväksyntäprosessilla tarkoitetaan prosessia, jonka päätteeksi turvallisuusjärjestelyt hyväksyvä viranomainen (Viestintäviraston NCSA) antaa virallisen lausunnon hyväksytystä järjestelmästä. Sekä siitä, että hyväksytty järjestelmä on hyväksytty käytettäväksi määritellyssä turvaluokassa, tiettyä toimintatapaa noudattaen joka takaa järjestelmän turvallisuuden käyttöympäristössään hyväksytyllä riskitasolla. Tämä perustuu siihen, että hyväksytyt tekniset, fyysiset, organisatoriset ja menettelyyn liittyvät turvatoimet on toteutettu.

Arvioinnilla vastaavasti tarkoitetaan prosessia, jonka päätteeksi viranomainen joka hyväksyy turvallisuusjärjestelyt antaa virallisen lausunnon täyttääkö järjestelmä sille kohdistuvat vaatimukset. Tämä arviointiprosessi on tyypillisesti hyväksyntäprosessin osaprosessi.

Tarkastuksella tarkoitetaan riippumattoman osapuolen suorittamaa kohteen tai toiminnan ja toiminnan tulosten usein määräajoin tapahtuvaa tutkimista selvittääkseen vastaako tarkastuksen kohteena oleva järjestelmä sille kohdistuvat vaatimukset. (NCSA 2017)

3.1.1 Tekniset tietoturvallisuustarkastukset

Tekniset tietoturvallisuustarkastuksen sisältämät osakokonaisuudet pitävät sisällään hallinnollisen tietoturvallisuuden niiltä osin kuin tarkastettavana oleva järjestelmä vaatii. Fyysisen turvallisuuden vastaavasti niiltä osin kuin tarkastettavana oleva järjestelmä niin vaatii. Kohteista pyritään käyttämään aina olemassa olevaa materiaalia jonka muut turvallisuusviranomaiset tai arviointilaitokset ovat tuottaneet raportin muodossa.

Tekninen tietoturvallisuustarkastus voidaan jaotella 11 eri osakokonaisuuteen. Ensimmäisenä tehtävänä on tutustua tarkastettavana olevan kohteen dokumentaatioon ja määritellä mahdolliset kriittiset osat. Tämän jälkeen vuorossa on tavallisesti verkkoliikenteen passiivinen rajapinta-analyysi. Tähän sisältyy verkkokuvien tai järjestelmäkuvien rakentaminen ja liikenneanalyysit.

Kolmas osakokonaisuus on järjestelmäkonfiguraatioiden turvallisuuden tarkastus, jonka piiriin kuuluvat muun muassa palvelinten ja työasemien käyttöjärjestelmät, verkkolaitteiden ja tietokantojen konfiguraatiot sekä muut järjestelmän turvallisuuteen vaikuttavat ohjelmistot. Neljäs osakokonaisuutta sisältää aktiivisen rajapintatarkastelun, joka käsittää porttiskannaukset, haavoittuvuusskannaukset ja toimintavarmuustestaukset. Tavallisesti toimintavarmuustestauksella tarkoitetaan virheellisen syötteen lähettämiseen perustuvaa testausta. Edellä mainittua testausta vaaditaan ainoastaan turvallisuuden kannalta kriittisiin järjestelmäosiin. Viides osio käsittää sovellusturvallisuuden tarkastelun järjestelmätyypeittäin. Tämän osion tarkastusmenetelmä kattaa kohteen turvallisuuteen vaikuttavien sovelluskomponenttien tarkastelut kuten java -palvelin ja asiakasohjelmistot, web-sovellukset ja ERP -järjestelmien sisäiset pääsynhallintamekanismit. Teknisen tietoturvallisuustarkastuksen kuudes osakokonaisuus pitää sisällään salausratkaisujen turvallisuuden tarkastamisen. Seitsemännessä osiossa testataan järjestelmän käytettävyyttä ja kuormitusta, tämä osakokonaisuus korostuu järjestelmissä joissa on korkea käytettävyysvaatimus. Korkean

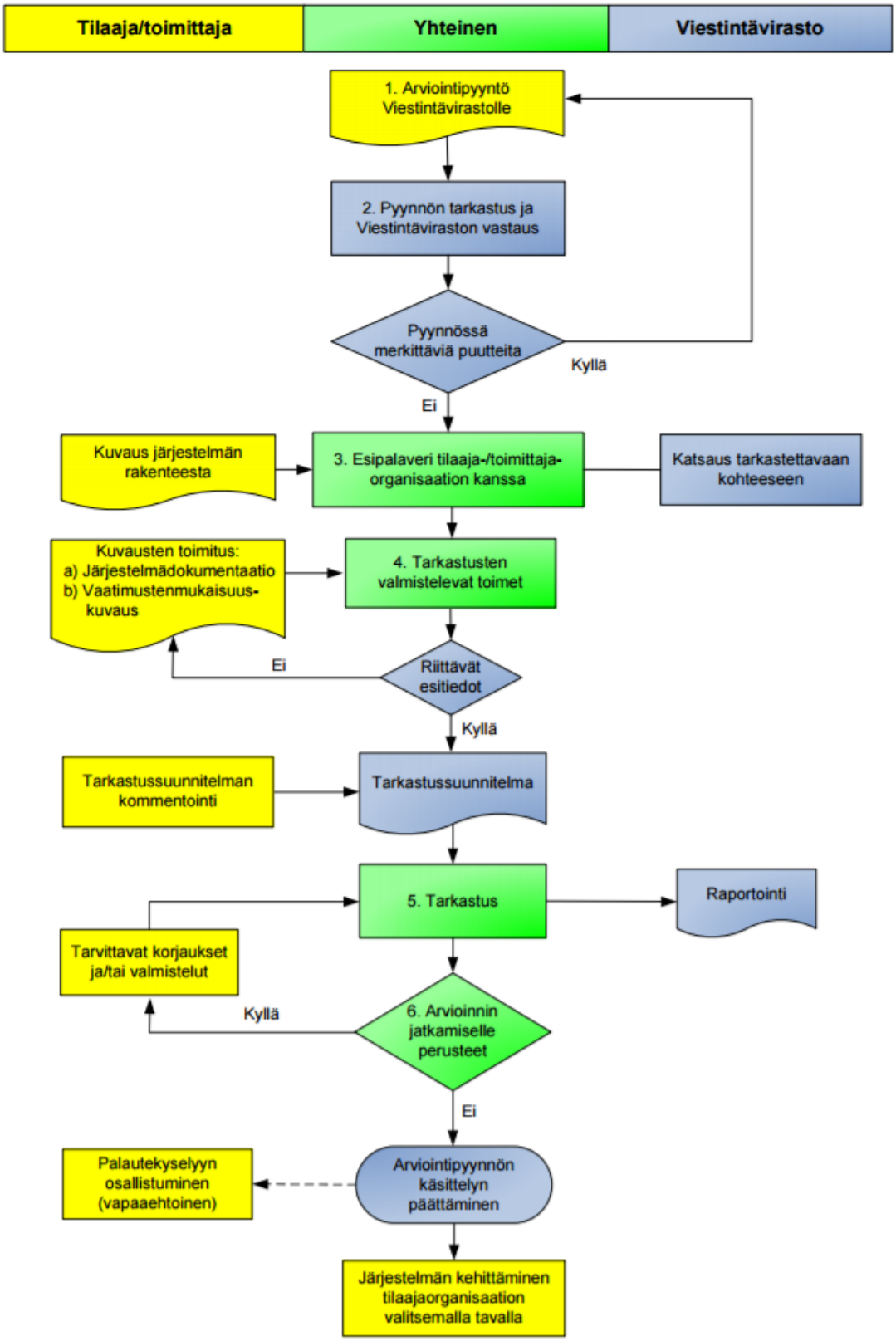
käytettävyysvaatimuksen omaavia järjestelmiä ovat esimerkiksi ihmishenkiä suojaavat turvajärjestelmät.

Kahdeksas kohde on yhdyskäytäväratkaisujen turvallisuuden tarkastaminen eri suojaustason ympäristöjen välillä. (NCSA todentamismenetelmät 2016) Seuraava teknisen tietoturvallisuustarkastuksen osakokonaisuus sisältää sähkömagneettisten hajasäteilysuojausten todentamisen. Hajasäteilyllä tarkoitetaan elektronisten laitteiden lähettämää sähkömagneettista säteilyä, josta on mahdollista selvittää tietyillä laitteilla ja optimaalisissa olosuhteissa käsiteltyjen tietojen sisältö. (Tempest 2013) Kymmenes osakokonaisuus käsittää luvattomien teknisten laitteiden olemassaolon todentamisen, nämä kaksi edellä mainittua teknisen tietoturvallisuustarkastuksen osakokonaisuutta on mahdollista ulkoistaa DSA-viranomaiselle (Designated Security Authority) eli valtuutetulle turvallisuusviranomaiselle. Viimeinen ja yhdestoista osakokonaisuudessa on tarkoitus niputtaa saadut tiedot, analysoida löydökset ja raportoida tulokset (NCSA todentamismenetelmät 2016).

3.1.2 Tietojärjestelmän arviointi ja arviointiprosessi

Tietojärjestelmän tietoturvallisuuden arvioinnin päämääränä on varmentaa, että tarkastuksen kohteena oleva tietojärjestelmä vastaa sille asetettuja tietoturvallisuutta koskevia vaatimuksia. Arviointitehtävään eivät sisälly tietojärjestelmään talletettavien tietojen lainmukaisuuden arviointi tai muut tietojärjestelmän sisällön arviointiin sisältyvät kysymykset. Arviointitehtävässä on tarkoitus selvittää täyttääkö arvioinnin kohde siltä edellytettävät tekniset ominaisuudet.

Seuraavaksi käsitellään ja havainnoidaan kaavion avulla arviointiprosessia. Arviointiprosessi rakentuu useista eri suoritteista sekä täydentävistä osasuoritteista joita on kuvattu seuraavaan taulukkoon (Taulukko 1).



Taulukko 1. Arviointiprosessi. (NCSA 2017)

Ensimmäiseksi tilaajaorganisaatio lähettää NCSA:lle arviointipyynnön. Arviointipyynnöstä tulee käydä selville järjestelmän nimi, luonnehdinta järjestelmästä ja järjestelmän laajuudesta. Pyynnöstä tulee myös ilmetä käsitteleekö järjestelmä kansainvälistä, kansallista vai sekä kansallista että kansainvälistä salassa pidettävää tietoa, myös korkein käsiteltävä turvaluokka tulee tulla selville. Olennaiset tiedot arviointipyynnössä ovat järjestelmän omistaja, rakentaja ja ylläpitäjä sekä onko järjestelmän nykytila suunnitteilla, rakenteilla, valmiina käyttöönottoon vai jo käytössä oleva. Pyynnöstä tulee käydä ilmi järjestelmään liittyvät sisäiset ja ulkoiset vaatimukset, sekä mahdollinen käyttöönottopäivämäärä yhteyshenkilön ja yhteystietojen kera.

Toinen arviointiprosessin vaihe on NCSA:n vastaus tilaajaorganisaation lähettämään arviointipyyntöön. Tämä pyritään antamaan kahden viikon kuluessa arviointipyynnön saapumisesta, mikäli pyynnössä ei ilmene täydennettävää. Arviointiprosessin aloittamisen edellytysten täytyessä tilaajaorganisaatiolle ehdotetaan yhteiseksi sopivaa esipalaverin päivämäärää ja esipalaveriin vaadittavia dokumentteja.

Seuraavaksi vuorossa on prosessin kolmas vaihe, joka on esipalaveri tilaajaorganisaation kanssa. Esipalaverissa viranomaiselle annetaan mahdollisimman kattavat kuvaukset ja dokumentaatiot arvioinnin kohteena olevasta järjestelmästä. Optimaalisessa tapauksessa tilaajaorganisaatio antaa vaatimusmäärittelyn (SSRS), verkkokuvat, listauksen käytetyistä käyttöjärjestelmistä ja ohjelmistoversiotietoineen, tiedot aikaisemmista tarkastuksista ja arvioinneista raportteineen sekä itsearvioinnin järjestelmän vaatimustenmukaisuudesta NCSA:lle ennen esipalaveria tai esipalaverin yhteydessä. Näistä dokumentaatioista käy ilmi tapauskohtaisesti esimerkiksi verkon rakenne, vyöhykkeet, IP-osoitteet, palomuurisäännöt, ohjelmistoversiot ja asetukset sillä tarkkuudella, että dokumentaatioiden perusteella sivullinen voisi korjata epäkuntoisen käyttöjärjestelmän tai verkon käyttökuntoon.

Prosessin neljäs vaihe kattaa tarkastusten valmistelevat toimet, tässä kuvataan yleisellä tasolla tarkastuksen kohteena olevan järjestelmän tarkastamiseen liittyvät asiakokonaisuudet sekä aikataulutukset. Tässä vaiheessa prosessia tilaajalla on mahdollisuus kommentoida tarkastussuunnitelmaa. Tilaajan pitää toimittaa

tarkastussuunnittelun vaatimat tiedot ja sitouduttava kuvattuun aikataulutukseen. Tilaajalta tulee järjestää tarkastuksen mahdollistavat menettelyt tarkastus kohteessa, joihin voi sisältyä esimerkiksi soveltuvat asiantuntija- ja tilavaraukset sekä tarvittavat pääsyoikeuksien järjestämiset.
Tämän prosessivaiheen jälkeen vuorossa on itse tarkastus. Tähän sisältyy arvioitavan kohteen tietoturvallisuuden tutkiminen, jotta saadaan selville täyttääkö kohteen tietoturvallisuuden tila vaadittavat vaatimukset. Tarkastus osio pitää sisällään hallinnollisen, fyysisen turvallisuuden ja teknillisen osuuden. Tilaajalle annetaan tarkastuksen päätteeksi poikkeamalista havaituista poikkeamista sekä pyydettäessä raportti tilaajan arviointipyynnön kohteesta.

Kuudes prosessivaihe on arvioinnin jatkamisen perusteet. Arviointiprosessia jatketaan lähtökohtaisesti tilaajan tarpeiden mukaisesti. Arviointiprosessi voidaan myöskin lopettaa tilanteessa, jossa tarkastusta ei pystytä aloittamaan tahi tarkastuksessa ilmitulleiden poikkeamien korjausten etenemisestä ei voida saada näyttöä puolen vuoden aikana. Arviointiprosessi voidaan lopettaa mikäli tilaaja pyytää prosessin päättämistä.

Prosessin viimeinen ja seitsemäs osio on kun vaatimukset täyttävälle tietoa käsittelevälle järjestelmälle voidaan myöntää todistus vaatimustenmukaisuudesta. Hyväksyntä edellyttää, että tarkastuksen kohde sitoutuu turvallisuuden tason ylläpitämiseen. NCSA:n todistus voidaan myöntää määräajaksi, jos tähän on erityinen syy. Todistus raukeaa, mikäli tarkastetussa kohteessa tapahtuu merkittävää turvallisuuteen vaikuttavaa muutosta. Esimerkiksi verkkorakenteen, henkilöstön, turvakäytäntöjen tai toimitilojen merkittävät muutokset ovat syitä todistuksen raukeamiselle. Suuret ja merkittävät muutokset tulee hyväksyttää aina ajoissa NCSA:lla. (NCSA 2017)

3.1.3 Teknisen tietoturvatarkastuksen työkalut

Tietojärjestelmän teknisen tietoturvallisuustarkastuksen suoritusjärjestys on pitkälti tarkastusta suorittavien tarkastajien päätettävissä. Tyypillisesti tarkastus alkaa hallinnollisen tietoturvallisuuden kartoittamisen osuudella.

Verkkoliikenteen ja verkkotopologian analysoinnissa käytetään tyypillisesti Clarified network analyzer, Tcpdump tai Wireshark -työkalua. Haavoittuvuuksien havaitsemiseen verkossa ja porttiskannaukseen käytetään usein Nessus, Nmap tai Burp Suite -ohjelmaa. (Clarified network analyzer 2017) (Nessus 2017) (Nmap 2017) (Tcpdump 2017) (Wireshark 2017)

Windowsin suojausasetusten vaatimustenmukaisuuden tarkastus suoritetaan Microsoft Security Compliance Managerin avulla. Web-sovelluksen turvallisuus ja pääsynhallintaa testataan muun muassa Burp Suite, OWASP Zed Attack Proxy (ZAP) sekä W3af -työkaluilla. (Burp Suite 2017) (OWASP ZAP 2017) (W3af 2017)

Burp Suite sopii mainiosti web-sovelluksen manuaaliseen testaukseen. Lisensoitu Burp Suite -työkalu sisältää monipuolisesti työkaluja, joilla voi testata kaikkia web-sovelluksen osia ja toimintoja. Lisensoitua Burp Suite -työkalua ja sen lisäosia päivitetään nopealla tahdilla. Case-yrityksen web-sovelluksen turvallisuuden tilan arvioinnissa käytettiin versiota pro v1.7.15. (Burp Suite 2017)

OWASP Zed Attack Proxy on ilmainen vaihtoehto Burp Suitelle, se taipuu suhteellisen hyvin monitahoiseen manuaaliseen testaukseen. OWASP ZAP:n työkalut eivät ole yhtä monipuoliset ja tehokkaat kuin Burp Suitessa, mutta se tuo kuitenkin nipun lisämahdollisuuksia automaattisen skannerin rinnalle. Se toimii Burp Suite:n tavoin Proxy-palvelimena selaimelle eli sen kautta voidaan ohjata kaikki selaimen liikenne. (OWASP ZAP 2017)

Ohjelmiston käytettävyyttä ja robustisuus testausta eli Fuzzausta toteutetaan usein Radamsa tai Codenomiconin Defensics työkaluilla. Testi virus EICAR on virallinen

antivirus ja hälytystestaus tiedosto jota käytetään usein sovellusturvallisuuden testauksissa. Tietoturvan toteutumista kuten palomuurien suodatusta ja yhdyskäytävä ratkaisuissa käytetään Hping, Netcat, Python sekä Scapy -työkaluja. (Radamsa 2017) (Codenomicon 2017)

Vaatimustenmukaisuuden ja konfiguraatioiden verifiointia testataan manuaalisesti sekä omatekoisten skriptien avulla. Verkko- ja sovellusturvallisuuden käytettävyys- ja käyttöönottotestausta suoritetaan muun muassa Hping, Slowloris ja LOIC (LowOrbit Ion Canon) -työkaluilla.

Seuraavan sivun taulukossa on listattu yleisesti teknisessä tietoturvallisuuden tarkastuksessa käytettyjä työkaluja ja niiden käyttötarkoitus (Taulukko 2).

TYÖKALUT	TEHTÄVÄ
Clarified Network analyzer, Tcpdump, Wireshark	Verkkoliikenteen- ja verkkotopologian analysointi
Burp Suite, Nessus, Nmap	Porttiskannaus ja haavoittuvuuksien havaitseminen verkossa
Microsoft Security Compliance Manager	Windowsin suojausasetusten vaatimustenmukaisuuden tarkastus
Burp Suite, OWASP Zed Attack Proxy (ZAP), W3af	Web-sovelluksen turvallisuus ja pääsynhallinta testaus
Defensics, Radamsa	Ohjelmiston käytettävyys ja robustisuus testaus (Fuzzing)
Test virus EICAR	Virallinen antivirus ja hälytystestaus tiedosto
Hping, Netcat, Python, Scapy	Tietoturvan toteutuminen mm. palomuuri suodatuksessa ja yhdyskäytävä ratkaisuissa
Manuaalinen testaus, Omatekoiset skriptit	Vaatimustenmukaisuuden ja konfiguraatioiden verifiointi
Hping, LOIC (LowOrbit Ion Canon), Slowloris	Verkko- ja sovellusturvallisuuden käytettävyys- ja käyttöönottotestaus

Taulukko 2. Tarkastuksissa käytettyjä työkaluja ja niiden käyttötarkoitukset. (Vatanen 2014: 14−15)

3.2 Lainsäädäntö

Tässä luvussa käsitellään tietojärjestelmien tietoturvallisuudenarvioinnin kannalta keskeiset normit, jotka tietojärjestelmien tietoturvallisuustarkastajan on syytä hallita. Valtiovarainministeriön tietoturvallisuuden arviointiohjeistuksen mukaisesti tietoturvallisuutta koskevassa lainsäädännössä ei ole asetettu yleistä velvoitetta vaatia tietojärjestelmille tai tiedonkäsittelylle viranomaishyväksyntää. Tietoturvallisuuden arviointi perustuu hyvän tiedonhallintatavan ja tietoturvallisuusasetuksen vaatimuksiin. Erityisissä tilanteissa tiedonkäsittely kuitenkin vaatii viranomaishyväksyntää. Kansainvälisiin tietoturvallisuusvelvoitteisiin kuuluu tämän kaltaisia vaatimuksia. EU:n turvallisuusluokiteltuja tietoja sisältävien tietojärjestelmien on käytävä läpi hyväksymisprosessi. Näin pyritään varmistamaan, että kaikki mahdolliset turvatoimet on toteutettu ja tarvittava turvataso saavutetaan. Suomea sitovan turvallisuusluokitellun tiedon suojaamista koskevat valtiosopimukset vaativat henkilöiden ja yritysten turvallisuusselvityksiä turvallisuusluokasta III turvallisuusluokka I:een. Tapauksissa, jossa tietoa siirretään valtioiden välillä sähköisessä muodossa, tarvitaan edellisten lisäksi DSA:n (Designated Security Authority) välistä sopimusta. (Vahti 2/2014) Tietoturvallisuuden viranomaisarviointia edellytetään myös julkisen hallinnon turvallisuusverkkotoiminnasta. (TUVE 10/2015)

3.2.1 Laki viranomaisten toiminnan julkisuudesta

Viranomaisten velvollisuus on noudattaa hyvää tiedonhallintatapaa, eli tämä tarkoittaa asiakirjojen ja tietojärjestelmien sekä näihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä, suojaamisesta ja eheydestä huolehtimista koskee julkisuusperiaate, josta on säädetty laki viranomaisten toiminnan julkisuudesta (621/1999). Viranomaisten asiakirjat ovat julkisia, jollei viranomaisten toiminnan julkisuudesta annetusta laissa toisin säädetä. Julkisuuslain 6 luvun salassapitovelvoitteisiin kuuluvat asiakirjasalaisuus, vaitiolovelvollisuus ja hyväksikäyttökielto, salassa pidettävät viranomaisen asiakirjat sekä salassapito- ja luokitusmerkintä.

Viranomaisen asiakirjaan on tehtävä merkintä sen salassa pitämisestä, jos asiakirja on salassa pidettävä toisen tai yleisen edun vuoksi. Asianosaiselle on annettava tieto salassapitovelvollisuudesta myös tapauksessa, kun salassa pidettävä tai pidettävät tiedot annetaan suullisesti.
Asiakirjaan voidaan tehdä luokitusmerkintä, tämä osoittaa minkälaisia tietoturvallisuusvaatimuksia asiakirjaa käsiteltäessä on noudatettava. (Finlex julkisuus 1999)

3.2.2 Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista

Eduskunnassa on säädetty 22.12.2011 laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista. Viestintäviraston tehtävistä yritysturvallisuusselvitystä laadittaessa on säädetty erikseen turvallisuusselvityslaissa (726/2014). Yritysturvallisuusselvitystä voi hakea yritys, joka tarvitsee selvitystä laissa tai sen nojalla säädetyn taikka kansainvälisestä tietoturvallisuusvelvoitteesta johtuvan velvoitteen toteuttamiseksi. Valtionhallinnon viranomaisilla on mahdollisuus käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain tässä laissa tarkoitettua menettelyä tai sellaista arviointilaitosta, joka on saanut Viestintäviraston hyväksynnän tietoturvallisuuden arviointilaitoksista annetun lain mukaan (Laki1405/2011).

Tällä hetkellä Viestintäviraston hyväksymiä tietoturvallisuuden arviointilaitoksia on KPMG IT Sertifiointi Oy, Nixu Certification Oy ja Inspecta Sertifionti Oy. KPMG IT Sertifiointi Oy:n kelpoisuus on suojaustasolle IV, Katakri II ja 2015, ISO/IEC 27001:2013 sekä VAHTI -ohjeistusta käyttäen. Nixu Certification Oy:n pätevyysalue kattaa suojaustason IV,VAHTI ja ISO/IEC 27001:2013 ohjeistusta käyttäen. Inspecta Sertifionti Oy:n pätevyysalue on ISO/IEC 27001:2013. (Arviointilaitokset 2017)

Viestintäviraston tehtävinä on arvioida viranomaisen pyynnöstä tietojärjestelmän tai tietoliikennejärjestelyjen tietoturvallisuuden vaatimuksenmukaisuutta sekä antaa sen

hyväksymistä osoittava todistus. Viestintäviraston tehtäviin kuuluu tehdä valtiovarainministeriön pyynnöstä selvityksiä valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta. (Laki 1406/2011)

3.2.3 Turvallisuusselvityslaki

Turvallisuusselvityslaissa säädetään muun muassa henkilö- ja yritysturvallisuusselvitysten laatimisen edellytyksistä, selvitysten laadinnassa noudatettavasta menettelystä sekä turvallisuusselvityksen ja sen perusteella annetun todistuksen voimassaolosta ja todistuksen peruuttamisesta.

Yritysturvallisuusselvitystä voi hakea joka tarvitsee selvitystä laissa tai sen nojalla säädetyn tietoturvallisuusvelvoitteesta johtuvan velvoitteen toteuttamiseksi. Selvitystä voi hakea myös viranomainen, jonka on tarkoitus tehdä sopimus selvityksen kohteen kanssa, jos sopimuksen yhteydessä yritykselle annetaan tai sopimuksen johdosta syntyy suojaustasoon I, II tai III kuuluvaksi luokiteltuja asiakirjoja. (Turvallisuusselvityslaki 2014)

3.2.4 Tietojärjestelmän tietoturvallisuuden tarkastajan vastuut ja rajoitukset

Tietojärjestelmän tietoturvallisuustarkastuksen yhteydessä ilmenevät poikkeavuudet tai tunnistetut järjestelmä rikkomukset, on tarkastajan sallittua ilmoittaa asiasta ainoastaan järjestelmän omistajalle. Suomessa omistajan vastuulla on ilmoittaa asiasta eteenpäin poliisille tietoturvaloukkauksesta ja vastaavasti poliisi on vastuussa tietoturvaloukkauksen tai vastaavan tutkimuksessa.

Tietoturvallisuustarkastuksissa aika ja resurssit ovat usein hyvin rajallisia. Näin ollen tarkastuksissa käytettävät laitteistot ja työkalut tulee olla toiminta tarkastettu ennen tarkastusta ja joissakin tapauksissa kohdeorganisaatio saattaa tarkastaa työkalut ennen tarkastusta. Toisin sanoen tämä tarkoittaa, että tarkastustyökalut ja menetelmät on oltava nopeasti tarkastajan luettavissa ja mahdollisesti kustomoitavissa. Tarkastustyökalut

eivät saa myöskään tehdä minkäänlaisia muutoksia kohdejärjestelmään. Näin ollen erityisesti antivirus- tai eheystarkastuksissa on tärkeää ajaa tarkastus työkaluilla "vain tarkistus" -tilassa (Verify Only), jotta tarkastuksen kohteena oleva tieto välttyy mahdolliselta tuhoutumiselta väärän hälytyksen tapauksessa (False Positive).

3.3 Tietoturvallisuuden arviointikriteeristöt

Tässä luvussa kuvataan yleiset reunaehdot vaatimusten tulkintakäytännöille tehtäessä tietoturvallisuusarviointeja ja -tarkastuksia. Siinä tapauksessa että samalla järjestelmällä on useamman omistajan tietoa tulee kaikkien tiedon omistajien asettamat suojausvaatimukset täyttyä. Edellä kuvattu esimerkki voi olla jos järjestelmässä on esimerkiksi kansallista ja EU:n turvaluokiteltua tietoa. Jos eri vaatimukset ovat ristiriitaisia tai päällekkäisiä, tulee tilanteissa vaatimukset täyttää tiukimman kriteeristön mukaisesti.

3.3.1 Katakri 2015

Katakri on kansallisen turvallisuusviranomaisen julkaisema auditointityökalu. Sitä käytetään viranomaisten salassa pidettävien tietoaineistojen käsittelykyvyn arvioimiseksi. Siihen on koostettu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset. Katakri ei aseta itse tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen koostetut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. Katakria on tarkoitus käyttää silloin, kun arvioidaan velvoittaviin sitoumuksiin perustuvien tietoturvallisuusvaatimusten toteutumista. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa on sen keskeisin kansalliseen lainsäädäntöön kuuluva vaatimuslähde. EU:n neuvoston turvallisuussääntöjä (2013/488/EU) on vastaavasti käytetty kansainvälisenä lähteenä. EU:n turvallisuusluokiteltujen tietojen suojaamiseen vastaavasti sovelletaan neuvoston päätöstä EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä. (EU 2013)

Katakrin vaatimukset on koottu niin, että vaatimuksista muodostuu riittävä kokonaisuus kansallisten tai kansainvälisten salassa pidettävien tietojen suojaamiseksi oikeudettomalta paljastumiselta ja käsittelyltä. Kun tarkoituksena on todentaa, täyttävätkö viranomaisten tai yritysten tietojärjestelmät ja toiminta niiltä edellytettävät

kansalliset tai kansainväliset tietoturvavaatimukset voidaan tuolloin Katakria käyttää auditointityökaluna. (Katakri 2015)

3.3.2 VAHTI-ohjeet

Valtiovarainministeriön asettama Valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmä (VAHTI) kehittää ja päivittää jatkuvasti VAHTI-ohjeistusta. Ohjeistus pitää sisällään kaikki tietoturvallisuuden osa-alueet.
Kansallista suojattavaa tietoa sisältävien järjestelmien suojausvaatimukset on esitetty tietoturvallisuusasetuksessa. Asetuksen toimeenpanon ohjaukseen ja täyttämisen arviointiin tarkoitetut vaatimukset on esitetty valtiovarainministeriön ohjeissa eli VAHTI-julkaisuissa.

Tietoturvallisuuden arviointiohje, VAHTI 2/2014, kuvaa tietoturvallisuuden arvioinnista seuraa:

> "Tietoturvaturvallisuusasetuksen 4 §:ssä säädetään kymmenen vaatimusta tietoturvallisuuden perustasolle. Näitä vaatimuksia täsmentää ja täydentää VAHTI-ohje 2/2010, jossa tietoturvatasojen kaikkien kolmen tason vaatimukset on kuvattu yksityiskohtaisesti. Nämä vaatimukset kohdistuvat menettelytapoihin ja prosesseihin eikä niiden perusteella voida tehdä päätöksiä teknisistä yksityiskohdista ja ratkaisuista, joiden avulla tasovaatimukset voidaan täyttää. Tämän seikan korjaamiseksi tietoturvatasot on huomioitu kaikissa asetuksen voimaantulon jälkeen julkaistuissa VAHTI-ohjeissa, joissa annetaan vaatimuksia ja suosituksia eri tietoturvatasoilla sovellettavista ratkaisuista.
> Tietoturvatasovaatimuksia toteutettaessa ja arvioitaessa on huomioitava VAHTI 2/2010 -ohjeen lisäksi erityisesti seuraavat ohjeet:
>
> VAHTI 3/2010 Sisäverkko-ohje
> VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohje
> VAHTI 3/2012 Teknisen ympäristön tietoturvataso-ohje
> VAHTI 1/2013 Sovelluskehityksen tietoturvaohje
> VAHTI 2/2013 Toimitilojen tietoturvaohje
> VAHTI 4/2013 Henkilöstön tietoturvaohje
> VAHTI 5/2013 Päätelaitteiden tietoturvaohje".

Tietoturvallisuusarviointeja ja -tarkastuksia tehdessä sovelletaan edellä mainittua ohjeistusta niin, että VAHTI-kriteeristöä vasten arvioitaessa arviointi kattaa VAHTI-

ohjeissa 2/2010, 3/2010, 3/2012, 1/2013, 2/2013 ja 5/2013 esitetyt vaatimukset soveltuvin osin. Jos tarkastuksessa on keskenään ristiriitaisia vaatimuksia kuten Katakri ja VAHTI, niin vaatimusten täyttämistä tulkitaan siten, että tiukin vaatimus vaihtoehto täyttyy. (VAHTI 2/2014)

3.3.3 OWASP - The Open Web Application Security Project

The Open Web Application Security Project eli OWASP on avoin voittoa tavoittelematon järjestö, jonka tehtävänä on edistää luotettavien sovellusten kehittämistä, valmistamista ja ylläpitämistä. OWASP Top 10 on järjestön tunnetuin projekti. OWASP Top 10 pitää yllä luetteloa vaarallisimmista haavoittuvuuksista joita esiintyy verkkosovelluksissa. OWASP pitää myös yllä muitakin projekteja, joista on kehittynyt runsaasti tekstitiedostoja ja koodikirjastoja sekä työkaluja tietoturvatestaukseen. (OWASP 2017)

Muita arviointikriteeristöjä

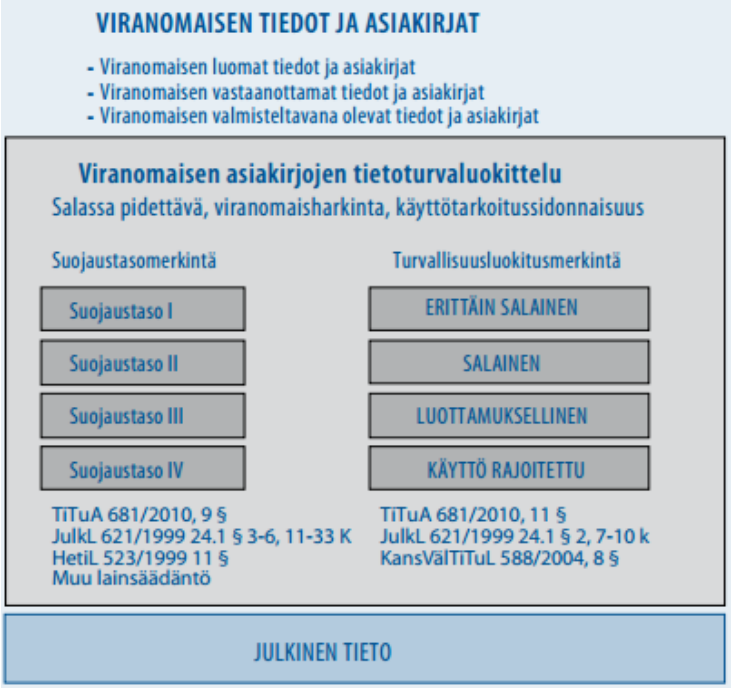
Tietoturvallisuuden hallintaan on olemassa useita eri kriteeristöjä sekä standardeja. Lakien ja asetusten lisäksi toimintaa voi ohjata esimerkiksi ISO 27000 -sarjan standardien pohjalta. Näistä ISO 27000 -sarjan standardeista ISO 27001 keskittyy tietoturvallisuuden yleiseen hallintaan organisaatiossa. (SFS 2017)

NIST - National Institute of Standards and Technology - Technical Guide to Information Security Testing and Assessment National Institute of Standards and Technology on yhdysvaltalainen kauppaministeriön alainen virasto, jonka tehtävänä on kehittää ja viedä eteenpäin mittaustekniikoita ja standardeja. Virasto käytti aikaisemmin vuosina 1901–1988 nimeä National Bureau of Standards (NBS). (NIST 2017)

3.4 Tietoaineistojen luokittelu

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa säätää valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista. (Asetus tietoturvallisuudesta valtionhallinnossa 2010)
Julkisuuslaissa määritellään viranomaisten asiakirjat, salassapitovelvollisuus ja niiden julkisuus. Julkisuuslain lähtökohdaksi on asetettu viranomaisten asiakirjojen julkisuus.
Kokonaan tai osittain salassa pidettävät asiakirjat on laissa erikseen määritelty. Salassa pidettäviä asiakirjoja saavat käsitellä vain yksinomaan henkilöt, joilla on siihen oikeus. Salassa pidettävän asiakirjan käsittelyoikeus on voimassa niin kauan, kuin salassapitovelvollisuus on voimassa.

Salassa pidettävän ja käyttörajoitteisen sekä harkinnanvaraisesti julkisen tietoaineiston käsittelyä ohjataan suojaustasojen avulla tietoturvallisuusasetuksen 9 §:ssä osoitetulla tavalla. VAHTI-ohjeistuksen mukaan: "Osaan näistä asiakirjoista voidaan tehdä turvallisuusluokittelua koskeva merkintä tietoturvallisuusasetuksen 11 §:ssä säädetyin edellytyksin. Turvallisuusluokitusmerkintää on sallittua käyttää vain niissä tietoaineistoissa, joissa olevien tietojen oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille yleisille eduille siten kuin tietoturvallisuusasetuksessa säädetään". (VAHTI 2/2010)



Kuva 4. Viranomaisen asiakirjojen turvaluokittelu.

Yllä olevassa kuvassa (kuva 4) on havainnollistettu viranomaisten tietojen ja asiakirjojen suojaustasomerkinnät ja turvallisuusluokitusmerkinnät vastaavat toisiaan. Näiden asiakirjojen ja tietojen käsittelyyn liittyy käsittelyrajoitus. Henkilöllä tulee olla oikeus niiden käsittelyyn. Osa tästä aineistosta on salassa pidettävää, osa viranomaisharkintaan perustuvaa ja osa käyttötarkoitussidonnan alaista.

3.4.1 Suojaustasot

Salassa pidettävät asiakirjat tai niihin sisältyvät tiedot luokitellaan sen mukaan, minkälaisia tietoturvallisuutta koskevia vaatimuksia niiden käsittelyssä on tarpeen noudattaa. Valtionhallinnon salassa pidettävien tietojen luokittelujärjestelmän suojaustasot on jaoteltu välille I - IV. Suojaustaso I edellyttää vaativimmat ja suojaustaso IV vähäisimmät suojausmenettelyt. Tietoturvalasetuksen 9 § määrittää suojaustasot seuraavanlaisesti:

"Salassa pidettävien asiakirjojen luokittelussa käytetään seuraavia luokkia:

> 1) suojaustaso I, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle;
>
> 2) suojaustaso II, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle;
>
> 3) suojaustaso III, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle;
>
> 4) suojaustaso IV, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle." (Asetus tietoturvallisuudesta, 9 §)

Esimerkkinä, jos asiakirja sisältää henkilötunnuksen tulee sitä käsitellä suojaustason IV mukaisesti. Jos asiakirja ei sisällä muuta tietoa, minkä vuoksi sen käsittelyvaatimukset tulisi olla korkeamman suojaustason mukainen. (VAHTI 2010)

3.4.2 Turvallisuusluokitusmerkinnät

Tietoturvallisuusasetuksen 12§:ssä viitatuissa tapauksissa viranomaisten asiakirjoihin on mahdollista tehdä turvallisuusluokitusmerkintä. Turvallisuusluokitusmerkintöjä voidaan osoittaa neljälle eri tasolle. Turvallisuusluokka ilmaisua on myös käytetty usein turvallisuusluokiteltavin asiakirjojen yhteydessä. (VAHTI tietoaineistojen luokittelu 2016)

> "Jos asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2 ja 7—10 kohdassa tarkoitetulla tavalla, salassa pidettävän asiakirjan suojaustasoa koskevan merkinnän yhteyteen tai sen sijasta voidaan tehdä erityinen turvallisuusluokitusmerkintä.
>
> Turvallisuusluokitusmerkintä tehdään:
> 1) suojaustasoon I kuuluvaan asiakirjaan merkinnällä "ERITTÄIN SALAINEN";
> 2) suojaustasoon II kuuluvaan asiakirjaan merkinnällä "SALAINEN";
> 3) suojaustasoon III kuuluvaan asiakirjaan merkinnällä "LUOTTAMUKSELLINEN";
> 4) suojaustasoon IV kuuluvaan asiakirjaan merkinnällä "KÄYTTÖ RAJOITETTU"."
> (Asetus tietoturvallisuudesta valtionhallinnossa 2010)

Turvallisuusluokitusmerkintää ei saa käyttää muissa kuin valtionhallinnon tietoturvallisuuden asetuksen 1 momentissa tarkoitetuissa tapauksissa. Mikäli turvallisuusluokitusmerkinnän tekeminen ei ole tarpeen kansainvälisen tietoturvallisuusvelvoitteen saavuttamiseksi tahi asiakirja ei muutoin liity kansainväliseen yhteistyöhön.

Suojaustaso	Turvallisuusluokitusmerkintä	Tietoturvallisuustaso
Suojaustaso I	Erittäin salainen	Korkea taso + lisävaatimukset
Suojaustaso II	Salainen	Korkea taso
Suojaustaso III	Luottamuksellinen	Korotettu taso
Suojaustaso IV	Käyttö rajoitettu	Perustaso

Taulukko 3. Turvallisuusluokitusmerkintöjen ja suojaustasojen vastaavuudet

Yllä olevassa taulukossa (Taulukko 3) kuvaillaan edellä mainittujen turvallisuusluokitusmerkintöjen ja suojaustasojen suhdetta toisiinsa. VAHTI-ohjeistuksen mukaisesti suojaustason IV materiaalia on mahdollista käsitellä perustason tietojenkäsittely-ympäristössä selväkielisenä. Suojaustason I materiaalin tulee olla aina salattu vahvasti ja sen käsittely on sallittu vain valvotuissa erillisverkoissa. (valtiovarainministeriö /VAHTI 2010)

Turvallisuusluokitusmerkintöjen kansainväliset vastaavuudet

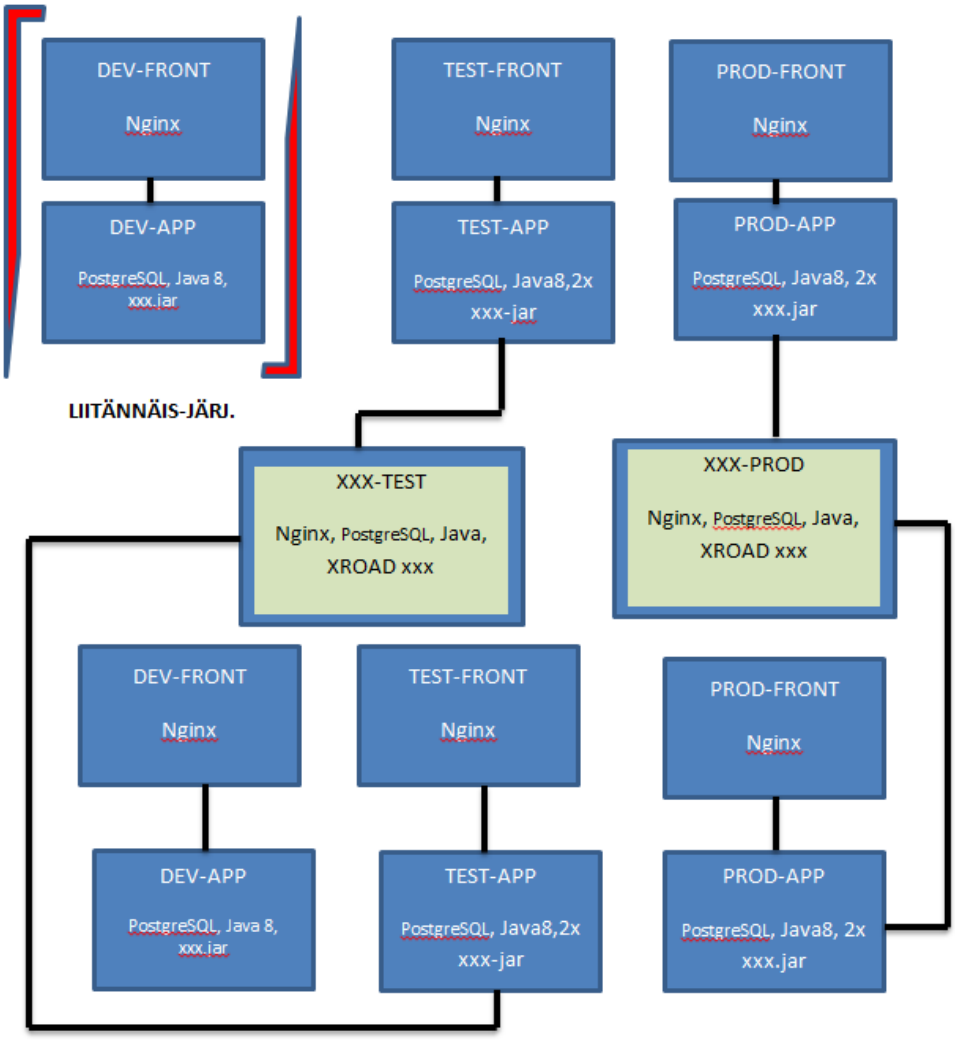
Vierailta valtiolta ja kansainvälisiltä järjestöiltä voi olla käytössä omia luokitusmerkintöjä. Suomeen tulleissa toisen valtion asiakirjoihin tehdään vastaavaa turvallisuusluokitusta koskeva merkintä, mikäli turvallisuusluokiteltujen tietojen molemminpuolisesta suojelusta on obligatorinen sopimus (VAHTI 2016 tietoaineistojen luokittelu).

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa kuvaa seuraavasti turvallisuusluokitusmerkintöjen kansainväliset vastaavuudet:

> "Jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu, turvallisuusluokitusmerkintää "ERITTÄIN SALAINEN" vastaa kansainvälisen tietoturvallisuusvelvoitteen mukainen luokka "TOP SECRET" tai sitä vastaava muun kielinen ilmaisu; merkintää "SALAINEN" vastaa "SECRET" tai sitä vastaava muun kielinen ilmaisu; merkintää "LUOTTAMUKSELLINEN" vastaa "CONFIDENTIAL" tai sitä vastaava muun kielinen ilmaisu; merkintää "KÄYTTÖ RAJOITETTU" vastaa "RESTRICTED" tai sitä vastaava muun kielinen ilmaisu." (Asetus tietoturvallisuudesta valtionhallinnossa)

4 CASE-YRITYKSEN JÄRJESTELMÄKUVAUS

Tietojärjestelmän tietoturvallisuuden arvioinnin kohteena olevan case-yrityksen järjestelmä koostuu kohtuullisen pelkistetystä kokonaisuudesta. Käytännössä samalla palvelimella sijaitsee kahdentamaton applikaatiopalvelin sekä postgreSQL-tietokantapalvelin. Edustapalvelimella työskentelee Nginx-palvelin. Tietojärjestelmän konfiguraatiot ja käyttöönotot (deployt) on automatisoitu Ansible -automaatiokoneella (Kuva 5).



Kuva 5. Järjestelmäkuvaus.

PostgreSQL on avoimen lähdekoodin olio-relaatiotietokantapalvelin. Vastaavia vaihtoehtoja vapaan lähdekoodin tietokantajärjestelmille on muun muassa Firebird ja MySQL. PostgreSQL ei ole yksittäisen yrityksen tai henkilön kontrolloima, vaan perustuu kansainväliseen ohjelmoijien ja yritysten muodostaman yhteisön tekemään kehitystyöhön, samoin kuin esimerkiksi Apache ja BSD-variantit. (PostgreSQL 2017)

Nginx [engine x] on WWW- ja proxy-palvelin. Se kehitettiin ensin hakukoneeksi ja web-portaalin palvelimeksi. Vuonna 2004 siitä julkaistiin ensimmäinen versio. Osapuilleen palvelinta käytetään neljänneksessä maailman vilkkaimmista web-sivustoista. Palvelin ohitti Vuoden 2012 alussa Microsoftin IIS:n ja nousi maailman toiseksi käytetyimmäksi, kun huomioidaan pelkästään aktiiviset web-sivut, laskusta jätetään huomioimatta domainparkit. (Wikipedia 2017) Netcraft Internet-palveluyhtiön tutkimuksen mukaan Nginx palveli tai välityspalveli 28,72% vilkkaimpia sivustoja huhtikuussa 2017, kuten Netflix, Wordpress.com, FastMail.FM. (Nginx 2017)

Java on Sun Microsystemsin kehittämä ohjelmistoalusta. Siihen kuuluu esimerkiksi laitteistoriippumaton oliopohjainen ohjelmointikieli sekä ajoaikainen ympäristö virtuaalikoneineen sekä luokkakirjastoineen. Java-alustan käyttöä ei ole rajattu pelkästään Java-ohjelmointikieleen, myös Python-, Ruby- ja Scheme-kielille on saatavilla kääntäjä, joka tuottaa Java-tavukoodia. Java-alustaa käytetään ympäri maailmaa, noin 3,8 miljardissa laitteessa aina matkapuhelimista supertietokoneisiin. (Wikipedia 2017b)

Ansible on avoimen lähdekoodin automaatiokone, joka automatisoi pilvi provisioinnin, konfiguraationhallinnan ja sovellusten käyttöönoton. (Wikipedia 2017c)

Järjestelmä käyttää X-Road tiedonsiirtoprotokollaa. X-Road on Virossa kehitetty ja käytössä oleva ohjelmisto. Palveluväylään liittyminen edellyttää, että liitettävä järjestelmä pystyy lähettämään ja vastaanottamaan SOAP-sanomia X-Roadin edellyttämässä muodossa. Tämä tarkoittaa sitä, että SOAP-sanomien on sisällettävä tietyt X-Road-tiedonsiirtoprotokollan määrittelemät otsikkotiedot. (X-Road 2016)

5 TUTKIMUSSUUNNITELMA

Tutkimussuunnitelma perustuu osin case-yrityksen web-pohjaisen tietojärjestelmän tietoturvallisuusarvionnin tarkastussuunnitelmaan. Vuoden 2016 alkupuoliskolla saadun arviointipyynnön perusteella tehtäväksi tuli tehdä tarkastus arvioinnin tilaaman case-yrityksen ylläpitämän sovelluksen tietoturvallisuuden nykytilasta. Tarkastuksen tavoitteena oli arvioida case-yrityksen web-sovelluksen nykytila suhteessa kansallisen suojaustason IV aineiston käsittelyvaatimuksiin. Vaatimusmäärittelynä oli tilattu käytettäväksi Tietoturvallisuuden auditointityökalua viranomaisille (Katakri, 2015). Case-yrityksen tietoturvallisuuden nykytilan vaatimusten mukaisuuden varmentamisessa käytettiin Katakrin ohella myös OWASP:n Applicaton Security Verification Standard Project 3:sta (ASVS3), jota käytetään yleisesti oppaana sovellusten tietoturvan varmistamiseen ja testaukseen.

Sovelluksen kehitys- ja testiympäristön fyysisen turvallisuuden auditointi ja case-yrityksen hallinnollisen turvallisuuden auditointi on tarkoitus rajata tämän sovelluskokonaisuuden auditoinnin ulkopuolelle. Tämän tarkastuksen tarkoitus on kohdentua pelkästään sovellustestaukseen. Sovelluskokonaisuuden tekniset testit on tarkoitus suorittaa sovelluksen testiympäristössä etäyhteyden välityksellä.

5.1 Tarkastuksen lähtökohta ja laajuus

Tarkastuksen kohteena olleeseen järjestelmään on tehty lähivuosien aikana useita tietoturvallisuusarviointeja, jotka liittyvät muun muassa järjestelmän sovellusturvallisuuteen. Tarkastuksen kohteena olevaan järjestelmään liittyvään web-sovellukseen on edellisen tarkastuksen jälkeen toteutettu uusia ominaisuuksia. Juuri näiden uusien ominaisuuksien johdosta tämä tietoturvallisuusarviointi toteutetaan. Järjestelmän palvelinalustaan, ylläpitokäytäntöihin tai muihin järjestelmän tietoturvallisuuteen vaikuttaviin osiin ei ole kohdistunut minkäänlaisia muutoksia.

Tämän vuoksi järjestelmän muutosten tarkastaminen rajoittuu web-sovelluksen muutosten katselmointiin.

5.2 Aikataulu ja alustava työmääräarvio

Tavoitteena on aloittaa tarkastukset vuoden 2016 alkuvuoden aikana. Tarkastuksen aikataulu tulee tarkentumaan työn edetessä. Tavoitteena on saada tarkastus suoritettua loppuun ennen vuoden 2016 kesäkuun loppua, jonka tuloksena laaditaan loppuraportti arvioinnin tilaajalle. Tarkastuksen alustava työmääräarvio perustuu toimitetun aineiston perusteella saatuihin tietoihin ja aikaisempiin kyseisen case-yrityksen tietojärjestelmän web-sovelluksen tietoturvallisuusarviointeihin. Työmääräarvio (2-3 kk) pitää sisällään dokumentaatioon tutustumisen, tarkastuksen suunnittelun, teknisen turvallisuuden todentamisen ja raportoinnin.

5.3 Menetelmät ja työkalut

Turvallisuusjohtamisen osa-alueeseen kuuluvat hallinnollinen turvallisuus ja henkilöstöturvallisuus rajattiin tarkastuksessa järjestelmäarvioinnin piirin ulkopuolelle.

Fyysinen turvallisuuden osa-alueen kattavat tiloja ja laitteita koskevat vaatimukset, luvattoman pääsyn estäminen, salakatselulta ja kuuntelulta suojaaminen ja toiminnan jatkuvuuden hallinta rajattiin myös tämän tarkastuksen ulkopuolelle

Tavanomaisissa auditoinneissa tapahtuva teknisen tietoturvallisuuden todentamisen menetelmät on kuvattu laajemmin luvussa 3.1.2 , joka käsittää tietojärjestelmien arviointi- ja hyväksyntäprosessit.

Case-yrityksen web-sovellukseen tehtyjen muutoksien teknisen tietoturvallisuuden vaatimustenmukaisuus on tarkoitus todentaa seuraavilla menetelmillä ja työkaluilla, tarkemmin luvussa 3.1.4 .

Case-yrityksen web-sovelluksen teknisen tietoturvallisuuden tilan todentamiseen on tarkoitus käyttää aktiivista rajapinta-analyysi menetelmää.
Aktiivinen rajapinta-analyysi menetelmä tulee pitämään sisällään tunnettujen haavoittuvuuksien haavoittuvuusskannaukset, porttiskannaukset ja toimintavarmuustestaukset. Tässä testaus tapauksessa toimintavarmuustestauksella (Fuzz testing) pyritään virheellisen syötteen lähettämiseen pohjautuvaa koettelemusta.
Haavoittuvuuksien havaitseminen verkossa ja porttiskannaus on tarkoitus suorittaa Nmap ja Burp Suite -ohjelmilla.

Aktiivisen rajapinta-analyysin lisäksi web-sovelluksen teknisen tietoturvallisuuden tilan todentamisessa on suunnitelmissa käyttää sovellusturvallisuus menetelmää. Sovellusturvallisuus menetelmä käsittää testauksen kohteen turvallisuuteen vaikuttavien sovelluskomponenttien tarkastelut. Web-sovelluksen turvallisuutta ja pääsynhallintaa on aikomus koetella niin ikään Burp Suite sekä OWASP Zed Attack Proxy (ZAP) työkaluilla. Muutostiedoston katselmointia on suunniteltu tutkittavan manuaalisesti. Kun tiedämme käytössä olevat palvelut etukäteen, voidaan järjestelmään kohdistaa palvelukohtaisia skannauksia sqlmap exploit-työkalulla, mikäli se on mahdollista aikataulun sallimassa rajoissa.

5.4 Ennakkovaatimukset

Ennakkovaatimuksena case-yrityksen tekemät toimenpiteet liittyvät järjestelmän testiympäristön porttiavaruuksien konfigurointeihin. Etäyhteyden välityksellä tapahtuva testaus edellyttää että testattavana oleva kohde tekee tarvittavat avaukset ennen testauksen alkua, jotta pääsemme haluamasta IP- osoitteesta suoraan testipalvelimelle.

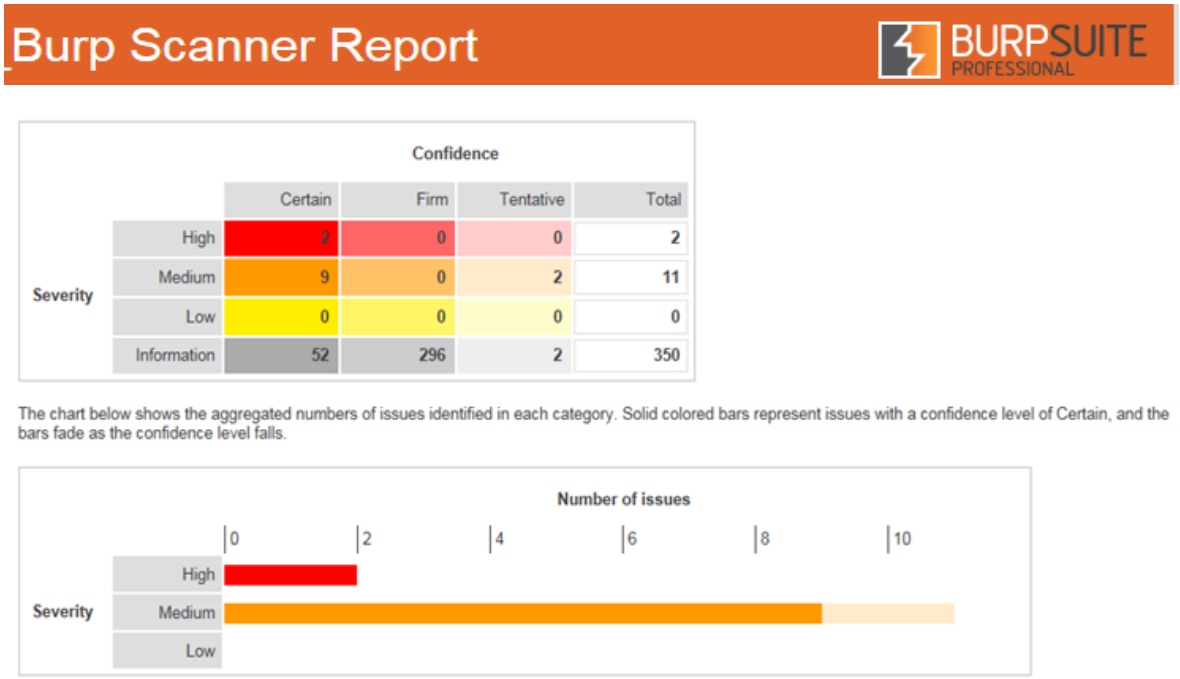
6 TUTKIMUKSEN TOTEUTUS

Tarkastuksen käytännön toteutus tapahtui melko tarkasti suunnitelman mukaisesti. Case-yrityksen ilmoitettua, että vaadittavat yhteydet ennalta sovittuihin portteihin ja IP-osoitteiseen oli avattu, aloitimme tutkimuksen teknisen toteutuksen. Case-yrityksen web-sovelluksen teknisen tietoturvallisuuden tilan todentamisessa käytettiin suunnitelman mukaisesti aktiivista rajapinta-analyysi menetelmää. Tutkimussuunnitelmasta poikettiin jättämällä varsinainen toimintavarmuustestaus, Fuzz testing, tutkimuksen ulkopuolelle. Tutkimussuunnitelman mukaisesti haavoittuvuuksien havaitseminen verkossa ja porttiskannaus suoritettiin Nmap ja Burp Suite -ohjelmilla.

Tutkimussuunnitelman mukaisesti seuraavana vuorossa oli web-sovelluksen teknisen tietoturvallisuuden tilan todentaminen. Tässä osiossa käytettiin suunnitelman mukaisesti sovellusturvallisuudenarviointi menetelmää. Sovellusturvallisuus menetelmä käsitti tutkimuksen kohteen turvallisuuteen vaikuttavien sovelluskomponenttien tarkastelut. Web-sovelluksen turvallisuutta ja pääsynhallintaa koeteltiin niin ikään tutkimussuunnitelman mukaisilla työkaluilla, jotka koostuivat Burp Suite sekä OWASP Zed Attack Proxy (ZAP) -työkaluista. Muutostiedoston katselmointia tutkittiin manuaalisesti. Kireästä aikataulutuksesta johtuen tutkimussuunnitelmasta poiketen palvelukohtaiset skannaukset sqlmap exploit-työkaluilla jätettiin tutkimuksen ulkopuolelle. Tutkimuksen tekninen toteutus saatiin kokonaisuudessa toteutettua ennalta suunnitellussa aikataulussa.

7 TUTKIMUKSEN TULOKSET JA HAVAINNOT

Testaussuunnitelman mukaisesti itse testauksen toteutus suoritettiin eri työkalulla ja useita testiskannauksia tehden. Tutkimuksen tuloksista voidaan nostaa esiin yhden Burp Suite -ohjelman skannausraportin yhteenveto (Kuva 6), jossa huomataan, että pelkästään yhden testiajon havainnot koostuvat lukuisista havainnoista. Tässä esimerkissä havaintoja esiintyi 350 kappaletta. Burp Suite -raportin yhteenvetotaulukko koostuu vakavuus (Severity) ja luottamuksellisuus (Confidence) sarakkeista. Vakavuudet on luokiteltu neljään osioon, ylin vakavuusluokka on korkea (High), toinen vakavuusluokka on keskitaso (Medium), kolmas luokka on matala (Low) ja viimeinen neljäs luokka on informatiivinen (Information). Luottamuksellisuudet on luokiteltu kolmeen osioon, korkein luottamuksellisuuden luokka on nimetty tunnetuksi (Certain), toinen luottamuksellisuuden luokka on vakaa (Firm), kolmas luokka on alustava (Tentative). Skannausraportin neljäs pystysarake on yhteenvetosarake johon on koostettu kaikki yhden Burp Suite skannaussessiossa löydetyt tulokset.



Kuva 6. Skannaustuloksen yhteenveto.

Kuten aina tietojärjestelmän teknisissä tietoturvallisuusarvioinneissa myös case-yrityksen tapauksessa kaikki havainnot analysoitiin ja tarkistettiin myös manuaalisesti. Tällä toimenpiteellä varmistetaan ja todennetaan muun muassa, että havainnoissa ei ole false positive -tapauksia.

Seuraavaksi esittelen tarkastuksessa esille tulleita tuloksia. Ensimmäinen haavoittuvuusskannauksen esimerkki tulos on yksi yleisimmistä web-sovellushaavoittuvuuksista, XSS eli Cross Site Scripting (Kuva 7). Kyseistä XSS-haavoittuvuutta voidaan hyödyntää sijoittamalla käyttäjän selaimeen haitallinen komentojono eli hyökkäyksen kohde ei ole varsinaisesti itse web-palvelu, vaan palvelun käyttäjä. Kyseisellä menetelmällä hyökkääjä yrittää saada ajaa luvatonta koodia käyttäjän selaimessa web-sovellukseen sijoitetun hyökkääjän koodin avulla. Cross Site Scripting haavoittuvuus voi olla voimassa pelkästään istuntokohtaisesti. Syötetty haitallinen koodi suoritetaan vain yhden kerran tai se voidaan tallentaa web-palveluun, jolloin koodi suoritetaan aina kaikilla käyttäjillä, jotka vierailevat kyseisellä sivustolla. (Engebretson 2011, 123.)

Cross-site scripting (reflected)

Summary

Severity:	**High**
Confidence:	**Certain**
Host:	**https://testi.xxxxxxxxxxxxxxx.fi**
Path:	**/xxxxxxxxxxreturn**

Request

```
POST /xxxxxxxxxxreturn HTTP/1.1
Host: testi.xxxxxxxxxxxxxx.fi
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testi.xxxxxxxxxxxxx.fi/xxxxmock
Cookie: JSESSIONID=byueeccoyq0gqrg4jvb5ymh8
Connection: close
Content-Type: application/x-www-form-urlencoded
```

```
Content-Length: 399

RCVID=ASIAKAS1&APPID=xxxxxxxxxxxxxxx.fi&TIMESTMP=20160222144546193&SO=6&LG=fi&R
ETURL=javascript%3aalert(1)%2f%2ff592dfb2&CANURL=https%3A%2F%2Ftesti.xxxxxxxxxxxxxx.fi
%2Ffi%2Flogin&ERRURL=https%3A%2F%2Ftesti.xxxxxxxxxxxxxx.fi%2Ffi%2Flogin&TRID=&first_na
me=xxxxxx+&last_name=xxxxxx&municipality_fi=xxxxxxx&municipality_sv=
...[SNIP]...
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 22 Feb 2016 13:39:12 GMT
Content-Type: text/html;charset=utf-8
Connection: close
Content-Language: fi
Strict-Transport-Security: max-age=15768000
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block;
Content-Length: 4485

<!DOCTYPE HTML>
<html>
<head></head>
<body>

<form action="javascript:alert(1)//f592dfb2" method="post">

<input type="hidden" name="RCVID" value="ASIAKAS1"/>
<input type="hidden" name
...[SNIP]...
```

Kuva 7. Cross-site scripting.

Toinen Burp Suite haavoittuvuusskannauksen esimerkkitulos on Frameable response (potential Clickjacking) (Kuva 8). Tämän haavoittuvuuden vakavuusluokitus on informatiivinen. Kyseinen Frameable response hyökkäys voi mahdollistaa hyökkääjän käyttämään clickjacking hyökkäysmenetelmää, jossa hyökkääjä korvaa kohdesovelluksen alkuperäisen sivun omalla liitännällä.

Frameable response (potential Clickjacking)

Summary

Severity:	**Information**

Confidence:	**Firm**
Host:	**https://testi.xxxxxxxxxxxxxx.fi**
Path:	**/api/**

Request

```
GET /api/ HTTP/1.1
Host: testi.xxxxxxxxxxxxx.fi
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Cookie: CSRFToken=0j7UPSCSwP6.HmCxGLAuc6LHRJYflt4M;
JSESSIONID=1cy3a9ry0s4vk1gqhb5t598g8a
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 22 Feb 2016 13:00:06 GMT
Content-Type: text/html;charset=utf-8
Connection: close
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Language: fi
Strict-Transport-Security: max-age=15768000
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block;
Content-Length: 28048


<!DOCTYPE HTML>

<!--[if lt IE 7 ]> <html lang="fi" class="no-js ie6"> <![endif]-->
<!--[if IE 7 ]> <html lang="fi" class="no-js ie7"> <![endif]-->
<!--[if IE 8 ]> <html lang="fi" class="no-
...[SNIP]...
```

Kuva 8. Frameable responce (potential Clickjacking).

Kolmas haavoittuvuusskannauksen esimerkkitulos on Cacheable HTTPS response (Kuva 9). Tämän haavoittuvuuden vakavuusluokitus on informatiivinen eli matala. Kyseinen haavoittuvuus hyödyntää selaimelle tallennetun paikallisen välimuistikopion sisällön joka on saatu web-serveriltä. Joidenkin selainten
välimuistin sisältöön pääsee käsiksi HTTPS:n kautta, jolloin myöhemmin samaa tietokonetta käyttävä henkilö saattaa päästä käsiksi arkaluontoisiin tietoihin (Portswigger 2016).

Cacheable HTTPS response

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://fonts.gstatic.com**
Path:	**/s/ptsans/v8/0XxGQsSc1g4rdRdjJKZrNPk_vArhqVIZ0nv9q090hN8.woff2**

Request

```
GET /s/ptsans/v8/0XxGQsSc1g4rdRdjJKZrNPk_vArhqVIZ0nv9q090hN8.woff2 HTTP/1.1
Host: fonts.gstatic.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: application/font-woff2;q=1.0,application/font-woff;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: identity
Referer: https://fonts.googleapis.com/css?family=PT+Sans:400,700,400italic,700italic
Origin: https://testi.xxxxxxxxxxxxxxxx.fi
Connection: close
```

Response

```
HTTP/1.1 200 OK
Content-Type: font/woff2
Access-Control-Allow-Origin: *
Timing-Allow-Origin: *
Date: Wed, 17 Feb 2016 00:11:12 GMT
Expires: Thu, 16 Feb 2017 00:11:12 GMT
Last-Modified: Mon, 06 Oct 2014 20:39:39 GMT
X-Content-Type-Options: nosniff
Server: sffe
Content-Length: 50664
```

```
X-XSS-Protection: 1; mode=block
Cache-Control: public, max-age=31536000
Age: 477182
Connection: close
wOF2.....h.....|.p.`..,.,    ....
..H..    ....6.$.....z..N.. ..<..v...[....}..f.....*Q
.F.<....:.e..m.....w[.x...8.`.<.....dC\....R[I.".~□2T.....@.y..`.eU....
...[SNIP]...
```

Kuva 9. Cacheable HTTPS response.

Neljäs Burp Suite haavoittuvuusskannauksen esimerkki tulos on Cross-domain Referer leakage (Kuva 10). Tämän haavoittuvuuden vakavuusluokitus on alin eli informatiivinen. Kyseissä tapauksessa selaimen tekemä resurssipyyntö eri verkkotunnukselle voi aiheuttaa arkaluontoisen tiedon vuotamisen eli tietoturvan vaarantumisen mikäli kyseessä ei ole täysin luotettu verkkotunnus (Portswigger 2016b).

Cross-domain Referer leakage

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://testi.xxxxxxxxxxxxxxxx.fi**
Path:	**/fi/hae**

Request

```
GET /fi/hae?minSupportCount=on&show=waiting&orderBy=leastTimeLeft HTTP/1.1
Host: testi.xxxxxxxxxxxxxxx.fi
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer: https://testi.xxxxxxxxxxxxx.fi/fi/hae
Cookie: CSRFToken=0j7UPSCSwP6.HmCxGLAuc6LHRJYflt4M;
JSESSIONID=1cy3a9ry0s4vk1gqhb5t598g8a
```

Response

```
HTTP/1.1 500 Server Error
Server: nginx
Date: Mon, 22 Feb 2016 13:11:49 GMT
Content-Type: text/html;charset=utf-8
Connection: close
Pragma: no-cache
Content-Language: fi
Content-Length: 6237


<!DOCTYPE HTML>
<html lang="fi">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
<meta name="viewport" content="width=device-width, initial-scale=1"/>

<title>
...[SNIP]...
<li>
<a class="active" href="https://www.xxxxxxxxxxxxxx.fi/fi">xxxxxxxxxxxxx.fi</a>
...[SNIP]...
```

Kuva 10. Cross-domain Referer leakage.

Viimeinen Burp Suite haavoittuvuusskannauksen esimerkki tulos on Cross-Site Request Forgery (CSRF) (Kuva 11). Tämän haavoittuvuuden vakavuusluokitus on keskitasoa. CSRF hyökkäystyypissä hyökkääjä lähettää käyttäjältä pyyntöjä palvelimelle eli kyseessä on palvelimen käyttäjään kohdistaman luottamuksen hyväksikäyttäminen. Tapauksessa hyökkääjä erehdyttää käyttäjän selaimen lähettämää pyyntöä hyökkääjän parametreilla kohteena olevalle palvelimelle. Palvelimelle hyökkääjän pyyntö näyttää tulevan käyttäjältä.

Cross-site request forgery

Summary

Severity:	**Medium**
Confidence:	**Tentative**
Host:	**https://testi.xxxxxxxxxxxxxxx.fi**

Path:	**/xxxxxxxxxxxreturn**

Request 1

```
POST /xxxxxxxxxxxreturn HTTP/1.1
Host: testi.xxxxxxxxxxxxx.fi
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testi.xxxxxxxxxxxxxxx.fi/xxxxxmock
Cookie: JSESSIONID=byueeccoyq0gqrg4jvb5ymh8
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 399

RCVID=ASIAKAS1&APPID=xxxxxxxxxxxxxxxx.fi&TIMESTMP=20160222144546193&SO=6&LG=fi
&RETURL=https%3A%2F%2Ftesti.xxxxxxxxxxxxxxxx.fi%2Ffi%2Flogin&CANURL=https%3A%2F%2
Ftesti.xxxxxxxxxxxxx.fi%2Ffi%2Flogin&ERRURL=https%3A%2F
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 22 Feb 2016 13:37:47 GMT
Content-Type: text/html;charset=utf-8
Connection: close
Content-Language: fi
Strict-Transport-Security: max-age=15768000
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block;
Content-Length: 4509

<!DOCTYPE HTML>
<html>
<head></head>
<body>

<form action="https://testi.xxxxxxxxxxxxxxx.fi/fi/login" method="post">

<input type="hidden" name="RCVID" value="ASIAKAS1"/>
<input type="
...[SNIP]...
```

Request 2

```
POST /xxxxxxxxxxreturn HTTP/1.1
Host: testi.xxxxxxxxxxxxxxx.fi
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

```
Referer: https://ISlZjtCqOWuwmskMvmuJd.fi/vetumamock
Cookie: JSESSIONID=nvv3pbh8kw1qvwqbuhibwhfb;
CSRFToken=IsO1O.ez2ngVOnF069Ab4ciOqDaBbk.8
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 391

RCVID=&APPID=xxxxxxxxxxxxxxxx.fi&TIMESTMP=20160222144546193&SO=6&LG=fi&RETURL=h
ttps%3A%2F%2Ftesti.xxxxxxxxxxxxfi%2Ffi%2Flogin&CANURL=https%3A%2F%2Ftesti.xxxxxxxxxx
xxx.fi%2Ffi%2Flogin&ERRURL=https
...[SNIP]...
```

Response 2

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 22 Feb 2016 13:42:26 GMT
Content-Type: text/html;charset=utf-8
Connection: close
Content-Language: fi
Strict-Transport-Security: max-age=15768000
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block;
Content-Length: 4501

<!DOCTYPE HTML>
<html>
<head></head>
<body>

<form action="https://testi.xxxxxxxxxxxxx.fi/fi/login" method="post">

<input type="hidden" name="RCVID" value=""/>
<input type="hidden"
...[SNIP]...
```

Kuva 11. Cross-Site Request Forgery (CSRF).

Havainnot tarkastuksesta

Tutkimuksen kohteena olevasta case-yrityksen palvelusta ei havaittu tietoturvaa merkittävästi vaarantavia löydöksiä, jotka vaatisivat erityisiä korjauksia. Järjestelmän tekninen toteutus on tarkastettujen muutosten jälkeen edelleen hyväksynnän edellyttämällä tasolla.

Case-yrityksen palveluun suositellaan kuitenkin joitakin toimia järjestelmän turvallisuuden parantamiseksi. Suositeltavia korjaustoimenpiteitä löytyi Application

Security Verification Standard 3.0 (ASVS V3) -taulukon seuraavista kohdista: autentikointi, session hallinnointi, HTTP-turvallisuus, haitallisen syötteen käsittelyn todentamisvaatimuksen sekä virheenkäsittelyn ja lokituksen osioista.

7.1 OWASP ASVS:n hyödyntäminen tutkimuksessa

Web-sovellushaavoittuvuudet

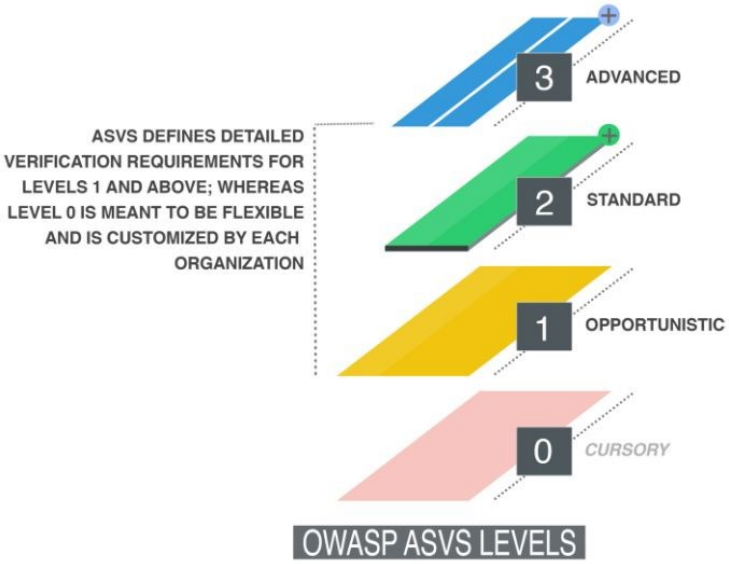
Useimmilla yrityksillä on käytössä web-sivut ja erilaisia web-sovelluksia. Joten todennäköisiä paikkoja puutteellisten tietoturva-asetusten löytämiseksi ovat juurikin web-sovellukset. Näitä haavoittuvuuksia hyväksikäyttämällä pystytään ohittaamaan palomuurit ja muut infrastruktuurin turvamenetelmät. Hyökkäykset pystytään kohdistamaan sovelluksen käyttäjiin tai sovellukseen liitettyihin muihin palveluihin. Sovellustietoturvan ympärille kehitetty OWASP (Open Web Application Security Project) organisaatio jakaa sovellustietoturvaan liittyvää tietoa, työkaluja sekä korkealaatuisia käytänteitä. OWASP on puolueeton, eikä sitä ole sidottu mihinkään sovellus- tai laitevalmistajaan. Se on voittoa tavoittelematon kansainvälinen organisaatio, jonka tuottamat dokumentit ja työkalut ovat ilmaisia ja vapaassa käytössä. OWASP julkaisee alan laajasti arvostettua listaa yleisimmistä web-sovellusten haavoittuvuuksista. (OWASP 2013.)

Seuraavana on listattuna OWASP:n Top 10 -listan viisi yleisintä web-sovellusten haavoittuvuutta vuodelta 2013, täydellinen OWASP Top 10 -lista websovellusten haavoittuvuudet löytyy liitetaulukon kohdasta Liite 1. (OWASP Top 10):

1. (Injection) - Taustajärjestelmäkyselyn rakenne ei säily.
2. (Broken Authentication and Session Management) - Puutteellinen tunnistusmenettely ja istunnonhallinta
3. (XSS) (Cross Site Scripting (XSS)) - Verkkosivun rakenne ei säily
4. (Insecure Direct Object Reference) - Turvaton suora viittaus tietoalkioon
5. (Security Misconfiguration) - Puutteelliset tietoturva-asetukset

OWASP Top10 listan kahden kärki ei ole muuttunut vuosien 2007 ja 2010 aikana. Injektio-hyökkäys web-sovelluksen taustajärjestelmään johtuu usein huonosti tarkastetusta syötteestä. Listan kärkipaikalla on SQL-injektio (SQL injection). Seuraavaksi yleisin web-sovellusten haavoittuvuus on Cross Site Scripting (XSS), joka sijoittaa haitallisen komentojonon käyttäjän selaimeen. Kohde ei ole varsinaisesti web-palvelu itsessään vaan se kohdistuu web-palvelun käyttäjiin. Hyökkääjän tavoitteena on ajaa luvaton koodi käyttäjän selaimen web-sovellukseen sijoitetun hyökkääjän koodin avulla. Esimerkkejä tällaisesta koodista ovat arkaluontoisen tiedon anastaminen, näppäinpainallusten tallentaminen tai istunnon kaappaaminen. Web-sovellusten tietoturvaa voidaan testata tähän tarkoitukseen kehitetyillä työkaluilla, joita ovat muun muassa Burp Suite, OWASP ZAP (Zed Attack Proxy), Nikto, WATOBO ja Uniscan Saarinen 2014).

OWASP Application Security Verification Standard Project (ASVS) on projekti, joka tarjoaa alustan ja standardin sovelluksen turvatarkastusten testaukseen (OWASP ASVS 2017). Sovelluksen omistajat ja kehittäjät voivat käyttää ASVS:n ohjeistusta mittarina arvioidessaan verkkosovellustensa luotettavuutta. ASVS auttaa kehittäjiä tietoturvatarkastusten laatimisessa, jotta tietoturvavaatimukset täyttyvät.



Kuva 12. OWASP ASVS tasot.

OWASP Application Security Verification Standard Project (ASVS) projekti koostuu 19:stä eri yksityiskohtaisesta todentamisvaatimusluvusta (Liite 2). ASVS määritellään kolmeen turvallisuuden todentamisen tasoon (Kuva 12). ASVS:n ensimmäinen taso on tarkoitettu kaikille ohjelmistoille. ASVS:n toinen taso on tarkoitettu sovelluksiin, jotka sisältävät arkaluonteistia tietoja, jotka on suojattava. ASVS:n kolmas ja kriittisin taso on sovelluksille, jotka suorittavat arvokasta liiketoimintaa, arkaluontoisia potilastietoja tai minkä tahansa sovelluksen, joka vaatii korkean tason luottamuksen. Todentamisvaatimuksia ASVS:n kolmannessa versiossa on yhteensä 207 kappaletta. (OWASP ASVS 2017)

ASVS V3 korjaussuositukset

Tutkimuksessa syntyneitä haavoittuvuusskannaustuloksia analysoitiin ja tarkasteltiin ensin manuaalisesti, jonka jälkeen validit havainnot uudelleen ajettiin case-yrityksen järjestelmässä. Näin saatiin varmennus skannaustulosten oikeellisuudesta. ASVS V3:a hyödynnettiin tulosten tulkinnassa ja korjaussuositusten laatimisessa. Alla on muutama esimerkki case-yritykselle esitetystä ASVS V3 korjaussuosituksista (Kuva 13).

ASVS ID	Vaatimus	Arviointitulos	Vakavuus	Kuvaus
V2 – Todennus				
V2.12	Verify that all suspicious authentication decisions are logged. This should include requests with relevant metadata needed for security investigations.	Suositellaan korjattavaksi	Lievä	Lähdekoodin katselmoinnin perusteella epäonnistuneita kirjautumisia ei lokiteta.
V3 – Istunnonhallinta				
V3.7	(Versio2) Verify that the session id is changed on login to prevent session fixation. (Versio 3) Verify that all successful authentication and re-authentication generates a new session and session id.	Suositellaan korjattavaksi	Ei vaikutusta tuotantop alveluun	Testi-tunnistautumisen yhteydessä palvelun istuntotunniste ei vaihdu sisäänkirjautumisen yhteydessä. Havainto koskee ainoastaan TESTI-tunnistautumista, eikä aiheuta tietoturvaongelmaa tuotannossa.
V3.16	(Versio 2) Verify that the application does not permit duplicate concurrent user sessions, originating from different machines. (Versio 3) Verify that the application limits the number of active concurrent sessions.	Suositellaan korjattavaksi	Lievä	Palvelussa ei havaittu estoa saman käyttäjän samanaikaisille istunnoille. Käytössä on vahva tunnistus ja varsin lyhyet istuntojen eliniät, on todellinen riski vähäinen. Suositus, että käyttäjän kirjautumisen yhteydessä suljetaan saman käyttäjän vanhat istunnot.

Kuva 13. ASVS V3 korjaussuositukset.

8 JOHTOPÄÄTÖKSET

Tämän tutkimuksen tavoitteena oli tutkia case-yrityksen teknistä tietoturvallisuuden tasoa ja selventää kuinka tietojärjestelmän turvallisuusarviointi toteutetaan.

Case-yrityksen tietojärjestelmän tietoturvallisuusarvioinnilla oli tavoitteena ylläpitää ja edistää kohdeorganisaation tietoturvallisuutta sekä antaa luotettavaa arviota tietojärjestelmän ja tietoliikennejärjestelyiden tietoturvallisuuden tasosta.

Johtopäätöksenä kohdeorganisaation kokonaisvaltaisesta tietoturvasta voidaan todeta, että se on erittäin hyvällä tasolla. Tarkastusprosessi sujui tutkimussuunnitelman mukaisesti sekä käytettyjen menetelmien että aikataulun osalta. Tutkimuksessa löydetyt havainnot olivat vakavuudeltaan vähäisiä eli lähinnä informatiivisellä tasolla. Näin ollen havaitut löydökset eivät johtaneet välittömiin tietoturvallisuutta korjaaviin toimenpiteisiin. Kohdeorganisaatiolla on vuosien kokemus tietojärjestelmiensä tietoturva-auditoinneista. Tämä todennettiin, kun kävimme aikaisemman auditointiraportin tuloksia läpi ja vertasimme niitä uusimpiin haavoittuvuuslöydöksiin. Kohdeorganisaatio oli tehnyt tarvittavat korjaustoimenpiteet edellisen arviointiraportin suositusten mukaisesti. Sovellustestauksen tuloksena löytyi muutamia pienempiä korjausehdotuksia tietojärjestelmän omistajalle. Kohdeorganisaation tietojärjestelmiä tullaan testaamaan myös jatkossa kolmannen osapuolen eli Viestintäviraston tai sen hyväksymän arviointilaitoksen toimesta. Case-yrityksen tietojärjestelmän turvallisuusarviointi sujui lähestulkoon normaalin arviointiprosessin mukaisesti. Arviointiprosessin mukaista esipalaveria ei pidetty arvioinnin tilaajan kanssa, koska tarkastuksen kohteena oleva tietojärjestelmä oli arvioinnin suorittavalle taholle entuudestaan tuttu.

Suositeltavat jatkotoimenpiteet sekä arviointiraportti lähetettiin arvioinnin kohteena olevalle case-yritykselle. Case-yrityksen tietojärjestelmään tehtävät tulevat ohjelmistopäivitykset on edelleen jatkossa hyväksyttävä kolmannella osapuolella ennen uusien päivityksien asentamista, jotta tarkastuspäätös pysyy voimassa.

Ohjelmistopäivitysten hyväksynnässä muutokset, joilla ei ole toiminnallista vaikutusta järjestelmän toimintaan eivät edellytä kolmannen osapuolen hyväksyntää.

Tietokantakyselyihin tai ohjelmistoalustaan kohdistuvat muutokset edellyttävät kolmannen osapuolen hyväksynnän. Tällaiset muutokset on ilmoitettava kolmannelle osapuolelle kuukautta ennen niiden asentamista.

Viimeiseksi suurimmat muutokset, jotka kohdistuvat esimerkiksi alustamuutoksiin tai koostuvat yli 100:sta edellisen kohdan muutoksesta tulee ilmoittaa kolmannelle osapuolelle 3 kuukautta ennen niiden asentamista. Case-yrityksen tapauksessa, kun kyse on kansallisesta tietojärjestelmästä, lopullisen tietojärjestelmän käyttöönottopäätöksen tekee tiedon omistaja.

LÄHDELUETTELO

Engebretson P. (2011). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Elsevier Inc. United States of America.

Järvinen P. (2012) *Arjen tietoturva*. Jyväskylä. Docendo. Finland Oy. ISBN 978-951-0-38948-5

Järvinen P. (2002). *Tietoturva & Yksityisyys*. Docendo. Jyväskylä. ISBN: P951846152X

Stallings W. (2008). *Computer Security: Principles and Practice*. Pearson International Education. 798. ISBN-13: 978-0-13-513711-6

Stallings W. (2012). *Operating Systems: Internals and Design Principles*.7.Edition. ISBN-13: 978-0-13-230998-1

Tan,Hock & Moreau Luc. (2002) *Certificates for mobile code security. Proceedings of the 2002 ACM symposium on Applied computing*. 76–81. Saatavana: http://dl.acm.org.proxy.tritonia.fi/citation.cfm?id=508791.508807&coll=DL&dl=ACM&CFID=458126520&CFTOKEN=63452832

Android Security (2015). [online] [1.6.2016]. Saatavana: http://static.googleusercontent.com/media/source.android.com/en/security/reports/Google_Android_Security_2015_Report_Final.pdf

Arviointilaitokset. (2017). [online][7.4.201]. Saatavana: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvallisuudenarviointilaitokset/hyväksytytarviointilaitokset.html

Asetus tietoturvallisuudesta valtionhallinnossa (2010). *Valtioneuvoston asetustietoturvallisuudesta valtionhallinnossa 681/2010*. [online][3.10.2016]. Saatavana: http://www.finlex.fi/fi/laki/alkup/2010/20100681

Burp Suite (2016). *Burp Suite*. [22.4.2017]. Saatavana: releases.portswigger.net/2016/02/1638.html

Clarified network analyzer (2017). *Clarified network analyzer*. [24.4.2017]. Saatavana: https://www.clarifiednetworks.com/Clarified%20Analyzer

Codenomicon (2017). *Codenomicon Defensics* [24.4.2017]. Saatavana: http://www.codenomicon.com/files/pdf/Defensics-Brochure.pdf

Digitoday (2010). [9.5.2014]. Saatavana: http://www.digitoday.fi/viihde/2010/03/25/youtube-kaatui-tunniksi/20104371/66

EU (2012). *Eur-Lex*. [online][13.7.2016]. Saatavana: http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32013D0488

Finlex julkisuus (1999). [online][1.4.2016]. Saatavana: http://www.finlex.fi/laki/ajantasa/1999/19990621

Ficora TTN (2016). *Kyberturvallisuus, Tietoturva nyt!*. [online][16.7.2016]. Saatavana: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/07/ttn2016 07141223.html

F-secure (2014). *Ambulance virus*. Saatavana: http://www.f-secure.com/v-descs/ambulanc.shtml

Katakri (2015). *Tietoturvallisuuden auditointityökalu viranomaisille*. [online][3.10.2016]. Saatavana: http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointit yokalu_viranomaisille.pdf

Laki 1405/2011 (2011). *Laki tietoturvallisuuden arviointilaitoksista*. [online][3.10.2016]. Saatavana: http://www.finlex.fi/fi/laki/alkp/2011/20111405

Laki 1406/2011 (2011). *Laki viranomasten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista*. [online][3.10.2016]. Saatavana: http://www.finlex.fi/filaki/ajantasa/2011/20111406

NCSA (2017). *Viestintäviraston NCSA-toiminnon suorittamat tietoturvallisuustarkastukset*. [online][25.4.2017]. Saatavana: https://www.viestintävirasto.fi/attachments/Viestintaviraston_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf

NCSA todentamismenetelmät (2016). *Ohje_tietoturvallisuuden_arviointilaitoksille.* [online][3.10.2016]. Saatavana: https://www.viestintavirasto.fi/attachments/Ohje_tietoturvallisuuden_arviointilaitoksille.pdf

Nessus (2017). *Nessus*. [25.4.2017]. Saatavana: https://www.tenable.com/products/nessus-vulnerability-scanner

Nginx (2017). *Netcraft April 2017 Web Server surveys*. [3.5.2017]. Saatavana: https://news.netcraft.com/archives/2017/04/21/april-2017-web-server-survey.html

NIST (2017). *National institute of standards and technology*. [online][19.1.2017]. Saatavana: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Nmap (2017). *Nmap*. [24.4.2017] Saatavana: https://www.nmap.org

OWASP ZAP (2016). *OWASP ZAP 2.4.3*. [22.4.2017]. Saatavana: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

OWASP (2017). *OWASP*. [online][12.1.2017]. Saatavana: https://www.owasp.org/index.php/About_OWASP

OWASP Top 10 (2017). *OWASP Top 10*. [online][11.1.2017]. Saatavana: https://www.owasp.org/index.php/Top_10_2013-Top_10

OWASP ASVS (2017). *OWASP Application security verification standard 3.0*. [online][19.1.2017]. Saatavana: https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf

PostgreSQL (2017). [4.1.2017]. Saatavana: https://fi.wikipedia.org/wiki/PostgreSQL

Portswigger (2016). [9.4.2017]. Saatavana: https://portswigger.net/KnowledgeBase/issues/Details/005009a0_FrameableresponsepotentialClickjacking

Radamsa (2004). *Radamsa*. [24.4.2017]. Saatavissa: https://www.ee.oulu.fi/research/ouspg/Radamsa

Sanastokeskus (2004). *Tietoturvasanasto*. [10.5.2014]. Saatavissa: http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf

Saarinen J. (2014). *OWASP Top 10:n suositusten huomioiminen ohjelmistokehityksessä*. [online][9.4.2017]. Saatavissa: https://helda.helsinki.fi/bitstream/handle/10138/136109/gradu_Jussi_Saarinen_01192604pdf?sequence=2

SFS (2017). *ISO 27000 Tietoturvallisuuden hallinta*. [online][8.3.2017]. Saatavissa: http://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_iec_27000_tietoturvallisuuden_hallinta

Symantec (2014). [19.5.2014]. Saatavissa: http://securityresponse.symantec.com/fi/fi/norton/library/familyresource/article.jsp?aid=article1_08_06

Tcpdump (2017). *Tcpdump.* [24.4.2017]. Saatavissa: http://www.tcpdump.org/

Tekniikan Maailmalla. (2011). *Ensimmäinen PC virus täyttää 25 vuotta*. [Siteerattu 19.5.2014]. Saatavissa: http://tekniikanmaailma.fi/muu-tekniikka/muut/ensimmainen-pc-virus-tayttaa-25-vuotta

Tempest (2013). *Kansallinen TEMPEST-ohje*. [online][1.4.2016].
Saatavissa: https://www.viestintavirasto.fi/attachments/Kansallinen_TEMPEST-ohje.pdf

Tietoturvaopas a. (2008). *Tietoturvaopas*. [19.5.2014]. Saatavissa: http://www.tietoturvaopas.fi/uhatjaniidentorjunta/huijaukset.html

Tietoturvaopas b. (2008). [19.5.2014]. Saatavissa: http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haittaohjelmat.html

Tietosuojavaltuutettu (2014). *Pharming mitä se on*. Saatavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6Jfq9mcbP/Pharming_mita_se_on.pdf

Tietotekniikan termitalkoot (2003). [19.5.2014]. Saatavissa: http://www.tsk.fi/tsk/termitalkoot/en/node/267?page=get_id&id=ID0214&vocabulary_code=TSKTT

Turvallisuusselvityslaki (2014). [online][1.4.2016]. Saatavissa: http://finlex.fi/fi/laki/ajantasa/2014/20140726

TUVE 10/2015 (2015). *Laki julkisen hallinnon turvallisuusverkkotoiminnasta*. [online][1.4.2016]. Saatavissa: http://www.finlex.fi/fi/alkup/2015/20150010#Pidp3565696

VAHTI 2/2014 (2014). *Tietoturvallisuudenarviointi ohje*. [online][3.10.2016]. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ce1ccede-8669-4166-b084-9cafbe6e1e60&groupId=10229

VAHTI (2016). *Tietoaineistojen luokittelu*. [online][20.10.2016]. Saatavissa: https://www.vahtiohje.fi/web/guest/tietoaineistojen-luokittelu

Valtionhallinnon tietoturvasanasto. (2008). *Valtionhallinnon tietoturvasanasto*. [Siteerattu 19.5.2014]. Saatavissa: https://www.vahtiohje.fi/web/guest/maaritelmat-e

Valtionvarainministeriö. [9.5.2014]. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20090217Valtio/03_Taustamuistio_VNpp_1722009-v07.pdf

Vatanen Mikko (2014). *Intrusion Detection During IT Security Audits* [online]. [9.5.2016]. Saatavissa: https://theseus32-kk.lib.helsinki.fi/bitstream/handle/10024/81542/Vatanen_Mikko.pdf?sequence=1

Viestintävirasto (2014a). *Tietomurto eBay-verkkohuutokauppa*. [22.5.2014]. Saatavissa: https://www.cert.fi/tietoturvanyt/2014/05/ttn201405221021.html

Viestintävirasto (2016). *Toimialakatsaus 1/2016*. [3.10.2016]. Saatavissa: https://www.viestintavirasto.fi/attachments/toimialatieto/Toimialakatsaus_1_2016_FI.pdf

W3af (2017). *W3af versio*.[25.4.2017]. Saatavissa: http://w3af.org/

Wikipedia (2014). *Computer worm*. [online][14.5.2014]. Saatavissa: http://en.wikipedia.org/wiki/Computer_worm

Wikipedia (2014). *Computer virus*. [online][18.5.2014]. Saatavissa: http://en.wikipedia.org/wiki/Computer_virus

Wikipedia (2017b). *Java*. [online][4.1.2017]. Saatavissa: http://en.wikipedia.org/wiki/Java

Wikipedia (2017c). *Ansible*. [online][3.1.2017]. Saatavissa: https://en.wikipedia.org/wiki/Ansible_(software)

Wikipedia (2017). *Nginx*. [online][4.1.2017]. Saatavissa: https://fi.wikipedia.org/wiki/Nginx

Wikipedia (2014). *Trojan horse*. [online][13.5.2014]. Saatavissa: http://en.wikipedia.org/wiki/Trojan_horse_(computing)

Wikipedia (2014). *Timeline of computer viruses and worms*. [online][9.5.2014]. Saatavissa: http://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms

Wireshark (2017). *Wireshark.* [online][24.4.2017]. Saatavissa: https://www.wireshark.org

X-Road (2016). *Suomi.fi-palveluväylä-X-Road-tiedonsiirtoprotokolla*. [online] [4.1.2017] Saatavissa: https:// confluence.csc.fi/pages/viewpage.action?pageId=50873043

LIITTEET

Liite 1. OWASP Top 10. (2017)

OWASP Top 10 - kymmenen yleisintä web-sovellusten haavoittuvuutta vuonna 2013:

1. Injection -
   Taustajärjestelmäkyselyn rakenne ei säily.
2. Broken Authentication & Session Management -
   Puutteellinen tunnistusmenettely ja istunnonhallinta
3. Cross Site Scripting (XSS) -
   Verkkosivun rakenne ei säily
4. Insecure Direct Object Reference -
   Turvaton suora viittaus tietoalkioon
5. Security Misconfiguration -
   Puutteelliset tietoturva-asetukset
6. Sensitive Data Exposure -
   Arkaluontoisen tiedon paljastuminen
7. Missing Function Level Access Control -
   Puuttuva funktiotason pääsyvalvonta
8. Cross Site Request Forgery (CSRF) -
   Puutteellinen pyynnön alkuperän tarkastus
9. Using Known Vulnerable Components -
   Tunnettujen haavoittuvien osien käyttäminen
10. Unvalidated Redirects and Forwards -
    Varmistamattomat uudelleenohjaamiset

Liite 2. OWASP ASVS. (2017)

ASVS V3:n Todentamisvaatimuksen luvut:

V1: Arkkitehtuuri, suunnittelu ja uhkamallinnus
V2: Autentikoinnin todentamisvaatimukset
V3: Session hallinnan todentamisvaatimukset
V4: Pääsynhallinnan todentamisvaatimukset
V5: Haitallisen syötteen todentamisvaatimukset
V6: Output encoding / escaping
V7: Kryptografian todentamisvaatimukset
V8: Virheenkäsittely ja lokituksen todentamisvaatimukset
V9: Tietosuojan todentamisvaatimukset
V10: Tietoliikenneturvallisuus todentamisvaatimuksista
V11: HTTP suojauskokoonpanolla todentamisvaatimuksista
V12: Suojausasetusten todentamisvaatimukset
V13: Haittaohjelman tarkastuksen todentamisvaatimukset
V14: Sisäinen turvallisuuden todentamisvaatimuksista
V15: Business logiikan todentamisvaatimukset
V16: Tiedostojen ja resurssien todentamisvaatimukset
V17: Mobiili todentamisvaatimukset
V18: Web-palveluiden todentamisvaatimukset
V19. konfiguraatiot