jamk.fi

TIETOTURVATAPAHTUMIEN HALLINTA

Operaattoritoiminta JYVSECTEC-projektissa

Miika Viinikainen

Opinnäytetyö
Toukokuu 2014

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

KUVAILULEHTI

Tekijä(t) Viinikainen, Miika	Julkaisun laji Opinnäytetyö	Päivämäärä 12.5.2014
	Sivumäärä 128	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty (X)

Työn nimi
TIETOTURVATAPAHTUMIEN HALLINTA, Operaattoritoiminta JYVSECTEC-projektissa

Koulutusohjelma
Tietotekniikan koulutusohjelma

Työn ohjaaja(t)
Hautamäki, Jari; Piispanen, Juha

Toimeksiantaja(t)
Jyväskylä Security Technology
Vatanen, Marko

Tiivistelmä

Opinnäytetyö toteutettiin Jyväskylän ammattikorkeakoulun JYVSECTEC -hankkeeseen. JYVSECTEC-hanke on kyberturvallisuusteknologian kehittämisprojekti. Projekti käynnistettiin syyskuussa 2011 ja se jatkuu kesään 2014 saakka.

Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa tietoturvatapahtumien hallintaprosessi, tiketöintijärjestelmä ja dokumentaatio JYVSECTEC -hankkeeseen operaattoritoimintaa varten. Projektilla ei ollut käytössään aiempaa tietoturvatapahtumien hallintaprossia tai tiketöintijärjestelmää.

Työn teoriaosuus keskittyy tietoturvatapahtumien hallinnan parhaisiin käytäntöihin ja standardeihin. Operaattoritoiminnan tietoturvatapahtumien hallinnan erityspiirteitä käsiteltiin lainsäädännön näkökulmasta.

Työn tuloksena JYVSECTEC-hankkeelle toteutettiin tietoturvatapahtumien hallintaprosessi ja tiketöintijärjestelmä. Prosessista laadittiin yksityiskohtainen kuvaus ja tiketöintijärjestelmän käytöstä ohjeet. Tietoturvatapahtumien hallintaprosessista ja tiketöintijärjestelmästä laadittiin koulutussuunnitelma. Työssä esitettiin kehittämisideoita ja prosessimittareita. Tietoturvan kehittäminen hankkeessa jatkuu tämän opinnäytetyön pohjalta.

Avainsanat (asiasanat)
Tietoturva, JYVSECTEC, Tietoturvatapahtumien hallinta, Tietoturvaheräte, Tietoturvatapahtuma, SFS ISO/IEC 27035

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s)	Type of publication	Date
Viinikainen, Miika	Bachelor´s Thesis	12052014
	Pages 128	Language Finnish
		Permission for web publication (X)

Title
INFORMATION SECURITY INCIDENT MANAGEMENT; Telecom operations in JYVSECTEC-project

Degree Programme
Information Technology

Tutor(s)
Hautamäki, Jari; Piispanen, Juha

Assigned by
Jyväskylä Security Technology
Vatanen, Marko

Abstract

The thesis was assigned by and implemented for JYVSECTEC -project at JAMK University of Applied Sciences. The JYVSECTEC -project is a development project of cyber security. The project was started in September 2011 and it continues till summer 2014.

The objective of the thesis was to create information security incident management process, a ticketing system and documentation for telecom operation in JYVSECTEC -project. The project did not have an existing security incident management process or a ticketing system.

The theory part of the thesis concentrates on the best practices and standards of security incident management. The characteristics of incident management concerning telecom operation security were processed from legislative perspective.

As a result of the thesis, the process of information security incident management and a ticketing system were implemented in JYVSECTEC -project. Detailed description of process and instructions for the use of ticketing system were created. The training plan of information security incident management process and ticketing system were implemented. Development ideas and process metrics were introduced in the thesis. The project on information security development continues based on the thesis.

Keywords
Information security, JYVSECTEC, Information security incident management, Information security event, Information security incident, SFS ISO/IEC 27035

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

1 LÄHTÖKOHDAT

1.1 Taustatiedot

Opinnäytetyön tilaaja oli JYVSECTEC-hanke (Jyväskylä Security Technology). Hanke on kyberturvallisuusteknologian kehittämisprojekti, joka käynnistettiin syyskuussa 2011, ja se jatkuu kesään 2014 saakka. Koordinoinnista ja toteutuksesta vastaa Jyväskylän ammattikorkeakoulu. Hanke kehittää ja ylläpitää kyberturvallisuuden kehitysympäristöä (RGCE, Realistic Global Cyber Enviroment). Ympäristö on eristetty julkisista verkoista. Ympäristössä on käytössä julkisia verkkoja vastaavat rakenteet ja palvelut. JYVSECTEC-hanke tarjoaa kyberharjoitus, tilannekuva-, kehitys-, testaus- ja koulutuspalveluita yhteistyöverkoston käyttöön. Tavoitteena on tarjota yrityksille mahdollisuus verkostoitua kansainvälisten toimijoiden ja yritysten kanssa ja lisätä tietoisuutta Keski-Suomen tarjoamista kehitysmahdollisuuksista koulutukseen, tutkimukseen ja tuotekehitykseen kybertoimialalla. (JYVSECTEC – Jyväskylä Security Technology 2013.)

1.2 Ajankohtaisuus

Tietoturvatapahtumien hallinnan merkitys organisaatioissa kasvaa jatkuvasti. Voimme kuulla toistuvasti uutisia tietoturvahyökkäyksistä, salasanojen paljastumisista ja erilaisista tietoturvamurroista organisaatioiden tietojärjestelmiin.

CERT-FI on Suomen viestintävirastossa toimiva kansainvälinen tietoturvaviranomainen. CERT-FI:n tehtävänä on tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaisu, sekä tietoturvauhkista tiedottaminen (CERT-FI 2013). CERT-FI mainitsee

tietoturvaraportissaan heidän käsitelleen vuonna 2012 271 tietomurtotapausta, mikä oli 74 % enemmän kuin edellisenä vuonna 2011. Suurin osa yhteydenotoista CERT-FI:lle koski haittaohjelmia. Tämä trendi on ollut CERT-FI:n mukaan selkeä vuodesta 2006 alkaen. Erilaisten tietoturvaloukkausten motiiveiksi CERT-FI mainitsee huomiohakuisuuden ja organisaatioiden arkaluontoisten tietojen varastamisen. (Vuosikatsaus 2012 2013.)

CERT-FI:n tietoturvakatsauksessa 3/2013 mainitaan pitkäkestoisena ilmiönä selainten, selainlisäosien ja julkaisujärjestelmien haavoittuvuuksien käyttö. Saastuneet työasemat ja murretut www-palvelimet toimivat kyberrikollisuuden polttoaineena. Työasemilla ja palvelimilla säilytettävät tiedot ovat rahanarvoisia joko itsessään tai uusien hyökkäysten mahdollistajina. (Pitkäkestoiset ilmiöt 2013)

Viime aikoina Suomessa on esiintynyt palvelinhyökkäysaalto, joista julkisuudessa esillä olivat MTV:n katsomopalveluun ja viestintäviraston CERT-sivustoon kohdistetut hyökkäykset. Hyökkäyksillä estettiin palvelujen käyttäminen. CERT-FI:n mukaan sähköisten tiedotusvälineiden ja viranomaisten palvelut ovat suosittuja hyökkäyskohteita. Tiedotusvälineiden verkkosivuihin kohdistuu palvelunestohyökkäyksiä jatkuvasti. Hyökkäysten motiivit jäävät usein tuntemattomiksi. Palvelunestohyökkäyksissä on käytetty välineenä bottiverkkoja ja yhteyksien testaamiseen käytettävän chargen-palvelun ominaisuutta, jossa merkityksetöntä dataa sisältävillä vastauspaketeilla saadaan verkkoon muodostettua suuria määriä liikennettä ilman, että hyökkääjä paljastuu. Viestintävirasto suosittaa tietoliikenneoperaattoreita suodattamaan liikennettä, jos siitä ei aiheudu haittaa käyttäjille. Viestintäviraston mukaan osa teleoperaattoreista ja yrityksiä on ottanut suodatuksen käyttöön. Viestintäviraston määräys internet-palvelujen tietoturvasta (M13) määrää operaattoreita suodattamaan vieraista lähdeosoitteista syntyvää liikennettä omissa verkoissaan. Operaattoreiden on myös

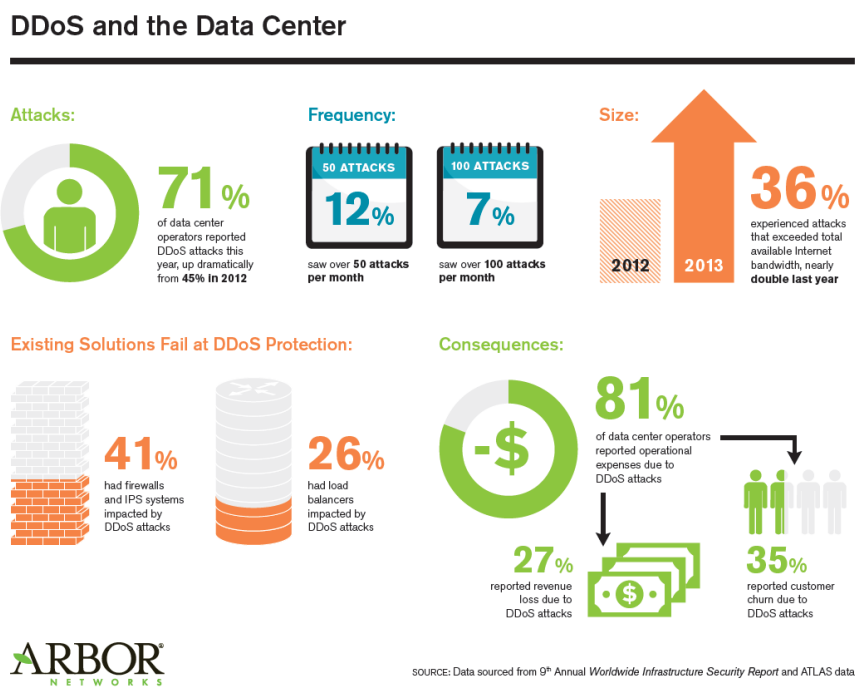
selvitettävä mistä haitallista liikennettä heidän verkkoihinsa muodostuu. (Uudet ilmiöt 2013.)

CERT-FI mainitsee tietoturvakatsauksessaan myös tietomurtojen sarjan, jossa käyttäjien tunnuksia ja salasanoja varastettiin. Selvitysten perusteella satojen tuhansien käyttäjätietoja oli hankittu yli sadan sivuston kautta. Sivustojen kautta murrettuja käyttäjätunnuksia ja salasanoja oli käytetty myös muissa palveluissa. (Uudet ilmiöt 2013.)

Tietoturva nyt! -seminaarissa 2013 verkko-operaattori TDC:n teknologiajohtaja Jorma Mellin (2013) puhui esityksessään teleyrityksen mahdollisuuksista rajoittaa verkkohyökkäyksiä. Hän mainitsee esityksessään tietoturvahyökkäysten motiiveiksi huomion saamisen omalle asialleen, huomion viemisen toisaalle oleellisen asian sijaan ja rahan. Mellinin mukaan tietoturvahyökkäyksien tekijöitä ovat tietoteknisesti orientoituneet aktivistit eli haktivistit, rikolliset ja erilaiset militaristiset tahot, kuten tiedusteluorganisaatiot. Tietoturvahyökkäysten kohteiksi Mellin listaa median, poliittiset kampanjat, finanssisektorin ja erilaiset pelisivustot. (Mellin 2013.)

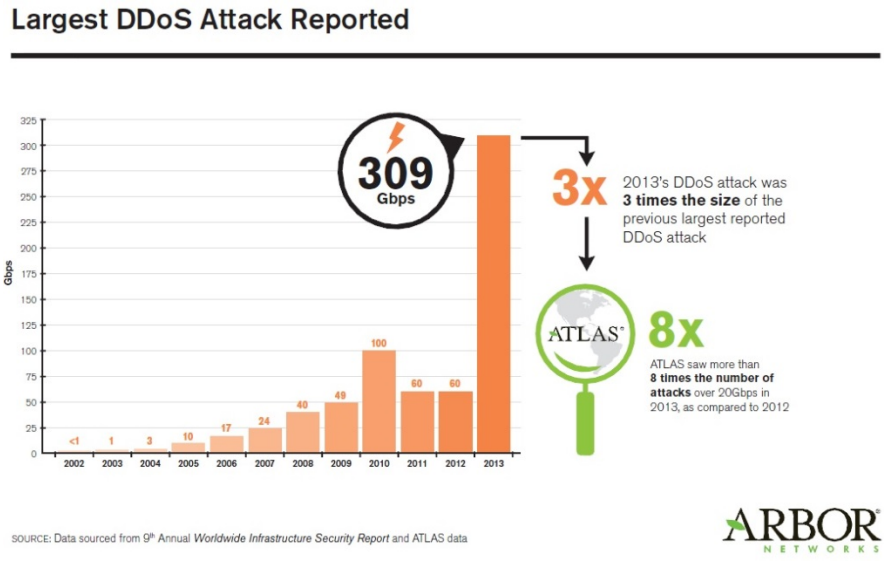
Mellin kertoi liikenteen rajoittamisen olevan ongelmallista, koska liikenne voi tulla sadoista yhdysliikennepisteistä ja oikeiden lähteiden ja kohteiden liikenteen rajoittaminen on haasteellista. Haasteita liittyy myös tapahtumien todentamiseen, toimenpiteiden kestoon ja niiden seurantaan. Tyypillisimmiksi liikenteen rajoittamisen keinoiksi Mellin mainitsi palomuurit, tunkeutumisen havaitsemis – ja estojärjestelmät sekä palvelun hajauttamisen eri verkkoihin ja useille operaattoreille. Rajoittamisen keinoina on myös liikenteen suodatus, liikenteen ohjaus vaihtoehtoisille reiteille tai pakettipesureille ja liikenteen sormenjäljen jakaminen muille teleyrityksille liikenteen estämiseksi. (Mellin, 2013.)

Arbor Networks on vuonna 2000 perustettu yritys. Yritys on keskittynyt tietoverkoissa tapahtuvien uhkien tutkimiseen, havaitsemiseen ja vähentämiseen. Maailmanlaajuisesti 70 % tietoliikenneoperaattoreista käyttää Arbor Networksin tuotteita. (About us 2014a.) Vuosittaisessa tietoturvaraportissaan Arbor Networks esittelee tietoliikenneoperaattoreiden verkon turvallisuuteen liittyviä haasteita. Tutkimus perustuu kyselyyn, joka tehdään yritys-, pilvi- ja hosting-palveluita tarjoaville yrityksille sekä tietotoliikenneoperaattoreille. Vuoden 2013 raporttiin saatiin 220 vastausta, joista 68 % edusti palveluntarjoajia. Tärkeimpinä tuloksina Arbor Networks esittelee 36 % prosentin kasvun yrityksiin kohdistuvissa APT-hyökkäyksissä (Advanced Persistent Threat), matkapuhelinverkkoihin kohdistuvien hyökkäyksien kaksinkertaistumisen, sovelluskerroksella tapahtuvien hyökkäysten lisääntymisen ja laajojen palvelunestohyökkäysten dramaattisen kasvun verrattuna edelliseen vuoteen. Myös data- ja palvelinkeskukset ovat usein hyökkäysten kohteina ja DNS-palvelut ovat haavoittuvaisia hyökkäyksille. Palvelinkeskuksiin kohdistuvista palvelunestohyökkäyksistä vuonna 2013 on nähtävissä tilastotietoa kuviossa 1. Kuviossa 2 on nähtävissä tilastotietoa suurimmista palvelunestohyökkäyksistä ja niissä käytetystä verkkokapasiteetista vuosittain. (Worldwide Infrastructure Security Report 2013.)



Kuvio 1. DDoS and the Data Center

(Attacks Agains Data Centers 2013)



Kuvio 2. Largest DDOS Attack Reported

(Largest DDOS Attack Reported. 2013)

1.3 Tavoitteet

Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa tietoturvatapahtumien hallintaprosessi JYCSECTEC-hankkeen operaattoritoimintaa varten. Hallintaprosessin suunnittelussa ja toteutuksessa käytettiin tietoliikennealan parhaiden käytäntöjen malleja ja standardeja. Työn tavoitteena oli myös toteuttaa tietoturvatapahtumien hallintaprosessia tukeva tiketöintijärjestelmä ja ohjeet JYVSECTEC-hankkeen käyttöön. JYVSECTEC-hankkeella ei ole käytössään aiempaa tietoturvatapahtumien hallintaprosessia tai tiketöintijärjestelmää.

Työssä tarkastellaan, kuinka CSIRT (Computer Security Incident Response Team) tulisi perustaa. CSIRTin roolit ja palvelut määritetään alan parhaiden käytäntöjen mukaisesti. Työssä määritetään tietoturvallisuustapahtumien hallintaprosessiin osallistuvat tahot. On tärkeää tunnistaa, mistä rajapinnoista ja sidosryhmistä mahdollisia herätteitä prosessille syntyy ja kuka vastaa herätteiden käsittelystä.

Työssä laaditun koulutussuunnitelman avulla tietoturvatapahtumien hallintaprosessi ja tiketöintijärjestelmän toiminta voidaan esitellä organisaation jäsenille. Tietoturvallisuustapahtumien hallintaprosessille esitellään mittareita ja kuinka hallintaprosessia voidaan kehittää. Työssä esitellään havaitut ongelmat ja esitetään ehdotuksia ongelmien korjaamiseksi.

Työssä selvitetään viranomaisten asettamat vaatimukset ja lait, jotka ohjaavat operaattoreiden tietoturvallisuustapahtumien hallintaa. Työssä keskitytään erityisesti teleyritysten oikeuksiin ja velvollisuuksiin.

1.4 Tuotokset

Työn tärkein tuotos oli tietoturvatapahtumien hallintaprosessi, josta laadittiin sanallinen kuvaus ja prosessikaavio. Tietoturvatapahtumien hallintaprosessia tukeva tiketöintijärjestelmä asennettiin virtuaalipalvelimelle, otettiin käyttöön ja luovutettiin JYVSECTEC -organisaatiolle. Toteutuksen yhteydessä laadittiin ohje OTRS-tiketöintijärjestelmän käytöstä tietoturvatapahtumien hallintaprosessin eri vaiheissa. Työssä laadittiin ohje JYVSECTEC-organisaatiolle siitä, millaisia henkilörooleja ISIRTissä on ja millaisia palveluita se tarjoaa. Taulukossa 1 on nähtävissä työn tuotokset.

Taulukko 1. Tuotokset

Tuotos	**Hyväksyntäkriteeri**	**Hyväksyjä**
Tietoturvallisuustapahtumien hallintaprosessi	Organisaation johdon tai tilaajan hyväksyntä	Marko Vatanen
OTRS-tiketöintijärjestelmä ja virtuaalipalvelin	Organisaation johdon tai tilaajan hyväksyntä	Marko Vatanen
Ohje tiketöintijärjestelmän käytöstä tietoturvatapahtumien hallintaprosessin aikana	Organisaation johdon tai tilaajan hyväksyntä	Marko Vatanen
Ohje CSIRTin rooleista ja palveluista	Organisaation johdon tai tilaajan hyväksyntä	Marko Vatanen

1.5 Rajaukset

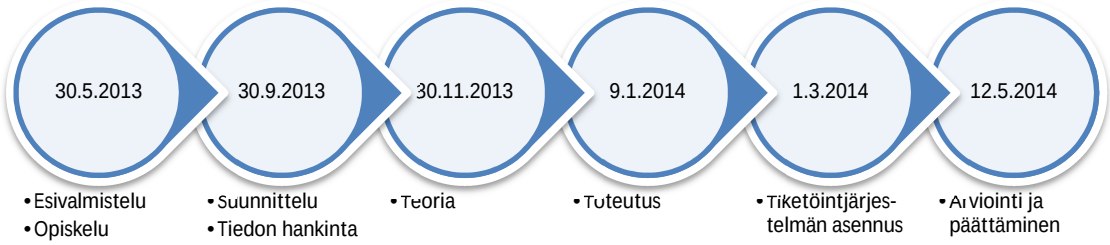
Tietoturva on aiheena erittäin laaja. Työn ulkopuolelle rajattiin tietoturvallisuustapahtumien käytännön tunnistaminen. Aihe olisi erittäin mielenkiintoinen ja haastava, mutta laajuutensa vuoksi sitä oli mahdotonta käsitellä opinnäytetyön yhteydessä. Työssä käydään läpi tietoturvatapahtumien tunnistamista esimerkkien avulla ja esitellään yleisempiä tietoturvatapahtumatyyppejä. Tietoturvatapahtumien hallintaprosessissa keskityttiin siihen, kuinka organisaatio toimii havaittuaan tietoturvaherätteen, -tapahtuman tai haavoittuvuuden.

Yleinen organisaation tietoturvallisuuden suunnittelu, toteuttaminen ja hallinta rajattiin opinnäytetyön aihepiirin ulkopuolelle. Mikko Nisonen (2013) on omassa opinnäytetyössään Tietoturvallisuuden hallintajärjestelmä JYVSECTEC-hankkeeseen käsittelyt yleistä tietoturvaa, tietoturvan suunnittelua, toteutusta ja hallintaa varsin laajasti ja kattavasti SFS ISO/IEC 17799-, SFS ISO/IEC 27001- ja SFS ISO/IEC 27005-standardien pohjalta. Nisosen läpi käymiä aiheita käsitellään opinnäytetyössä yleisellä tasolla ja siltä osin kuin se on aiheen kannalta välttämätöntä.

Tietoturvatapahtuman hallinnan kannalta on oleellista määrittää hallintaprosessiin osallistuvat tahot. Työssä tutkittiin, kuinka CSIRT perustetaan, millaisia rooleja tiimissä on ja mitä palveluita ryhmä tarjoaa. CSIRTin käytännön perustaminen rajattiin työn ulkopuolelle.

1.6 Aikataulu

Työn tarve tuli esiin tilaajan toimesta toukokuun 2013 lopussa. Opiskelu ja työn esivalmistelu tapahtui kesän 2013 aikana. Työn suunnittelu ja tiedon hankinta käynnistyi lokakuun 2013 alussa ja kesti marraskuun 2013 loppuun. Teoriaosuuden kirjoitustyö alkoi joulukuun 2013 aikana. Tietoturvatapahtumien hallintaprosessin toteutus aloitettiin tammikuun 2014 aikana. Tiketöintijärjestelmän asennus ja testaus aloitettiin maaliskuun 2014 alussa. Valmiit tuotokset esiteltiin työn tilaajalle toukokuun 2014 puolivälissä. Kuviossa 3 on esitetty opinnäytetyön aikataulu.



Kuvio 3. Opinnäytetyön aikataulu

1.7 Tietoperusta

Tietoturvallisuustapahtumien hallintaan liittyvää lähdemateriaalia on runsaasti saatavilla. Alalla toimii useita kaupallisia toimijoita, jotka julkaisevat maksullisia standardeja ja parhaiden käytäntöjen malleja. Myös useat kansalliset ja kansainväliset tietoturvaorganisaatiot julkaisevat suosituksia ja parhaiden käytäntöjen malleja.

Työssä tutustuttiin laajasti eri organisaatioiden tarjoamiin malleihin ja valikoitiin työn kannalta sopivimmat. Opinnäytetyön tärkeimmät lähteet olivat:

- SFS ISO/IEC 27000 (2010)
- SFS ISO/IEC 17999 (2006) / SFS ISO/IEC 27002 (2013)
- SFS ISO/IEC 27035 (2011)
- Good Practice Guide for Incident Management (2010)

International Organization for Standardization (ISO) on kansainvälisten standardien kehittäjä. ISO on perustettu 1947. Tähän päivään mennessä ISO on julkaissut 19500 standardia. ISO muodostuu kansallisten standardointijärjestöjen verkostosta. ISO standardien avulla varmistetaan, että tuotteet ja palvelut ovat turvallisia, luotettavia ja laadukkaita. Liiketoiminnalle standardit tarjoavat strategisen työkalun virheiden ja turhien työvaiheiden poistamiseen tuotannon tehostamiseksi. Standardien mukainen toiminta helpottaa myös yrityksen markkinointia. (ISO International Organization for Standardization 2014).

International Electrotechnical Comission (IEC International Electrotechnical Commission 2014.) on sähkö- ja elektroniikka-alojen ja edellä mainittuihin aloihin liittyvien teknologioiden standardoimisjärjestö. IEC on perustettu 1906. IEC tekee yhteistyötä muiden standardointijärjestöjen kanssa tarvittaessa. (IEC 2014). ISO ja IEC ovat muodostaneet ISO/IEC JTC1 yhteistyökomitean IT (Information technology) ja ICT (Information and Communication Technology) -alojen standardien kehitykseen (JTC1 mission and principles 2014).

SFS ISO IEC 27000-standardi (2010) esittää yleiskatsauksen tietoturvallisuuden hallintajärjestelmästä ja määrittelee aiheeseen liittyvät termit. SFS ISO/IEC 17999:fi-standardi (2006) sisältää suuntaviivat ja yleisperiaatteet tietoturvallisuuden hallin-

taan. Standardin uudempi versio on SFS ISO/IEC 27002 (2013). Standardissa kuvataan, miten turvallisuuden parantamiseen tähtäävät toimet käynnistetään ja toteutetaan ja kuinka turvallisuushallintoa ylläpidetään ja kehitetään. (Hakala, Vainio & Vuorinen 2006, 47). Standardissa on 11 pääturvallisuuskategoriaa, jossa käydään läpi kategorioihin liittyviä valvontatavoitteita, turvamekanismeja ja toteuttamisohjeita (SFS ISO/IEC 17799:fi 2006, 24).

SFS ISO/IEC 27035-standardi (2011) kattaa tietoturvaherätteiden, -tapahtumien ja -haavoit-tuvuuksien hallinnan. Standardin rakenne on jaettu viiteen osaan. Osat ovat suunnittelu ja valmistautuminen, tunnistaminen ja raportointi, arviointi ja päätöksenteko, vastatoimet sekä opetukset. (SFS ISO/IEC 27035 2011, III.)

ISO/IEC-standardit sopivat hyvin opinnäytetyön päälähteiksi, koska ne käsittelevät erittäin laajasti tietoturvan hallintaa. ISO/IEC-standardit ovat myös luotettavia ja niillä on hyvä maine. Standardit ovat hyvä ja kattava läpileikkaus aiheesta julkaistuun materiaaliin ja aikaisempiin standardeihin.

European Network and Information Security Agency (ENISA) on perustettu maaliskuussa 2004. ENISAn tarkoituksena on varmistaa korkeatasoinen ja tehokas verkko- ja tietoturvallisuuden taso ja kehittää verkko- ja tietoturvallisuuskulttuuria kansalaisia, kuluttajia, yrityksiä ja julkisen sektorin organisaatiota varten Euroopan unionissa. (Incident Management Guide 2010, 8.)

ENISAn julkaisema Good Practise Guide for Incident Management on opas tietoturvatapahtumien hallinnan hyvistä käytännöistä. Opas tukee CSIRTin toimintaa. Oppaassa kuvataan hyviä käytäntöjä, käytännön tietoja ja ohjeita verkko- ja tietoturvatapahtumien hallintaan painottaen tietoturvatapahtumien käsittelyä. (Incident Management Guide 2010, 8-9.)

1.8 Työskentelytavat

Tämä opinnäytetyö on kehitystyö ja luonteeltaan projektinomainen. Työssä määritettiin työn tarve ja tavoitteet, selvitettiin tietoperusta, kartoitettiin nykytilanne, kuvattiin työvaiheet ja toteutus haluttuun lopputulokseen pääsemiseksi, sekä esitettiin lopputulokset työn tilaajalle. Työvaiheiden eteneminen raportoitiin työn tilaajalle työn tekemisen aikana.

Lähdemateriaalin rajaaminen tilanteeseen sopivaksi arvioitiin työn haastavimmaksi osuudeksi. Standardit ja parhaiden käytäntöjen mallit ovat varsin laajoja kokonaisuuksia. Standardeissa ja parhaiden käytäntöjen malleissa on runsaasti päällekkäisyyksiä ja termien käyttö ei ole yhtenäistä. Tämä otettiin huomioon työn aikataulun suunnittelussa.

1.9 Viestintä ja raportointi

Viestintä ja raportointi ovat tärkeä osa työn onnistumista. Työn etenemisestä raportoitiin JYVSECTEC-organisaation kanssa pidetyissä yhteistyöpalavereissa. Raportointi tapahtui suullisesti ja kirjallisina dokumentteina. Ohjaavana tahona työlle toimi palavereissa työn tilaaja.

31.5.2013 aloituspalaverin aiheena oli työn tarpeen esittely ja aiheen rajaus. Palaverissa tutustuttiin työhön osallistuviin JYVSECTEC-organisaation jäseniin. Aiherajauksen perusteella tuli laatia suunnitelma opinnäytetyön toteuttamiseksi.

31.11.2013 pidettiin palaveri opinnäytetyösuunnitelman hyväksymiseksi. Suunnitelman osalta käytiin läpi työhön sisältyvät pääkohdat ja niiden sisältö. Suunnitelma

hyväksyttiin tilaajan toimesta. Suunnitelman pohjalta voitiin aloittaa teoriataustan ja käytännön toteutuksen laadinta.

9.1.2014 palaverissa esiteltiin teoriatausta ja käytiin läpi alustava toteutus. Teoriatausta hyväksyttiin pääpiirteittäin ja saadun palautteen avulla voitiin aloittaa käytännön toteutus. Käytännön toteutuksen osalta selvitettiin lähtötilanne.

17.3.2014 palaverissa tarkasteltiin työn etenemisessä ja käytännön toteutuksessa ilmenneitä haasteita. Saadun palautteen perusteella pystyttiin rajaamaan käytännön toteutus lopulliseen muotoonsa.

8.4.2014 palaverissa esiteltiin tietoturvatapahtumien hallintaprosessi JYVSECTEC -organisaatioille ja esiteltiin tiketöintijärjestelmän ominaisuuksia. Tietoturvatapahtumien hallintaprosessi ja tiketöintijärjestelmä hyväksyttiin muutamia muutosehdotuksia lukuun ottamatta. Muutosehdotukset kirjattiin ylös ja muutokset sovittiin sisällytettävän valmiiseen työhön.

2 TIETOTURVA

2.1 Määritelmä ja tavoite

Tietoturvallisuus muodostuu kolmesta pääasiasta. Ne ovat luottamuksellisuus (confidentiality), saatavuus (availability) ja eheys (integrity). (SFS ISO/IEC27000 2010, 22.) Tietoturvallisuuteen voi sisältyä myös muita ominaisuuksia, kuten aitous, vastuullisuus, kiistämättömyys ja luotettavuus (SFS ISO/IEC 17999:fi 2006, 20).

Luottamuksellisuudella (confidentiality) tarkoitetaan, että tietoa ei anneta saataville tai paljasteta luvattomille henkilöille, tahoille tai prosesseille. Saatavuudella (availability) tarkoitetaan, että kohde on saatavilla ja käyttökelpoinen valtuutetun tahon niin vaatiessa. Eheydellä (integrity) tarkoitetaan suojattavan kohteen virheettömyyttä ja täydellisyyttä. (SFS ISO/IEC 27000 2010, 12-15.)

Suojattavalla kohteella (asset) tarkoitetaan mitä tahansa, jolla on arvoa organisaatiolle. Suojattavia kohteita voivat olla esimerkiksi informaatio, ohjelmistot, fyysiset kohteet, palvelut, ihmiset, ihmisten pätevyys, taidot ja kokemukset sekä muut aineettomat kohteet. (SFS ISO/IEC 27000 2010, 10.)

Tietoturvallisuuden tavoitteena on liiketoiminnan kestävä menestys, jatkuvuus ja haittavaikutusten minimointi (SFS ISO/IEC 27000 2010, 22). Riskien minimoimisella mahdollistetaan investointien ja liiketoiminnan synnyttämien tuottomahdollisuuksien maksimointi (SFS ISO/IEC 17999:fi 2006, 14).

Tietoturvallisuus voidaan saavuttaa toteuttamalla soveltuvia turvamekanismeja, jotka on valittu riskien hallintaprosessin avulla ja joita hallitaan tietoturvallisuuden hallintajärjestelmällä. Turvamekanismilla (control) tarkoitetaan riskin hallitsemiseen käytettäviä keinoja, jotka voivat olla toimintaperiaatteita, menettelyjä, ohjeita, käytäntöjä tai organisaatiorakenteita. Organisaatiorakenteet voivat olla hallinnollisia, teknisiä, juridisia tai johtamiseen liittyviä. (SFS ISO/IEC 27000 2010, 12, 22.)

Tietoturvasta puhuttaessa kuulee usein lauseen: ”Tietoturva ei ole projekti vaan prosessi”. Tietoturva ei ole koskaan valmis vaan tietoturvatyö on jatkuvaa. Seuraavaksi avataan keskeisiä tietoturvallisuuden hallintaan liittyviä käsitteitä. Johdon sitoutuminen, organisaation tietoturvallisuutta ohjaavat politiikat, tietoturvallisuuden hallinta-

järjestelmä, suojattavat kohteet, turvallisuusvaatimukset ja riskien hallinta liittyvät olennaisesti opinnäytetyön pääaiheeseen tietoturvatapahtumien hallintaan.

2.2 Tietoturvapolitiikat

Tietoturvapolitiikan tavoitteena on tarjota johdon ohjaus ja tuki tietoturvallisuudelle liiketoimintatavoitteiden ja asiaan kuuluvien lakien ja asetusten mukaisesti. Tietoturvallisuudelle on luotava joukko johdon asettamia ja hyväksymiä tietoturvapolitiikoita. Tietoturvapolitiikat julkaistaan henkilökunnan ja asiaankuuluvien organisaation ulkopuolisten tahojen käyttöön. Tietoturvapolitiikoita tulee katselmoida suunnitellusti ja säännöllisesti tai kun merkittäviä muutoksia tapahtuu. Katselmoinneilla voidaan varmistaa tietoturvapolitiikoiden soveltuvuus, asianmukaisuus ja vaikuttavuus. (SFS ISO/IEC 27002 2013, 2-3.)

Ylimmällä tasolla johdon hyväksymällä tietoturvapolitiikalla esitetään organisaation menettelytavat tietoturvatavoitteiden saavuttamiseksi. Tietoturvapolitiikan tulisi käsitellä vaatimuksia, jotka liiketoimintastrategia, säännökset, lait, sopimukset ja organisaation tietoturvaympäristö asettaa. Tietoturvapolitiikan tulisi sisältää julkilausumia tietoturvallisuuden määrittelystä, tavoitteista ja periaatteista, jotka ohjaavat kaikkea tietoturvallisuuteen liittyvää toimintaa. Tietoturvapolitiikassa tulee määrittää vastuut tietoturvallisuuden hallintaan ja käsitellä prosessit poikkeamien hallintaan. (SFS ISO/IEC 27002 2013, 2.)

Alemmilla tasoilla tätä tietoturvapolitiikkaa tulee tukea aihekohtaiset politiikat, joilla valtuutetaan aiheeseen liittyvät hallintakeinot eri kohderyhmille organisaation sisällä. Esimerkkeinä aihekohtaisista politiikoitten aiheista voidaan mainita pääsynhallinta, tiedon luokittelu, fyysinen ja ympäristön turvallisuus, loppukäyttäjiä ohjaavat ai-

heet, tiedonsiirto, varmistukset, haittaohjelmien ja tietoturvahaavoittuvuuksien hallinta, tiedon salaus, viestintä, yksityisyyden ja henkilötietojen suoja sekä alihankinta. Aihekohtaiset politiikat tulee tiedottaa ja kouluttaa niitä tarvitseville organisaation jäsenille ja ulkoisille sidosryhmille. (SFS ISO/IEC 27002 2013, 3.)

Tietoturvapolitiikoita voi esiintyä monella tasolla. Politiikat voivat olla julkisia kannanottoja koko organisaatiolle ja asiakkaille. On olemassa myös aihekohtaisia yksityiskohtaisempia tietoturvapolitiikoita, jotka on suunnattu vain tietylle kohderyhmälle. SFS ISO/IEC 27002-standardi (2013) varoittaa tietoturvapoliitikoihin liittyvistä arkaluontoisista tiedoista. Organisaation tulee varmistua, että arkaluontoisia tietoja ei paljasteta ulkopuolisille. (SFS ISO/IEC 27002 2013, 4.)

2.3 Hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmä on malli, jolla voidaan suunnitella, toteuttaa, noudattaa, seurata, arvioida, ylläpitää ja kehittää tietoturvallisuutta (Andreasson & Koivisto 2013, 41). Tietoturvallisuudella tuloksia, yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 (2007) määrittää tietoturvallisuuden hallintajärjestelmän viitekehykseksi, joka koostuu seuraavista toimintamalleista ja dokumenteista:

- tietoturvapolitiikka ja -strategia
- tietoturvakäytännöt ja -periaatteet, jotka kuvaavat käytössä olevat turvakäytännöt
- tietoturvallisuuden kehittämissuunnitelma
- tietoturvallisuuden perus- ja lisäohjeistus
- tietoturva-arkkitehtuurit (topologia ja ratkaisujen periaatekuvaukset)

- tietoturvaraportointi johdolle
- pelastus -, jatkuvuus- ja valmiussuunnitelmat
- toimintaan liittyvät tietoturvaprosessit
- auditointisuunnitelma

Hallintajärjestelmällä voidaan toteuttaa organisaation strategiaa. Hallintajärjestelmä kattaa tietoturvallisuuden organisoinnin, politiikat, suunnittelun, vastuut, menettelytavat, prosessit ja tarvittavat resurssit. Hallintajärjestelmän avulla on mahdollista seurata tietoturvatoimien tehokkuutta ja tarkoituksenmukaisuutta. Järjestelmän jatkuva kehittäminen on tärkeää, jotta organisaatio voi parantaa edellytyksiään hallita systemaattisesti tietoturva-asioitaan. (Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 2007, 40.)

SFS ISO/IEC 27001-standardissa (2013) esitetään tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset (SFS-ISO/IEC 27001, 6). SFS ISO/IEC 27002-standardi (2013) on tietoturvallisuuden hallintaa koskeva menettelyohje. Standardissa esitellään yleisesti hyväksyttyjä valvontatavoitteita ja turvamekanismien parhaita käytäntöjä. Standardin tarkoituksena on antaa ohjeita tietoturvamekanismien toteuttamiseen. (SFS-ISO/IEC 27000 2010, 36.)

2.4 Turvallisuusvaatimukset

Organisaation turvallisuusvaatimusten määrittäminen on tärkeä osa organisaation tietoturvaa. Turvallisuusvaatimuksia voidaan määrittää organisaation suorittamilla riskinanalyyseilla, joissa huomioidaan organisaation liiketoiminta ja tavoitteet. Riskien arvioinnin avulla suojattaviin kohteisiin kohdistuvat uhkat voidaan tunnistaa. Ris-

kien arvioinnin yhteydessä arvioidaan myös suojattavan kohteen alttius vahingoille, vahingon todennäköisyys ja mahdolliset vaikutukset. (SFS ISO/IEC 17999:fi 2006, 15.)

Lainsäädäntö, asetukset, säännökset, sopimukset ja sosiokulttuurinen ympäristö asettavat turvallisuusvaatimuksia, joita organisaation on noudettava. Organisaation omat tietojenkäsittelyn periaatteet, tavoitteet ja liiketoiminnalliset vaatimukset luovat myös turvallisuusvaatimuksia. (SFS ISO/IEC 17999:fi 2006, 16.)

2.5 Riskien hallinta ja turvamekanismit

Riskillä tarkoitetaan tapahtuman todennäköisyyden ja sen seurauksen yhdistelmää (ISO/IEC 17999, 22). Andreasson ja Koivisto (2013) määrittelevät riskin epävarmuuden vaikutuksella tavoitteisiin (Andreasson & Koivisto 2013, 40).

Riskien hallinnalla tarkoitetaan koordinoituja toimenpiteitä, joilla johdetaan ja ohjataan organisaation riskienkäsittelyä. Riskien arvioinnilla tarkoitetaan riskianalyysin suorittamista ja riskien vaikutusten arviointia. Riskien arvioinnin tulisi sisältää järjestelmällinen tapa riskien tunnistamiseen ja suuruusluokan arviointiin (riskianalyysi) sekä riskien vertaaminen riskikriteereihin merkittävyyden selvittämiseksi (riskien vaikutusten arviointi). (SFS ISO/IEC 17999:fi 2006 22, 26.)

Riskien arvioinnin avulla voidaan yksilöidä riskit, määritellä riskien suuruus ja asettaa riskit tärkeysjärjestykseen suhteutettuna organisaation tavoitteisiin ja riskien hyväksymiskriteereihin. Riskien arviointi tulisi ohjata yrityksen johtoa hallintatoimenpiteissä ja turvamekanismien käyttöönotossa. (SFS ISO/IEC 17999:fi 2006, 26.)

Riskien arviointia tulisi suorittaa säännöllisin väliajoin, jotta voidaan huomata muutokset turvallisuusvaatimuksissa ja riskitilanteissa. Riskitilanteet voivat liittyä suojat-

taviin kohteisiin, uhkiin, haavoittuvuuksiin, vaikutuksiin ja riskien vaikutusten arviointiin. (SFS ISO/IEC 17999:fi 2006, 20.)

Turvallisuusriskejä käsiteltäessä organisaation tulee päättää kriteerit, joiden perusteella riskit hyväksytään tai ei hyväksytä. Tunnistetun riskin osalta on tehtävä myös päätös kuinka riskejä käsitellään. (SFS ISO/IEC 17999:fi 2006, 26.)

Turvamekanismit voidaan valita ja toteuttaa, kun turvallisuusvaatimukset ja riskit ovat tunnistettu sekä päätökset riskien käsittelystä tehty. Turvamekanismilla riski voidaan pienentää hyväksyttävälle taholle. (SFS ISO/IEC 17999:fi 2006, 20.)

3 TIETOTURVAHERÄTE JA –TAPAHTUMA

3.1 Määritelmä

Voidaksemme ymmärtää tietoturvaherätteitä ja -tapahtumia, meidän täytyy määritellä mitä ne tarkoittavat. Tietoturvaheräte määritellään ISO/IEC 27035-standardissa seuraavasti: ”Tietoturvaheräte on tunnistettu järjestelmän, palvelun tai verkon tila, joka viittaa mahdolliseen tietoturvallisuuden murtumiseen, tietoturvapolitiikan murtumiseen, turvamekanismien pettämiseen tai aikaisemmin tuntematon tilanne, jolla saattaa olla merkitystä turvallisuudelle.” (SFS ISO/IEC 27035 2011, 2.)

Palvelunhallinnan näkökulmasta heräte ja tapahtuma ovat keskeisiä käsitteitä. ITIL version 3 Service Operation –viitekehyksessä (2007) heräte määritetään seuraavasti: ”Heräte voidaan määritellä tunnistettavaksi tai havaittavaksi tapahtumaksi, jolla on merkitystä IT-infrastruktuurin hallinnalle tai saatavuudelle ja jonka arvioitu vaikutus

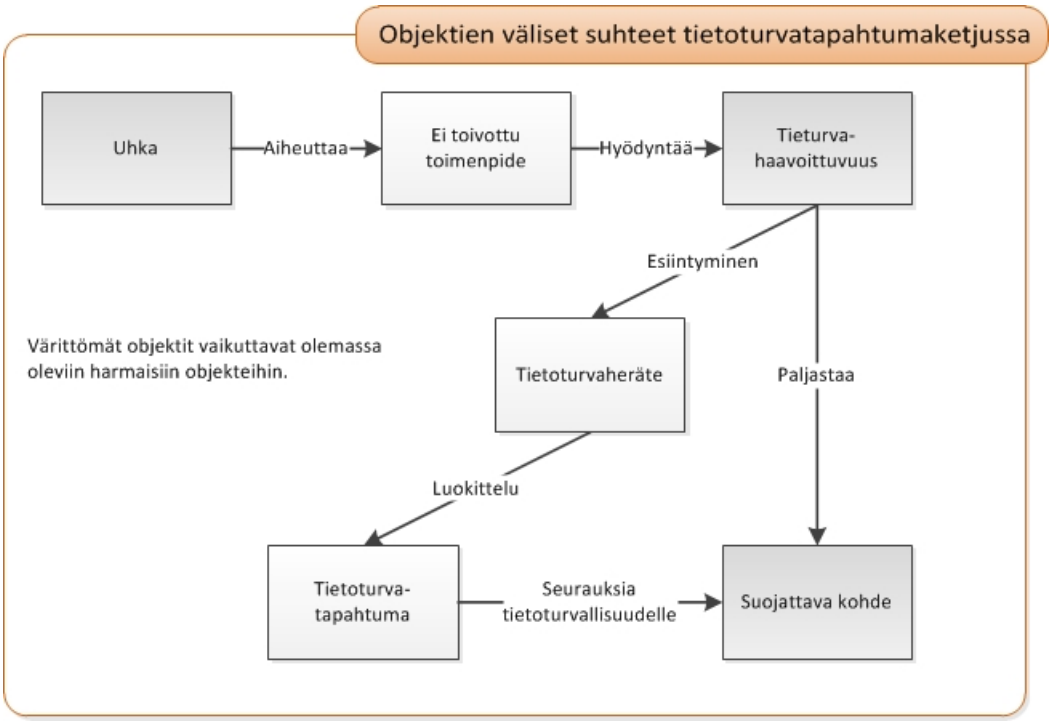
saattaa aiheuttaa poikkeaman palveluille.” (ITIL version 3 Service Operation 2007, 35-36.)

Keskeistä on ymmärtää, että tietoturvaheräte ei välttämättä tarkoita onnistunutta hyökkäystä tai seuraamuksia luottamukselle, eheydelle tai saatavuudelle. Kaikkia tietoturvaherätteitä ei luokitella tietoturvatapahtumiksi (SFS ISO/IEC 27035 2011, 2). Herätteet voivat tuottaa ainoastaan informatiivista arvoa ja kertoa myös normaaleista tilan muutoksista järjestelmissä, palveluissa tai verkoissa.

Tietoturvatapahtuma määritellään SFS ISO/IEC 27035-standardissa (2011) seuraavasti: ”Tietoturvatapahtuma on yksi tai useampi epätoivottu tai ennalta arvaamaton tietoturvaheräte, joka huomattavalla todennäköisyydellä vaarantaa liiketoimintaa tai uhkaa tietoturvallisuutta.” (SFS ISO/IEC 27035 2011, 2.)

Palvelunhallinnan kannalta tapahtuma määritellään suunnittelemattomaksi keskeytykseksi tai palvelun alenemaksi. Myös tapahtuma, joka ei vielä ole aiheuttanut keskeytystä tai palvelun alenemaa määritellään tapahtumaksi. (ITIL version 3 Service operation 2007, 46.)

Tietoturvahaavoittuvuudella tarkoitetaan turvattavan kohteen tai turvamekanismin heikkoutta, jota uhka voi käyttää hyväksi. Uhkalla tässä yhteydessä tarkoitetaan mahdollista syytä epätoivottuun tapahtumaan, josta voisi seurata haittaa järjestelmälle tai organisaatiolle. (SFS ISO/IEC 27000 2010, 18-19.) Kuviossa 4 on esitelty tietoturvaherätteen, -haavoittuvuuden ja -tapahtuman välisiä suhteita.



Kuvio 4. Objektien väliset suhteet tietoturvatapahtumaketjussa

(SFS ISO/IEC 27035 20144, 3)

3.2 Esimerkkejä

3.2.1 Yleistä

Tietoturvatapahtumat voivat olla tahallisia tai tahattomia. Tietoturvatapahtumia voivat aiheuttaa esimerkiksi luonnonilmiöt tai virhetilanteet ja tapahtumat voivat olla luonteeltaan fyysisiä tai teknisiä. Tietoturvatapahtumien seurauksena voi olla tiedon paljastuminen, muuttuminen, tuhoutuminen tai käytettävyyden estyminen. Tietoturvatapahtuma voi olla myös esimerkiksi organisaation suojattavan kohteen vahingoittuminen tai varkaus. (SFS ISO/IEC 27035 2011, 7.)

ISO/IEC 27035-standardin (2011) liitteessä Annex B esitellään muutamia tietoturvatapahtumia. Lista ei ole kattava vaan ainoastaan informatiivinen. Esimerkkien avulla voimme ymmärtää millaisia tietoturvatapahtumat voivat olla luonteeltaan ja mitä ne saattavat aiheuttaa organisaation liiketoiminnalle.

3.2.2 Palvelunestohyökkäys

Palvelunestohyökkäys (Denial of Service) tai hajautettu palvelunestohyökkäys (Distributed Denial of Service) voi aiheuttaa järjestelmän, palvelun tai tietoverkon toiminnan vikaantumisen. Vikaantuminen voi aiheuttaa suojatun kohteen käytön estymisen tai suorituskyvyn aleneman. Tyypillisiä tahallisia DOS/DDOS-hyökkäyksiä ovat esimerkiksi:

- verkon broadcast-osoitteen pingaaminen tavoitteena verkon kapasiteetin täyttäminen.
- virheellisessä muodossa olevan datan lähettäminen järjestelmälle, palvelulle tai tietoverkolle tarkoituksena estää tai häiritä kohteen toimintaa.
- useiden istuntojen avaaminen kohteena olevaan järjestelmään, palveluun tai tietoverkkoon tavoitteena kohteen ylikuormittuminen.
- DDOS-hyökkäykset tehdään usein käyttämällä niin kutsuttuja bottiverkkoja (botnet). Bottiverkot voivat koostua sadoista haittaohjelmien (malicious code) avulla hallittavista tietokoneista. (SFS ISO/IEC 27035 2011, 47.)

Palvelunesto voi aiheutua myös vahingossa suojattavan kohteen virheellisen asetusten takia. Usein palvelunestohyökkäykset ovat kuitenkin tahallisia, hyökkäykset suoritetaan anonyyminä tai hyökkääjän identiteetti ei ole oikea. Palvelun eston voi aihe-

uttaa myös esimerkiksi varkaus, ilkivalta, laitteen rikkoutuminen, tulipalo, vesivahinko tai toimintahäiriöt. (SFS ISO/IEC 27035 2011, 47.)

3.2.3 Luvaton pääsy

Luvaton pääsy (unauthorized access) tarkoittaa tietoturvatapahtumaa, jossa pyritään tunkeutumaan tai väärinkäyttämään järjestelmää, palvelua tai tietoverkkoa ilman asiaankuuluvia käyttöoikeuksia. Hyökkäyksissä voidaan yrittää saada selville salasanatiedostoja, käyttää hyväksi puskurin ylivuotoa (buffer overflow) järjestelmänvalvojan oikeuksien saamiseksi tai päästä käsiksi tietoon tai resursseihin, joihin ei ole käyttöoikeutta. Myös fyysisen turvallisuuden loukkaukset, virheelliset asetukset käyttöjärjestelmissä, hallitsemattomat järjestelmän muutokset tai toimintahäiriöt voivat mahdollistaa pääsyn luvattomiin tietoihin. (SFS ISO/IEC 27035 2011, 48.)

3.2.4 Haittaohjelmat

Haittaohjelmalla (malicious code) tarkoitetaan ohjelmaa tai ohjelman osaa, jolla pyritään muuttamaan alkuperäisen ohjelman suunniteltua toimintaa. Yleisesti tarkoituksena on suorittaa haitallisia toimenpiteitä kuten tieto- ja identiteettivarkauksia, tuhota tietoa, estää palvelun toiminta tai lähettää roskapostia. (SFS ISO/IEC 27035 2011, 48.)

Haittaohjelmahyökkäyksiä voidaan suorittaa esimerkiksi virusten, matojen, troijalaisten hevosten, mobile code -hyökkäysten tai blended-hyökkäysten avulla. Haittaohjelmia käytetään myös kohdistettuihin hyökkäyksiin luomalla muunnelmia tunnetuista haittaohjelmista. (SFS ISO/IEC 27035 2011, 48.) Kohdistettujen haittaohjelma hyökkäysten englanninkielinen nimitys on Advanced Persistent Threat (APT).

CERT-FI:n artikkelissa Kohdistetut haittaohjelmahyökkäykset kerrotaan, että kohdistetulla hyökkäyksellä tarkoitetaan sellaista tietoturvaloukkausta, joka kohdistuu tiettyyn organisaatioon tai rajattuun joukkoon henkilöitä. Hyökkäysten työkaluina käytetään yleensä räätälöityjä, yksilöllisesti toteutettuja haittaohjelmia, joiden havaitseminen ei onnistu yleensä virustorjuntaohjelmistojen avulla. Haittaohjelmia levitetään esimerkiksi sähköpostiviestien tai USB-muistitikkujen avulla. Haittaohjelmat voivat käyttää ensimmäiseksi saastunutta konetta sillanpääasemana, jonka kautta voidaan tunkeutua muualle organisaation tietokoneisiin. Haittaohjelmat voivat myös välittää tietokoneista löytyneitä tietoja hyökkääjälle ja kommunikoida organisaation verkosta ulospäin. Kehittyneimmät haittaohjelmat tarjoavat salatun etäyhteyden tartunnan saaneeseen koneeseen. Käytetyt ohjelmistot ovat niin kehittyneitä, että haittaohjelmien tekijöillä voidaan epäillä olevan runsaasti asiantuntemusta ja työvoimaa hyökkäysten toteuttamiseen. Haittaohjelmien taustalta löytyy usein järjestäytyneitä ryhmiä ja valtiollisten toimijoiden mukana oloa on epäilty. On tullut ilmi tapauksia, joissa haittaohjelmat ovat toimineet organisaation verkoissa useiden vuosien ajan. (Kohdistetut haittaohjelmahyökkäykset 2013.)

3.2.5 Sopimaton käyttö

Tietoturvatapahtuma voi ilmetä, jos käyttäjä rikkoo organisaation tietoturvapolitiikkaa. Nämä tapahtumat eivät ole varsinaisia hyökkäyksiä, mutta vaativat käsittelyä. Sopimaton käyttö voi pitää sisällään esimerkiksi hakkerointityökalujen lataamista ja asentamista organisaation työasemalle, organisaation sähköpostin käyttöä roskapostitukseen, luvattomien web-sivujen julkaisua yrityksen palvelimilla tai peer-to-peer ohjelmien käyttöä musiikin, elokuvien tai ohjelmistojen lataamiseen. (SFS ISO/IEC 27035 2011, 48.)

3.2.6 Tiedon keräily

Tiedon keräilyllä (information gathering) pyritään yleensä potentiaalisten kohteiden etsintään ja havaitsemiseen sekä tietojen hankintaan kohteen palveluista. Tiedon etsijä pyrkii vahvistamaan kohteen olemassaolon, ymmärtämään kohdetta ympäröivää verkkotopologiaa ja selvittämään kohteen kommunikointirutiinit. Myös heikkouksien etsintä kohteesta tai kohdetta ympäröivästä tietoverkosta on yleistä. Tiedon keräilyyn voi liittyä esimerkiksi verkko-osoitteiden pingaaminen suojattavien kohteiden IP-osoitteiden selvittämiseksi tai verkkoskannauksia avointen porttien, palvelujen tai haavoittuvuuksien löytämiseksi. (SFS ISO/IEC 27035 2011, 49.)

4 TIETOTURVATAPAHTUMIEN HALLINTA

4.1 Määritelmä ja tavoitteet

Tietoturvapolitiikat tai hallinnolliset toimenpiteet eivät pelkästään riitä organisaation tietoturvallisuuden takaamiseen. Kun hallinnolliset toimenpiteet on toteutettu, tietoturvahaavoittuvuudet voivat vaarantaa tietoturvallisuuden, mahdollistaa tietoturvatapahtumien esiintymisen ja haitata liiketoimintaa suorasti tai epäsuorasti. On myös väistämätöntä, että uusia tunnistamattomia uhkia ilmenee ajan kuluessa. Organisaation puutteellinen valmistautuminen tämän kaltaisiin tapahtumiin tekee vastatoimista vähemmän tehokkaita ja kasvattaa liiketoiminnalle aiheutuvia haitallisia vaikutuksia. On erittäin tärkeää, että millä tahansa organisaatiolla on jäsennelty ja suunnitelmallinen tapa tietoturvatapahtumien hallintaan. (SFS ISO/IEC 27035 2011, VI.)

Tietoturvatapahtumien hallinnan tavoitteena on varmistaa yhtenäinen ja tehokas toimintamalli tietoturvaherätteiden, -tapahtumien ja -haavoittuvuuksien hallintaan (ISO/IEC 27002, 67). Tietoturvatapahtumien hallinta on yksi osa SFS ISO/IEC 27001-(2013) ja ISO/IEC 27002-standardeissa(2013) käsiteltyä tietoturvan hallintajärjestelmää, jolla pyritään varmistamaan liiketoiminnan kestävä menestys, jatkuvuus ja haittavaikutusten minimointi.

Keskeisenä osana organisaation tietoturvastrategiaa organisaation tulisi mahdollistaa jäsennelty ja hyvin suunniteltu tietoturvatapahtumien hallinta. Liiketoiminnan näkökulmasta ensisijaisena tavoitteena on välttää tai eristää tietoturvatapahtuman aiheuttama vaikutus vähentäen suoria tai epäsuoria tapahtuman aiheuttamia kustannuksia. Ensisijaiset toimenpiteet tietoturvatapahtumille ovat:

- pysäyttäminen ja eristäminen
- hävittäminen
- analysointi ja raportointi seuranta
  (SFS ISO/IEC 27035 2011, 3.)

Jäsenneltyyn ja hyvin suunniteltuun lähestymistapaan kuuluu, että tietoturvaherätteet, -tapahtumat ja -haavoittuvuudet havaitaan ja käsitellään tehokkaasti. Tunnistamisen jälkeen tehdään päätös luokitellaanko tietoturvaheräte tietoturvatapahtumaksi. Tunnistetut tietoturvatapahtumat arvioidaan ja niihin vastataan tehokkaasti parhaalla mahdollisella tavalla. Tietoturvatapahtumien haittavaikutukset organisaatiolle ja sen liiketoiminnalle minimoidaan tietoturvatapahtumien vastatoimilla. On tärkeää oppia tietoturvatapahtumista. Oppiminen mahdollistaa tietoturvatapahtumien esiintymisen estämisen ja parantaa hallinnollisten toimenpiteiden toteuttamista tulevaisuudessa. Oppimisella voidaan parantaa koko tietoturvatapahtumien hallintaan liittyvää kokonaisuutta. Se mahdollistaa parannuskohteiden tunnistamisen ja turvamekanismien ja tietoturvatapahtumien käsittelymallin kehittämisen. (SFS ISO/IEC 27035 2011, 3.)

4.2 Hyödyt

Tietoturvatapahtumien hallinnan jäsenneltyyn ja ennalta suunniteltuun toimintaan liittyy merkittäviä etuja. Jäsennelty malli tietoturvatapahtumien tunnistamiseen, raportointiin ja arviointiin mahdollistaa nopean ja tehokkaan tunnistamisen ja tapahtumaan vastaamisen. Jäsennellyllä mallilla voidaan parantaa organisaation yleistä tietoturvallisuutta ja estää samankaltaisten tietoturvatapahtumien esiintyminen tulevaisuudessa. Organisaation uskottavuutta on myös mahdollista lisätä parhaiden

käytäntöjen mukaisella tietoturvatapahtumien käsittelyllä. (SFS ISO/IEC 27035 2011, 3.)

Jäsennellyllä tietoturvatapahtumien hallinnalla voidaan estää tietoturvatapahtumiin liittyviä haittoja liiketoiminnalle. Liiketoiminnan haittoja voivat olla esimerkiksi taloudellinen tappio ja maineen tai uskottavuuden menettäminen. Käytännön toiminnan kannalta jäsennelty tietoturvatapahtumien hallinta lisää organisaation tietoisuutta asiasta ja auttaa ehkäisemään vaaratilanteita organisaation sisällä. Tietoturvatapahtumien priorisointia voidaan parantaa ottamalla käyttöön tietoturvatapahtumien vakavuuden luokitteluasteikko (classification scale) ja ryhmittelyasteikko (categorization scale) tietoturvatapahtumien tyypin mukaan. Priorisointi mahdollistaa tutkinnan keskittymisen ensimmäisenä kaikkein tärkeimpiin tietoturvatapahtumiin. Selkeät tutkintamenetellyt varmistavat myös todisteiden keräämisen ja niiden juridisen luotettavuuden. (SFS ISO/IEC 27035 2011, 3.)

Tietoturvatapahtumien hallinnan jäsennelty malli auttaa tietoturvatapahtumien hallintaan käytettävän budjetin ja resurssien kohdistamisessa. Tietoturvaherätteiden käsittelyyn voidaan käyttää henkilökuntaa, jolla ei ole syvällistä erikoisosaamista. Asiantuntijoiden resurssit on mahdollista kohdentaa tapahtumiin, jotka vaativat erikoisosaamista. Mittareiden avulla tietoturvatapahtumien hallintaprosessista voidaan saada selville kuinka kauan eri prioriteetin tietoturvatapahtumien käsittely vie aikaa ja löytää prosessin mahdolliset ongelmakohdat. Mittarit tuottavat arvokasta informaatiota tietoturvatapahtumien hallinnan strategia- ja investointipäätöksiin. (SFS ISO/IEC 27035 2011, 3-4.)

Tietoturvaherätteistä kerättävän tiedon avulla voidaan analysoida minkä tyyppisiä haavoittuvuudet ja uhkat ovat. Nämä tiedot ovat hyödyllisiä arvioitaessa vaikutuksia liiketoiminnalle ja auttavat parantamaan riskinhallinnan laatua. Jäsennelty tietotur-

vatapahtumien käsittely mahdollistaa myös organisaation tietoturvallisuustietoisuuden lisäämisen koulutusten avulla. Tietoisuus tietoturvatapahtumista auttaa vähentämään sekaannusta ja paniikkia tietoturvatapahtumien ilmaantuessa. Jäsennelty toimintatapa tietoturvatapahtumien hallinnassa saattaa toimia myös arvokkaana herätteenä organisaatiolle tietoturvallisuuspolitiikkojen ja tietoturvallisuuteen liittyvän dokumentoinnin arvioimiseen ja päivittämiseen. (SFS ISO/IEC 27035 2011, 4.)

4.3 Vertailua

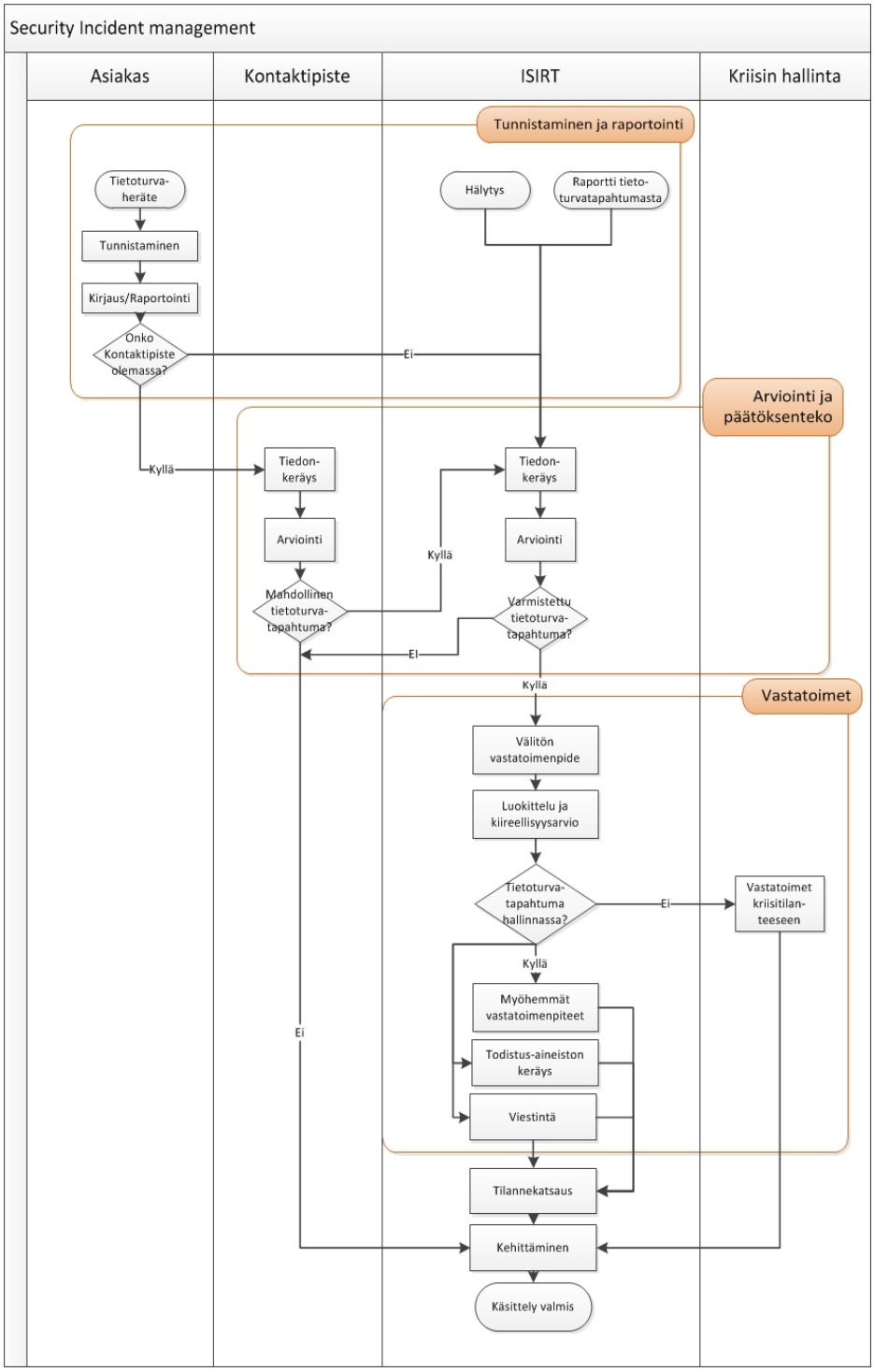
Tietoturvatapahtumien hallinnalle esitetään SFS ISO/IEC 27035-standardissa(2011) tietoturvatapahtumien hallintamalli (incident management scheme), jossa on viisi päävaihetta. Päävaiheet ovat:

- Suunnittelu ja valmistautuminen
- Tunnistaminen ja raportointi
- Arviointi ja päätöksen teko
- Vastatoimet
- Opetukset
  (SFS ISO/IEC 27035 2011, 6.)

Suunnittelu ja valmistautuminen mahdollistavat tietoturvatapahtumien hallinnan. Muut neljä pääkohtaa käsittelee tietoturvatapahtumien hallinnan operatiivisia vaiheita. (SFS ISO/IEC 27035 2011, 6.) Kuviossa 5 on esitelty tietoturvatapahtumien hallintamallin ja päävaiheiden sisältöä.

Kuvio 5. Tietoturvatapahtumien hallintamallin vaiheet

(SFS ISO/IEC 27035 2011, 7.)

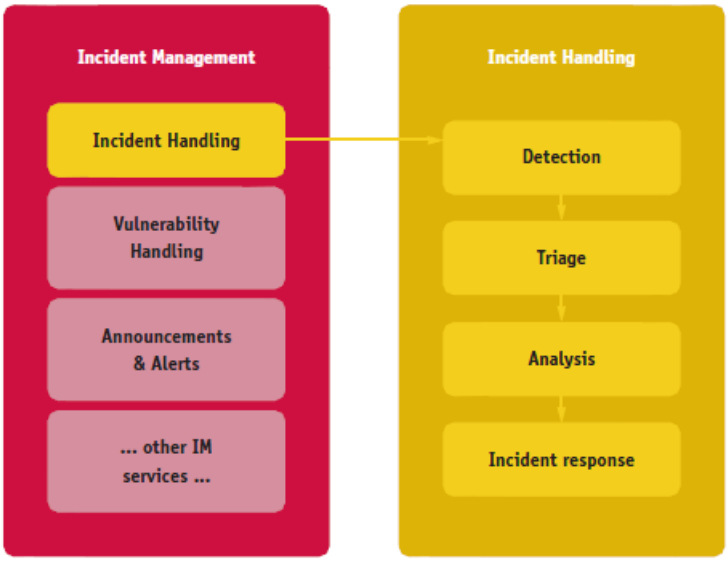


Kuvio 6. Tietoturvaherätteiden ja -tapahtumien hallintaprosessi

(ISO/IEC 27035, 23.)

Kuviossa 6 on tietoturvatapahtumien prosessikaavio, jossa on nähtävissä operatiivisten vaiheiden sisältämät työvaiheet ja päätöksentekokohdat. Kuviosta 6 voidaan nähdä myös vastuiden jakautuminen prosessin aikana. Päävaiheiden sisältö avataan opinnäytetyön luvuissa 4.4 – 4.7.

ENISA (European Network and Information Security Agency) esittelee oppaassaan Good Practice for Incident Management (2010) useita eri prosessimalleja tietoturvatapahtumien hallintaan ja käsittelyyn. Opas pyrkii auttamaan oikeanlaisen kuvauksen valinnassa. Oppaan esittelemissä malleissa on nähtävissä yhtäläisyyksiä SFS ISO/IEC 27035-standardin (2011) tietoturvatapahtumien hallintamallin kanssa.

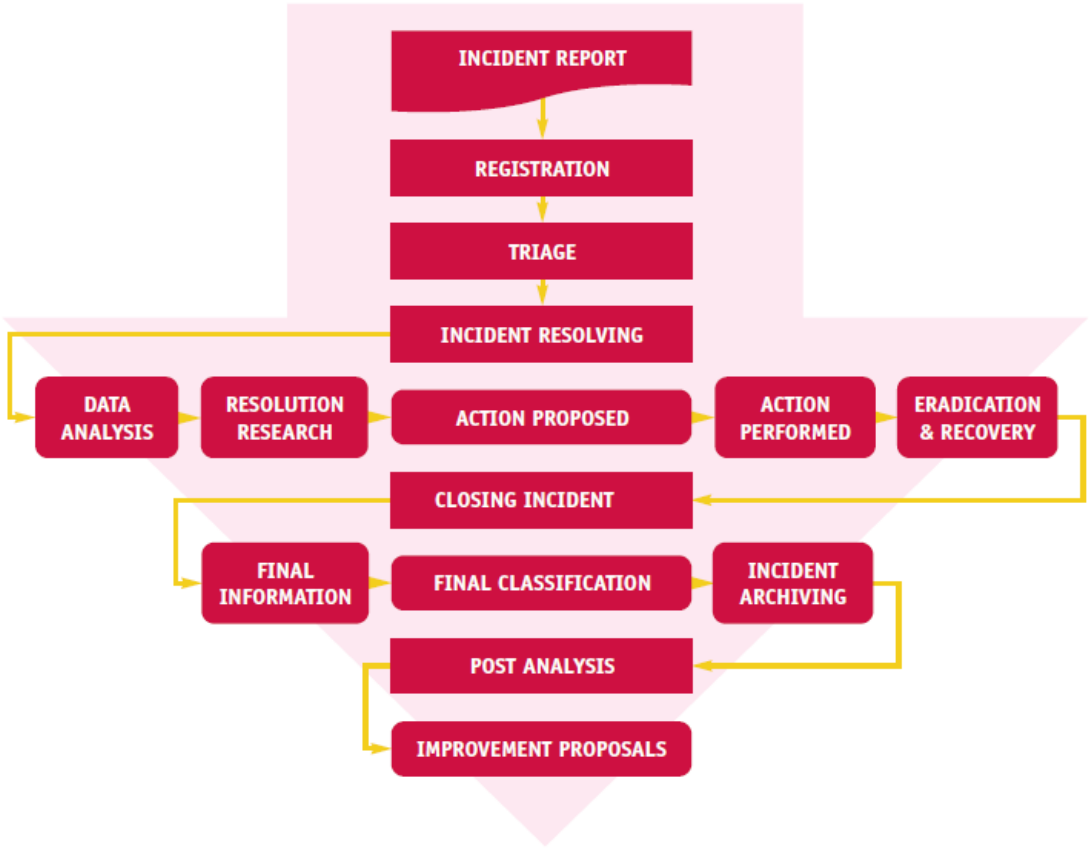


Kuvio 7. Tapahtumien hallinta ja käsittely

(Good Practice for Incident Management 2010, 34.)

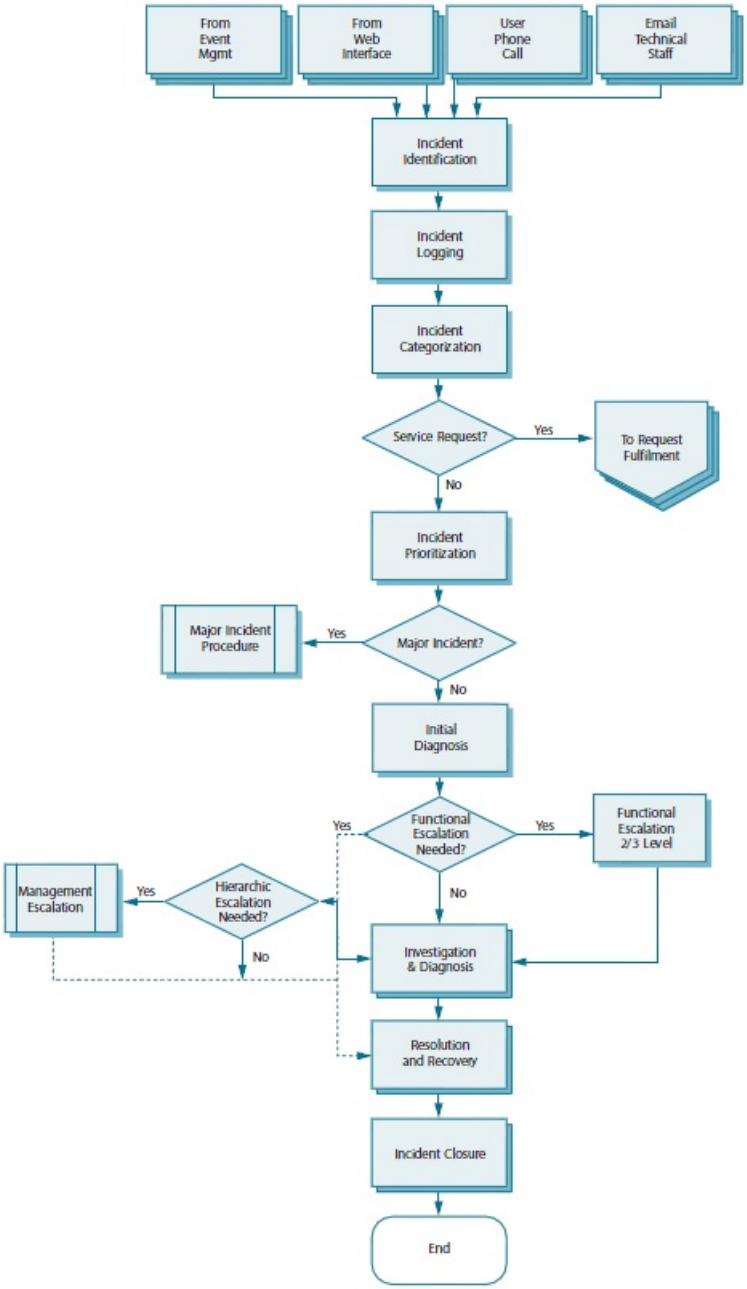
ENISAn esittelemä malli kuviossa 7 koostuu neljästä päävaiheesta, jotka ovat tunnistaminen, kiireellisyysjärjestys (triage), analysointi ja tapahtumaan vastaaminen. ENISAn esittelemä malli kuviossa 8 on kuviossa 6 esitetyn tietoturvaherätteiden ja -

tapahtumien hallintaprosessin kaltainen, joissa kuvataan tapahtuman käsittelyn työvaiheita yksityiskohtaisemmin. Kuviossa 9 voidaan nähdä ITIL -viitekehyksessä käytettävä IT-palvelutuotannon tapahtumien hallintaprosessi, jota ei ole suunniteltu tietoturvatapahtumien hallintaan. ITIL -viitekehys käsittelee tietoturvatapahtumien hallintaa suunnittelun näkökulmasta kirjassa ITIL version 3 Service desing (2007), mutta tietoturvatapahtumien käytännön käsittelyn näkökulma on hyvin suppea. Palvelutuotannon tapahtumienkäsittelyä ITIL-viitekehyksessä kuvataan laajasti.



Kuvio 8. Tapahtuman käsittelyn työnkulku

(Good Practice for Incident Management 2010, 34).



Kuvio 9. Palvelutuotannon tapahtumien hallinta

(ITIL version 3 Service Operation 2007, 48.)

Kaikista esitetyistä malleista on löydettävissä samankaltaisia tapahtuman tunnistamiseen, kirjaamiseen, analysointiin, priorisointiin ja tapahtumaan vastaamiseen liittyviä vaiheita. Jälkiarviointi ja parannusten tekeminen on sisällytetty kaikkiin malleihin, paitsi pelkistetyimpään malliin kuviossa 7.

4.4 ISIRTin perustaminen

4.4.1 Nimeäminen

ISIRT (Information Security Incident Response Team) on ryhmä osaavia ja luotettavia henkilöitä, jotka käsittelevät tietoturvatapahtumia koko niiden elinkaaren ajan (SFS ISO/IEC 27035 2011, 1). Tietoturvatapahtumien hallinnasta ja käsittelystä vastaavia tiimejä voidaan kutsua myös seuraavilla nimillä:

- CERT tai CERT/CC (Computer Emergency Response Team / Coordination Centre)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)
- Abuse team
- WARP (Warning, Advice and Reporting Point)
  (Terms and Definitions 2014)

ISIRTin perustaminen ja vastuiden määrittäminen on osa SFS ISO/IEC 27035-standardissa (2011) esiteltävän hallintamallin suunnittelu ja valmistautuminen -vaiheen toimintoja. ISIRT käsitteen ymmärtäminen on olennaista, koska tietoturva-

tapahtumien hallintaa on hankala käsitellä ilman henkilöitä, jotka ovat vastuussa tietoturvatapahtumien käsittelystä.

4.4.2 Roolit

ISIRTin tehtäviä suorittaville henkilöille tulee jakaa vastuut. Organisaation koosta riippuen yksi henkilö voi toimia useammassa roolissa. Ryhmä voidaan muodostaa pelkästään ISIRTin tehtäviä varten tai ryhmään voi kuulua henkilöitä muista organisaation osista virtuaaliroolien avulla. ISIRTIn perustamisen yhteydessä laaditaan koulutusohjelmat henkilöstölle. Myös virtuaaliroolien kautta muodostettava ISIRT on mahdollinen. Virtuaalisissa rooleissa toimivat henkilöt voivat olla ISIRTin kanssa läheisessä toiminnassa olevista organisaation osista, kuten ICT-ylläpidosta, ulkoistetuista yrityksen osista, lakiosastolta tai tiedotuksesta. Virtuaalisella ryhmällä voi olla myös erillinen tukiryhmä, joka koostuu asiantuntijoista, jotka ovat erikoistuneet tiettyyn aihealueeseen. Asiantuntijat hälytetään apuun vain siinä tapauksessa, jos tietoturvatapahtuma liittyy asiantuntijan osaamisalueeseen. (SFS ISO/IEC 27035 2011, 8-9.) ENISA Incident Management Guide (2010) esittelee CSIRT rooleja ja roolien tehtäväkuvauksia. Roolit ja tehtäväkuvaukset ovat nähtävissä taulukossa.

Taulukko 2. ISIRTin roolit

(Incident Management Guide 2010, 18.)

Rooli	**Kuvaus**
Duty officer	Kaikkien palvelupyyntöjen ja määräajoin tehtävien rutiinien käsittely.
Triage officer	Tiimille tulevien tai tiimin havaitsemien tietoturvatapahtumien käsittely ja kiireellisyyden arviointi. Päätöksenteko tapahtuman käsittelijästä ja käsittelyn ajankohdasta.
Incident Handler	Tietojen analysointi, väliaikaisten ratkaisujen tekeminen, tapahtuman ratkaisu, kommunikointi Incident Managerin ja asianomaisten kanssa.
Incident Manager	Tietoturvatapahtumien hallinnan koordinointi ja tiimin edustaminen.

Esimerkiksi tiedotus- ja suhdetoiminta (public relations), lakiasiat, ryhmän johtaminen ja hotline-palvelut voivat vaatia erillisiä rooleja tai tehtävien jakamista olemassa oleville organisaation jäsenille. (Incident Management Guide 2010, 30.)

Organisaation tulisi muodostaa tarvittavat suhteet ja yhteydet ulkoisiin ja sisäisiin organisaatioihin, jotka liittyvät suoraan tietoturvaherätteiden, -tapahtumien ja -haavoittuvuuksien hallintaan. Tietoturvatapahtumien hallintaa ja ISIRTIn toimintaa tukemaan tulisi perustaa ja käynnistää tarvittavat tekniset tukitoiminnot ja muu organisaatiolta tarvittavat tukitoiminnot. (SFS ISO/IEC 27035 2011, 9.)

4.4.3 Palvelut

Taulukosta 3 nähdään esimerkkejä palveluista, joita ISIRT voi tarjota. Taulukossa palvelut ovat jaettu reaktiivisiin, ennakoiviin ja laadun hallinnallisiin palveluihin. Monet toiminnoista kuten kaikki reaktiiviset palvelut, tapahtumista tiedottaminen, teknologian seuranta ja tunkeutumisen havainnointi liittyvät suoranaisesti tietoturvatapahtumien käsittelyyn, joka on ISIRTIn tärkein tehtävä.
(Incident Management Guide 2010, 26.)

Taulukko 3. ISIRTin tarjoamat palvelut
(Incident Management Guide 2010, 26)

Reaktiiviset palvelut	**Ennakoivat palvelut**	**Laadun hallinta**
Hälytysten ja varoitusten käsittely	Ilmoitukset / tiedonanto	Riskianalyysit
Tapahtumien käsittely	Teknologian seuranta	Liiketoiminnan jatkuvuus- ja toipumissuunnitelmat
Haavoittuvuuksien käsittely	Auditoinnit ja arvioinnit	Tietoturvallisuuskonsultoiti

Virhehavaintojen käsittely	Tietoturvallisuuden hallinnan työkalujen, sovellusten ja infrastruktuurin konfigurointi, ylläpito ja kehitys	Tietoisuuden lisääminen
	Tunkeutumisen havainnointi	Kouluttaminen
	Tiedottaminen tietoturvallisuuteen liittyvistä asioista	Tuotearvionnit ja -sertifionnit

ISIRTin perustamista käsitellään monissa oppaissa. Lisää tietoa voi hankkia esimerkiksi ENISAN julkaisemasta oppaasta Step-by-step approach on how to set up a CSIRT (Bronk, Thorbruegge & Hakkaja 2006) tai oppaasta Handbook for Computer Security Incident Response Teams (West-Brown, Stikvoort, Kossakowski, Killcrece, Ruefle & Zajicek 2003).

4.5 Suunnittelu ja valmistautuminen

4.5.1 Hallintapolitiikka ja sidokset muihin politiikoihin

Tehokas tietoturvatapahtumien hallinta vaatii suunnittelua ja valmistautumista. Organisaation tulisi laatia tietoturvaherätteiden, -tapahtumien ja -haavoittuvuuksien hallintapolitiikka, johon ylempi organisaation johto on sitoutunut. (ISO/IEC 27035, 8.) Tietoturvatapahtumien hallintapolitiikka voi olla itsenäinen dokumentti tai osa SFS ISO/IEC27001-standardin (2013) mukaista tietoturvan hallintajärjestelmäpolitiikkaa tai osa SFS ISO/IEC27002-standardin (2013) mukaista tietoturvapolitiikkaa. Politiikka tulee olla kaikkien organisaation jäsenten ja yhteistyökumppaneiden saatavilla ja aiheesta tulisi järjestää koulutuksia. (SFS ISO/IEC 27035 2011, 10.)

Tietoturvaherätteiden, -tapahtumien ja -haavoittuvuuksien hallintapolitiikan sisällön tulee ilmaista organisaation johdon sitoutuminen politiikkaan ja korostaa tietoturvatapahtumien hallinnan tärkeyttä. Hallintapolitiikan tulee antaa yleiskuva tietoturvaherätteiden, -tapahtumien ja -haavoittuvuuksien tunnistamisesta, raportoinnista, käsittelystä ja käsittelyn jälkeisestä tilannearviosta sekä oppimisesta ja kehitystoimenpiteistä. Hallintapolitiikan tulee kuvata ISIRTin rakenne, tavoitteet, toiminnot, johto, avainhenkilöt ja sidokset muihin organisaation osiin. Hallintapolitiikka voi antaa myös yleiskuvauksen teknisistä tukitoiminnoista, yleiskuvan tietoturvatapahtumien hallinnan koulutuksesta ja tietoturvatapahtumien hallintaan liittyvistä juridisista näkökulmista. Politiikka voi kertoa kuinka ja missä tietoturvatapahtumien hallintaan liittyvää dokumentaatiota, prosessikuvauksia ja tietoturvatapahtumien hallintamallin dokumentointia säilytetään. (SFS ISO/IEC 27035 2011, 11 -12.)

Organisaatioon tulee ylläpitää tietoturva ja riskienhallintapolitiikkoja organisaatio-, järjestelmä-, palvelu- ja verkkotasolla. Näiden tulisi toimia referensseinä tietoturvaherätteiden, -tapahtumien ja -haavoittuvuuksien hallinnalle. (SFS ISO/IEC 27035 2011, 8.)

Organisaation tulee sisällyttää tietoturvatapahtumien hallintapolitiikka olemassa oleviin tietoturva- ja riskienhallintapolitiikoihin. Politiikkojen integroinnin tavoitteena on varmistaa politiikkojen yhtenäisyys, osoittaa tietoturvatapahtumien hallintamallin tärkeys, osoittaa johdon sitoutuminen ja varmistaa ennalta suunniteltu, systemaattinen ja rauhallinen vaste tietoturvatapahtumiin. (SFS ISO/IEC 27035 2011, 12.)

4.5.2 Tietoturvatapahtumien hallintamalli

Tietoturvatapahtumien hallintamallin (Incident management scheme) tarkoituksena on dokumentoida yksityiskohtaisesti toimenpiteet ja proseduurit tietoturvaherätteiden, -tapahtumien ja -haavoittuvuuksien käsittelyyn ja viestintään. Hallintamallissa käydään yksityiskohtaisesti läpi tietoturvatapahtumien hallintapolitiikka ja tietoturvatapahtumien viisi päävaihetta, jotka ovat suunnittelu ja valmistautuminen, tunnistaminen ja raportointi, arviointi ja päätöksen teko, vastatoimet sekä opetukset. Mallia käytetään aina kun tietoturvaheräte, -tapahtuma tai -haavoittuvuus havaitaan. (SFS ISO/IEC 27035 2011, 13-14.)

Hallintamalliin sisältyy esittely tietoturvatapahtumien hallintamallista ja sitä ohjaavasta tietoturvatapahtumien hallintapolitiikasta. Hallintamallin tulee sisältää yksityiskohtaiset toimenpiteet, prosessit ja informaatio, joka liittyy tietoturvatapahtumien hallintamallin viiteen päävaiheeseen. (SFS ISO/IEC 27035 2011, 13). Hallintamallin tulisi sisältää dokumentaatio kaikista lomakkeista, ohjeista, proseduureista, organisaation osista ja työkaluista, jotka liittyvät tietoturvatapahtumien hallintaan. Dokumentaatioon tulisi kuulua lomakkeet ja käsittelyohjeet tietoturvaherätteiden, -tapahtumien ja -haavoittuvuuksien raportointiin ja tietoturvatapahtumien arviointiin käytettävät luokittelu- (classification scale) ja kategorisointiasteikot (categorization scale). Hallintamallin tulisi sisältää suunnitelma ISIRTin käynnistämisestä ja dokumentit ISIRTin prosesseista, toimintaohjeista, resursseista ja vastuista. On myös tärkeää luoda sisäiset ja ulkoiset kontaktit, joita tarvitaan tietoturvaherätteiden, -tapahtumien ja -haavoittuvuuksien hallintaan. (SFS ISO/IEC 27035 2011, 8-9.)

Hallintamalliin sisällön tulee käsitellä myös organisaation käytössä olevia työkaluja, tukitoimintoja ja -mekanismeja, jotka voivat auttaa tietoturvatapahtumien hallinnassa. Näitä ovat esimerkiksi turvallisuusauditoinnit ja -arvioinnit, haavoittuvuuksien

hallinta ja haavoittuvuuksiin liittyvien ohjelmistopäivitysten tekeminen, teknologian seuranta uusien haavoittuvuuksien havaitsemiseksi, tunkeutumisen havaitsemisjärjestelmät, tietoverkkojen monitorointi- ja suojauslaitteistot sekä virusohjelmistot. (SFS ISO/IEC 27035 2011, 8-9.)

Hallintamallin tulisi sisältää myös suunnitelma, kuinka organisaation tietoisuutta lisätään tietoturvaherätteiden, -tapahtumien ja -haavoittuvuuksien hallinnasta koulutusten ja tiedotustilaisuuksien avulla. Hallintamallin tulisi ottaa myös kantaa kuinka hallintamallia ja siihen liittyviä prosesseja ja toimintaohjeita voidaan testata ja arvioida. (SFS ISO/IEC 27035 2011, 10.)

Ennen tietoturvatapahtumien hallintamallin mukaisen toiminnan aloittamista on organisaation varmistettava, että proseduurit on dokumentoitu, tarkistettu ja saatavilla. Jokaisen proseduurin tulee sisältää vastuulliset tahot proseduurien toteuttamiseen ja hallintaan. Proseduurit sisältävät ISIRTin ja kontaktipisteen lisäksi kaikki asianomaiset tahot, jotka osallistuvat tietoturva-analyysiin ja kriisitoimenpiteisiin. (SFS ISO/IEC 27035 2011, 15-16.)

Dokumentoitujen proseduurien tulisi olla linjassa tietoturvatapahtuminen hallintamallin kanssa. Kaikkien menettelytapojen ei tarvitse olla julkisia. Tietoturvatapahtumien hallintamallin yksityiskohtien paljastuminen saattaa mahdollistaa tutkinnan vaikeuttamisen ja oleellisen tiedon salaamisen. Esimerkiksi organisaation henkilökunnan ei tarvitse välttämättä tietää ISIRTin sisäisiä toimintatapoja, jotta he voivat kommunikoida heidän kanssaan. ISIRTin tulee kuitenkin varmistaa, että tietoturvatapahtumien hallinnasta on saatavilla neuvontaa ja ohjeita esimerkiksi yrityksen intranetissä. (SFS ISO/IEC 27035 2011, 16–17.)

ISIRTillä on keskeinen rooli organisaation tietoturvallisuudessa. On erittäin tärkeää että ISIRTillä on organisaation ja ulkoisten toimijoiden luottamus. Organisaation tulee varmistaa, että tietoturvatapahtumien hallintamalli ottaa huomioon tilanteet ja organisaatio luo säännökset, joissa tietoturvatapahtumista ilmoittavien henkilöiden yksityisyyden suoja voidaan varmistaa. (SFS ISO/IEC 27035 2011, 17.)

Tietoturvatapahtumien hallintaan liittyvä informaatio saattaa sisältää salassa pidettävää tietoa. Organisaation tulisi varmistaa menetelmät arkaluontoisen tiedon suojaamiseksi ja vaatia luottamuksellista tietoa käsitteleviä henkilöitä allekirjoittamaan salassapitosopimukset. Organisaation tulisi varmistaa, että tietoturvatapahtumien malli ottaa kantaa, kuinka tietoturvatapahtumista ja haavoittuvuuksista tiedotetaan ulkoisille tahoille, kuten yhteistyökumppaneille, medialle, lainvalvontaorganisaatioille ja suurelle yleisölle. (SFS ISO/IEC 27035 2011, 17-18.)

4.5.3 Tietoturvatapahtumien hallintamallin koulutus ja testaus

Koulutuksen ja tietoisuuden lisäämisen suunnittelu ja kehittäminen on tärkeää organisaatiossa. Organisaation jäsenille tulee kouluttaa tieturvaherätteiden, -tapahtumien ja -haavoittuvuuksien hallintasuunnitelma. Organisaation jäsenten tulee tietää kuinka tietoturvaherätteistä, -tapahtumista ja -haavoittuvuuksista tulee ilmoittaa. Koulutustilaisuuksia tulee järjestää säännöllisesti ja ylläpitää tietoisuutta tietoturvatapahtumien hallinasta henkilövaihdosten varalta.
(SFS ISO/IEC 27035 2011, 20-21.)

Tietoturvatapahtumien hallintasuunnitelma tulee testata prosessien ja proseduurien osalta. Testaamisessa ei tulisi keskittyä vain todellisten tilanteiden testaamiseen vaan myös varmistaa kuinka ISIRT toimii paineen alla useiden samanaikaisten tietoturvatapahtumien ilmaantuessa. Testaukset tulisi suorittaa säännöllisesti. Erityistä

huomiota tulisi kiinnittää todellisia uusia tietoturvauhkia käsittelevien testien luomiseen. (SFS ISO/IEC 27035 2011, 21.)

4.5.4 Luokittelu- ja kategorisointiasteikko

Tietoturvatapahtumien hallintamallin tulisi sisältää luokitteluasteikko (classification scale) ja kategorisointiasteikko (categorization scale), joiden avulla tietoturvatapahtumia voidaan arvioida. Näiden asteikkojen avulla on mahdollista helpottaa ja automatisoida tietoturvatapahtumien kirjaamista, arviointia ja vastatoimia, parantaa tietoturvatapahtumien hallinnan tehokkuutta ja tunnistaa tietoturvatapahtumien vakavuusaste johdonmukaisin perustein (SFS ISO/IEC 27035 2011, 50.) Taulukossa 4 on nähtävissä tietoturvatapahtumien kategoriat, kuvaukset ja esimerkkejä tietoturvatapahtumasta. Kategorisointi ei ole kattava, vaan esimerkinomainen. Organisaation tulee muokata kategoriat käyttöönsä sopiviksi.

Taulukko 4. Tietoturvatapahtumien kategoriat

(SFS ISO/IEC 27035 2011, 52-53).

Tietoturvatapahtumat		
Kategoria	**Kuvaus**	**Esimerkkejä**
Luonnononnettomuus	Tietoturvallisuuden vaarantuminen on aiheutunut luonnon-onnettomuudesta.	Maanjäristys, tulivuorenpurkaus, tulva, myrsky, salama, tsunami yms.
Sosiaalinen levottomuus	Tietoturvallisuuden vaarantuminen on aiheutunut yhteiskunnan epävakaudesta.	Terrorismi, sota, politiikka yms.
Fyysinen vikaantuminen	Tietoturvallisuuden vaarantuminen on aiheutunut tahallisesta tai tahattomasta fyysisestä toiminnasta.	Tulipalo, vesivahinko, ympäristötekijät (saasteet, kuumuus, jäätyminen), laitteen tai tiedon tuhoutuminen, varkaus yms.

Infrastruktuurin vikaantuminen	Tietoturvallisuuden vaarantuminen on aiheutunut infrastruktuurin vikaantumisesta.	Virran syötön, ilmastoinnin tai vedenjakelun vikaantuminen yms.
Säteilyn aiheuttama häiriö	Tietoturvallisuuden vaarantuminen on aiheutunut säteilystä.	Sähkömagneettinen säteily tai pulssi, lämpösäteily, sähköinen häirintä, jännitevaihtelu yms.
Tekninen vika	Tietoturvallisuuden vaarantuminen on aiheutunut teknisestä viasta.	Laitevika, ohjelmistovika, ylikuormitus yms.
Haittaohjelma	Tietoturvallisuuden vaarantuminen on aiheutunut haittaohjelmasta.	Virus, mato, troijalainen hevonen, muu haittaohjelma yms.
Tekninen hyökkäys	Tietoturvallisuuden vaarantuminen on aiheutunut hyökkäyksestä tietojärjestelmiä tai tietoverkkoja vastaan.	Verkkoskannaus, haavoittuvuuksien hyödyntäminen, takaovien käyttö, kirjautumisyritykset, palvelunestohyökkäykset, häirintä yms.
Sääntöjen rikkominen	Tietoturvallisuuden vaarantuminen on aiheutunut tahallisesta tai tahattomastasääntöjen rikkomisesta.	Luvaton resurssien käyttö, tekijänoikeusrikkomukset yms.
Väärinkäytös	Tietoturvallisuuden vaarantuminen on aiheutunut tahallisesta tai tahattomasta väärinkäytöksestä.	Käyttöoikeuksien väärinkäyttö tai väärentäminen, suorittujen toimenpiteiden kieltäminen yms.
Tiedon vaarantuminen	Tietoturvallisuuden vaarantuminen on aiheutunut tahallisesta tai tahattomasta informaation eheyden, saatavuuden tai luottamuksellisuuden vaarantamisesta.	Salakuuntelu, vakoilu, tiedon sieppaaminen, varastaminen, kalastelu tai paljastaminen, käyttäjän manipulointi, tahaton tietovirhe tietoa käsiteltäessä yms.
Haitallinen sisältö	Tietoturvallisuuden vaarantuminen on aiheutunut ei-toivottavan sisällön paljastamisesta.	Laiton sisältö, haitallinen sisältö, loukkaava sisältö, paniikin lietsonta, syytökset yms.
Muut	Tapahtumaa ei ole kategorisoitu	

Tietoturvatapahtumien luokitteluasteikolla pyritään arvioimaan tietoturvatapahtuman vaikutuksia (impact) ja kiireellisyyttä (urgency). Kirjassa ITIL Service Operation (2007) esitellään tapahtumien priorisointiin yksinkertainen malli, jossa otetaan huomioon kuinka kiireellisesti organisaation liiketoiminta tarvitsee ratkaisun tapahtumaan ja vaikutukset, jotka tapahtuma aiheuttaa. Tapahtumien luokittelu ei ole välttämättä yksinkertaista, sillä arviointiin vaikuttaa esimerkiksi tapahtuman aiheuttamat riskit henkilöille, vaikutusten alaisten palvelujen lukumäärä, liiketoiminnan taloudelliset tappiot ja lait tai viranomaismääräykset. (ITIL version 3 Service Operation 2007, 51.)

Taulukossa 5 tapahtumalle annetaan vaikutuksen ja kiireellisyyden perusteella tapahtuman prioriteettia kuvaava numero. Prioriteettinumeron perusteella organisaatio osaa arvioida kuinka nopeasti tapahtumaan tulee löytää ratkaisu.

Taulukko 5. Luokitteluasteikko

(ITIL version 3 Service Operation 2007, 51.)

	Impact	High	Medium	Low
Urgency				
High		1	2	3
Medium		2	3	4
Low		3	4	5

Priority code	**Description**	**Resolution time**
1	Critical	1 hour
2	High	8 hours
3	Medium	24 hours
4	Low	48 hours
5	Planning	Planned

ISO/IEC27035-standardi esittelee standardin liitteessä ANNEX C erilaisia malleja tietoturvatapahtumien luokitteluun. Ensimmäisessä liitteen mallissa arviointi perustuu tietojärjestelmän tärkeyteen, liiketoiminnan tappioon ja sosiaalisiin vaikutuksiin. Luokitteluperusteiden pohjalta on luotu neliportainen asteikko, jolla kuvataan tapahtuman kiireellisyyttä. (SFS ISO/IEC 27035 2011, 52-55.) Asteikko on jaettu seuraavasti:

- Erittäin vakava (luokka IV)
- Vakava (luokka III)
- Vähemmän vakava (luokka II)
- Vähäinen (luokka I)
  (SFS ISO/IEC 27035 2011, 55.)

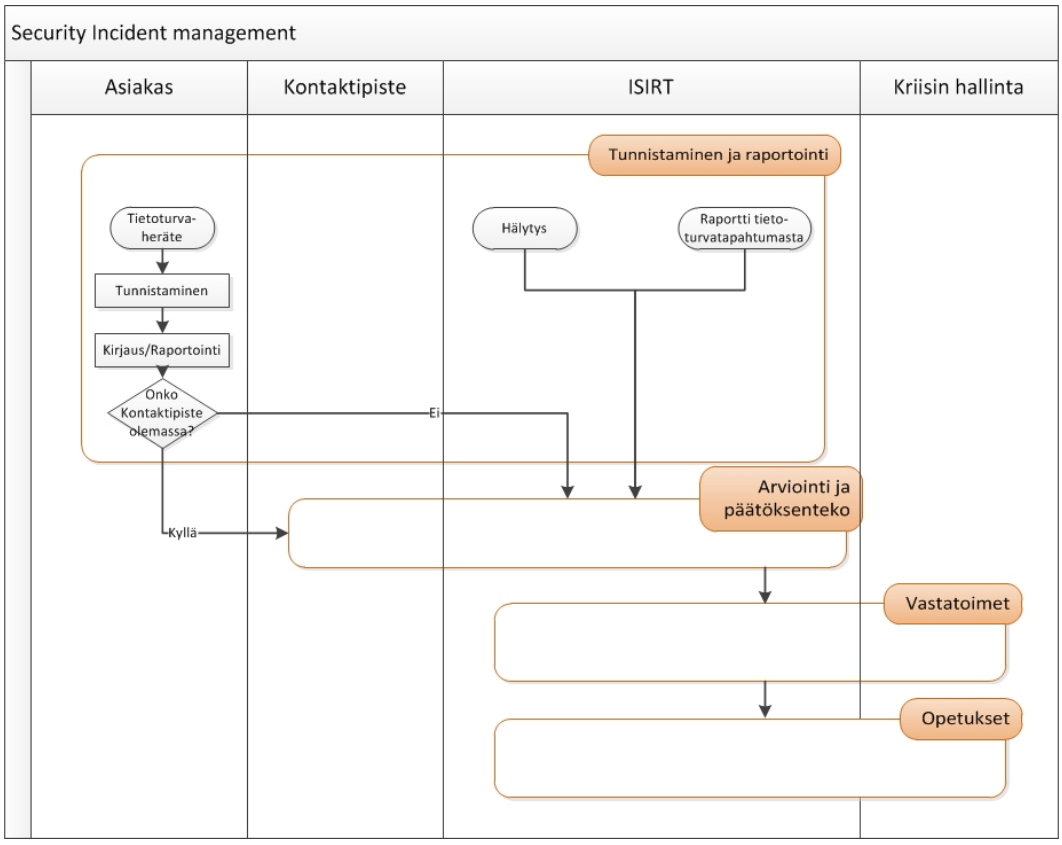
Standardi korostaa, että luokittelu on vain esimerkinomainen. Usein luokittelussa yhdistetään kategorisointi ja vakavuuden arviointi. Mallissa jokaiselle tietoturvatapahtuman kategorialle voi olla oma vakavuusasteikkonsa. Tietoturvatapahtuman vakavuusluokkaan vaikuttaa myös tapahtuman luonne. Tietoturvatapahtuma voi olla esimerkiksi tahallinen tai kohdennettu. (SFS ISO/IEC 27035 2011, 55-56.)

ISO/IEC27035-standardin liitteessä ANNEX C esiteltävä toinen luokittelumalli on huomattavasti monimutkaisempi. Mallissa arviointi perustuu osa-alueisiin, jotka ovat liiketoiminnan tappiot ja häiriö liiketoiminnalle, kaupalliset ja taloudelliset edut, henkilötiedot, lakisääteiset velvollisuudet, johtaminen ja liiketoiminta ja liikearvo tai mainearvo (goodwill). Mallissa jokainen tapahtumaan liittyvä osa-alue arvioidaan ja sille määritettään vakavuusasteikon perusteella numeerinen arvo, joka toimii pohjana tapahtuman kriittisyyden arvioinnille. (SFS ISO/IEC 27035 2011, 56-61.)

4.6 Tunnistaminen ja raportointi

4.6.1 Yleistä

Tunnistaminen ja raportointi ovat tietoturvatapahtumien hallinnan ensimmäinen operatiivinen vaihe. Toisessa vaiheessa tietoturvaheräte arvioidaan ja päätetään, onko kyseessä tietoturvatapahtuma. Kolmannessa vaiheessa tietoturvatapahtumalle suoritetaan vastatoimenpiteet ja neljänneksi tunnistetaan ja tutkitaan mitä on opittu. Kuviossa 10 esitetään tunnistaminen ja raportointi -vaiheen liittyminen muihin tietoturvatapahtumien hallinnan vaiheisiin.



Kuvio 10. Tunnistaminen ja raportointi

4.6.2 Tunnistaminen

Ensimmäisessä tietoturvatapahtumien hallinnan operatiivisessa vaiheessa organisaation tulisi tunnistaa ja raportoida tietoturvaherätteen tai tietoturvahaavoittuvuuden esiintyminen. Tietoturvaherätteitä tai -haavoittuvuuksia voidaan huomata automaattisesti tai organisaation henkilökunnan toimesta. Tietoturvaherätteiden tunnistus voi tapahtua henkilökunnan havaitessa jotain arveluttavaa tai huomiota herättävää. Heräte voi liittyä tekniikkaan, fyysiseen turvallisuuteen tai toimintatapoihin. Tunnistus voi tapahtua esimerkiksi palohälyttimestä osoituksena mahdollisesta tulipalosta. Murtohälyttimen luoma heräte voi kertoa mahdollisesta henkilön tunkeutumisesta organisaation tiloihin. (SFS ISO/IEC 27035 2011, 23-25.)

Herätteiden ja haavoittuvuuksien havaitsemiseen on monia eri tapoja. Herätteitä ja haavoittuvuuksia voidaan havaita esimerkiksi hälytyksinä monitorointijärjestelmistä, tunkeutumisen havaitsemis- tai estojärjestelmistä, antivirusohjelmistoista, tietoturvan hallintajärjestelmistä tai analysoimalla eri laitteiden ja palvelujen lokitietoja. On mahdollista käyttää myös niin kutsuttuja hunajapurkkeja (honey pot), joissa tarjotaan tarkoituksellisesti kiinnostavaa tai arvokasta sisältöä. Sisällöstä ei ole kuitenkaan hyötyä hyökkääjälle. Tarpit-järjestelmillä pyritään hidastamaan tai paljastamaan mahdollisia hyökkäyksiä. (SFS ISO/IEC 27035 2011, 24.)

Tietoturvaherätteistä voidaan saada tietoa myös palvelujen käyttäjiltä, palveluntuotannosta tai asiakaspalvelupisteistä. Kolmannet osapuolet, kuten tietoturvaviranomaiset, tietoliikenneoperaattorit, tietoturvapalveluita tarjoavat yritykset, muut ISIRTit ja ulkoistetut sidosryhmät julkaisevat ilmoituksia havaituista tietoturvahaavoittuvuuksista. Herätteiden havaitsemiseen voi osallistua myös media, sanomalehdet, televisio tai web-sivustot, jotka liittyvät tietoturvallisuuteen tai tietoturvan tutkimukseen. (SFS ISO/IEC 27035 2011, 24-25.)

4.6.3 Herätteen raportointi

Ensimmäisen operatiivisen vaiheen toimintoja ovat informaation kerääminen tietoturvaherätteestä tai -haavoittuvuudesta ja toimenpiteiden, päätösten ja ratkaisujen kirjaaminen myöhempää analysointia varten kontaktipisteessä. Tässä yhteydessä tulisi myös kerätä sähköinen todistusaineisto ja säilyttää se turvallisesti. (SFS ISO/IEC 27035 2011, 24.)

Kaikki informaatio tietoturvaherätteistä, -tapahtumista ja -haavoittuvuuksista tulisi tallentaa ISIRTin ylläpitämään tietokantaan. Kunkin tapauksen raportoitu informaatio tulisi olla mahdollisimman täydellistä, jotta se voi toimia perustana myöhemmin tapahtuvalle arvioinnille, päätöksenteolle ja toimenpiteille. (SFS ISO/IEC 27035 2011, 24.)

Herätteen raportointiin tulisi olla selkeät käytännöt ja tarvittavat raportointikeinot tietoturvatapahtumien hallintamallin mukaisesti. Ohjeet raportoinnin suorittamiseen tulisi olla henkilökunnan tiedossa ja saatavilla. Ohjeiden tulisi sisältää lomake herätteestä raportointiin ja tiedot kontaktipisteestä, johon raportointi suoritetaan. Herätteen havaitsijan tulee saattaa raportti kontaktipisteen tietoon, joka ennalta laaditun ohjeistuksen mukaisesti aloittaa herätteen ja raportin käsittelyn. Jos heräte sisältää poikkeuksellisen arkaluontoista tietoa, tulee organisaatiolla olla valmius käsitellä tietoa siten, että tiedon luottamuksellisuus ei vaarannu. (SFS ISO/IEC 27035 2011, 25.)

On tärkeää saada raportteja ja vihjeitä mahdollisista herätteistä, vaikka tiedot raporteissa eivät olisi täydellisiä. Raportoinnin keinona voi toimia paperinen lomake, sähköposti tai web-lomake. Kun ISIRT ottaa vastaan raportin ja kirjaa herätteen omaan tietoturvaherätteiden, -tapahtumien ja -haavoittuvuuksien hallintajärjestelmään, ISIRT täydentää raportin. (SFS ISO/IEC 27035 2011, 26.)

Aina kun mahdollista, olisi hyvä käyttää automatisoitua järjestelmää johon herätteet ja tapahtumat voidaan kirjata ja seurata niiden käsittelyä. Tietoturvaherätteiden, -tapahtumien ja -haavoittuvuuksien hallintajärjestelmän etuna on, että herätteen käsittelijä voi seurata tiettyä kaavaa tai tarkistuslistaa raportin kirjaamisessa. (SFS ISO/IEC 27035 2011, 26.)

Opinnäytetyön liite 1, Lomake tietoturvaherätteestä, havainnollistaa millaisia tietoja tietoturvaherätteestä tulisi raportoida. Lomakkeelle tulee kirjata herätteen tapahtuma-aika ja antaa tapahtumalle yksilöllinen tunnistamista helpottava tunnistenumero. Lomakkeelle tulee tallentaa myös ilmoittajan yhteystiedot, kuvaus mitä, kuinka ja miksi on tapahtunut, arvio herätteen vaikutuksessa olevista suojattavista kohteista ja arvio mahdollisista haitoista liiketoiminnalle. Raporttiin tulee täydentää myös herätteen yksityiskohtia.

Opinnäytetyön liite 2, Lomake tietoturvatapahtumasta, havainnollistaa millaisia tietoja tietoturvatapahtumasta tulisi raportoida. Lomakkeella pyydetään kirjaamaan samankaltaisia tietoja kuin lomakkeelle tietoturvatapahtumasta. Lomakkeelle tulee kirjata myös tietoturvatapahtuman kategoria, jolla pyritään ryhmittelemään tietoturvatapahtuma. Tietoturvatapahtuman vaikutuksessa olevat suojattavat kohteet tulee myös arvioida ja täydentää lomakkeelle. Tapahtuman vaikutuksia ja kustannuksia tulee arvioida ja luokitella organisaation luokitteluasteikon mukaisesti. Lopuksi kirjataan tapahtuman ratkaisuun liittyvät yksityiskohdat, tapahtumaan osalliset tahot, tapahtuman motiivit, jatkotoimenpiteet ja johtopäätökset, sekä tietoturvatapahtumasta tiedotetut tahot.

ISO/IEC27035-standardi (2011) käyttää tietoturvatapahtumien käsittelyssä termejä raportti (report) ja tietoturvaheräte, -tapahtuma ja -haavoittuvuustietokanta (information security event/incident/vulnerability database), minne raportit tallennetaan.

Standardi suosittaa myös tietojärjestelmien käyttöä raporttien hallintaan. Opinnäytetyössä käytetään jatkossa raportti sanan tilalla sanaa tiketti ja tietoturvaheräte, -tapahtuma ja -haavoittuvuustietokannan tilalla sanaa tiketöintijärjestelmä. Tiketillä kuvataan raportin sähköistä vastinetta, johon kaikki tiedot tietoturvaherätteestä, -tapahtumasta tai -haavoittuvuudesta kirjataan. Tiketit tallennetaan tiketöintijärjestelmään.

ISIRTissä tulisi olla vuororooli, joka on vastuussa herätteiden ja tikettien käsittelystä ja päättää jatkotoimenpiteistä. Tietoja herätteistä voidaan saada esimerkiksi sähköpostitse, puhelimitse tai ISIRTille osoitetuilla raporteilla. (SFS ISO/IEC 27035 2011, 26.)

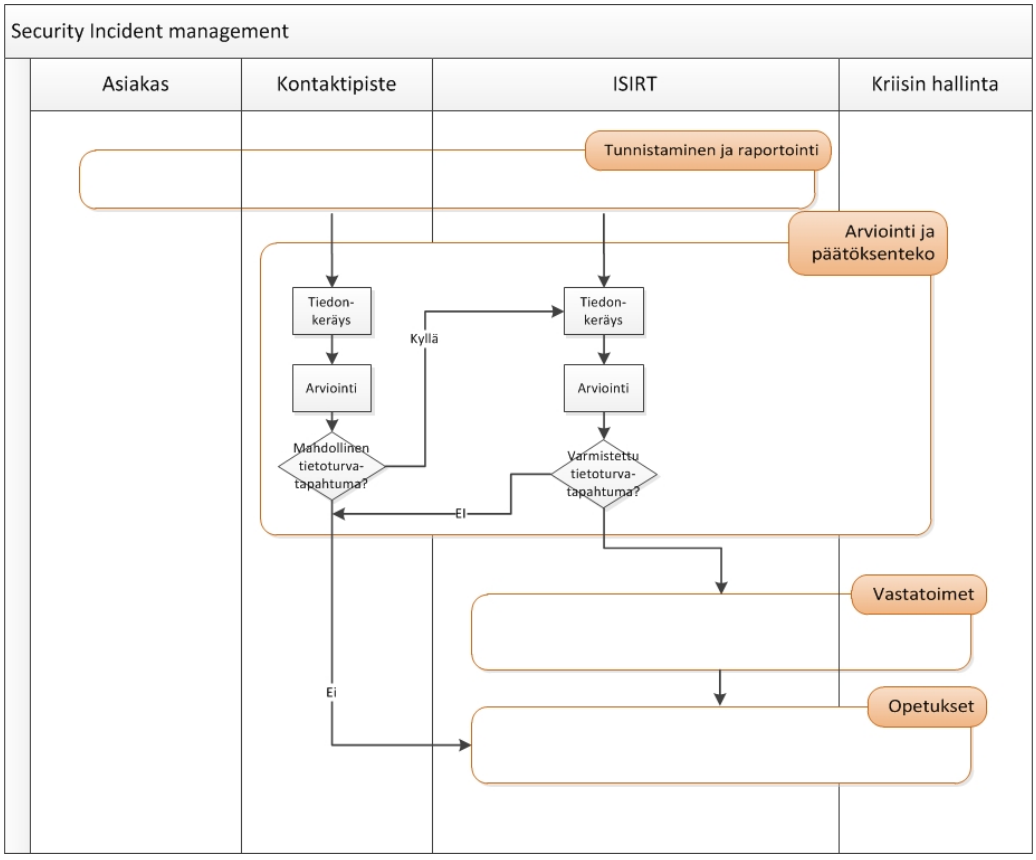
Raportoinnissa tietojen oikeellisuuden lisäksi merkittävä asia on oikea-aikaisuus. Raportointia ei tule viivyttää sillä perusteella, että tiketin sisältöä tulisi parantaa laadullisesti. Jos kaikesta informaatiosta ei olla varmoja, tulisi se mainita tiketissä ja täydentää tietoja mahdollisesti myöhemmin. On myös mahdollista, että raportointimekanismit tai hallintajärjestelmät joutuvat itse hyökkäyksen kohteeksi, jolloin tulisi käyttää vaihtoehtoisia kommunikointitapoja. Vaihtoehtoisia keinoja, kuten puhelinta, tekstiviestejä tai suoria keskusteluja tulisi käyttää erityisesti silloin kun on syytä olettaa, että kyseessä on tietoturvatapahtuma, joka on mahdollisesti merkittävä. (SFS ISO/IEC 27035 2011, 26)

On mahdollista, että tietoturvatapahtuma voidaan ratkaista paikallisia resursseja käyttäen paikallisen johdon avustuksella. Johdon tulisi olla tietoinen ISIRTin arviointi- ja toimintatavoista. On tärkeää estää päällekkäinen työ ISIRTin kanssa ja tiedottaa heitä tapahtuneesta ja kirjata tapahtuma tiketöintijärjestelmään. On mahdollista, että heräte tulkitaan myös vääräksi hälytykseksi. Myös väärät hälytykset on syytä kirjata ISIRTin käyttämään tiketöintijärjestelmään. (SFS ISO/IEC 27035 2011, 26.)

4.7 Arviointi ja päätöksenteko

4.7.1 Yleistä

Toinen operatiivinen vaihe tietoturvatapahtumien hallintaprosessissa on herätteeseen liittyvän tiedon arviointi ja tarvittaessa tietoturvaherätteen luokittelu tietoturvatapahtumaksi. Vaiheen aikana kontaktipiste kerää ja arvioi tarvittavat tiedot. Mahdollinen tietoturvatapahtuma ohjataan ISIRTille joka vahvistaa kontaktipisteen tekemät arviot oikeiksi tai suorittaa uuden arvioinnin. Kuviossa 11 esitetään kuinka arviointi ja päätöksenteko -vaihe liittyy tietoturvatapahtumien hallintamallin muihin vaiheisiin.



Kuvio 11. Arviointi ja päätöksenteko

Arviointi ja päätöksenteko vaiheen aikana voi olla tarpeellista myös siirtää tapahtuman käsittely seuraavalle tasolle (escalation) tehdyn arvioinnin perusteella. (SFS ISO/IEC 27035 2011, 26.) Eskaloinnilla tarkoitetaan tässä yhteydessä esimerkiksi tilanteen kärjistyessä tapahtuman käsittelyn siirtämistä kriisin hallinnasta vastaaville tahoille tai organisaation johdolle. Tämä vastuun siirto voidaan tehdä missä tilanteessa tahansa tehtyjen arvioiden perusteella.

Kaikki kerätty tieto tietoturvaherätteistä, -tapahtumista tai haavoittuvuuksista, suoritetut toimenpiteet ja tehdyt päätökset tulisi tallentaa ISIRTIn ylläpitämään tiketöintijärjestelmään parhaan arvioinnoin ja päätöstenteon varmistamiseksi. Sähköisen todistusaineiston kerääminen ja turvallinen säilytys on varmistettava. Todistusaineiston säilytystä tulisi valvoa, jos oikeustoimille tai sisäisille kurinpitotoimenpiteille ilmenee tarvetta. (SFS ISO/IEC 27035 2011, 26.)

4.7.2 Kontaktipisteen suorittama arviointi ja alustava päätöksenteko

Kontaktipisteen tulee vastaanottaa ilmoitus tietoturvaherätteestä ja kirjata se tiketöintijärjestelmään ja tarkistaa kirjaus. Ilmoittajalta tulee saada selvitys tapahtuneesta ja kerätä kaikki saatavilla oleva tieto. Kontaktipisteen tulee suorittaa arvio, onko heräte tietoturvatapahtuma vai onko kyseessä väärä hälytys. Arvioinnin tulee sisältää herätteen tai tapahtuman luokittelu organisaation luokitteluasteikon mukaisesti. Arvioitaessa herätteen tai tapahtuman aiheuttamaa vaikutusta palveluille tai suojattaville kohteille, on syytä tarkastella vaikutuksia luotettavuudelle, eheydelle ja saatavuudelle. Vaikutusten arvioinnissa tulisi tunnistaa herätteen tai tapahtuman vaikutukseen kuuluvat fyysinen tai looginen toimialue, suojattavat kohteet, infrastruktuuri, informaatio, prosessit, palvelut ja sovellukset. Kontaktipisteen tulisi tunnistaa myös herätteen tai tapahtuman aiheuttamat vaikutukset liiketoiminnan ydintoiminnoille. (SFS ISO/IEC 27035 2011, 26 -28.)

Tietoturvaheräte voi olla myös väärä hälytys. Tällöin herätteestä tallennuttu tiketti voidaan sulkea ja kirjata herätteen käsittelyn kulku tiketöintijärjestelmään. Herätteen käsittelyn päättäminen tiedotetaan ISIRTille, ilmoittajalle ja mahdollisesti ilmoittajan esimiehelle. (SFS ISO/IEC 27035 2011, 28.)

Todisteiden kerääminen on tässä vaiheessa tarpeellista mahdollisten juridisten tai kurinpidollisten toimien takia. Toimenpiteiden päivämäärä- ja aikatietojen lisäksi on tarpeellista kirjata mitä havaittiin ja tehtiin, todistusaineiston sijaintipaikka, miten todistusaineisto on saatu ja tallennettu, miten todistusaineiston vahvistus ja tarkistus on suoritettu ja todistusaineiston sijoituspaikan yksityiskohdat. (SFS ISO/IEC 27035 2011, 28.)

Jos tietoturvaheräte tunnistetaan mahdolliseksi tietoturvatapahtumaksi ja kontaktipisteen henkilöstöllä on riittävä osaaminen, voidaan tietoturvatapahtumaa arvioida syvällisemmin. Tunnistettaessa tietoturvaheräte erittäin merkittäväksi tietoturvatapahtumaksi tapahtuman käsittely voidaan siirtää esimerkiksi kriisin hallinnalle, ISIRTin tai organisaation johdolle. Kriisitilanteissa tulee toimia kriisienhallintasuunnitelman mukaisesti. Todennäköisin tilanne on, että tietoturvatapahtuma ohjataan ISIRTille arvioitavaksi ja jatkotoimenpiteitä varten. (SFS ISO/IEC 27035 2011, 28.)

Kontaktipisteen tulisi kirjata mahdollisimman paljon tietoa tiketille. Tiketille tulisi kirjata tiedot mikä tietoturvatapahtuma on, miten tietoturvatapahtuma aiheutui ja arvio vaikutuksista tai mahdollisista vaikutuksista. Tärkeää on tunnistaa myös kenen toimesta tapahtuma aiheutui ja mikä on tapahtuman kohde. Tiketille tulee kirjata myös arvio tapahtuman aiheuttamista vaikutuksista organisaation liiketoiminnalle käyttäen apuna organisaation tietoturvatapahtumien luokitteluasteikkoa. Tiketille tulee kirjata kaikki suoritetut toimenpiteet ja arviot. (SFS ISO/IEC 27035 2011, 29.)

Tietoturvatapahtuman mahdollisesti aiheuttamia vaikutuksia organisaation liiketoiminnalle voivat olla esimerkiksi luvaton tietojen luovuttaminen tai muuttaminen, palvelun tai tiedon saatavuuden estyminen tai tuhoutuminen ja palvelun suorituskyvyn alenema. Kun on arvioitu tietoturvatapahtuman aiheuttamia todellisia vaikutuksia organisaation liiketoiminnalle, voidaan tietoturvatapahtumalle suorittaa kategorisointi. Jos tietoturvatapahtuma ratkaistaan, tiketille on kirjattava tehdyt toimenpiteet ja mitä tapahtumasta opittiin. Tiketti tulee tallentaa ISIRTin käyttämään tiketöintijärjestelmään. (SFS ISO/IEC 27035 2011, 29.)

4.7.3 ISIRTin suorittama arviointi ja tapahtuman vahvistus

ISIRTin tulee ensimmäisenä kuitata kontaktipisteestä saatu tiketti vastaanotetuksi. ISIRTin tulee vahvistaa kontaktipisteen tekemän arvioinnin tulokset oikeiksi tai vääriksi ja suorittaa herätteen tai mahdollisen tapahtuman luokittelu uudelleen tietoturvatapahtumien luokitteluasteikon avulla. ISIRTin vahvistaessa tietoturvatapahtuman oikeaksi kirjataan mahdollisia täydentäviä tietoja tiketille. ISIRTin suorittamaan päätöksentekoon tulisi sisältyä priorisointi, jonka avulla muodostetaan näkemys kenelle tietoturvatapahtuman käsittely siirretään, kuinka kiireellistä tapahtuman käsittely on ja mitä seuraavassa vaiheessa vastatoimet, tekninen analyysi ja tiedotus pitävät sisällään. ISIRT arvioi lomakkeen sisällön ja pyytää tarvittaessa lisätietoja kontaktipisteeltä, tietoturvaherätteestä ilmoittaneelta henkilöltä tai muulta tarvittavalta taholta. (SFS ISO/IEC 27035 2011, 27-30.)

Tietoturvatapahtuma tulee verrata muihin ilmoitettuihin tietoturvaherätteisiin ja -tapahtumiin. On mahdollista, että tietoturvatapahtumat liittyvät toisiinsa. Vertailu on tärkeää myös tietoturvatapahtumien käsittelyn priorisoinnin kannalta. (SFS ISO/IEC 27035 2011, 30.)

Tietoturvatapahtuman ollessa todellinen ISIRTin tulee suorittaa tarkempi arviointi. ISIRTin tulee selvittää, mikä tietoturvatapahtuma on, kuinka se aiheutui ja kenen toimesta. ISIRTin on arvioitava minkälaisia vaikutuksia tai mahdollisia vaikutuksia tietoturvatapahtumalla on liiketoiminnalle. Näiden tietojen perusteella ISIRT pystyy arvioimaan tietoturvatapahtuman merkittävyyttä. Jos tietoturvatapahtuma aiheuttaa vakavia seurauksia, voi olla tarpeellista käynnistää kriisinhallinnan toimenpiteet. (SFS ISO/IEC 27035 2011, 30.)

Priorisoinnin perusteella ISIRTin tulee ohjata tietoturvatapahtuman käsittely parhaalle mahdolliselle henkilölle tai ryhmälle riittävän vastatoimen aikaan saamiseksi. Priorisointi on erittäin tärkeää varsinkin useiden yhtäaikaisten tietoturvatapahtumien aikana. Tapahtumien prioriteetit tulee asettaa liiketoimintaan liittyvien vaikutusten perusteella. Lisäksi tulee arvioida, kuinka suuri panostus tarvitaan vastatoimien suorittamiseen. (SFS ISO/IEC 27035 2011, 31.)

Jos tietoturvatapahtuma todetaan vääräksi hälytykseksi, se kirjataan tiketöintijärjestelmään. Tiketin ratkaisu lähetetään tiedoksi kontaktipisteelle, tapahtumasta ilmoittaneelle henkilölle ja hänen esimiehelleen. (SFS ISO/IEC 27035 2011, 30.)

4.8 Vastatoimet

4.8.1 Yleistä

Kolmannessa operatiivisessa vaiheessa tietoturvatapahtumien hallintamallissa suoritetaan vastatoimet tietoturvatapahtumalle, huomioon ottaen arviointi ja päätöksentekovaihe. Vastatoimet voivat olla reaaliaikaisia tai lähes reaaliaikaisia ja jotkut saat-

tavat vaatia rikosteknisen tietoturva-analyysin (security forensics analysis) suorittamisen. (SFS ISO/IEC 27035 2011, 31.)

ISIRTIn tulee ottaa selvää onko tietoturvatapahtuma hallinnassa. Tämä voi vaatia joko välittömän vastatoimenpiteen (immediate response), joka käynnistää palauttamistoimenpiteet ja tarvittaessa tiedottamisen tarvittaville tahoille tai pidempikestoisen vastatoimen (later response), jolla esimerkiksi varmistetaan palvelun palautuminen tapahtumasta. (SFS ISO/IEC 27035 2011, 31.)

Jos tietoturvatapahtuma ei ole hallinnassa ja tapahtumalla saattaa olla merkittäviä vaikutuksia organisaation ydintoimintoihin, tulee ISIRTin siirtää tapahtuman käsittely organisaation kriisinhallinnalle. Kriisinhallinasta vastaava taho on vastuussa tietoturvatapahtuman hallinnasta yhteistyössä ISIRTin kanssa kriisinhallintasuunnitelman mukaisesti. Kriisinhallinasta vastaavaan henkilökuntaan voi kuulua ISIRTIn lisäksi esimerkiksi kriisihallintajohtaja tai -ryhmä. (SFS ISO/IEC 27035 2011, 31.)

Organisaation on varmistettava, että tietoturvatapahtumaan vastaamiseen on osoitettu tarvittavat sisäiset ja ulkoiset resurssit. Vastatoimet- vaiheen aikana voi olla myös tarpeellista suorittaa rikostekninen tietoturva-analyysi (information security forensics analysis). (SFS ISO/IEC 27035 2011, 31.)

ISIRTin ja kaikkien osapuolten tulee tallettaa kaikki toimenpiteet myöhempää analyysiä varten tietoturvatapahtuman käsittelyyn liittyvälle tiketille. Kaikki saatu tieto tulee tallettaa mahdollisimman täydellisenä sen hetkisten tietojen perusteella. Tällä varmistetaan, että tieto voi toimia jatkossa pohjana arvioinneille, päätöksille ja toimenpiteille. Vastatoimet-vaiheen aikana tulee kerätä myös elektroninen todistusaineisto ja säilyttää todistusaineisto turvallisesti. Todistusaineiston säilyttämistä tulee

valvoa mahdollisten juridisten syytteiden tai sisäisen kurinpidon takia. (SFS ISO/IEC 27035 2011, 32.)

Vaiheen aikana tietoturvatapahtuman esiintymisestä ja sen tarpeellisista yksityiskohdista tulee tiedottaa mahdollisia suojattavien kohteiden omistajia sekä tarvittavia sisäisiä ja ulkoisia tahoja. Näitä henkilöitä saatetaan tarvita tietoturvatapahtuman ratkaisemisessa. (SFS ISO/IEC 27035 2011, 32.)

Kun tietoturvatapahtuma on määritetty ja vastatoimet sovittu, organisaation tulee jakaa vastuut tietoturvatapahtuman hallinnan vaatimista toimenpiteistä turvallisuudesta vastaavan henkilökunnan ja normaalin henkilökunnan välillä. Kaikille asianomaisilla tulisi pystyä osoittamaan proseduurit, joita he voivat seurata työvaiheiden aikana. Näitä työvaiheita ovat tapahtuman uudelleen tarkastelu, kehittäminen, vahingon uudelleen arviointi ja tarvittavien tahojen tiedottaminen.
(SFS ISO/IEC 27035 2011, 32.)

Organisaation tulisi päivittää tietoturvatapahtumiin liittyviä ohjeita tietoturvatapahtuman käsittelyn ja jatkokäsittelyn kannalta. Kun mahdollinen tietoturvatapahtuma on käsitelty onnistuneesti, tulee tapahtuma sulkea virallisesti ja tallettaa tiketöintijärjestelmään. Organisaation tulee varmistaa, että tässä vaiheessa suoritetaan vastatoimet myös havaituille tietoturvahaavoittuvuuksille. Tietoturvahaavoittuvuuden käsittely tulee myös tallentaa tiketöintijärjestelmään. (SFS ISO/IEC 27035 2011, 32.)

4.8.2 Välittömät vastatoimet

Useimmissa tapauksissa ISIRTin henkilökunnan jäsenen tehtävänä on tunnistaa välitön vastatoimenpide tietoturvatapahtumalle, tallentaa tietoturvatapahtuman yksityiskohdat tiketille ja tiedottaa tarvittavia tahoja, kuten esimerkiksi ISIRTin johtajaa.

Hätätapauksissa on mahdollista, että vaaditaan toimenpiteitä esimerkiksi tietoturvatapahtuman vaikutuksessa olevan tietojärjestelmän, palvelun tai verkkoelementin sammuttamiseksi. (SFS ISO/IEC 27035 2011, 32.)

Tietoturvatapahtuman merkittävyys tulee arvioida organisaation ennalta määritetyn luokitteluasteikon mukaisesti viimeistään tässä vaiheessa. Luokittelun perusteella voi olla tarpeellista tiedottaa yrityksen ylempää johtoa tapahtumasta tai ohjata käsittely kriisinhallinnalle. (SFS ISO/IEC 27035 2011, 33.)

Yleiset tavoitteet tietoturvatapahtuman vastatoimenpiteillä on rajoittaa mahdollisia tietoturvatapahtuman aiheuttamia vaikutuksia ja parantaa tietoturvaa. Ensisijainen tavoite tietoturvanhallinnan mallilla (scheme) ja siihen liittyvillä toimenpiteillä on minimoida tietoturvatapahtuman aiheuttamat vaikutukset liiketoiminalle. Toissijaisena tavoitteena voidaan pitää hyökkääjän tunnistamista. (SFS ISO/IEC 27035 2011, 32-33.)

Esimerkkinä välittömistä vastatoimista voidaan käyttää tilannetta, jossa tapahtuu tahallinen hyökkäys järjestelmää, palvelua tai verkkoa vastaan. Välitön vastatoimenpide voi olla hyökkäyksen kohteena olevan järjestelmän, palvelun tai verkon toimintaan jättäminen. Tämä mahdollistaa liiketoimintakriittisten palveluiden normaalin toiminnan ja mahdollistaa tiedon keräämisen hyökkääjästä siten, että hyökkääjä ei tiedä tarkkailusta. On erittäin tärkeää noudattaa ennalta suunniteltuja toimintatapoja ja ottaa huomioon, että hyökkääjä voi havaita, että häntä tarkkaillaan. Hyökkääjä saattaa aiheuttaa lisää vahinkoa hyökkäyksen kohteelle tai hävittää tietoja joiden avulla on mahdollista jäljittää hyökkääjä. On tärkeää valmistautua järjestelmän, palvelimen tai verkon nopeaan eristämiseen tai sammuttamiseen. (SFS ISO/IEC 27035 2011, 33.)

4.8.3 Tietojen päivitys tietoturvatapahtumasta

Mikä tahansa seuraava askel on, ISIRTin henkilökunnan jäsenen tulee päivittää tietoturvatapahtumatiketille kaikki mahdollinen tieto, lisätä se tiketöintijärjestelmään ja tiedottaa tarvittavia tahoja. Henkilökunnan tulisi pystyä vastaamaan seuraaviin kysymyksiin:

- mikä tietoturvatapahtuma on?
- miten tietoturvatapahtuma aiheutui, kenelle ja kenen toimesta?
- mitkä ovat vaikutukset tai mahdolliset vaikutukset?
- mitkä ovat vaikutukset organisaation liiketoiminnalle?
  (SFS ISO/IEC 27035 2011, 34.)

Lisäksi tietoturvatapahtuma luokittelua tulee uudelleentarkastella ja muuttaa luokittelua tarvittaessa. Tärkeää on myös kirjata tiketille tähän asti suoritetut toimenpiteet. Jos tietoturvatapahtuma ratkaistaan, tiketille tulee kirjata kaikkia tehdyt toimenpiteet ja mitä opittiin. ISIRT on vastuussa tietoturvatapahtumaan liittyvän tiedon säilyttämisestä tarkempaa analysointia varten ja mahdollisia juridisia toimenpiteitä varten. (SFS ISO/IEC 27035 2011, 34.)

4.8.4 Jatkotoimenpiteet

ISIRTin henkilökunnan varmistaessa tietoturvaherätteen olevan todellinen, tulee ISIRTin suorittaa tarvittaessa rikostekninen analyysi ja informoida tiedottamisesta vastaavia sisäisiä ja ulkoisia tahoja, mitä tietoja he voivat käyttää tietoturvatapahtumasta viestimiseen. ISIRTin tulisi ohjeistaa myös kenelle tiedot voi kertoa. Jos tietoturvatapahtuman käsittely kestää kauemmin kuin organisaatiossa on ennalta sovittu,

tulee ISIRTin laatia tilapäinen raportti (interim report) tietoturvatapahtumasta. (SFS ISO/IEC 27035 2011, 35.)

ISIRITIn jäsenten tulee tietää tietoturvatapahtumien hallintamalliin perustuen, milloin on tarpeellista siirtää tietoturvatapahtuman käsittely ylemmälle tasolle ja kenelle vastuun siirto tulee suorittaa. ISIRTIn tekemien toimenpiteiden jälkeen tulee suorittaa myös tarvittavat muutoshallinnan proseduurit. Etukäteen on hyvä perustaa myös viestintätavat siten, että kommunikointi ei vaarannu mahdollisesta tietoturvatapahtumasta johtuen. (SFS ISO/IEC 27035 2011, 35.)

4.8.5 Tietoturvatapahtuman hallintatilanteen arviointi

ISIRTin käynnistettyä välittömät vastatoimet, suoritettua rikosteknisen tietoturva-analyysin ja viestinnän, on nopeasti selvitettävä, onko tietoturvatapahtuma ISIRTin hallinnassa. Jos tietoturvatapahtuma on hallinnassa, ISIRTIn jäsenen tulee arvioida tarvitaanko myöhempiä vastatoimia, rikosteknistä tietoturva-analyysia tai viestintää tarvittaville tahoille, tietoturvatapahtuman päättämiseksi ja palvelun normaalin toiminnan palauttamiseksi. Jos tietoturvatapahtuma ei ole hallinnassa, tulee ISIRTIn jäsenen käynnistää kriisitoimenpiteet. (SFS ISO/IEC 27035 2011, 35.)

Tietoturvatapahtuma liittyessä menetettyyn saatavuuteen (availability), katkon kestoaika saattaa olla merkittävä mittarille sille, onko tilanne hallinnassa vai ei. Organisaation tulee määritellä suojattaville kohteille, riskianalyysien perusteella, mikä on hyväksyttävä keskeytyksen kesto kullekin suojattavalle kohteelle. Kun hyväksyttävä aika ylittyy, tietoturvatapahtuma ei ole enää mahdollisesti hallinnassa. (SFS ISO/IEC 27035 2011, 35.)

Tietoturvatapahtumat, jotka liittyvät luottamuksellisuuden tai eheyden menetykseen saattavat vaatia erilaista päätöksiä arvioitaessa, onko tietoturvatapahtuma hallinnassa. Tässä voidaan käyttää apuna kriisinhallintasuunnitelman mittareita. (SFS ISO/IEC 27035 2011, 36.)

4.8.6 Pitkäkestoiset vastatoimet

Tietoturvatapahtuman ollessa hallinnassa kriisitoimenpiteitä ei tarvita. ISIRTin tulee arvioida, mitä jatkotoimenpiteitä tietoturvatapahtuman käsittely vaatii. Nämä toimenpiteet saattavat sisältää vaikutuksen alaisena olleen tietojärjestelmän, palvelun tai verkon palauttamisen normaalin tilaan. Tiketille tulee tallentaa tiedot toimenpiteistä ja niiden suorittajista. Kun toimenpiteet on suoritettu, yksityiskohdat tulee päivittää tiketille, sulkea tiketti ja tiedottaa tietoturvatapahtuman käsittelyn lopettamisesta tarvittavia tahoja. (SFS ISO/IEC 27035 2011, 36.)

Pitkäkestoisia toimenpiteitä voivat olla esimerkiksi kriisinhallintasuunnitelman päivittäminen tiettyjen tietoturvatapahtumien osalta, IT-järjestelmän päivittäminen tunnetun tietoturvahaavoittuvuuden varalta tai valvonnan konfigurointi, jotta tietoturvaherätteet voidaan tunnistaa jatkossa oikein. (SFS ISO/IEC 27035 2011, 36.)

4.8.7 Vastatoimet kriisitilanteissa

ISIRTin tunnistaessa, että tietoturvatapahtuma ei ole hallinnassa, ISIRTin tulee käsitellä tapahtuma ennalta laaditun kriisinhallintasuunnitelman mukaisesti. Riskinhallintasuunnitelman tulisi sisältää parhaat vaihtoehdot tämän kaltaisten tietoturvatapahtumien käsittelyyn. Näiden toimenpiteiden tulisi liittyä suoraan organisaation liiketoiminnan prioriteetteihin, palautumisaikoihin ja kuinka pitkäkestoinen poikkeama voidaan sallia. Strategissa tulisi tunnistaa ennaltaehkäisevät ja kestävät krii-

sinhallinnan toimenpiteet, organisaatiorakenne ja vastuut kriisitilanteisiin vastaamiseen sekä rakenne ja hahmoteltu sisältö kriisihallintasuunnitelmalle. (SFS ISO/IEC 27035 2011, 36-37.)

Kriisinhallintasuunnitelma ja sitä tukevat testatut turvamekanismit muodostavat pohjan kriisinhallinnan tapahtumien käsittelylle ja mahdollistavat kärjistyneiden tietoturvatapahtumien käsittelyn. Kriisinhallinnan toimenpiteet voivat liittyä esimerkiksi tulipalon tukahduttamiseen ja evakuointiproseduureihin, pommin käsittelyyn ja evakuointiproseduureihin, tietojärjestelmiin liittyvien petosten tutkintaan tai teknisten hyökkäysten tutkintaan. (SFS ISO/IEC 27035 2011, 37.)

4.8.8 Rikostekninen tietoturva-analyysi

ISIRTin tulee aiemman arvion perusteella tarvittaessa suorittaa rikostekninen tietoturva-analyysi (Information security forensics analysis) todisteiden keräämiseksi. Sen tulisi pitää sisällään dokumentoitujen toimintatapojen mukaista IT-pohjaisten tutkintatekniikoiden ja työkalujen käyttöä tarkempien tietojen löytämiseksi. Proseduurit tulee suorittaa järjestelmällisesti ja tunnistaa, mitä voidaan käyttää todisteena sisäisissä tai juridisissa toimenpiteissä. (SFS ISO/IEC 27035 2011, 37.)

Rikosteknisen tietoturva-analyysin toimenpiteet tulee dokumentoida täysin. Dokumentoinnin tulee pitää sisällä esimerkiksi valokuvia, lokitietoja ja analyysejä. Informaatio tietoturvatapahtumasta, kuvaus rikosteknisen tietoturva-analyysin toimenpiteistä ja tallennusvälineet (media) tulee säilyttää fyysisesti turvallisessa ympäristössä. Pääsy tietoon tai tiedon muuttamiseen tulee estää. Analyysin suorittamiseen käytettävien standardien mukaisten työkalujen ja ISIRTin käyttämien fyysisten tilojen tulee olla sellaisia, ettei saatuja tuloksia voida kiistää juridisesti. (SFS ISO/IEC 27035 2011, 37.)

Rikosteknisen tietoturva-analyysin proseduurien päätarkoitus on varmistaa, että todisteet säilyvät eheinä ja todisteet ovat juridisesti päteviä. Rikostekninen tietoturva-analyysi tulee suorittaa alkuperäisen datan tarkalle kopiolle. Tällä voidaan estää analysointityön aiheuttama datan eheyden muuttuminen. (SFS ISO/IEC 27035 2011, 37-38.)

4.8.9 Viestintä

ISIRTin tunnistaessa tietoturvatapahtuman on usein tarpeellista viestiä sisäisesti ja ulkoisesti tietoturvatapahtumasta. Tiedottaminen voi olla aiheellista tietoturvatapahtuman käsittelyn eri vaiheissa, kuten tunnistettaessa tietoturvatapahtuma, saataessa tietoturvatapahtuma hallintaan, tapahtuman vaatiessa kriisinhallintaa, suljettaessa tietoturvatapahtuma ja johtopäätösten sekä jälkiselvitystyön valmistuttua. (SFS ISO/IEC 27035 2011, 39.)

Viestinnän ollessa tarpeellista on huolehdittava mitä viestitään ja mille sidosryhmälle. Sidosryhmiä voivat olla esimerkiksi:

- sisäiset sidosryhmät, kuten kriisinhallinta ja organisaation johto
- ulkoiset sidosryhmät, kuten asiakkaat, alihankkijat ja yhteistyökumppanit
- muut ulkoiset sidosryhmät kuten lehdistö tai muu media
  (SFS ISO/IEC 27035 2011, 39.)

Sidosryhmät saattaa tarvita erityistä tietoa, jonka pitäisi olla saatavissa organisaatiosta oikeita kanavia pitkin. Tärkeää on tiedon saannin turvaaminen sisäisille sidosryhmille ja tärkeimmille ulkoisille sidosryhmille. Näiden sidosryhmien tulee saada tietoa ennen kuin informaatio on saatavilla julkisesta mediasta. Tiedottamista voidaan val-

mistella laatimalla alustavia tiedotteita sidosryhmille sopiviksi. Viestinnän tulisi noudattaa organisaation tiedotuspolitiikkaa. (SFS ISO/IEC 27035 2011, 39.)

4.8.10 Vastuunsiirto tietoturvatapahtuman kärjistyessä

Äärimmäisissä olosuhteissa, kun tietoturvatapahtuma ei ole hallinnassa ja vaarat liiketoiminnalle ovat suuret, voi olla tarpeellista suorittaa vastuunsiirto (eskalointi). Tämän kaltaiset tietoturvatapahtumat tulee siirtää liiketoiminnan jatkuvuussuunnitelman mukaisesti joko ylemmälle johdolle, ryhmälle organisaation sisällä tai ulkoiselle ryhmälle. Vastuunsiirto tilanteen kärjistyessä voidaan suorittaa päätösten aikaansaamiseksi, suositeltujen toimenpiteiden tunnistamiseksi tai arvioiden saamiseksi, mitä toimenpiteitä tarvitaan. Ohjeistus vastuunsiirron suorittamisesta tietoturvatapahtuman kärjistyessä tulee sisällyttää tietoturvatapahtumien hallintamallin dokumentaatioon ja niiden organisaation jäsenten tietoon, jotka todennäköisesti joutuvat vastuunsiirron suorittamaan. Tämän kaltaisia organisaation osia ovat esimerkiksi ISIRT tai mahdollinen kontaktipiste. (SFS ISO/IEC 27035 2011, 39.)

4.8.11 Toimenpiteiden kirjaaminen ja muutoshallinta

Kaikkien tietoturvatapahtumien hallintaan osallistuvien tulisi tallentaa kaikki suoritetut toimenpiteet myöhempää analysointia varten. Tämä pitää sisällän tietoturvatapahtumasta muodostetun tiketin ajantasaisena pitämisen koko tietoturvatapahtuman käsittelyn ajan ja tiketin tallennuksen tiketöintijärjestelmään. Nämä tiedot tulee säilyttää turvallisesti ja suorittaa varmuuskopiointi asian mukaisesti. Muutokset tietoturvatapahtumien raportointiin ja tiketöintijärjestelmään tulee suorittaa virallisen muutoshallinnan mallin mukaisesti. (SFS ISO/IEC 27035 2011, 40.)

4.9 Opetukset

Neljäs operatiivinen vaihe käynnistyy tietoturvatapahtuman ratkaisemisen ja sulkemisen jälkeen tarkastelemalla, miten tapahtuma käsiteltiin ja hoidettiin. Organisaation on selvitettävä onko tarvetta lisätutkimuksiin, kuten rikosteknisen tietoturva-analyysin suorittamiseen. Tietoturvatapahtumista ja haavoittuvuuksista tulee tunnistaa se, mitä niistä on opittavissa. Opetuksien perusteella voidaan tunnistaa puutteet ja arvioida sekä parantaa olemassa olevia turvamekanismeja tai tietoturvapolitiikkoja. Myös uusien tietoturvamekanismien luominen tarvittaessa on mahdollista. (SFS ISO/IEC 27035 2011, 40.)

On tärkeää tunnistaa parannuskohteet sekä arvioida ja parantaa organisaation riskinarviointia ja -hallintaa. Opetukset-vaiheen aikana tulee myös arvioida kuinka tehokkaasti organisaatio, prosessit, proseduurit ja raportointitavat toimivat tietoturvatapahtumia käsiteltäessä. Parannuskohteet tulee tunnistaa ja parannukset tulee tehdä tietoturvatapahtumien hallintamalliin ja dokumentaatioon. Opetusten perusteella voi olla tarpeellista päivittää tietoturvaheräte, -tapahtuma ja haavoittuvuustietokantaa. Tuloksia saattaa olla tarpeellista arvioida ja käsitellä myös luotetuissa yhteisöissä (trusted community). (SFS ISO/IEC 27035 2011, 40.)

Tietoturvatapahtumien hallinnan toiminnot ovat toistuvia. Organisaation tulee tehdä jatkuvasti parannuksia tietoturvatapahtumista ja niihin vastaamisesta syntyvän tiedon perusteella. (SFS ISO/IEC 27035 2011, 40.)

4.9.1 Turvamekanismien kehittäminen

Tarkasteltaessa suljettuja tietoturvatapahtumia tai -haavoittuvuuksia voidaan havaita tarve muutoksille olemassa oleviin turvamekanismeihin tai tarve uusille turvameka-

nismeille. Kaikki uudet turvamekanismit eivät ole välttämättä taloudellisti tai toiminnallisesti toteutettavissa välittömästi, jolloin ne on huomioitava organisaation pitkän aikavälin suunnitelmissa. Esimerkkinä voidaan mainita uuden palomuurin hankinta. (SFS ISO/IEC 27035 2011, 41.)

Suositukset huomioon ottaen organisaation tulee ottaa käyttöön uudet tai päivitetyt turvamekanismit. Nämä voivat olla teknisiä tai fyysisiä turvamekanismeja ja saattavat vaatia laitteistopäivityksiä, henkilökunnan koulutuksia ja tietoturvaohjeiden ja standardien tarkastuksia. Organisaation tietojärjestelmien, palvelujen ja tietoverkkojen tulee olla säännöllisten haavoittuvuusarviontien kohteena. Organisaation tulee näiden arviointien pohjalta jatkuvasti parantaa organisaation tietoturvaa. (SFS ISO/IEC 27035 2011, 41.)

Tietoturvapoliitikoiden ja proseduurien jatkuva parantaminen tulee olla ISIRTIn pitkän tähtäimen tavoite. Mitkä tahansa puutteet tai häiriöt tietoturvatapahtumien hallintaprosessin aikana tulisivat käynnistää kehitystoimenpiteet. (SFS ISO/IEC 27035 2011, 41.)

4.9.2 Riskinarvioinnin ja -hallinnan kehittäminen

Tietoturvatapahtumien ja -haavoittuvuuden mahdollisista vaikutuksista ja vakavuudesta riippuen riskinarvioinnissa voi olla tarpeellista ottaa huomioon uusia uhkia ja haavoittuvuuksia. Riskinarvioinnin ja -hallinnan päivittämisen seurauksena voi olla tarpeellista ottaa käyttöön muuttuneita tai uusia turvamekanismeja. (SFS ISO/IEC 27035 2011, 41.)

4.9.3 Tietoturvatapahtumien hallintamallin kehittäminen

ISIRTin johtajan tai vastaavan tahon tulee arvioida kuinka tietoturvatapahtuman käsittelyssä ja vastatoimissa onnistuttiin. Analyysin tarkoituksena on selvittää, mitkä tietoturvatapahtumien hallintamallin osat toimivat hyvin ja mitä puutteita ja kehityskohteita havaittiin. (SFS ISO/IEC 27035 2011, 41.)

Tietoturvatapahtuman ollessa riittävän vakava, organisaatio voi järjestää arviointipalavereja, johon osallistuvat kaikki asianomaiset heti tapahtuman jälkeen, kun tapahtuma on vielä muistissa. Tapaamisessa tulisi arvioida toimivatko tietoturvatapahtumien hallintamallissa määritetyt proseduurit kuten oli tarkoitettu, onko olemassa proseduureja tai toimintatapoja, joilla tietoturvatapahtuma olisi havaittu paremmin ja tunnistettiinko proseduureja tai työkaluja, jotka olisivat auttaneet tapahtuman vastatoimissa. On myös hyvä arvioida onko olemassa proseduureja, jonka avulla tietoturvatapahtumasta olisi toivuttu nopeammin ja oliko viestintä tehokasta tarvittaville tahoille tietoturvatapahtuman tunnistamisen, raportoinnin ja vastatoimien aikana. (SFS ISO/IEC 27035 2011, 41.)

Organisaation on varmistettava, että tunnistetut kehityskohteet tarkistetaan ja perustellut muutokset suoritetaan tietoturvatapahtumien hallintamalliin. Muutokset tietoturvatapahtumien hallintaprosessiin, -proseduureihin ja raportointiin tulee tarkistaa ja testata ennen käyttöönottoa. (SFS ISO/IEC 27035 2011, 41.)

5 TIETOSUOJALAINSÄÄDÄNTÖ

Tietosuojan käsitettä on alettu käyttää Suomessa 1970-luvun alussa. Tietosuoja sisältää kansalaisten yksityisyyden suojan ja oikeusturvan huomioon ottamisen tietojen rekisteröinnissä ja tiedostojen suojaamisessa luvattomalta ulkopuoliselta käytöltä. Tietosuoja on käsitteenä laaja-alaisempi kuin yksityisyyden suoja. Tietosuojalla viitataan rekisterin pitoon ja tietojenkäsittelyn toiminnalliseen puoleen. (Andreasson & Koivisto 2013, 27). Tietotuojavaltuutetun toimisto määrittelee, että tietosuojaan kuuluu ihmisten yksityisyyden suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä (Sanastoa 2014).

Henkilötietojen käsittelyä ohjaa ja valvoo Suomessa tietosuojavaltuutettu. Tietosuojavaltuutetun tehtävät on määritelty henkilötietolaissa, sekä laissa tietosuojalautakunnasta ja tietosuojavaltuutetusta (Andreasson & Koivisto 2013, 27). Tietosuojavaltuutetun tehtävänä on käsitellä ja ratkaista henkilötietojen ja luottotietojen käsittelyä henkilötietolakiin (523/1999) ja luottotietolakiin(527/2007) perustuen, henkilötietojen ja luottotietojen käsittelyn yleinen seuraaminen ja aloitteiden tekeminen, toimialaan kuuluva tiedottaminen ja henkilötietojen kansainvälisestä yhteistyöstä huolehtiminen (L 22.4.1999/524, 5§).

Suomen perustuslaki määrittää yksityiselämän suojan (11.6.1999/731, 10§). Oikeutta yksityisyyden suojaan toteuttavat konkreettisella tavalla henkilötietolaki, henkilöstötietojen käsittelyä koskevat erityissäännökset, laki viranomaisten toiminnan julkisuudesta, laki yksityisyyden suojasta työelämässä, sähköisen viestinnän tietosuojalaki ja Euroopan unionin antamat tietosuojaa koskevat kansainväliset normit ja ohjeet (Lait 2014).

5.1 Henkilötietolaki

Henkilötietolain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä. Lain tarkoituksena on myös edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. (L 22.4.1999/523, 1§.)

Henkilötietolaki on henkilötietojen käsittelyn perustuslaki. Henkilötietojen käsittelyä koskevia erikoissäännöksiä sovelletaan ensisijaisena henkilötietolain kyseisiin säännöksiin nähden. (Henkilötietolaki 2014.)

Henkilötietolakia sovelletaan henkilötietojen automaattiseen käsittelyyn. Lakia sovelletaan myös silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. (L 22.4.1999/523, 2§).

Henkilötietolaissa säädetään myös henkilötietojen käsittelyä koskevista yleisistä periaatteista, arkaluonteisten tietojen ja henkilötunnuksen käsittelystä, henkilötietojen käsittelystä erityisiä tarkoituksia varten, henkilötietojen siirrosta Euroopan unionin ulkopuolelle ja rekisteröidyn oikeuksista. (L 22.4.1999/523)

5.2 Sähköisen viestinnän tietosuojalaki

Sähköisen viestinnän tietosuojalain tarkoitus on turvata sähköisen viestinnän luottamuksellisuus ja yksityisyyden suojan toteutuminen. Lain tarkoituksena on myös edistää sähköisen viestinnän tietoturvaa ja sähköisen viestinnän palvelujen tasapainoista kehittymistä. (16.6.2004/516, 1§.) Lailla selkeytetään luottamuksellisten tunnistetietojen käsittelysääntöjä, tietoturvan toteuttamismahdollisuuksia ja annetaan peli-

säännöt evästeiden käytölle ja paikkatietojen käsittelylle. Laki sisältää myös suoramarkkinointisäännöksiä ja säännökset käyttäjän ja poliisin tiedonsaantioikeuksista. (Tietosuojavaltuutetun toimisto 2014, sähköisen viestinnän tietosuojalaki). Tunnistamistiedolla tarkoitetaan tietoa tilaajaan tai käyttäjään yhdistettävästä tiedosta, joka viestintäverkossa käsitellään viestin siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. Paikkatiedolla tarkoitetaan tietoa, joka ilmaisee liittymän tai päätelaitteen maantieteellisen sijainnin ja jota käytetään muuhun tarkoitukseen kuin verkko- tai viestintäpalvelun toteuttamiseen. (16.6.2004/516, 2§.)

Sähköisen viestinnän tietosuojalakia sovelletaan yleisissä viestintäverkoissa tarjottaviin verkko-, viestintä- ja lisäarvopalveluihin sekä palveluihin, joissa käsitellään käyttöä kuvaavia tietoja. Lakia sovelletaan myös suoramarkkinointiin, tilaajaluettelopalveluihin ja numerotiedotuspalveluihin. (16.6.2004/516, 3§.)

Pääasiassa Viestintävirasto valvoo sähköisen viestinnän tietosuojalain ja sen nojalla annettujen määräysten noudattamista. Tietosuojavaltuutettu valvoo suoramarkkinointia, puhelinluetteloita, numerotiedotuspalveluista ja käyttäjien erityistä tiedonsaantioikeutta koskevien säännösten noudattamista. (Sähköisen viestinnän tietosuojalaki 2014.)

5.3 Teleyrityksen tietoturva

Teleyrityksellä tarkoitetaan verkkoyritystä tai palveluyritystä. Verkkoyrityksellä tarkoitetaan yritystä, joka tarjoaa omistamaansa tai hallussaan olevaa viestintäverkkoa käytettäväksi viestien siirtoon, jakeluun tai tarjolla pitoon. Palveluyrityksellä tarkoitetaan yritystä, joka siirtää viestejä hallussaan olevassa tai verkkoyritykseltä käyttöön

saadussa viestintäverkossa. Palveluyritys voi myös jaella tai pitää tarjolla viestejä joukkoviestinverkossa. (23.5.2003/393, 2§.)

Teleyrityksellä on velvollisuus huolehtia tietoturvasta. Velvollisuuden määrittelee sähköisen viestinnän tietosuojalaki. Palvelun ja käsittelyn tietoturvasta huolehtiminen tarkoittaa toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto-ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamista toimenpiteiden avulla. Nämä toimet tulee suhteuttaa uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin (16.6.2004/516, 19§.)

5.3.1 Toimenpiteet teleyrityksen tietoturvan toteuttamiseksi

Teleyrityksen tulee suorittaa toimenpiteitä tietoturvan toteuttamiseksi. Teleyrityksellä on oikeus ryhtyä välttämättömiin toimiin viestintäverkoille ja niihin liitetyille palveluille haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi. Teleyritys voi suorittaa välttämättömiä toimia myös viestintämahdollisuuksien turvaamiseksi ja viestintäpalvelujen kautta toteuttavien laajojen maksuvälinepetosten ehkäisemiseksi. Toimenpiteet voivat käsittää viestin sisällön automaattisen analysoinnin, viestien välittämisen ja vastaanottamisen estämisen tai rajoittamisen, haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä tai muita näihin rinnastettavia toimenpiteitä. (16.6.2004/516, 19§.)

Toimenpiteet tulee toteuttaa huolellisesti ja mitoittaa torjuttavan häiriön vakavuuteen. Toimenpiteillä ei saa rajoittaa sananvapautta tai luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä. Viestinvirastolla on oikeus antaa teleyrityksille tarkempia määräyksiä toimenpiteiden teknisestä toteuttamisesta. (16.6.2004/516, 19§.)

5.3.2 Tunnistamistietojen käsittely

Verkossa viestinnästä jää aina jälki. Viestinnän tunnistamistiedolla tarkoitetaan tietoa, jonka perusteella verkko- tai viestintäpalvelun käyttäjä voidaan tunnistaa. Teleyritys saa käyttää tunnistetietoja vain laissa määriteltyihin tarkoituksiin. Tunnistamistietoja ovat esimerkiksi tiedot puhelun soittajasta tai vastaanottajasta. Tiedot sähköpostin lähettäjästä tai vastaanottajasta, IP-osoitteesta ja tiedot yhteyden kestosta, reitityksestä, ajankohdasta tai siirretyn tiedon määrästä ovat tunnistamistietoja. Tunnistamistietoja ovat myös tiedot, jotka voidaan yhdistää yritykseen. (Tunnistamistietojen käsittely 2013.)

Teleyritys voi käyttää tunnistamistietoja verkko- ja viestintäpalvelun käyttämiseksi, laskuttamiseksi, tietoturvan varmistamiseksi, teknisen vian havaitsemiseksi, teknistä kehittämistä varten sekä väärinkäytöstilanteissa, joissa verkko-, viestintä- tai lisäarvopalvelun maksullista palvelua käytetään maksutta. (Tunnistamistietojen käsittely 2013.)

Tunnistetietoja saa käyttää vain käsittelyn tarkoituksen laajuudessa. Luottamuksellisen viestin ja yksityisyyden suojaa ei saa rajoittaa enempää kuin on välttämätöntä. Tunnistetietoja saa luovuttaa vain niille tahoille, joilla on oikeus tietojen käsittelyyn. Viestit ja tunnistamistiedot on hävitettävä tai tehtävä sellaisiksi, ettei tunnistetietoja voida yhdistää tilaajaan tai käyttäjään. (16.6.2004/516, 8§.)

Teleyrityksellä on velvollisuus säilyttää tunnistetietoja viranomaistarpeita varten 12 kuukauden ajan viestinnän päivämäärästä. Näitä tunnistetietoja saa käyttää ainoastaan pakkokeinolaissa (806/2011) tarkoitettujen rikosten tutkimiseksi. (16.6.2004/516, 14 a §.)

5.3.3 Tietoturvaloukkausilmoitukset

Teleyrityksen velvollisuus on ilmoittaa viestintävirastolle verkko- ja viestintäpalveluiden merkittävistä tietoturvaloukkauksista ja -uhkista, joista teleyritys on tietoinen. Teleyrityksen on myös ilmoitettava tietoturvaloukkausten seuraukset ja toimenpiteet, joilla tietoturvaloukkausten ja uhkien esiintymien pyritään estämään. Viestintävirasto voi määrätä teleyrityksen tiedottamaan asiasta yleisesti. (16.6.2004/516, 21§.)

Palveluihin tai tietoverkkoihin kohdistuvista tietoturvaloukkauksista ja -uhkista on ilmoitettava myös tilaajalle ja käyttäjälle. Teleyrityksen on kerrottava käytettävissä olevista toimenpiteistä, kustannuksista sekä mistä asiasta on mahdollista saada lisätietoa. Kun teleyritys on torjunut palveluunsa liittyvän tietoturvaloukkauksen tai -uhan, on teleyrityksen ilmoitettava käytetyistä toimenpiteistä ja niiden mahdollisista vaikutuksista palvelun käyttöön. (16.6.2004/516, 21§.)

6 TOTEUTUS

6.1 Lähtötason määrittely ja analyysi

Organisaation tietoturvatapahtumien hallinnan lähtötason määrittelyllä selvitetään mitä dokumentteja, työkaluja, toimintatapoja tai resursseja organisaatiolla on tietoturvatapahtumien hallintamalliin liittyen. Opinnäytetyön tavoitteena on tietoturvatapahtumien hallintaprosessin luominen ja tiketöintijärjestelmän asentaminen ja käyttöönottaminen. Lähtötilanteen selvityksen jälkeen on mahdollista analysoida

millainen tietoturvatapahtumien hallintaprosessi organisaatiossa on mahdollista toteuttaa ja millaisia työkaluja ja dokumentteja tietoturvatapahtumien hallintaprosessissa voidaan käyttää tukena. Lähtötason määrittely ja analyysi suoritetaan SFS ISO/IEC 27035-standardin (2011) tietoturvatapahtumien hallintamallin päävaiheisiin perustuen.

6.1.1 Suunnittelu ja valmistautuminen

JYVSECTECin operaattoriympäristössä ei ole toimintaa ohjaavaa tietoturvan hallintamallia. Tietoturvapolitiikan tulisi ohjata organisaation tietoturvan hallintaa. Tietoturvatapahtumien hallintaa tulisi ohjata tietoturvaherätteiden, – tapahtumien ja – haavoittuvuuksien hallintapolitiikka, joka on sisällytetty organisaation tietoturvapolitiikkaan ja riskien hallintapolitiikkaan. Organisaatio tulisi tunnistaa ja määrittää operaattoriympäristön osalta turvallisuusvaatimukset ja suojattavat kohteet. Riskienhallinnan osalta tulisi toteuttaa tarvittavat riskianalyysit ja riskien vertaaminen riskikriteereihin. Organisaation tulisi perustaa tarvittavat turvamekanismit. Nämä toimet ja tiedot toimivat pohjana tietoturvatapahtumien hallinnalle.

Johdon roolin merkitys laboratorioympäristössä on myös vähäinen. Laboratoriossa rooleissa työskennellessä oletetaan, että työtä ohjaa johdon sitoutuminen ja tilanteet mallintavat normaaleja työelämän tilanteita.

Laboratoriossa kaikki tietoturvatapahtumien käsittelytilanteet hoitaa ISIRT mahdollisten asiantuntijoiden avulla. Organisaatiolla ei ole erillistä kontaktipistettä tietoturvatapahtumien hallintaan liittyen. ISIRTin henkilökunnan rooleissa normaaleissa laboratorioharjoituksissa on yleensä muutamia henkilöitä. ISIRTin rooleissa toimivat henkilöt voivat ohjata tietoturvatapahtumia 2. asteen asiantuntijoille, kun tilanne ei ole ISIRTin hallinnassa tai tarvitaan syvempää teknistä osaamista.

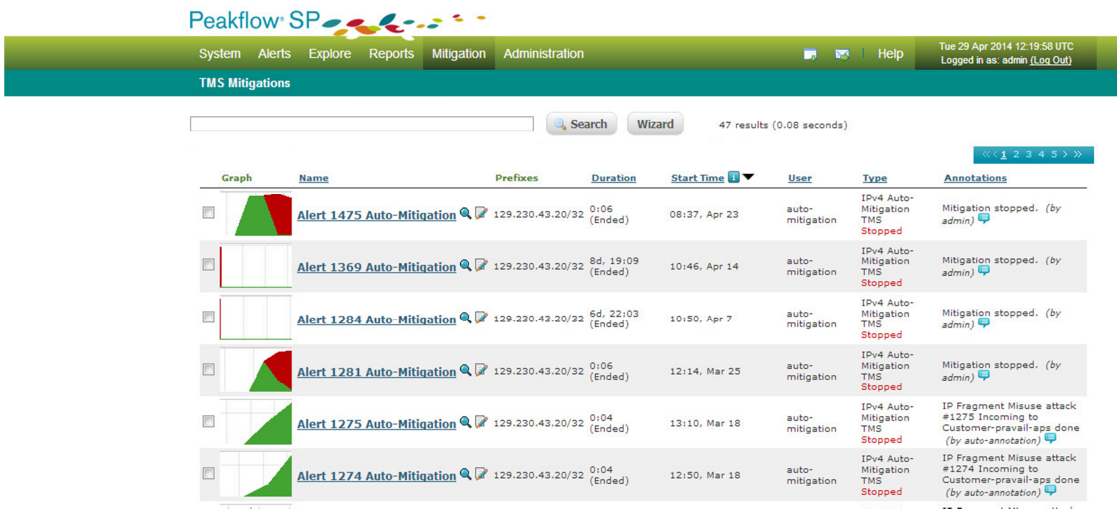
Tietoturvatapahtumien hallintaprosessin koulutus hoidetaan laboratorioharjoitusten yhteydessä tilanteen laajuus huomioon ottaen. Koulutus esitellään opinnäytetyön kohdassa 6.4.

6.1.2 Tunnistaminen ja raportointi

Laboratorioympäristössä on mahdollista tunnistaa tietoturvaherätteitä ja -tapahtumia asiakkaiden tai ISIRTin henkilökunnan toimesta. ISIRTin on mahdollista havaita tietoturvaherätteitä Arbor Networks Peakflow SP -tuotteella operaattoriverkosta. Arbor Peakflow -tuotteet on kehitetty kriittisten palvelujen, kuten puhe-, video-, web- ja sähköpostipalvelun suojaamiseen kohdennetuilta hyökkäyksiltä. Tuotteilla voidaan suojata infrastruktuuria tunnistamalla ja poistamalla hyökkäykset reitittimiä, kytkimiä, palomuureja, kaistanleveyttä tai DNS-palveluja vastaan ja estää väärän liikenteen pääsy verkkoon. Peaklow-tuotteilla voidaan valvoa verkon suorituskykyä mittareiden avulla ja saada tietoa verkon viiveistä, viiveen vaihteluista, läpäisyajasta ja pakettihäviöstä. Tuotteita voidaan käyttää myös verkon resurssien optimointiin. (Peakflow solution data sheet 2013)

Peakflow SP -ohjelmiston pääasiallinen tehtävä on muodostaa hälytyksiä verkossa tapahtuvista poikkeavista tilanteista. Nämä poikkeavuudet voivat olla merkki haitallisesta liikenteestä, laiteviasta, epätavallisesta kysynnän kasvusta tai konfigurointivirheistä. Operaattori voi hälytysten avulla huomata ongelmat, tunnistaa juurisyyn ja ryhtyä korjaaviin toimenpiteisiin. Peakflow SP -ohjelmiston avulla on mahdollista saada selville, mistä verkkoliikenne tulee, minne liikenne menee, mitä reittejä liikenne käyttää, mitkä verkon rajapinnat ovat eniten kuormitettuja ja ketkä kuormittavat verkkoa eniten. Tuotteen avulla on mahdollista seurata verkon liikenteen pitkä- ja lyhytaikaisia kuormitustrendejä ja laatia liikenteen käyttäytymisennusteita. (Peakflow

solution data sheet 2013.) Kuviossa 12 on nähtävissä Peakflow SP -tuotteen hallinta-konsoli ja hälytyksiä haitallisesta liikenteestä.

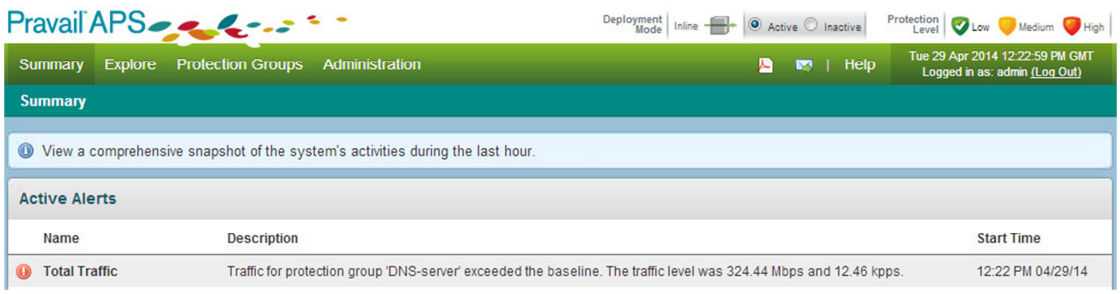


Kuvio 12. Arbor Networks Peakflow SP -konsoli

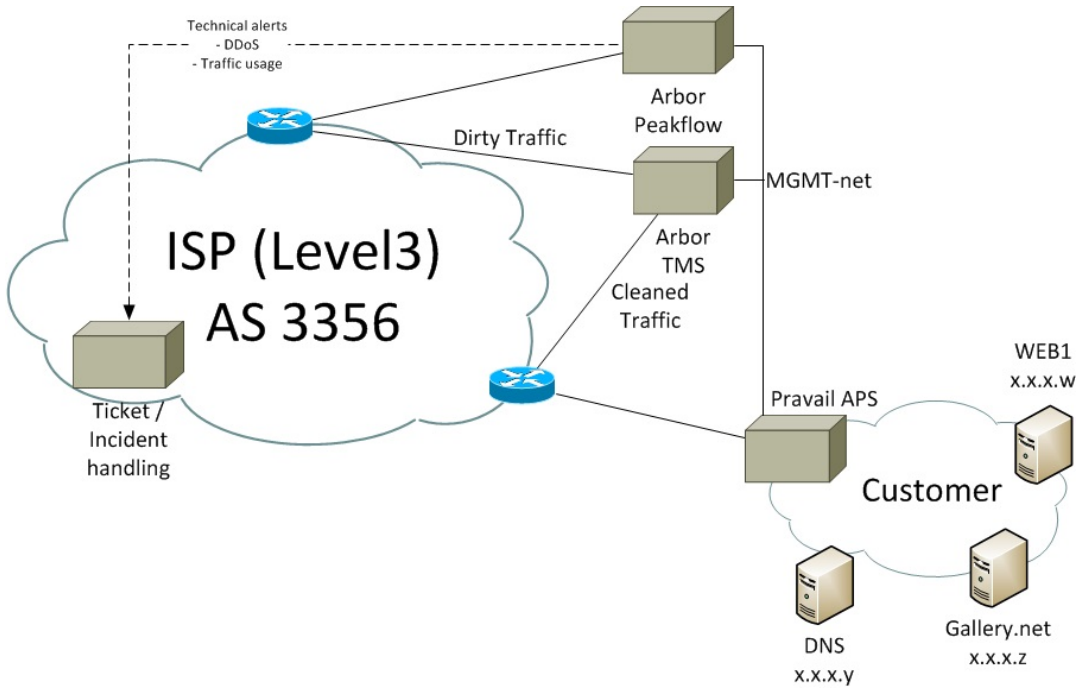
Peakflow Threat Management System (TMS) -työkalun avulla voidaan lieventää DDOS-hyökkäysten vaikutuksia. Liikenne voidaan ohjata Peakflow TMS -järjestelmään Arbor Peakflow SP -ohjelmiston tekemillä verkon reititysmuutoksilla. Peakflow TMS poistaa pakettivirrasta ainoastaan haitallisen liikenteen ja ohjaa edelleen sallitun liikenteen verkkoon. (Peakflow solution data sheet 2013)

Peakflow Pravail Availability Protection System (APS) tarjoaa suojan sovelluskerrokseen DDOS-hyökkäyksiä, hyökkäyksille verkkokapasiteettia ja state exhaustion -hyökkäyksiä vastaan, jotka uhkaavat palvelujen tai ohjelmistojen saatavuutta (Pravail availability protection system data sheet 2013). State exhaustion -hyökkäyksellä tässä yhteydessä tarkoitetaan yritystä vaikuttaa yhteyksien tilatauluihin, joita käytetään monissa laitteissa kuten kuormanjakajissa, palomuureissa ja sovelluspalvelimissa (About DDOS attacks 2013). Perinteiset palomuurit tai tunkeutumisen estojärjestel-

mät (IPS, Intrusion Prevention System), jotka läpäisevät esimerkiksi HTTP- ja DNS-liikenteen, eivät tarjoa suojaa sovelluskerroksen DDOS-hyökkäyksille. Pravail APS -työkalulla voidaan havaita haitallinen liikenne ja torjua se hyödyllisen liikenteen seasta. (Pravail availability protection system data sheet. 2013.) Kuviossa 13 on nähtävissä Pravail APS konsoli ja hälytys DNS-palvelimeen kohdistuvasta liikenteen kasvusta.



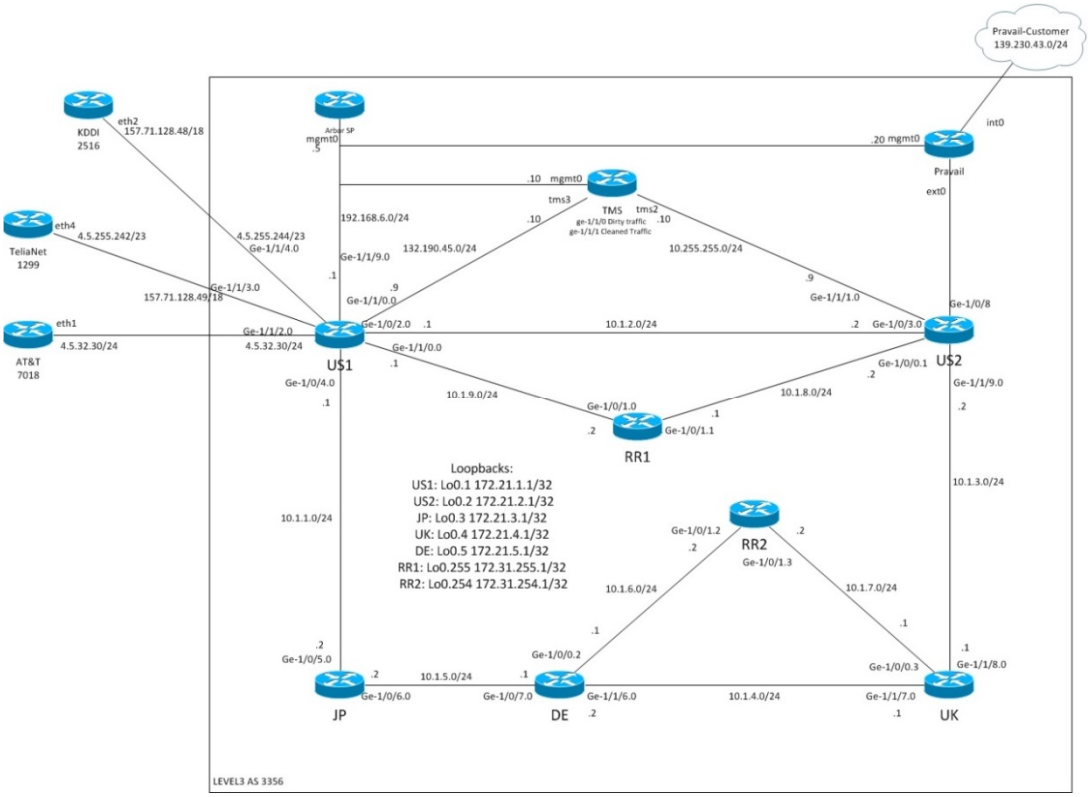
Kuvio 13. Arbor Networks Pravail APS -konsoli



Kuvio 14. DDOS-hyökkäysten tunnistus ja torjunta

Kuviossa 14 on nähtävissä operaattoriympäristössä oleva virtuaalinen autonominen järjestelmä (AS, Autonomous System) 3356, jonka omistaja on tietoliikenneoperaattori Level3. Autonomisella järjestelmällä tarkoitetaan tässä yhteydessä yksittäistä hallinnollista reititystoimialuetta (Huston, G 2006). Kuviossa 14 voidaan nähdä asiakas, joka tarjoaa verkossaan DNS- ja web-palveluja. Arbor Peakflow -tuotteella voidaan generoida hälytyksiä verkon poikkeavista tilanteista, Arbor TMS -tuotteella torjua ja puhdistaa liikennettä ja Peakflow Pravail APS -tuotteella suojautua sovelluskerroksen hyökkäyksiä vastaan.

Kuviossa 15 voidaan nähdä tarkempi kuva AS3356-toimialueesta ja sen liityntäpisteistä muiden operaattoreiden verkkoihin. Kuvion 15 oikeassa ylälaidassa on nähtävissä asiakas, jonka verkkoa suojataan Peakflow -tuotteilla.



Kuvio 15. Pravail-asiakas AS3356–toimialueessa

SFS ISO/IEC27035-standardi (2011) suosittaa, että organisaation tulisi käyttää tietoteknisiä järjestelmiä tietoturvaherätteiden, -haavoittuvuuksien ja -tapahtumien käsittelyssä ja raportoinnissa. JAMKin ja JYVSECTECin organisaatio on käyttänyt aiemmin OTRS-tiketöintijärjestelmää muiden toimintojen yhteydessä. Koska tiketöintijärjestelmä on organisaatiolle ennestään tuttu, OTRS-tiketöintijärjestelmää päätettiin käyttää tietoturvatapahtumien kirjaamiseen myös operaattoriympäristössä. OTRS-tiketöintijärjestelmää tai ohjelmiston käyttöön tarkoitettua palvelinta ei ole olemassa, joten tilaajan kanssa päädyttiin, että tiketöintijärjestelmä asennetaan ja otetaan käyttöön osana opinnäytetyön toteutusta. Tiketöintijärjestelmän asennus ja käyttöönotto kuvataan opinnäytetyön kappaleessa 6.2.2.

6.1.3 Arviointi, päätöksenteko, vastatoimet ja opetukset

Operaattoriympäristön suojattavat kohteet tulisi tunnistaa ja määritellä sekä suojattavien kohteiden riskinhallinta tulisi suorittaa. Tiedot vaikuttaisivat oleellisesti tietoturvatapahtumien kiireellisyyden ja vaikutusten arviointiin. Tässä opinnäytetyössä laaditaan tietoturvatapahtumille yleisluontoinen luokitteluasteikko (classification scale), jonka perusteella tietoturvatapahtumien kiireellisyyttä ja vaikutuksia arvioidaan. Organisaation tehtäväksi jää mahdollisen tietoturvatapahtumien kategorisointitaulukon laatiminen.

Vastatoimet-vaiheessa ISIRTin on mahdollista saada apua tietoturvatapahtumien käsittelyyn asiantuntijoilta. Kriisinhallinnan kehittäminen on rajattu tämän opinnäytetyön ulkopuolelle, joten se jää tulevaisuuden kehityskohteeksi.

6.2 OTRS ITSM –tiketöintijärjestelmä

6.2.1 Yleistä

OTRS (Open Technology Real Services) Group on OTRS-tuoteperheen luoja ja tarjoa konsultointi-, ohjelmistokehitys-, tuki-, ja hallintapalveluita OTRS-tuotteisiin liittyen (OTRS Group, Company). Organisaation juuret liittyvät avoimen lähdekoodin projektiin. OTRS -hanke perustettiin vuonna 2001. (About us 2014b). OTRS Open Source Community koostuu yli 5000 jäsenestä, asiantuntijasta ja harrastajasta, jotka osallistuvat avoimen lähdekoodin OTRS-projektiin. OTRS-ohjelmistojen lähdekoodi on ladattavissa ilmaiseksi. (Open Source Community 2014.)

OTRS Helpdesk Service -ohjelmisto, joka tunnetaan myös tiketöintijärjestelmänä tai help desk -työkaluna, auttaa organisaatiota asiakkaiden palvelupyyntöjen vastaan ottamisessa ja mahdollistaa palvelupyyntöjen edelleen ohjaamisen oikealle tiimille tai organisaation osastolle. Palvelupyyntö voidaan tunnistaa tikettinumeron avulla ja palvelupyynnön käsittelyn vaiheet voidaan tallentaa tiketille. OTRS-tiketöintijärjestelmä mahdollistaa asiakkaiden palvelupyyntöihin vastaamisen yhdestä web-pohjaisesta järjestelmästä, jossa organisaation työntekijät voivat käsitellä palvelupyyntöjä. Organisaation sisäinen kommunikointi on mahdollista palvelupyyntöön liittyvän tiketin välityksellä. (OTRS Group, Software.) OTRS-tiketöintijärjestelmä tarjoaa ominaisuuksia esimerkiksi tikettien hallintaan, asiakkaiden itsepalveluun, tiedonhallintaan, ajanhallintaan, palvelukuvaston tekemiseen ja hallitsemiseen, raportointiin ja asiakaskyselyiden tekemiseen (Software 2014).

OTRS IT Service Management (ITSM) -ohjelmisto tarjoaa IT-palveluntarjoajille työkalun palvelupyyntöjen, tapahtumien, ongelmien ja muutosten hallintaan. OTRS ISTM -ohjelmisto tarjoaa työkalun myös tunnistettavien kohteiden ja tiedon hallintaan.

OTRS ISTM -ohjelmisto tukee ITIL V3-viitekehyksen mukaista toimintaa. (Software 2014.) OTRS ISTM -ohjelmisto on tarkoitettu ensisijaisesti IT-palvelutuotannon tarpeisiin. Työssä sovitetaan ohjelmiston käyttö tietoturvatapahtumien hallintaan ja esitellään ohjelmiston ominaisuuksia tietoturvatapahtumien hallintaan liittyen. Kuviossa 16 on esitelty OTRS-tuotteiden ominaisuuksia.

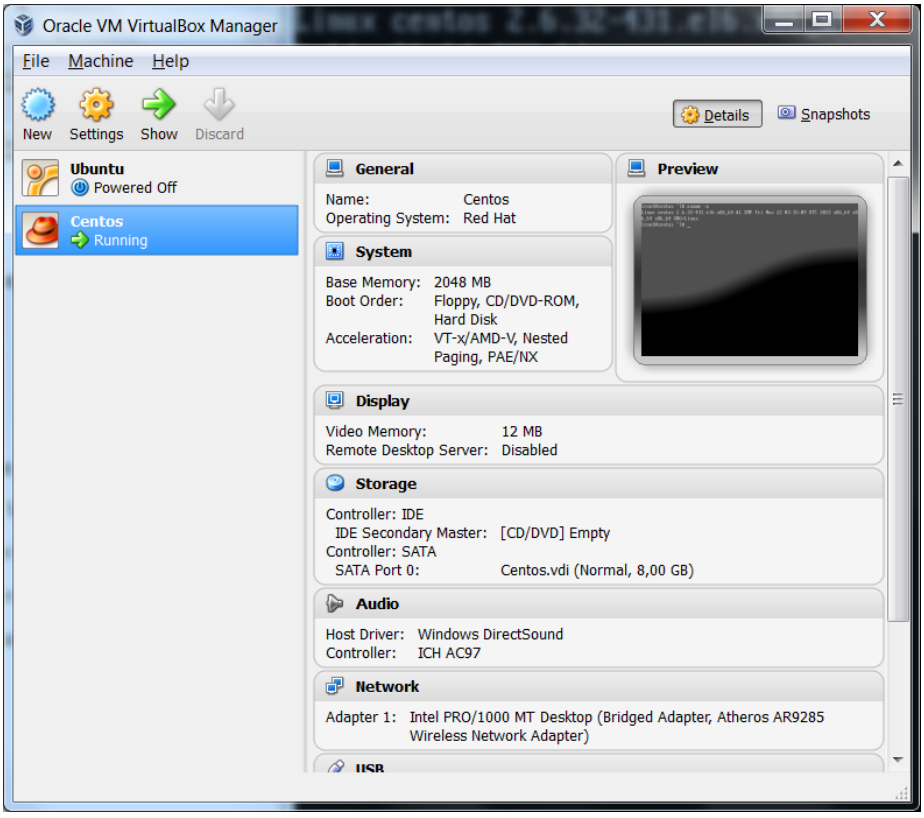
Kuvio 16. OTRS -ohjelmistojen ominaisuudet

(Software 2014).

6.2.2 Asennus

OTRS ISTM -ohjelmiston asennus ja käyttöönotto toteutettiin Oracle VM Virtual Box Manager -virtualisointisovelluksen avulla. Virtuaalikoneet mahdollistavat useiden käyttöjärjestelmien yhtäaikaisen käytön Windows-, Mac,- Linux- tai Solaris-käyttöjärjestelmissä. Käytännön rajoituksina toimivat isäntäkoneen resurssit, kuten esimerkiksi prosessoriteho, muisti ja levytila. (Oracle VM Virtualbox data sheet 2013).

Kuviossa 17 on nähtävissä Oracle VM VirtualBox Manager -konsoli ja virtuaalipalvelin CentOs sekä tietoja palvelimen käytössä olevista resursseista.



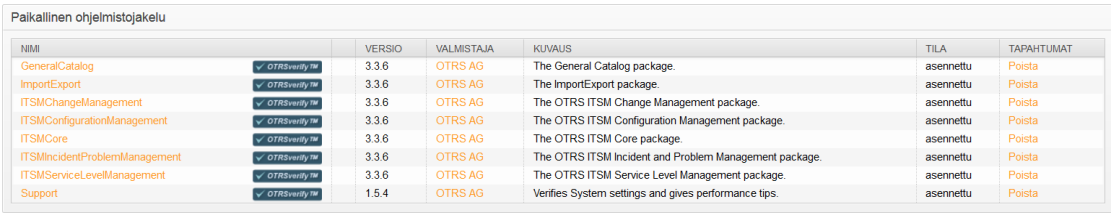
Kuvio 17. Oracle VM Virtualbox Manager

Virtuaalipalvelimen käyttöjärjestelmäksi valittiin CentOS6. Käyttöjärjestelmä asennettiin CentOS MinimalCD 6.5 64-bit -levykuvasta, joka on saatavilla ilmaiseksi CentOS:n kotisivulta. CentOS-käyttöjärjestelmää julkaisee Red Hat. Tärkein kriteeri käyttöjärjestelmän valinnalle oli, että OTRS tarjoaa käyttöjärjestelmälle valmiit asennuspaketit ja dokumentaation asentamiselle. Käyttöjärjestelmä on myös ilmainen. Käyttöjärjestelmän asennuksen vaiheita ei kuvata opinnäytetyössä. Käyttöjärjestelmään asennettiin OTRS-ohjelmistojen asennusta helpottamaan GNOME-työpöytäympäristö, Firefox-selain ja useita komentorivityökaluja.

OTRS ISTM vaatii toimiakseen OTRS Helpdesk Service -ohjelmiston asennuksen. OTRS-ohjelmistot käyttävät MySQL-tietokantaa ja ennen ohjelmiston asennusta tietokanta asennettiin ja valmisteltiin OTRS-sovelluksen asennusta varten. OTRS Helpdesk Service -asennuspakettien asentamisen jälkeen vaadittiin Apache web -palvelimen asentaminen. OTRS-ohjelmiston asennuspaketit eivät sisällä kaikkia ohjelmiston käyttämiä perl-kirjastoja ja ne asennettiin erikseen. Ongelmia OTRS-ohjelmiston käyttöönotossa tuotti myös CentOS-käyttöjärjestelmän Security Enchanded Linux -turvallisuusjärjestelmä. Turvallisuusjärjestelmällä rajoitetaan ohjelmistojen saamia käyttöoikeuksia käyttöjärjestelmässä. CentOS-käyttöjärjestelmään perehtyminen ei ole opinnäytetyön varsinainen tavoite, joten turvallisuusjärjestelmä poistettiin käytöstä OTRS-ohjelmiston moitteettoman toiminnan varmistamiseksi.

OTRS Helpdesk Service -ohjelmiston asennus jatkui web-pohjaisen asennustyökalun avulla. Asennusohjelman suorituksen aikana valittiin tietokanta, jota OTRS-sovellukset käyttävät ja kirjauduttiin kantaan OTRS-sovelluksen käyttäjätunnuksilla. Asennustyökalun vaatimien asetusten määrittämisen jälkeen oli mahdollista kirjautua OTRS Helpdesk Service -ohjelmistoon palvelimella osoitteessa http://localhost/otrs/index.pl.

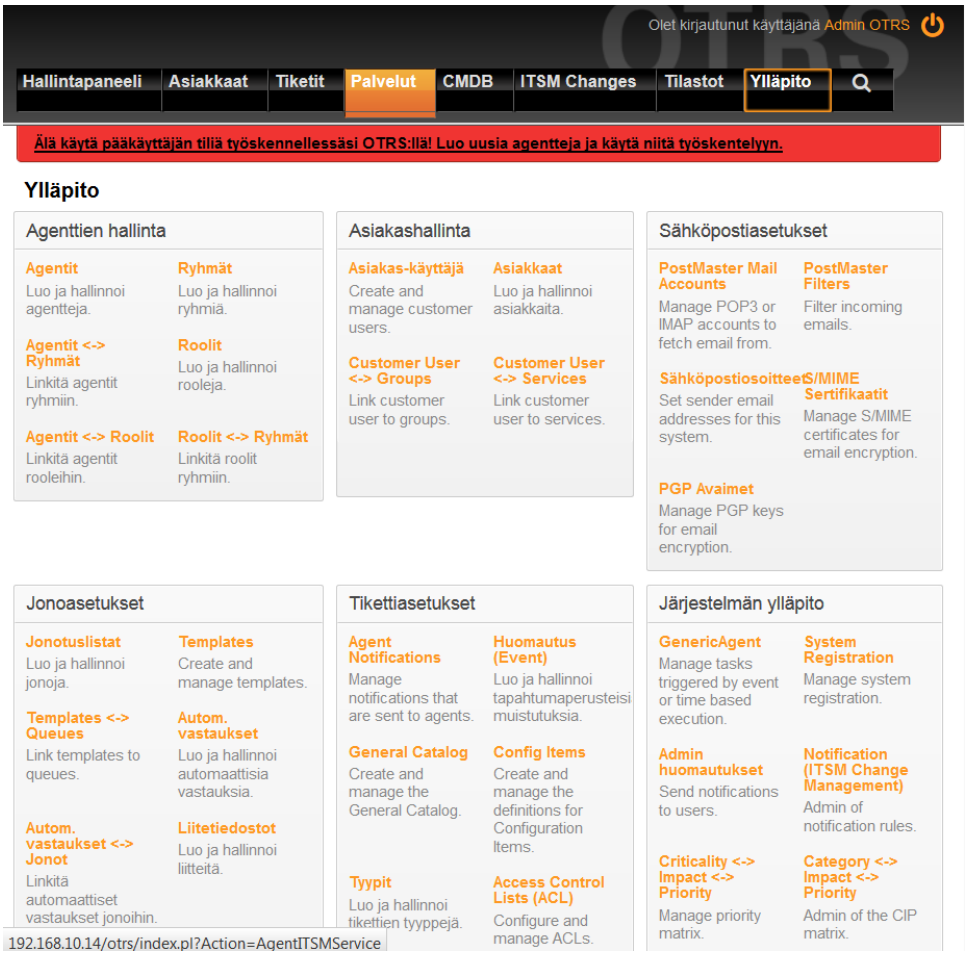
OTRS ISTM -ohjelmiston asennuspaketit asennettiin OTRS:n omalla pakettienhallintatyökalulla. Kuviossa 18 on nähtävissä asennetut ISTM -ohjelmistopaketit.



Kuvio 18. OTRS ISTM -ohjelmistopakettien asentaminen

6.2.3 Käyttöönotto

OTRS ISTM-ohjelmiston käyttöönotto JYVSECTEC-organisaatiossa tietoturvatapahtumien hallintaa varten vaatii ohjelmiston sisäisten asetusten määrittämistä. Ohjelmistoon on määritettävä asetukset agenttien hallintaa, asiakashallintaa, jonojen käyttöä ja tikettien käyttöä varten. Kuviossa 19 on nähtävissä ylläpitoon liittyvien asetusten hallintakonsoli. Asetukset määritettiin esimerkiksi ja organisaatio voi täydentää asetuksia omaan käyttöön sopiviksi tulevaisuudessa.



Kuvio 19. OTRS ISTM -järjestelmän ylläpito

Ohjelmistoon luotiin käyttäjät Agent1 ISIRTIn roolissa toimivaa henkilöä varten ja Specialist1 asiantuntijan roolissa toimivaa henkilöä varten. Ohjelmistoon luotiin ryhmät ISIRT ja Specialists. Agent1-käyttäjä liitettiin ryhmään ISIRT ja Specialist1-käyttäjä ryhmään Specialists. Ohjelmisto mahdollistaa myös käyttäjien hallinnan roolien avulla.

Asiakkaiden hallinnan asetuksilla on mahdollista tallettaa järjestelmään asiakastietoja ja asiakkaiden käyttäjien tietoja. Asiakkaaksi luotiin Customer1 ja asiakkaan käyttäjäksi User1. Asiakkaita on mahdollista liittää asiakasryhmiin ja asiakkaiden käyttäjiä on mahdollistaa linkittää asiakkaan palveluihin.

Tikettien käsittelyä ja siirtämistä varten ISIRTille ja asiantuntijoille luotiin ohjelmistoon ISIRT queue ja Specialist queue -nimiset jonot. Jonojen käyttäjille annettiin omassa työjonossa oleville tiketeille täydet luku ja kirjoitusoikeudet. Tiketin kirjaamisen nopeuttamista varten luotiin mallipohjat (template) tietoturvaherätteelle ja -tapahtumalle, jotka sisältävät kysymykset joihin ISIRTin jäsenen tulee tikettiä kirjatessaan vastata. OTRS ITSM tukee myös automaattisesti lähetettyjä viestejä, joita lähetään asiakkaalle tai halutulle jakelulistalle, kun tiketti vastaanotetaan, tiketin tila muuttuu, tiketti siirretään uuteen jonoon tai tiketti suljetaan.

Tikettiasetuksiin luotiin tikettityypit tietoturvaheräte (security event) ja tietoturvatapahtuma (security incident). Tikettityyppien avulla organisaatio voi suorittaa halutessaan myös tarkemman kategorisoinnin. Kategorisointia käsiteltiin opinnäytetyön kappaleessa 4.5.4. Virtuaalisessa operaattoriympäristössä tietoturvaherätteet ja -tapahtumat liittyvät usein teknisiin tilanteisiin. Kategorioiksi sopivia esimerkkejä voisivat olla esimerkiksi haittaohjelma, palvelunestohyökkäys, fyysinen vika tai konfiguraatiovirhe. Tiketin tilat muokattiin yksinkertaisemmaksi oletusasetuksiin verrattuna. Tiketin tila voi olla uusi (new), vastaanotettu (assigned), työn alla (work in progress), odottaa (pending) ja suljettu (closed). Ohjelmiston oletusasetuksia muutettiin niin,

että tiketin tilaa voidaan muuttaa kirjoitettaessa tiketille uusi huomautus (note). Tiketin prioriteettiasteikko on viisiportainen. Prioriteetit on nähtävissä kuviossa 20.

NIMI	KELPOISUUS	MUUTETTU	LUOTU
1 very low	Käytössä	16.03.2014 22:50	16.03.2014 22:50
2 low	Käytössä	16.03.2014 22:50	16.03.2014 22:50
3 normal	Käytössä	16.03.2014 22:50	16.03.2014 22:50
4 high	Käytössä	16.03.2014 22:50	16.03.2014 22:50
5 very high	Käytössä	16.03.2014 22:50	16.03.2014 22:50

Kuvio 20. Prioriteetit

Organisaatiolla ei ole tietoturvatapahtumien luokitteluun luokittelu- tai kategorisointiasteikoita. OTRS-tikettien prioriteettia määrittäessä arvioidaan vaikutusta (impact) palvelulle ja palvelun yleistä kriittisyyttä (criticality). Palvelun kriittisyys määrittyy tiketille automaattisesti suojattavan kohteen perusteella, mutta sitä voidaan muuttaa myös tapauskohtaisesti. Prioriteetin ja kriittisyyden yhteisvaikutus määrittää tiketin kiireellisyyden. Kuviossa 21 voidaan nähdä luokittelutaulukko.

Priority allocation

IMPACT / CRITICALITY	1 ERITTÄIN ALHAINEN	2 ALHAINEN	3 NORMAALI	4 KIIREELLINEN	5 ERITTÄIN KIIREELLINEN
1 Erittäin alhainen	1 Erittäin alhainen	1 Erittäin alhainen	2 Alhainen	2 Alhainen	3 Normaali
2 Alhainen	1 Erittäin alhainen	2 Alhainen	2 Alhainen	3 Normaali	4 Kiireellinen
3 Normaali	2 Alhainen	2 Alhainen	3 Normaali	4 Kiireellinen	4 Kiireellinen
4 Kiireellinen	2 Alhainen	3 Normaali	4 Kiireellinen	4 Kiireellinen	5 Erittäin kiireellinen
5 Erittäin kiireellinen	3 Normaali	4 Kiireellinen	4 Kiireellinen	5 Erittäin kiireellinen	5 Erittäin kiireellinen

Kuvio 21. Vaikutuksen ja kiireellisyyden arviointi

Järjestelmään luotiin palvelut DNS1 ja WEB1 ja ne linkitettiin käyttäjälle User1. DNS1-palvelun kriittisyys luokiteltiin erittäin kiireelliseksi ja WEB1-palvelun kriittisyys luokiteltiin kiireelliseksi. Ohjelmistolla voidaan luoda ja hallita palvelutasosopimuksia ja liittää palvelutasosopimukset asiakkaan palveluihin. Ohjelmistoon luotiin palvelutasosopimukset *bronze*, *silver* ja *gold*. Palvelutasosopimukset auttavat tietoturvahe-

rätteen ja -tapahtuman kiireellisyyden arvioinnissa. DNS1-palvelu liitettiin palvelutasosopimukseen gold ja WEB1-palvelu liitettiin palvelutasosopimukseen silver.

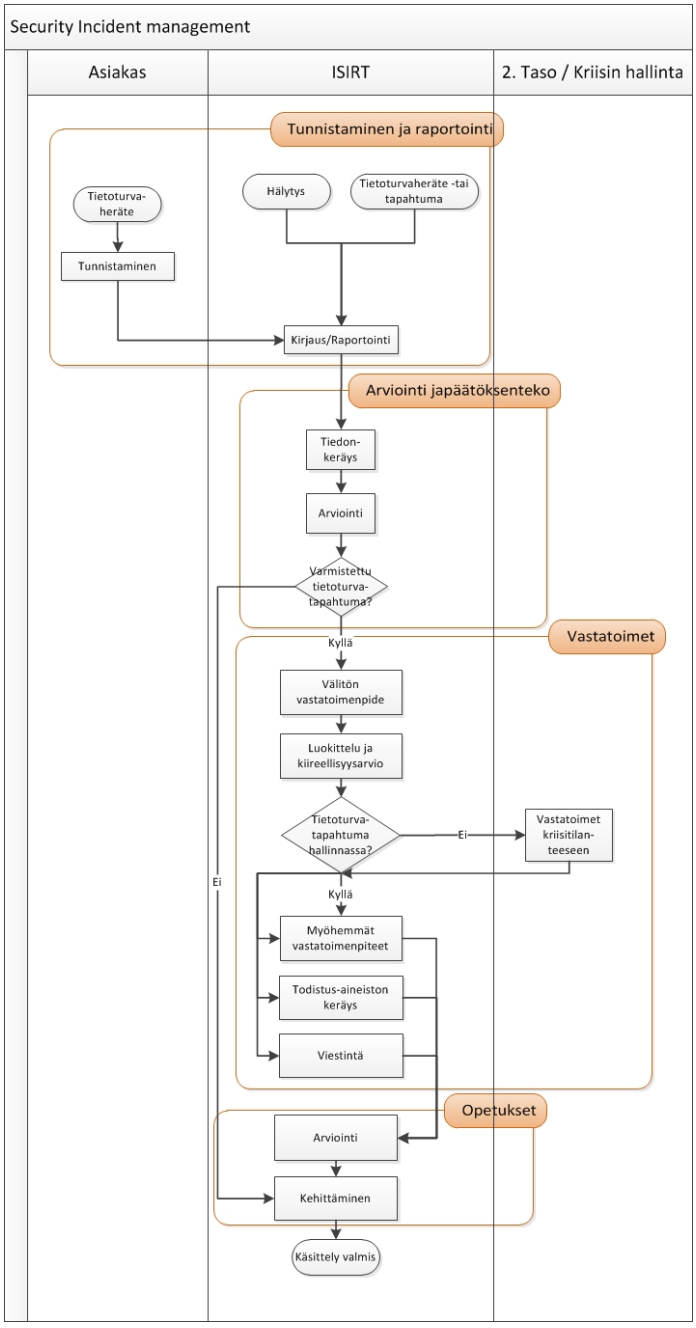
Ohjelma tukee tunnistettavien kohteiden listaamista ja tunnistettavien kohteiden kategorisointia. Oletuskategoriat tunnistettaville kohteille ovat computer, hardware, location, network ja software. Tunnistettavia kohteita voi liittää käsiteltäville tiketeille.

Ohjelmiston kaikki asetukset ovat muokattavissa organisaation tarpeisiin. Pienin muokkauksin oletusasetuksia on mahdollista käyttää tietoturvatapahtumien hallintaan. Ohjelmistojen asetuksiin perehtyminen vaatii organisaatiolta kuitenkin aikaa ja henkilöresursseja.

6.3 Tietoturvaherätteiden ja -tapahtumien hallintaprosessi

6.3.1 Yleistä

Kuviossa 22 on nähtävissä tietoturvaherätteiden ja -tapahtumien hallintaprosessi JYVSECTECin operaattoritoimintaa varten, joka on laadittu lähtötason selvitykseen perustuen. Prosessi on mukautettu organisaation rakenteisiin SFS ISO/IEC27035-standardin (2011) operatiivisiin päävaiheisiin perustuen. Tässä kappaleessa käydään läpi hallintaprosessin työvaiheet ja tiketöintijärjestelmän käyttö prosessin aikana. Kappale voi toimia työohjeena ja esimerkkinä virtuaalisessa operaattoriympäristössä toimittaessa.

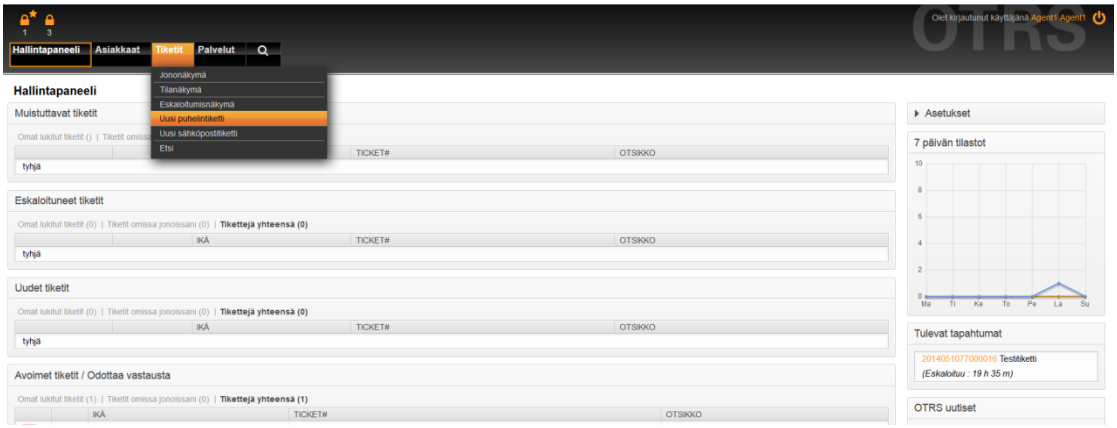


Kuvio 22. JYVSECTECin tietoturvaherätteiden ja -tapahtumien hallintaprosessi

6.3.2 Tunnistaminen ja raportointi

Laboratorioympäristössä tietoturvaherätteestä voi ilmoittaa asiakkaan roolissa toimiva henkilö. Herätteen tunnistamisen jälkeen asiakas ilmoittaa herätteestä ISIRTille puhelimella tai sähköpostilla. Tietoturvaherätteitä ja -tapahtumia voidaan havaita myös Arbor Networks Peakflow SP -ohjelmiston hälytyksistä tai ISIRT voi huomata tietoturvaherätteen tai -tapahtuman itse toimiessaan laboratorioympäristössä.

Asiakkaan soitosta tai sähköpostista kirjataan tiketti OTRS-tiketöintijärjestelmään. Samoin toimitaan havaittaessa hälytys tai tietoturvaheräte ISIRTin toimesta. ISIRTin roolissa toimiva henkilö kirjautuu OTRS-tiketöintijärjestelmään tunnuksella Agent1 ja asiantuntijan roolissa toimiva henkilö tunnuksella Specialist1 osoitteessa http://<palvelimen IP-osoite>/otrs/index.pl. Salasanat ja palvelimen käynnistämisohje toimitetaan JYVSECTECin organisaatiolle erillisenä dokumenttina. Kuviossa 23 voidaan nähdä kuinka OTRS-tiketöintijärjestelmän tiketit- valikosta voidaan luoda uusi puhelintiketti tai sähköpostitiketti.

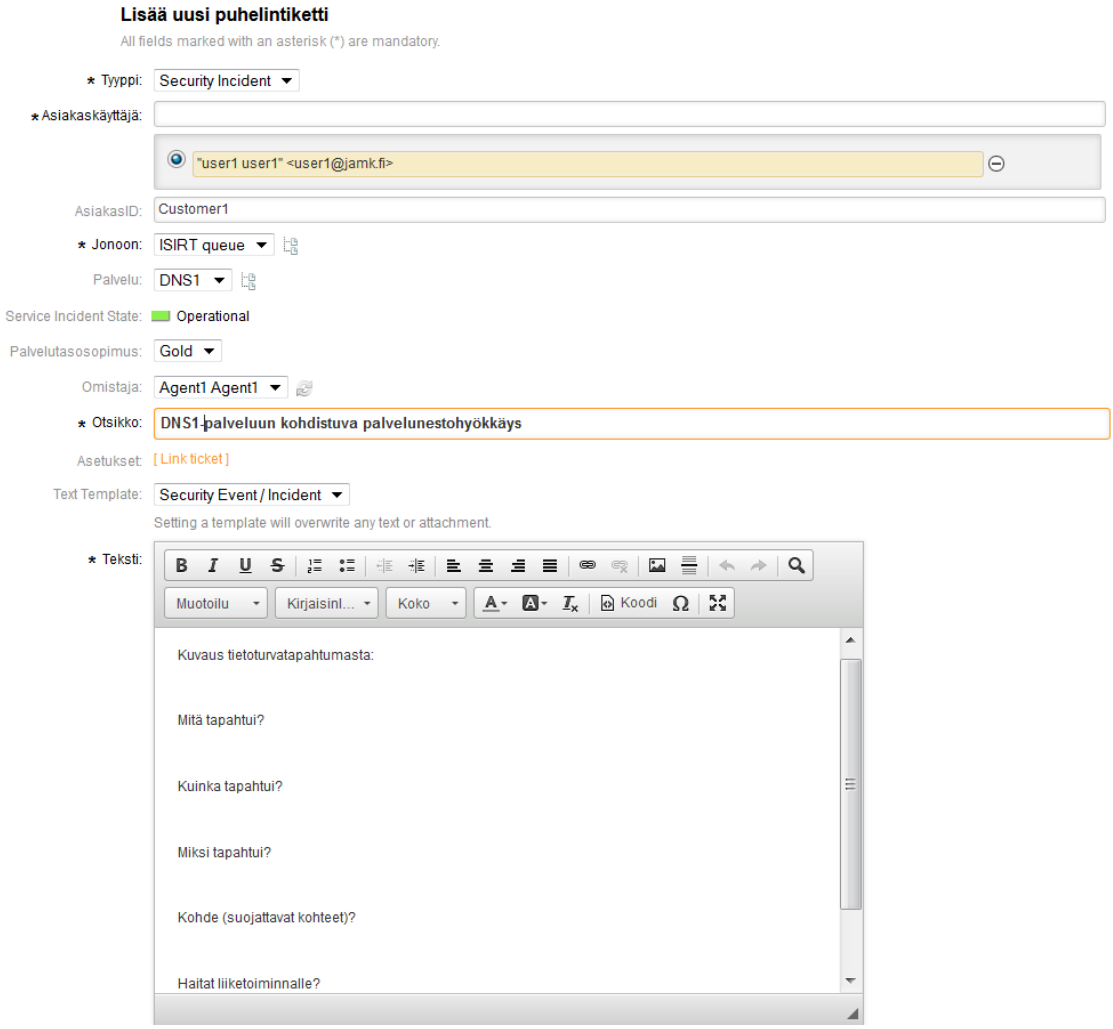


Kuvio 23. Tiketin luominen OTRS-tiketöintijärjestelmään

Tiketin kirjaamisen yhteydessä tehdään alustava arvio onko kyseessä tietoturvaherä-te vai -tapahtuma. Esimerkissä heräte on arvioitu tietoturvatapahtumaksi. Tietotur-vatapahtumasta ilmoittaa asiakkaan käyttäjä user1. Tiketti tallennetaan jonoon ISIRT queue. User1-käyttäjä ilmoittaa DNS1-palveluun kohdistuvasta palvelunestohyökkä-yksestä. Palveluksi valitaan DNS1 ja palvelutasosopimukseksi valitaan gold. Tiketin omistajaksi valitaan agent1. Otsikkoon kirjoitetaan kuvaus tietoturvatapahtumasta. Tekstipohjaksi valitaan security event/ incident, jolloin tiketin tekstikenttään muo-dostuu seuraavat tiketin kirjaamista helpottavat kysymykset:

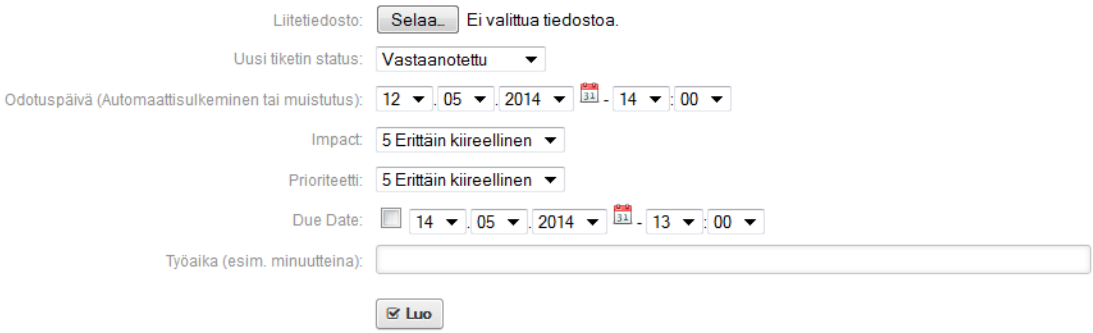
- Kuvaus tietoturvatapahtumasta
- Mitä tapahtui?
- Kuinka tapahtui?
- Miksi tapahtui?
- Kohde (suojattavat kohteet)?
- Haitat liiketoiminnalle?

Tiketin käsittelijä kirjaa tekstikenttään vastaukset kysymyksiin sen hetkisen parhaan tiedon perusteella. Tiketti on myös mahdollista liittää suojattavaan kohteeseen valit-semalla link ticket. Kuviossa 24 on nähtävissä esimerkki tiketin kirjaamisesta.



Kuvio 24. Tiketin kirjaaminen OTRS-tiketöintijärjestelmään

ISIRTIn tulee kerätä todistusaineistoa tietoturvatapahtumasta. Tiketille voidaan liittää asiakkailta saatavia todisteita liitetiedostoksi. Tiketin tilaksi kirjaamisen yhteydessä valitaan joko uusi tai vastaanotettu, jos tiketin käsittely jatkuu heti. Tiketille kirjataan myös alustava arvio tietoturvatapahtuman vaikutuksesta ja tärkeydestä opinnäytetyön kuviossa 21 nähtävän luokittelutaulukon avulla. Kuviossa 25 voidaan nähdä esimerkki alustavasta arvioinnista ja tiketin tilan asettamisesta vastaanotetuksi. Tiketti luodaan valitsemalla luo-painike.

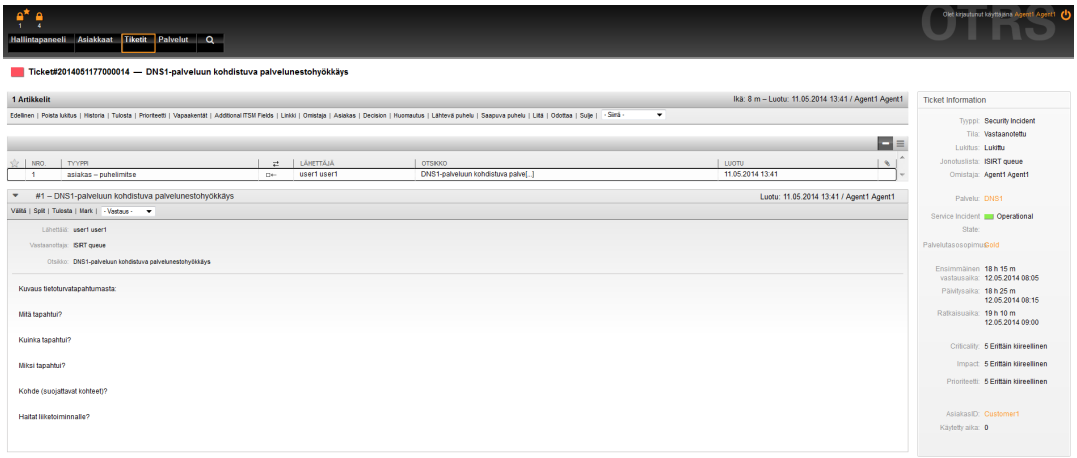


Kuvio 25. Alustava arviointi ja tiketin tilan valitseminen

Ohjelmiston asetuksiin on mahdollista määrittää, että asiakas saa uudesta tiketistä sähköpostin, jossa on tiketin tunnistenumero, tietoja tietoturvatapahtumasta ja tiketin tilasta ja mahdollisista ratkaisuajoista. Asiakasta on mahdollista myös informoida automaattisesti tiketin tilan vaihtuessa tai kun tiketti siirretään uuteen jonoon.

6.3.3 Arviointi ja päätöksenteko

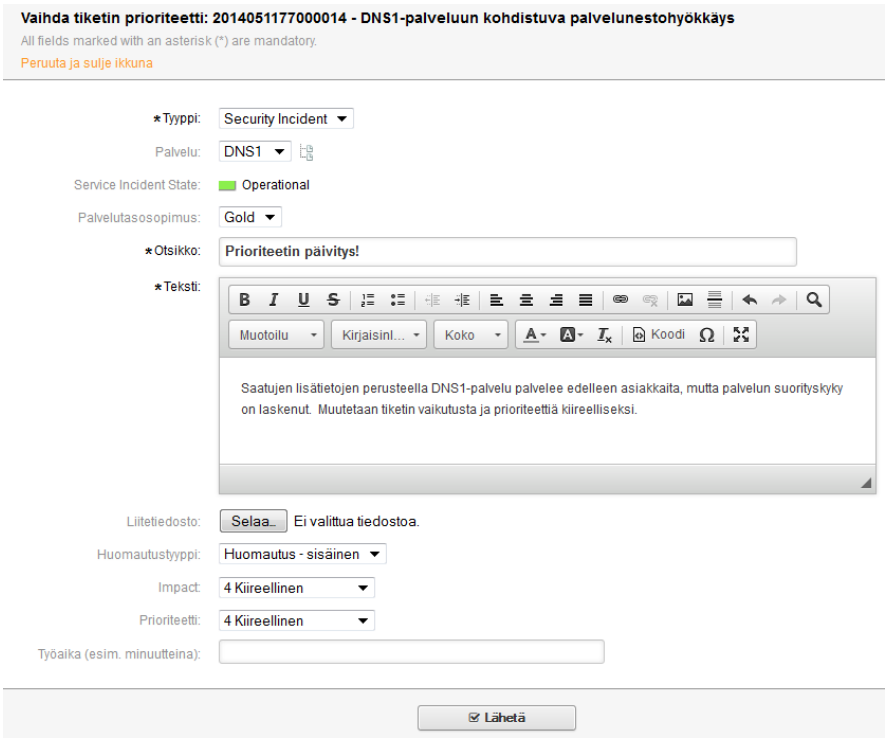
Kuviossa 26 voidaan nähdä tietoturvatapahtumasta muodostunut tiketti, joka on saanut tunnistenumero 2014051177000014. Tiketin tila on hyvä muuttaa työn alle aloitettaessa tiketin käsittely valitsemalla huomautus ja asettamalla uusi tiketin tila.



Kuvio 26. Tiketti tietoturvatapahtumasta

Tietoturvatapahtumasta tulee tiketin kirjaamisen jälkeen kerätä kaikki mahdollinen tieto ja kerätä mahdollinen todistusaineisto. Lisätietoja tiketille voidaan kirjata esimerkiksi valitsemalla valikosta huomautus.

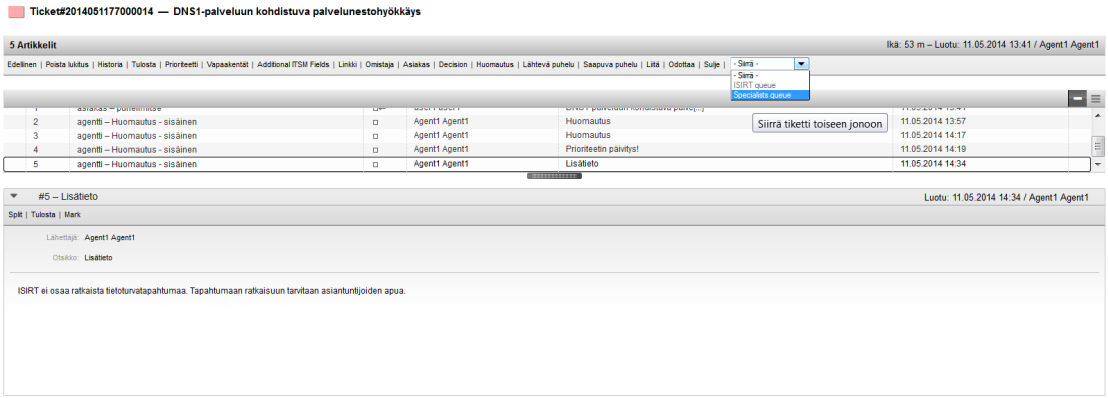
Tiketin käsittelyn aloitus ja arvio palvelun palautumisesta ja tiketin ratkaisuajankohdasta voidaan päivittää tiketille valitsemalla additional ITSM fields. ISIRTIn tulee myös arvioida tietoturvatapahtuman kiireellisyyttä ja vaikutuksia liiketoiminnalle. Päivittyneiden tietojen ja luokitteluasteikon avulla on mahdollista päivittää tiketin kiireellisyyttä valitsemalla prioriteetti. Kuviossa 27 voidaan nähdä esimerkki vaikutuksen ja kiireellisyyden arvioinnista ja päivittämisestä. ISIRTin tulee myös vahvistaa tietoturvatapahtuman olevan oikea ja todellinen. Jos tietoturvatapahtuma ei ole todellinen tiketti voidaan tiketti sulkea ja lähettää asiakkaalle tiedote tapahtuman käsittelyn päättämisestä ja johtopäätöksistä.



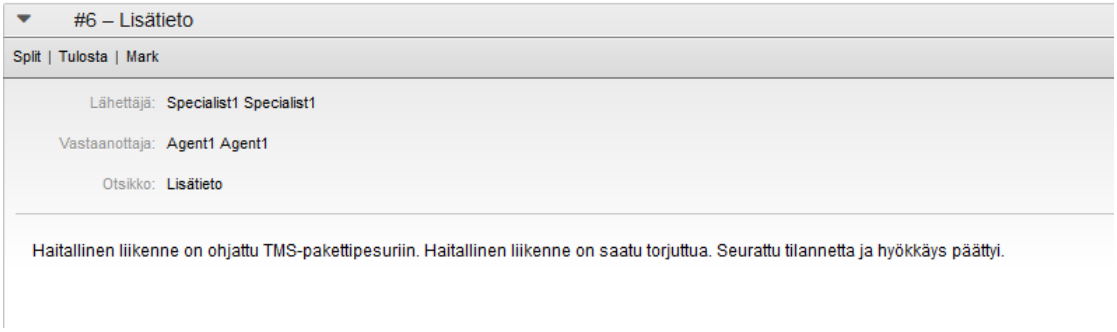
Kuvio 27. Vaikutuksen ja kiireellisyyden arviointi ja päivittäminen

6.3.4 Vastatoimet

Vastatoimet-vaiheen aikana ISIRT suorittaa tietoturvatapahtumalle tarvittaessa välittömät vastatoimet. Tehdyistä toimenpiteistä ja päätöksistä on mahdollista kirjata tiketille tietoa esimerkiksi valitsemalla valikosta huomautus tai päätös (decision). Tarvittaessa ISIRT voi arvioida tietoturvatapahtuman vakavuutta ja vaikutusta ja päivittää tiedot valitsemalla valikosta prioriteetti. Jos tietoturvatapahtuma ei ole hallinnassa, tiketti voidaan siirtää asiantuntijoiden käsiteltäväksi valitsemalla alasvetovalikosta siirrä ja specialists queue. Esimerkki tiketin siirrosta on nähtävissä kuviossa 28. Jos tiketti siirrettään asiantuntijoiden työjonoon, tiketti on nähtävissä järjestelmässä kirjauduttaessa specialist1-käyttäjätunnuksella järjestelmään. Kun asiantuntijat ovat ratkaisseet tietoturvatapahtuman, he voivat päivittää tiketille suoritetut toimenpiteet, mahdollisen rikosteknisen tietoturva-analyysin vaiheet, tehdyt päätökset ja kerätä tiketille tarvittavan todistusaineiston. Tarvittaessa he voivat myös päivittää tiketin ja tietoturvatapahtuman kiireellisyyttä ja vaikutusta muuttuneiden tietojen valossa. Kun toimenpiteet on tehty tiketti, voidaan siirtää takaisin ISIRTin käsiteltäväksi. Esimerkki asiantuntijoiden suorittamasta vastatoimesta voidaan nähdä kuviossa 29. Vastatoimenpiteiden jälkeen tiketti on siirretty takaisin ISIRTin jonoon.



Kuvio 28. Tiketin siirtäminen uuteen jonoon



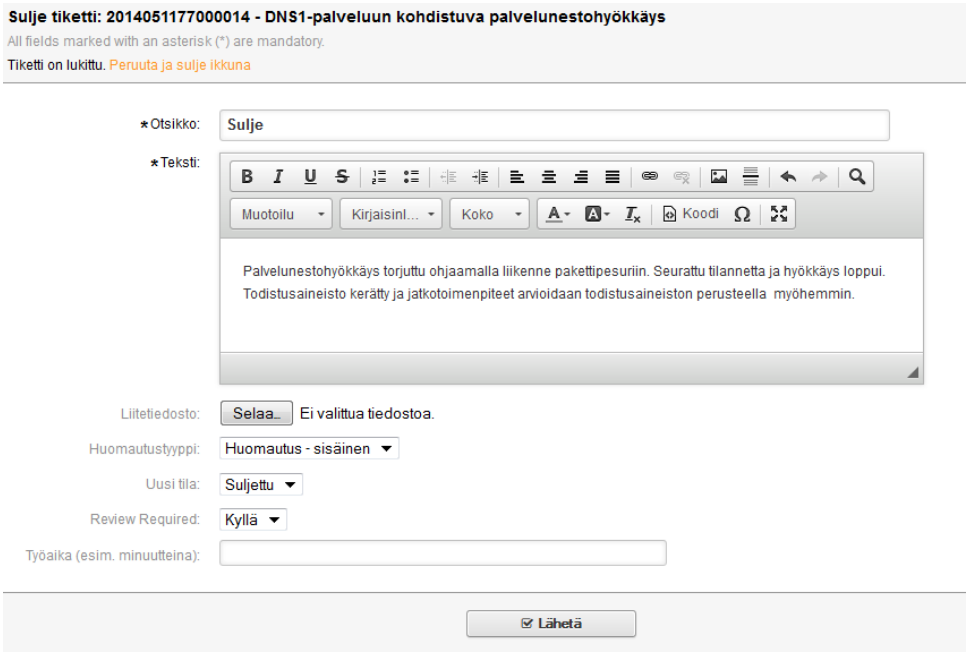
Kuvio 29. Esimerkki suoritetusta vastatoimesta

Jos tietoturvatapahtumaan saatiin ratkaisu, ISIRT voi päivittää tiketille palvelun palautumisajankohdan valitsemalla additional ISTM fields -painikkeen valikosta. ISIRT suorittaa tietoturvatapahtumalle tarvittavat pitkäkestoiset vastatoimenpiteet ja kirjaa tehdyt päätökset ja toimenpiteet tiketille. Pitkäkestoisia vastatoimia ovat esimerkiksi valvonnan päivittäminen, jotta tietoturvatapahtuma huomataan paremmin tai tietoturvahaavoittuvuuden torjuminen päivittämällä järjestelmä.

Vastatoimenpiteet vaiheen aikana ISIRT viestii tarvittaville tahoilla ja tiedottaa asiakasta tietoturvatapahtuman käsittelyssä tapahtuvista vaiheista. Tiedottaminen voidaan hoitaa automaattisesti tikettijärjestelmän avulla.

Tietoturvatapahtuman ja siitä tehdyn tiketin sulkeminen voidaan suorittaa tässä vaiheessa tai opetukset-vaiheessa. Tärkeää on kuitenkin tiedottaa asiakasta palvelun palautumisesta mahdollisimman nopeasti.

Tiketti suljetaan valitsemalla sulje. Tiketille kirjataan suoritetut toimenpiteet ja tallennetaan tiedot tikettijärjestelmään. Tiketin sulkemisen esimerkki voidaan nähdä kuviossa 30. Tikettiä suljettaessa voidaan tiketille merkitä tarvitaanko tietoturvatapahtuman jälkiarviointia.



Kuvio 30. Tiketin sulkeminen

6.3.5 Opetukset

Opetukset vaiheessa tarkastellaan kuinka tietoturvatapahtuman käsittely ja ratkaisu onnistui, pyritään tunnistamaan kehityskohteet ja tekemään tarvittavat parannukset. Organisaatio arvioi onko tarvetta jatkotoimenpiteille ja esimerkiksi rikostekniselle tietoturva-analyysille. Opetukset vaiheessa arvioidaan onko tietoturvatapahtuman esiintymisen takia syytä uudelleen arvioinnille, riskinhallinnan toimenpiteille, tietoturvatapahtumien hallintamallin ja turvamekanismien päivittämiselle tai luomiselle. Tarvittaessa tiedot tietoturvatapahtumasta tulee päivittää ISIRTin käyttämään ratkaisutietokantaan. OTRS-järjestelmään tallennettuja tietoja suojattavista kohteista voidaan päivittää tarvittaessa. OTRS-ohjelmistossa on mahdollista ottaa käyttöön ratkaisutietokanta.

6.4 Koulutussuunnitelma

Tietoturvatapahtumien hallintaprosessi ja tiketöintijärjestelmän käyttö on koulutettava organisaatiolle, jotta laboratoriossa osataan työskennellä oikein ja tavoite tietoturvatapahtumien tehokkaasta ja jäsennellystä käsittelystä saavutetaan. Koulutuksen tulisi esitellä SFS ISO/IEC 27035-standardin (2011) operatiiviset päävaiheet ja päävaiheissa tapahtuvat toimenpiteet. Suullisessa esityksessä voidaan käyttää apuna kuviossa 22 esiteltävää tietoturvatapahtumien hallintaprosessia.

OTRS-tiketöintijärjestelmän käyttöä voidaan harjoitella luvussa 6.3 esitetyn esimerkin pohjalta. Tiketöintijärjestelmän koulutuksesta tulisi vastata henkilö, joka tuntee hyvin tiketöintijärjestelmän ominaisuudet.

Koulutuksessa olisi hyvä esitellä myös suurempi kuva tietoturvallisuudesta ja kuinka tietoturvatapahtumien käsittely liittyy siihen. Esittely voi pitää sisällään esimerkiksi seuraavia tietoja. Organisaatiossa tulisi olla tietoturvan hallintamalli, jota ohjaavat tarvittavat tietoturvapolitiikat ja johdon sitoutuminen. Organisaatio on tunnistanut suojattavat kohteet. Suojattaville kohteille suoritetaan riskianalyysi ja kohteisiin liittyvät uhkat ja riskit tunnistetaan. Riskejä verrataan organisaation riskikriteereihin. Riskejä ja uhkia vastaan perustetaan tarvittavat turvamekanismit, joilla tietoturvallisuutta toteutetaan. Organisaation tietoturvallisuutta katselmoidaan ja arvioidaan jatkuvasti. Tämä ei kuitenkaan riitä vaan organisaation on varauduttava uusiin tietoturvauhkiin, -haavoittuvuuksin ja -tapahtumiin, joita ei ole vielä tunnistettu. Tietoturvatapahtumien hallintamallilla, joka tulee yhdistää organisaation tietoturvan hallintamalliin, voidaan vastata tähän haasteeseen ja varmistaa organisaation liiketoiminnan jatkuvuus. Tietoturvaherätteiden ja -tapahtumien hallintaprosessi on tietoturvatapahtumien hallintamallin yksi osa.

7 KEHITYSKOHTEET

7.1 Ongelmat ja puutteet

Opinnäytetyön aikana huomattiin, että organisaation tulisi laajentaa tietoturvatapahtumien hallintamalli operaattoriympäristöön. Hallintamallin sisältö vaikuttaa suuresti tietoturvatapahtumien hallintaan. Esimerkiksi tietoturvapolitiikat, tietoturvastrategia, johdon sitoutuminen, suojattavien kohteiden tunnistaminen, riskinhallinta ja turvamekanismit luovat pohjaa tietoturvatapahtumien hallintamallille. Tietoturvatapahtumien hallintamallia varten tulisi luoda tietoturvatapahtumien hallintapolitiikka, joka tulee sovittaa organisaation muihin tietoturvapoliitikoihin. Puutteeksi havaittiin myös tietoturvatapahtumien kategoria- ja luokitteluasteikkojen puuttuminen. Luokitteluasteikon käyttö mahdollistaa suojattavien kohteiden tunnistamisen ja riskien hallinnan. Tietoturvatapahtuman vaikutuksia ja kiireellisyyttä arvioitaessa on tiedettävä miten arvokas ja tärkeä suojattava kohde on liiketoiminnalle.

Tietoturvatapahtumien hallintamallia tulisi arvioida ja katselmoida säännöllisesti. Organisaation tulee arvioida tietoturvan tasoa ja tietoturvallisuuden hallintajärjestelmän vaikuttavuutta. Organisaation tulee määrittää, mitä tietoturvaprosesseja ja hallintakeinoja seurataan ja mitataan. Organisaation on myös määritettävä millä seuranta-, mittaus, analysointi- tai arviointimenetelmillä voidaan varmistaa kelvolliset tulokset. Valituilla menetelmillä tulisi saada vertailtavia ja toistettavia tuloksia, jotta niitä voidaan pitää kelvollisina. Organisaation tulee määrittää milloin seuranta, mittaaminen, analysointi ja arviointi suoritetaan ja ketkä suorittavat sen. Asianmukainen dokumentaatio seurannasta ja mittauksista tulee säilyttää todisteena. Arvioinnin ja seurannan keinoja ovat esimerkiksi sisäiset auditoinnit ja johdon katselmukset. (SFS ISO/IEC 27001 2013, 22).

Tietoturvatapahtumien hallintamallin, riskien hallinnan ja turvamekanismien kehittäminen sisältyy tietoturvatapahtumien hallintamallin päivittäiseen toimintaan. Arvokkaana lisänä kehittämistyöhän voi toimia myös auditoinnit, johdon katselmukset, mittaaminen ja analysointi.

7.2 Tietoturvatapahtumien hallintaprosessin kehittäminen

7.2.1 Yleistä

Tietoturvatapahtumien hallintaprosessia voidaan kehittää mittaamalla prosessia ja analysoimalla saatuja tuloksia. Tietoturvatapahtumien hallintaprosessin arviointiin ja mittaamiseen voidaan soveltaa normaaleja prosessin mittaamisen ja arvioinnin keinoja. ITIL version 3 Service Operation (2007) määrittää mittareita, joilla palvelutuotannon tapahtumien hallinnan tehokkuutta ja vaikuttavuutta voidaan arvioida. Mittareina voivat toimia esimerkiksi:

- tapahtumien kokonaismäärän seuranta
- tapahtumien jakautuminen eri vakavuusluokkien mukaan
- tapahtuman eri työvaiheisiin käytetty aika (vastaanotettu, työn alla ja suljettu)
- tapahtuman ratkaisuun kulunut aika
- palvelutasosopimusten mukaisesti ratkaistujen tapahtumien osuus kaikista tapahtumista
- Keskimääräiset kustannukset per tapahtuma.
  (ITIL version 3 Service Operation 2007, 54-55)

Mittareina voidaan käyttää myös lukumäärää ja prosenttiosuutta siitä, kuinka suuri osa tapahtumista ratkaistaan tietyn organisaation osan toimesta. Tapahtumien määrä kellon ajan perusteella voi mahdollistaa tapahtumien esiintymähuippujen ennustamisen ja resurssien määrittämisen tilanteeseen sopivaksi. (ITIL Service Operation 2007, 55).

Ajan kuluessa tietoturvatapahtumien hallintaprosessista tallentuu tietoa (data) tikettijärjestelmään. Tikettijärjestelmä tarjoaa arvokasta tietoa analyysien ja mittareiden laadintaan. Tietoa tutkimalla on mahdollista havaita mitä voidaan mitata ja mitä tuloksilla voidaan saavuttaa. Six Sigman Lean -prosessissa määritellään viisi vaihetta prosessien kehittämiseen. Vaiheet ovat määrittäminen (define), mittaaminen (measure), analysointi (analyze), kehittäminen (improve) ja ylläpitäminen (control). Sanojen englanninkielisistä alkukirjaimista muodostuu prosessille yleisesti käytetty nimi DMAIC. Mallissa olennaista on valita oikeat kohteet kehittämistyölle, jossa pyritään tunnistamaan ongelma, potentiaaliset kehityskohteet ja niihin liittyvä tieto. Mittaamalla ja analysoimalla tietoa voidaan löytää kehittämiskohteet. Kehittämistoimenpiteiden jälkeen parantunutta tilannetta ylläpidetään hallinnollisin keinoin. (The Basics of Lean Six Sigma N.d).

7.2.2 Ehdotukset JYVSECTECin mittareiksi

Organisaatio voi aloittaa mittareiden kehittämisen aluksi muutamilla mittareilla. Mittarien kehittäminen vaatii henkilöresursseja, pitkäjänteistä työtä ja perehtymistä tietoon, josta tuloksia mitataan. Aluksi organisaatio voi tarkastella tietoturvatapahtumien kokonaismäärää ja tapahtumien ajoittumista. Tiedon perusteella voidaan arvioida, kuinka paljon resursseja tietoturvatapahtumien käsittely vaatii ja mihin vuorokauden aikoihin resursseja tietoturvatapahtumien käsittelyyn tarvitaan eniten. Ajan kuluessa tietoturvatapahtumien kokonaismäärän arviointi kuukausittain ja tu-

losten vertaaminen edellisien vuosien vastaaviin ajankohtiin auttaa trendien ja resurssien määrittämisessä.

Kriittisimpien tietoturvatapahtumien määrä ja kategoria voivat toimia hyödyllisinä mittareina. Kaikkein kriittisimmät tietoturvatapahtumat aiheuttavat organisaation liiketoiminnalle suurimman uhan ja vaativat siksi eniten huomiota. On hyvä tietää mihin tilanteisiin tai suojattaviin kohteisiin kriittisimmät tapahtumat liittyvät ja voidaanko tapahtumista löytää yhtäläisyyksiä. Tämän kaltaiset mittarit voivat tukea myös tietoturvatapahtumien hallintaprosessin opetukset-vaiheen arviointeja.

Toiminnan tehokkuutta arvioitaessa voidaan mitata eri työvaiheisiin kulunutta aikaa. Tämä mahdollistaa tietoturvatapahtumien hallintaprosessin ongelmakohtien löytämisen ja parannusten tekemisen. Tapahtumien ratkaisemiseen käytetty aika ja sen vertaaminen palvelutasosopimuksiin kertoo, kuinka hyvin organisaatio pystyy vastaamaan tietoturvatapahtumien hallintaprosessin avulla sisäisten ja ulkoisten palvelutasosopimusten asettamiin vaatimuksiin. Palvelutasosopimusten rikkomukset aiheuttavat yleensä myös taloudellisia menetyksiä organisaatiolle.

7.3 OTRS-tiketöintijärjestelmän kehittäminen

Opinnäytetyön aikana suoritettiin OTRS-tiketöintijärjestelmän asennus ja käyttöönotto. Tiketöintijärjestelmä tarjoaa lukuisia kehitysmahdollisuuksia, jotka voivat helpottaa ja tehostaa tietoturvatapahtumien hallintaprosessia. Kun organisaatio on tunnistanut suojattavat kohteet ja suorittanut suojattaville kohteille riskinhallinnan, suojattavat kohteet voidaan tallentaa yksityiskohtaisin tiedoin OTRS ITSM -sovellukseen. Suojattavalle kohteelle on mahdollista määrittää valmiiksi prioriteetti, joka kuvaa

kuinka tärkeä suojattava kohde organisaatiolle on. Myös sisäisten ja ulkoisten palvelutasosopimusten käyttö helpottaa tapahtuman kriittisyyden arviointia.

Organisaatio voi ottaa käyttöön OTRS:n ratkaisutietokannan, josta voidaan etsiä dokumentteja tietoturvatapahtumiin ja suojattaviin kohteisiin liittyen. Ratkaisutietokannan käyttö nopeuttaa tapahtumien käsittelyä tiedon löytyessä samasta järjestelmästä kuin missä tikettien käsittely tapahtuu.

Organisaation tietoturvatapahtumien hallintaan liittyvien organisaation osien laajentuessa OTRS-ohjelmistoon on mahdollista luoda uusia työjonoja esimerkiksi kontaktipisteeseen tai kriisinhallintaan liittyen. Tietoturvatapahtumista tiedottaminen on mahdollista automatisoida sisäisille sidosryhmille ja ulkoisille asiakkaille. Kun organisaatio on käyttänyt OTRS-tiketöintijärjestelmää, ajan kuluessa voidaan huomata muutoksia, jotka tiketöintijärjestelmään tarvitaan. OTRS-ohjelmistojen dokumentaatio mahdollistaa monipuolisten muutosten tekemisen itse. Sovelluskehitykseen ei välttämättä tarvita organisaation ulkopuolisia resursseja.

7.4 Lainsäädännön aiheuttamat kehitystarpeet

Tässä opinnäytetyössä käsiteltiin tietosuojalainsäädäntöä teoriassa teleyrityksen näkökulmasta. Lainsäädännön aiheuttamat käytännön vaatimukset ja toimenpiteet on rajattu tämän opinnäytetyön ulkopuolelle ja ne jäävät tulevaisuuden kehityskohteiksi. Teleyritysten velvollisuutena on huolehtia tietoturvasta. Organisaation tietoturvatapahtumien hallintaan osallistuvien jäsenten tulee olla tietoisia, millaisia oikeuksia ja velvollisuuksia lainsäädäntö aiheuttaa tietoturvatapahtumia, henkilötietoja ja tunnistamistietoja käsiteltäessä. Lyhyenä perehdytyksenä asiaan voi toimia tämän opinnäytetyön kappale 5. Perehdytyksen keskeisimpänä sisältönä voi toimia henkilötietolain

ja sähköisen viestinnän tietosuojalain esittely. Organisaation tulisi kuitenkin laatia yksityiskohtaisempi koulutussuunnitelma aiheeseen liittyvästä lainsäädännöstä organisaation henkilökunnalle sen perusteella, millaisia tietoja he käsittelevät.

Henkilötietolakia sovelletaan henkilötietojen käsittelyyn ja henkilörekistereihin. Teleyrityksellä voi olla käytössään useita järjestelmiä, joissa säilytetään asiakkaiden arkaluontoisia tietoja. Organisaation on varmistuttava, että henkilörekisterit on suojattu asianmukaisesti ja organisaation jäsenet käsittelevät henkilötietoja oikein. Organisaation on myös ryhdyttävä toimenpiteisiin tietoturvan toteuttamiseksi turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi.

Tietoturvatapahtumia käsiteltäessä ja tutkittaessa voidaan joutua käsittelemään luottamuksellisia teletunnistetietoja. Organisaation jäsenten tulee tietää, mikä teletunnistetieto on ja miten sitä tulee käsitellä. On myös tärkeää ymmärtää, että teletunnistetietoja voidaan luovuttaa ainoastaan tahoille, joilla on oikeus tietojen käsittelyyn.

Teleyrityksissä toimivat henkilöt tulee kouluttaa myös tietoturvaloukkausilmoitusten käsittelyyn. Organisaation jäsenten tulee tietää, milloin viestintävirastolle, tilaajille ja käyttäjille on ilmoitettava tietoturvaloukkauksista ja uhkista.

8 POHDINTA

8.1 Aiheen rajaus ja teoriaosuus

Opinnäytetyön aiheen rajaus osoittautui juuri niin hankalaksi kuin etukäteen olin osannut odottaa. Tietoturva on erittäin laaja alue. Aiheen rajaus tarkentui koko opinnäytetyön laadinnan ajan. On vaikeaa käsitellä yksittäisiä tietoturvaan liittyviä aiheita selvittämättä niihin liittyviä muita teemoja. Varsinkin tietoturvallisuudessa käytettävät käsitteet vaativat paljon selittämistä ja kuvailua. Samaan ongelmaan törmäsin myös käyttämässäni lähdekirjallisuudessa. Tietoturvaan liittyviä asioita on käsitelty usein hyvin rajatusta näkökulmasta ja asiaan olennaisesti liittyviä käsitteitä ja asioita on jätetty selittämättä. Standardit ja parhaiden käytäntöjen mallit käsittelevät tietoturvan eri aiheita hyvin kattavasti ja laajasti. Standardeihin tutustuminen saattaa olla myös uuvuttava kokemus. Usein asian käsittely hoidetaan listoina kokonaisien lauseiden sijaan. Tämä jättää paljon tulkinnan varaa asian ymmärtämisen kannalta. Huomasin työn aikana, että on hyödyllistä lukea lähdekirjallisuutta, joka selittää standardien sisältöä ja käyttöä esimerkkien avulla. Ilokseni huomasin standardien kehittyvän ja sisällön selvenevän uusien versioiden ilmestyessä.

Tietoturvatapahtumien hallinta oli minulle aiheena uusi ja tämän opinnäytetyön laajin aihe. Laaja teorian käsittely loi hyvän pohjan JYVSECTECin tietoturvatapahtumien hallintaprosessin toteutukselle. Olen työskennellyt kahdeksan vuotta palvelutuotannossa tapahtumien hallinnan parissa. Tietoturvatapahtumien hallintaan liittyy paljon samanlaisia vaiheita kuin palvelutuotannon tapahtumien hallintaan. Aiempi tietämykseni tietoturvallisuudesta liittyi lähinnä koulussa saamaani teoriatietoon ja työelämässä opittuihin käytäntöihin. Opin teoriaosuuden laadinnan aikana valtavasti

uutta ja aihe oli erittäin kiinnostava. Toivottavasti voin soveltaa oppimaani tulevaisuuden projekteissa ja työtehtävissä.

Tietosuojalainsäädäntöön ja ISIRTin perustamiseen liittyvä osuus jäi työssä hieman irralliseksi. Alkuperäisen rajauksen mukaisesti aiheita käsiteltiin vain teoriassa ja käytännön toteutus olisi ollut mahdotonta toteuttaa tämän opinnäytetyön aikaresurssien puitteissa. Tässä opinnäytetyössä esitelty tietoturvatapahtumien hallintamalli olisi sovellettavissa lähes mihin tahansa organisaatioon. Lainsäädännön avulla tietoturvatapahtumien hallintaan pystyttiin liittämään operaattoritoiminnan erityispiirteitä. Tietosuojalainsäädännön käytännön vaikutukset ovat tulleet minulle aiemmin tutuksi työelämässä. ISIRTin roolien ja palveluiden esittely tarjoaa mielestäni organisaatiolle hyödyllistä tietoa. Aiemmin työelämässä olen ainoastaan seurannut ISIRTin toimintaa. Teoriaosuus toi näihin aiheisiin liittyen minulle arvokasta lisätietoa.

8.2 Toteutus ja tulokset

Tämän opinnäytetyön tuloksina JYVSECTECille laadittiin tietoturvatapahtumien hallintaprosessi, prosessia tukeva tiketöintijärjestelmä ja ohjeet tiketöintijärjestelmän käytöstä tietoturvatapahtumien käsittelyn aikana. Tässä opinnäytetyössä laaditun koulutussuunnitelman avulla JYVSECTEC voi esitellä tietoturvatapahtumien hallintaprosessin ja tiketöintijärjestelmän toimintaa organisaation jäsenille. Työn tuloksina esiteltiin ISIRTin käynnistämistä varten ISIRTin työrooleja ja mahdollisia palveluita. Työssä esiteltiin myös operaattoritoimintaan liittyvää lainsäädäntöä ja sen aiheuttamia kehitystarpeita. Kehityskohteita tunnistettiin ja ehdotuksia toimenpiteistä esitettiin myös tietoturvatapahtumien hallintamallin käyttöönottoon, tiketöintijärjestelmään ja tietoturvatapahtumien hallintaprosessiin liittyen.

Tietoturvatapahtumien hallintaprosessin aikaansaamiseksi työn alkuperäiseen rajauksen kuului tietoturvatapahtumien hallintaprosessin toteuttamissuunnitelma. Toteuttamissuunnitelma koostui kysymyksistä ja listasta selvitettäviä asioita. Tiedot lähtötilanteesta oli selvitettävä, jotta tietoturvatapahtumien hallintaprosessin luominen oli mahdollista. Toteuttamissuunnitelma selkeytti omaa työtäni paljon, mutta opinnäytetyön luettavuuden kannalta se toi tekstiin turhaa toistoa. Toteuttamissuunnitelmassa käsitellyt asiat sisällytettiin selvitykseen lähtötilanteesta. Tietoturvatapahtumien hallintaprosessi laadittiin SFS ISO/IEC 27035-standardiin (2011) perustuen ja sovitettiin organisaation rakenteisiin sopivaksi.

Toteutuksen aikana työssä asennettiin ja käyttöönotettiin OTRS-tiketöintijärjestelmä. Olen työskennellyt useiden tiketöintijärjestelmien kanssa aiemmin, mutta en ole koskaan itse asentanut ja käyttöönottanut tiketöintijärjestelmää. Järjestelmän asentaminen ja käyttöönotto eivät kuuluneet työn alkuperäiseen rajaukseen. Tiketöintijärjestelmän asennus ja käyttöönotto on organisaation toiminnan kannalta suuri työ. Pyyntö järjestelmän asentamisesta esitettiin tilaajan toimesta opinnäytetyöprosessin puolivälissä. Tiketöintijärjestelmän asentaminen vei paljon aikaa, viivästytti työn valmistumista ja oli teknisesti varsin haastava. Asennuksen yksityiskohtainen kuvaaminen sekä käytettyjen tekniikoiden ja komentojen selittäminen olisivat kasvattaneet tämän opinnäytetyön teorian ja toteutuksen sisältöä merkittävästi. Oman arvioni mukaan tiketöintijärjestelmien vertailu ja tekniikoiden esittely sekä järjestelmän asentaminen ja käyttöönotto olisivat itsessään voineet olla yhden opinnäytetyön aihe. Nyt tehty työ ei varsinaisesti näy tämän opinnäytetyön toteutusosuudessa tiketöintijärjestelmän ja siihen liittyvän palvelimen osalta, mutta palvelee opinnäytetyön luettavuutta ja kokonaisuutta paremmin. Opinnäytetyön lopputuloksen kannalta järjestelmän käyttöönotto oli erittäin hyvä asia. Tiketöintijärjestelmän ympärille oli helppo laatia selkeä ja kattava käytännön toteutus. Tietoturvatapahtumien hallinnan

näkökulmasta on tärkeämpää ymmärtää, kuinka asennettu työkalu tukee tietoturvatapahtumien hallintaprosessin mukaista käytännön toimintaa, kuin kuinka tiketöintijärjestelmä on asennettu. Tiketöintijärjestelmän toteutuksessa ei käytetty JYVSECTE-Cin resursseja.

Olen opinnäytetyön tuloksiin erittäin tyytyväinen ja koen, että tavoitteiden saavuttamisessa onnistuttiin hyvin. Sovitut tavoitteet täytettiin ja opinnäytetyön lopputulokset vastaavat odotuksia. Tämän opinnäytetyön laatiminen oli henkilökohtaisesti suuri ponnistus ja opetti minulle monia uusia toimintatapoja. Olen iloinen, että tuo ponnistus kannatti ja voin olla lopputulokseen tyytyväinen.

Tietoturva ei ole koskaan valmis. Tämän opinnäytetyön aihealue on vain pieni osa tietoturvan hallintamallia. Tehdyn työn perusteella organisaatiolla on hyvät edellytykset kehittää tietoturvatapahtumien hallintaa ja työssä esitettyjen kehitysehdotuksien perusteella laajentaa tietoturvatapahtumien hallintaprosessi osaksi tietoturvatapahtumien hallintamallia. Tietoturvatapahtumien hallintamalli on mahdollista sisällyttää tulevaisuudessa osaksi organisaation tietoturvan hallintamallia. Tietoturva ei ole projekti vaan prosessi.

LÄHTEET

About DDOS Attacks. 2013. Arbor Networksin kotisivut. 2013. Viitattu 5.5.2014. Http://www.arbornetworks.com/attack-ddos

About us. 2014a. Arbor Networksin kotisivut. Viitattu 27.4.2014. Http://www.arbornetworks.com/corporate/about-us.

About us. 2014b. OTRS Open Technology Real Services. Viitattu 10.5.2014. Http://www.otrs.com/company/about-us/

Andreasson K. & Koivisto J. 2013. Tietoturvaa toteuttamassa. Tallinna. Tietosanoma Oy.

Attacks Against Data Centers. 2013. Arbor Networksin kotisivut. Viitattu 27.4.2014. Http://pages.arbornetworks.com/rs/arbor/images/DataCenter_final_white.pdf

Bronk, H., Thorbruegge, M., Hakkaja, M. 2006. Step-by-step approach on how to set up a CSIRT. Viitattu 18.4.2014. Http://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide

CERT-FI. 2013. Viestintäviraston kyberturvallisuuskeskuksen kotisivut. Viitattu 7.12.2013. Http://www.cert.fi/index.html.

Company. 2014. OTRS Open Technology Real Services. 2014. Viitattu 10.5.2014. Http://www.otrs.com/company/

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä. Docendo Finland.

Henkilötietolaki. 2013. Tietosuojavaltuutetun kotisivut. Viitattu 4.5.2014. http://www.tietosuoja.fi/fi/index/lait/Henkilotietolaki.html

Huston, G. 2006. Exploring Autonomous System Numbers. The Internet Protocol Journal. Volume 9, Number 1. Viitattu 8.5.2014.

Http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-1/autonomous_system_numbers.html

IEC International Electrotechnical Commission. 2014. IEC:n kotisivu. Viitattu 28.4.2014. Http://www.iec.ch/about/?ref=menu.

Incident Management Guide. 2010. ENISA European Network and Information Security Agency. Viitattu 1.4.2014.
Http://www.enisa.europa.eu/activities/cert/support/incident-management

ISO International Organization for Standardization. 2014. ISO:n kotisivu. Viitattu 28.4.2014. Http://www.iso.org/iso/home/about.htm.

ITIL version 3 Service Operation. 2007. OGC Office for Goverment. TSO Publications, Norwich, UK.

ITIL version 3 Service Desing. 2007. OGC Office for Goverment. TSO Publications, Norwich, UK.

JTC1 mission and principles. 2014. International Organization for Standardization. Viitattu 28.4.2014.
Http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/jtc1_home.htm#JTC_1_mission_and_principles.

JYVSECTEC – Jyväskylä Security Technology. 2013. JYVSECTEC-hankkeen kotisivut. Viitattu 21.11.2013. Http://www.jyvsectec.fi.

Kohdistetut haittaohjelmahyökkäykset. 2013. Viestintäviraston kyberturvallisuuskeskuksen kotisivut. Viitattu 7.12.2013.
Https://www.cert.fi/tietoturvanyt/2013/11/ttn201311011336.html

Lait. 2014. Tietosuojavaltuutetun kotisivut. Viitattu 4.5.2014.
Http://www.tietosuoja.fi/fi/index/lait.html

Largest DDOS Attack Reported. 2013. Arbor Networksin kotisivut. Viitattu 27.4.2014.
Http://pages.arbornetworks.com/rs/arbor/images/AttackSize_final_white.pdf

L 23.5.2003/393. Viestintämarkkinalaki. Viitattu 5.5.2014. Http://www.finlex.fi, ajantasainen lainsäädäntö.

L 16.6.2004/516. Sähköisen viestinnän tietosuojalaki. Viitattu 6.5.2014. Http://www.finlex.fi, ajantasainen lainsäädäntö.

L 22.4.1999/523. Henkilötietolaki. Viitattu 6.5.2014. Http://www.finlex.fi, ajantasainen lainsäädäntö.

L 22.4.1999/524. Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta. Viitattu 5.5.2014. Http://www.finlex.fi, ajantasainen lainsäädäntö.

L 11.6.1999/731. Suomen perustuslaki. Viitattu 5.5.2014. Http://www.finlex.fi, ajantasainen lainsäädäntö.

Mellin, J. 12.8.2013. Teleyritysten mahdollisuudet rajoittaa verkkohyökkäyksiä. Esitelmä Tietoturva nyt -seminaarissa. Viitattu 7.12.2013. Https://www.viestintavirasto.fi/attachments/esitykset/Jorma_Mellin_DDoS-mitigation.pdf

Nisonen, M. 2013. Tietoturvallisuuden hallintajärjestelmä JYVSECTEC-hankkeeseen. Opinnäytetyö. Jyväskylän ammattikorkeakoulu, tekniikan ja liikenteen ala, tietotekniikan koulutusohjelma.

Open Source Community. 2014. OTRS Open Technology Real Services. 2014. Viitattu 10.5.2014. Http://www.otrs.com/software/open-source/

Oracle VM Virtualbox data sheet. 2013. Viitattu 1.5.2014. Http://www.oracle.com/us/technologies/virtualization/oraclevm/oracle-vm-virtualbox-ds-1655169.pdf

Peakflow solution data sheet. 2013. Viitattu 30.4.2014. Http://www.arbornetworks.com/docman-component/doc_download/683-peakflow-solution-data-sheet

Pitkäkestoiset ilmiöt. 2013. Viestintäviraston tietoturvakatsaus 3/2013. Viestintäviraston kyberturvallisuuskeskuksen kotisivut. Viitattu 7.12.2013. Http://www.cert.fi/katsaukset/2013/tt_katsaus_3_13/pitkat_ilmiot_3_13.html.

Pravail availability protection system data sheet. 2013. Viitattu 29.4.2014. Http://www.arbornetworks.com/component/docman/doc_download/498-pravail-aps-data-sheet-english?Itemid=442

Sanastoa. 2014. Tietosuojavaltuutetun kotisivut. Viitattu 5.5.2014. Http://www.tietosuoja.fi/27247.htm#kohta5

SFS ISO/IEC 17999:fi.2006. Tietoturvallisuuden hallintaa koskeva menettelyohje. Helsinki: Suomen Standardoimisliitto SFS. Viitattu 28.4.2014 Http://www.jamk.fi/kirjasto, Nelli-portaali, SFS-online.

SFS ISO/IEC 27000. 2010. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto. Helsinki: Suomen Standardoimisliitto SFS. Viitattu 28.4.2014 Http://www.jamk.fi/kirjasto, Nelli-portaali, SFS-online.

SFS ISO/IEC 27001. 2013. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardoimisliitto SFS. Viitattu 28.4.2014 Http://www.jamk.fi/kirjasto, Nelli-portaali, SFS-online

SFS ISO/IEC 27002. 2013. Information technology. Security techniques. Code of practice for information security controls. Helsinki: Suomen Standardoimisliitto SFS. Viitattu 29.4.2014 Http://www.jamk.fi/kirjasto, Nelli-portaali, SFS-online.

SFS ISO/IEC 27035. 2011. Information technology. Security techniques. Information security incident management. Helsinki: Suomen Standardoimisliitto SFS. Viitattu 28.10.2013 Http://www.jamk.fi/kirjasto, Nelli-portaali, SFS-online.

Software. 2014. OTRS Open Technology Real Services. Viitattu 10.5.2014. Http://www.otrs.com/software/

Sähköisen viestinnän tietosuojalaki. 2014. Tietosuojavaltuutetun kotisivut. Viitattu 5.5.2014. Http://www.tietosuoja.fi/fi/index/lait/sahkoisenviestinnantietosuojalaki.html

Tehtävät. 2014. Tietosuojavaltuutetun kotisivut. Viitattu 6.5.2014. Http://www.tietosuoja.fi/1552.htm

Terms and Definitions 2014. ENISA European Network and Information Security Agency. Viitattu 2.5.2014. Http://www.enisa.europa.eu/activities/cert/background/coop/terms-definitions-1

The Basics of Lean Six Sigma. N.d. Goleansigma. Viitattu 10.5.2014. Http://www.goleansixsigma.com/the-basics-of-lean-six-sigma/

Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007. 2007. Valtiovarainministeriö. Viitattu7.4.2014. Http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071128Tietot/name.jsp

Tunnistamistietojen käsittely. 2013. Viestintäviraston kotisivut. Viitattu 7.5.2014. Https://www.viestintavirasto.fi/tietoturva/teleyritystenoikeudetjavelvollisuudet/tunnistamistietojenkasittely.html

Uudet Ilmiöt. 2013. Viestintäviraston tietoturvakatsaus 3/2013. Viestintäviraston kyberturvallisuuskeskuksen kotisivut. Viitattu 7.12.2013. Http://www.cert.fi/katsaukset/2013/tt_katsaus_3_13/uudet_ilmiot_3_13.html.

Vuosikatsaus 2012. 2013. Viestintäviraston kyberturvallisuuskeskuksen kotisivut. Viitattu 7.12.2013. Http://www.cert.fi/katsaukset/2012/vuosikatsaus2012.html.

West-Brown, M., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., Zajicek, M. 2003. Handbook for Computer Security Incident Response Teams. Viitattu 15.5.2014. Http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6305

Worldwide Infrastructure Security Report. 2013. Arbor Networksin kotisivut. Viitattu 27.4.2014. Http://www.arbornetworks.com/resources/infrastructure-security-report

LIITTEET

Liite 1. Lomake tietoturvaherätteestä

Tapahtuma-aika: Herätteen tunnistenumero:

Liittyvät herätteet/tapahtumat:

Ilmoittajan yhteystiedot

Nimi: _____ Osoite: _____

Organisaatio:_____ Osasto: _____

Puhelin: _____ Sähköposti: _____

Kuvaus tietoturvaherätteestä

Mitä tapahtui? _____

Kuinka tapahtui? _____

Miksi tapahtui? _____

Suojattava kohde? _____

Haitat liiketoiminnalle? _____

Yksityiskohdat

Aika ja päivämäärä, jolloin heräte tapahtui:

Aika ja päivämäärä, jolloin tieto herätteestä havaittiin:

Aika ja päivämäärä, jolloin herätteestä ilmoitettiin:

Onko herätteelle suoritettu vastatoimet? (Kyllä/Ei)

Jos kyllä, kauanko heräte oli aktiivinen? (Päivät/tunnit/minuutit)

(ISO/IEC 27035,66).

Liite 2. Lomake tietoturvatapahtumasta 1/6

Tapahtuma-aika: Tapahtuman tunnistenumero:

Liittyvät herätteet/tapahtumat:

Ilmoittajan yhteystiedot

Nimi: _____ Osoite: _____

Organisaatio:_____ Osasto: _____

Puhelin: _____ Sähköposti: _____

Käsittelijän (ISIRT) yhteystiedot:

Nimi: _____ Osoite: _____

Organisaatio:_____ Osasto: _____

Puhelin: _____ Sähköposti: _____

Kuvaus tietoturvatapahtumasta

Mitä tapahtui? _____

Kuinka tapahtui? _____

Miksi tapahtui? _____

Suojattava kohde? _____

Haitat liiketoiminnalle? _____

Yksityiskohdat

Aika ja päivämäärä, jolloin tapahtuma tapahtui: _____

Aika ja päivämäärä, jolloin tieto tapahtuma havaittiin: _____

Aika ja päivämäärä, jolloin tapahtumasta ilmoitettiin: _____

Onko tapahtuma ohi? _____

Jos kyllä, kauanko tapahtuma oli aktiivinen? _____

Lomake tietoturvatapahtumasta 2/6

Kategoria

Onko tietoturvatapahtuma?

□ Todellinen/varmistettu □ Epäilty

□ Luonnon onnettomuus (esimerkiksi myrsky, maanjäristys tai tulivuorenpurkaus)
Kuvaile: _____

□ Yhteiskunnallinen tapahtuma (esimerkiksi terrori-isku, sota tai mellakka)
Kuvaile: _____

□ Fyysinen vahinko (esimerkiksi tulipalo, vesivahinko, sähköstaattinen tapahtuma, korroosio, likaantuminen, saastuminen, laitteen tuhoutuminen/vahingoittuminen, tallennusvälineen/tiedon tuhoutuminen, varkaus tai ilkivalta)
Kuvaile: _____

□ Infrastruktuurin vikaantuminen (esimerkiksi sähkönjakelun, tietoliikenneverkon, ilmastoinnin tai vedenjakelun ongelmatilanne)
Kuvaile: _____

□ Säteilyn aiheuttamat häiriöt (esimerkiksi sähkömagneettinen säteily tai pulssi, elektroninen häirintä, jännitevaihtelu tai lämpösäteily)
Kuvaile: _____

□ Tekninen vika (esimerkiksi laitevika, ohjelmiston toimintahäiriö, ylikuormitus tai ylläpidon laiminlyönti)
Kuvaile: _____

Lomake tietoturvatapahtumasta **3/6**

□ Haittaohjelma (malware) (esimerkiksi virus, verkkomato, troijalainen hevonen, bottiverkko (botnet) tai haitallinen koodi (malicious code)
Kuvaile: _____

□ Tekninen hyökkäys (esimerkiksi verkkoskannaus, palvelunestohyökkäys, haavoittuvuuden hyväksikäyttö, kirjautumisyritykset tai takaoven hyväksikäyttö)
Kuvaile: _____

□ Sääntöjen rikkominen (esimerkiksi resurssien luvaton käyttö tai tekijänoikeusrikkomus)
Kuvaile: _____

□ Toimintojen vahingoittaminen (Compromise of functions) (esimerkiksi oikeuksien väärinkäyttö, oikeuksien väärentäminen, toimenpiteiden suorittamisen estäminen, henkilöstön paikallaolon estäminen tai virheellinen toiminta)
Kuvaile: _____

□ Informaation vahingoittaminen (Compromise of information) (esimerkiksi sieppaus tai keskeytys (interception), vakoilu, salakuuntelu, paljastaminen, naamiointi, sosiaalinen manipulointi (social engineering), verkkourkinta (network phishing), datan varastaminen, datan menetys, datan peukalointi tai datan virhe)
Kuvaile: _____

□ Vahingollinen sisältö (esimerkiksi laiton, vahingollinen tai loukkaava sisältö)
Kuvaile: _____

Lomake tietoturvatapahtumasta 4/6

Vaikutuksen kohteena olevat suojattavat kohteet

Data/informaatio: _____

Laitteisto: _____

Ohjelmisto: _____

Tietoliikenne: _____

Dokumentit: _____

Prosessit: _____

Muu: _____

Arvioitu vaikutus liiketoiminnalle / tapahtuman vaikutukset

□ Luottamuksellisuuden rikkoutuminen

□ Eheyden rikkoutuminen

□ Saatavuuden rikkoutuminen

□ Kiistämättömyyden rikkoutuminen

Arvo liiketoiminnalle asteikolla (1-10), toimintaohjeet ja kustannukset:

_____

_____

Tietoturvatapahtumasta palautumisen kokonaiskustannukset

Arvo liiketoiminnalle asteikolla (1-10), toimintaohjeet ja todelliset kustannukset:

_____

Lomake tietoturvatapahtumasta 5/6

Tapahtuman ratkaisu

Tietoturvatapahtuman tutkinnan aloituspäivämäärä: _____

Tutkintaan osallistuneet henkilöt: _____

Tietoturvatapahtuman päättymispäivämäärä: _____

Vaikutuksen päättymispäivämäärä: _____

Tietoturvatapahtuman päättymispäivämäärä: _____

Viite ja tutkintalomakkeen sijainti: _____

Tietoturvatapahtumaan osalliset tahot

□ Henkilöt _____

□ Organisaatiot _____

□ Järjestäytyneet ryhmät _____

□ Onnettomuus _____

□ Ei tekijää _____

Todellinen tai koettu motivaatio

□ Rikollinen/Taloudellinen hyöty _____

□ Politiikka/Terrorismi _____

□ Kosto _____

□ Huvi / hakkerointi _____

Tietoturvatapahtuman ratkaisemiseksi suoritetut toimenpiteet:

_____

Tietoturvatapahtuman ratkaisemiseksi suunnitellut toimenpiteet:

_____

Lomake tietoturvatapahtumasta 6/6

Tarvittavat jatkotoimenpiteet:

_____

J**ohtopäätökset**:

_____

Sisäisesti tiedotetut henkilöt / tahot:

_____

Ulkoisesti tiedotetut henkilöt / tahot:

_____

Lopettaminen

Päivämäärä: _____

Nimi: _____

Rooli: _____

Allekirjoitus: _____

(ISO/IEC 27035, 67-72).